COMPILATION OF APPLICABLE LAWS AND REGULATIONS ON THE ADMISSIBILITY OF ELECTRONIC EVIDENCE OBTAINED FROM FOREIGN JURISDICTIONS, IN THE INVESTIGATION, PROSECUTION AND ADJUDICATION OF TERRORISM-RELATED CRIMES. SOUTH AND SOUTH-EAST ASIA
This compilation was made possible thanks to the generous financial support of the United Kingdom of Great Britain and Northern Ireland and the United States of America.

The legal provisions in this compilation are correct at the time of publication (June 2022).

It is incumbent on practitioners to ensure they are consulting the latest legislative provisions by referring to the national online libraries or to the SHERLOC Database of Legislation.
# TABLE OF CONTENT

## BANGLADESH

<table>
<thead>
<tr>
<th>Year</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>1872</td>
<td>Evidence Act</td>
</tr>
<tr>
<td>2001</td>
<td>Information and Telecommunication Act</td>
</tr>
<tr>
<td>2009</td>
<td>Anti-Terrorism Act</td>
</tr>
<tr>
<td>2018</td>
<td>Digital Security Act</td>
</tr>
</tbody>
</table>

## BHUTAN

<table>
<thead>
<tr>
<th>Year</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>Evidence Act</td>
</tr>
<tr>
<td>2004</td>
<td>Penal Code of Bhutan</td>
</tr>
<tr>
<td>2018</td>
<td>Information Communication and Media Act</td>
</tr>
</tbody>
</table>

## BRUNEI DARUSSALAM

<table>
<thead>
<tr>
<th>Year</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>1982</td>
<td>Internal Security Act</td>
</tr>
<tr>
<td>2000</td>
<td>Computer Misuse Act</td>
</tr>
<tr>
<td>2001</td>
<td>Telecommunications Order</td>
</tr>
<tr>
<td>2001</td>
<td>Authority for Info-Communications Technology Industry Order</td>
</tr>
<tr>
<td>2005</td>
<td>Mutual Assistance in Criminal Matters Order</td>
</tr>
<tr>
<td>2006</td>
<td>Evidence Act</td>
</tr>
<tr>
<td>2011</td>
<td>Anti-Terrorism Order</td>
</tr>
<tr>
<td>2007</td>
<td>BROADCASTING ACT (CHAPTER 180) BROADCASTING (CLASS LICENCE) NOTIFICATION, 2001</td>
</tr>
</tbody>
</table>

## CAMBODIA

<table>
<thead>
<tr>
<th>Year</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>Criminal Procedure Code</td>
</tr>
<tr>
<td>2007</td>
<td>Law on Counter Terrorism</td>
</tr>
<tr>
<td>2007</td>
<td>Law on Anti-money Laundering and Combating the Financing of Terrorism</td>
</tr>
<tr>
<td>2010</td>
<td>Prakas on Anti-Money Laundering and Combating the Financing of Terrorism relating to All Reporting Entities not regulated by the National Bank of Cambodia</td>
</tr>
</tbody>
</table>

## INDIA

<table>
<thead>
<tr>
<th>Year</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>1872</td>
<td>The Indian Evidence Act (Last updated:-13-3-2020)</td>
</tr>
<tr>
<td>1984</td>
<td>The Terrorist Affected Areas Act (Special Courts)</td>
</tr>
<tr>
<td>2000</td>
<td>The Information Technology Act</td>
</tr>
<tr>
<td>2008</td>
<td>The National Investigation Agency Act</td>
</tr>
<tr>
<td>2008</td>
<td>The Indian Penal Code</td>
</tr>
</tbody>
</table>

## INDONESIA

<table>
<thead>
<tr>
<th>Year</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>Law Number 1 Year 2006 Concerning Mutual Legal Assistance in Criminal Matters</td>
</tr>
<tr>
<td>2008</td>
<td>Law Number 8 Concerning the Criminal Procedure</td>
</tr>
<tr>
<td>2010</td>
<td>Law Number 8 Year 2010 on the Prevention of Crime of Money Laundering</td>
</tr>
<tr>
<td>2008</td>
<td>Law Number 11 Year 2008 Concerning Electronic Information and Transaction</td>
</tr>
</tbody>
</table>
### LAO PEOPLE’S DEMOCRATIC REPUBLIC

<table>
<thead>
<tr>
<th>Act</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1989 Penal Code</td>
<td>80</td>
</tr>
<tr>
<td>2004 Criminal Procedure Law</td>
<td>80</td>
</tr>
<tr>
<td>2016 Information, Communication and Technology Law</td>
<td>86</td>
</tr>
<tr>
<td>2015 Law on Prevention and Combating Cyber Crime</td>
<td>86</td>
</tr>
</tbody>
</table>

### MALAYSIA

<table>
<thead>
<tr>
<th>Act</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1950 Evidence Act</td>
<td>99</td>
</tr>
<tr>
<td>1960 Internal Security Act</td>
<td>111</td>
</tr>
<tr>
<td>1997 Computer Crimes Act</td>
<td>114</td>
</tr>
<tr>
<td>1998 Communications and Multimedia Act</td>
<td>114</td>
</tr>
<tr>
<td>2002 Mutual Assistance in Criminal Matters Act</td>
<td>126</td>
</tr>
<tr>
<td>Penal Code (as at 1 February 2013)</td>
<td>129</td>
</tr>
<tr>
<td>2015 Prevention of Terrorism Act</td>
<td>131</td>
</tr>
</tbody>
</table>

### MALDIVES

<table>
<thead>
<tr>
<th>Act</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1968 Penal Code of The Maldives</td>
<td>133</td>
</tr>
<tr>
<td>2005 Maldives Rules of Criminal Procedure</td>
<td>133</td>
</tr>
<tr>
<td>2015 Anti-Terrorism Act</td>
<td>139</td>
</tr>
<tr>
<td>2015 Mutual Legal Assistance in Criminal Matters Act</td>
<td>145</td>
</tr>
</tbody>
</table>

### NEPAL

<table>
<thead>
<tr>
<th>Act</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1974 Evidence Act</td>
<td>147</td>
</tr>
<tr>
<td>Mutual Legal Assistance Act, 2070 (2014)</td>
<td>151</td>
</tr>
<tr>
<td>2006 Electronic Transaction Act 2063 (2008)</td>
<td>155</td>
</tr>
<tr>
<td>2007 Electronic Transaction Rules 2064</td>
<td>157</td>
</tr>
</tbody>
</table>

### PAKISTAN

<table>
<thead>
<tr>
<th>Act</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act No. XVII OF 1996 An Act to provide for re-organization of telecommunication System</td>
<td>158</td>
</tr>
<tr>
<td>1898 Code of Criminal Procedure</td>
<td>159</td>
</tr>
<tr>
<td>1984 The Qanun-e-Shahadat Order</td>
<td>162</td>
</tr>
<tr>
<td>1997 Anti-Terrorism Act</td>
<td>165</td>
</tr>
<tr>
<td>2009 Prevention of Electronic Crimes Ordinance</td>
<td>166</td>
</tr>
<tr>
<td>2016 Prevention of Electronic Crimes Act</td>
<td>174</td>
</tr>
<tr>
<td>Mutual Legal Assistance (Criminal Matters) Act, 2020.</td>
<td>187</td>
</tr>
</tbody>
</table>

### PHILIPPINES

<table>
<thead>
<tr>
<th>Act</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000 Republic Act No. 8792 June 14, 2000</td>
<td>196</td>
</tr>
<tr>
<td>2001 Rules on Electronic Evidence</td>
<td>205</td>
</tr>
<tr>
<td>2012 Republic Act No. 10175</td>
<td>209</td>
</tr>
<tr>
<td>2012 Republic Act No. 10168</td>
<td>216</td>
</tr>
<tr>
<td>2019 Proposed Amendments to the 1989 Revised Rules on Evidence</td>
<td>216</td>
</tr>
</tbody>
</table>
## SINGAPORE

- 1893 Evidence Act                               218
- 2006 Mutual Assistance in Criminal Matters Act  221
- Computer Misuse and Cybersecurity Act           222
- (Revised Edition 2007)                           226
- 2019 Evidence Act                                228

## SRI LANKA

- 1896 Evidence Ordinance                        237
- Mutual Assistance in Criminal Matters Act, No. 25 of 2002  238
- Mutual Legal Assistance in criminal matters (amendment act), No. 24 of 2018  239
- 2007 Computer Crime Act                        244
- Offences under this Act, not to be political offences &c., for the purposes of the Extradition Law  249
- 2006 Electronic Transactions Act No. 19         250

## THAILAND

- 2007 Act on Commission of Offences Relating to Computer, B.E. 2550  261
- THE CRIMINAL PROCEDURE CODE                     265
- 2008 Criminal Code                              271
- The Act on Mutual Assistance in Criminal Matters B.E. 2535  273

## TIMOR-LESTE

- Cooperação Judiciária Internacional Penal       276
- Decree-Law No. 11/2003, Establishing the Bases for the Telecommunications Sector  276
- 2005 Criminal Procedure Code                    277
- Decree-Law No. 4/2005 of Special Regimes within the Criminal Procedure  277
- 2005 Framework for Cases of Terrorism, Violent or Highly Organized Crime  278

## VIETNAM

- 1999 Penal Code                                 280
- 2007 Law on Legal Assistance                    280
- 2003 Criminal Procedure Code                    282
- 2016 Law on Network Information Security        283
- 2018 Law on Cyber Security                      290
- Decree No.55/2001/ND-CP on the Management, Provision, and Use of Internet Services  294
The United Nations Security Council (SC) resolutions 2322 (2016) and 2396 (2017) noted, inter alia:

- the significant increase in requests for cooperation in gathering digital data and evidence from the Internet
- the importance of considering the re-evaluation of methods and best practices, as appropriate, in particular related to electronic evidence
- the challenges faced by Member States in obtaining admissible electronic evidence
- the importance of Member States’ capacity to cooperate with the private sector in accordance with applicable law.

Resolution 2396 (2017) called upon Member States to take measures to improve the collection, handling, preservation and sharing of relevant information and evidence, in accordance with domestic and international law.

This document has been developed as a support material for the Online Cross-Regional Meeting on Admissibility of Electronic Evidence Obtained from Foreign Jurisdictions in the Investigation, Prosecution and Adjudication of Terrorism-Related Crimes (held on 20 and 21 January 2021). As such, this compilation encompasses relevant sections from applicable national laws and regulations gathered from across the following countries: Bangladesh, Bhutan, Brunei Darussalam, Cambodia, India, Indonesia, Lao PDR, Malaysia, Maldives, Nepal, Pakistan, Philippines, Sri Lanka, Singapore, Thailand, Timor-Leste and Vietnam.

By virtue of the above-mentioned meeting's scope, this compilation has been tailored to support the work of investigators, prosecutors, judges and staff from central authorities engaged in requesting international assistance in criminal matters along the entire continuum of gathering collecting, storing, handling, preserving, sharing and disclosing electronic evidence, whether by means of directly contacting foreign officials/authorities or foreign-based service providers.

Fields of Law

This compilation encompasses excerpts from more than 80 laws and regulations, pertaining to the following Fields of Law:

- Criminal Law (including criminal procedural law and criminal forensic standards)
- Mutual Legal Assistance Law
- Evidence Law
- Telecommunication Law
- Counterterrorism and International Security Law and Cybercrime Law

Excerpts from other relevant Fields of Law such as Constitutional Law, Human Rights Law and Privacy Law were not considered in this compilation. These may, in the future, be the object of a different compilation.

Methodology

In compiling this material, the following five criteria were used to assess the extent to which a given section of the law/regulation is deemed applicable and hence reproduced in this compilation. The icons on the left column are used across this document to prompt the reader to provisions that specifically match the corresponding criteria.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>![person]</td>
<td>1) Is the section of the law/regulation relevant for the admissibility of evidence at court?</td>
</tr>
<tr>
<td>![briefcase]</td>
<td>2) Is it relevant for the purpose of electronic evidence or electronic data of probative value?</td>
</tr>
<tr>
<td>![globe]</td>
<td>3) Is it relevant in the context of international cooperation in criminal matters (i.e. investigations, prosecutions and adjudications involving foreign jurisdictions)?</td>
</tr>
<tr>
<td>![file]</td>
<td>4) Is it relevant in the context of data in possession and/or custody of foreign-based service providers?</td>
</tr>
<tr>
<td>![lightning bolt]</td>
<td>5) Is it relevant for the purpose of terrorism-related cases?</td>
</tr>
</tbody>
</table>
1872 EVIDENCE ACT

88. Presumption as to telegraphic messages

The Court may presume that a message, forwarded from a telegraph office to the person to whom such message purports to be addressed, corresponds with a message delivered for transmission at the office from which the message purports to be sent; but the Court shall not make any presumption as to the person by whom such message was delivered for transmission.

104. Burden of proving fact to be proved to make evidence admissible

The burden of proving any fact necessary to be proved in order to enable any person to give evidence of any other fact is on the person who wishes to give such evidence.

131. Production of documents which another person, having possession, could refuse to produce

No one shall be compelled to produce documents in his possession, which any other person would be entitled to refuse to produce if they were in his possession, unless such last-mentioned person consents to their production.

2001 INFORMATION AND TELECOMMUNICATION ACT

Chapter I PRELIMINARY

2. Definitions.

In this Act, unless the context otherwise requires,—
(1) «digital signature» means data in an electronic form, which—
(a) is related with any other electronic data directly or logically; and
(b) is able to satisfy the following conditions for validating the digital signature— (i) affixing with the signatory uniquely; (ii) capable to identify the signatory; (iii) created in safe manner or using a means under the sole control of the signatory; and (iv) related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.
(2) «digital signature certificate» means a certificate issued under section 36;
(3) «electronic» means electrical, digital, magnetic, wireless, optical, electromagnetic or any technology having equivalent such capability;
(4) «electronic data interchange» means transferring data from one computer to another computer electronically by following a standard for the purpose of organizing information;
(5) «electronic form» with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device or technology;
(6) «electronic gazette» means the official gazette published in the electronic form in addition to official printed...
& published gazette;

(7) «electronic record» means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche;

(8) «internet» means such an international computer network by which users of computer, cellular phone or any other electronic system around the globe can communicate with one another and interchange information and can browse the information presented in the websites;

(9) «electronic mail» means information generated electronically and transmitted using internet;

(10) «data» means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form including computer printouts, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer;

(11) «data message» means electronic, electronic data interchange including optical, electronic mail, telegram, telex, fax, telecopy, short message or created something similar, sent, received or stored information;

(12) «website» means document and information stored in computer and web server which can be browsed or seen by the user through internet;

(13) «computer» means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

(14) «computer network» means the interconnection of one or more computers through the use of satellite, microwave, terrestrial line, wireless equipment, wide area network, local area network, infrared, WiFi, bluetooth or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(15) «subscriber» means a person in whose name the Digital Signature Certificate is issued;

(16) «chairman» means a chairman appointed under cyber appeal tribunal of section 82 of this Act;

(17) «civil procedure» means Code of Civil Procedure, 1908 (Act V of 1908);

(18) «penal code» means Penal Code, 1860 (Act XLV of 1860);

(19) «prescribed» means prescribed by rules;

(20) «secure signature generating machine or technology» means any signature generating machine or technology subject to the conditions illustrated under section 17;

(21) «addressee» with reference to data message means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(22) «verification» means such procedure used to identify signatory or authentication of data message;

(23) «originator» with reference to data message means a person who sends or prepares data message before preservation or causes any data message to be sent, generated, stored or transmitted but does not include an intermediary;

(24) «regulation» means regulation prepared under this Act;

(25) «criminal procedure» means Code of Criminal Procedure, 1898 (Act V of 1898);

(26) "person" relates to unique person having any natural entity, partnership business, union, company, body corporate, cooperatives;

(27) “adjudicating officer” means an adjudicating officer of cyber tribunal constituted under section 68 of this Act;

(28) «rule» means rule prepared under this Act;

(29) “medium” means any person sending, receiving, advancing or saving any data message or any service rendering on this data message on behalf of any other person for a particular data message;

(30) “licence” means a licence granted under section 22 of this Act;

(31) “authentication service provider” means certificate issuing authority or any person rendering service related to digital signature.

(32) “certifying authority” means a person or authority who has been granted a licence under section 18 to be read with section 22 of this Act to issue a Digital Signature Certificate;

(33) “certification practice and description of procedure” means certification practice and description of procedure defined by the regulation where practices and procedures are written for issuing Digital Signature Certificate;

(34) “member” means a member of cyber appeal tribunal constituted under section 82 of this Act;

(35) “signatory” means a person providing signature generated through signature generating machine or procedure;

(36) “signature verification machine” means software or hardware used for verifying signature;

(37) “signature generating machine” means software or hardware used generating data for creating signature;

(38) “cyber tribunal” or “tribunal” means a cyber tribunal constituted under section 82 of this Act;

(39) “cyber appeal tribunal” means a cyber appeal tribunal constituted under section 82 of this Act.

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such information or matter is rendered or made available in an electronic form: Provided that such information or matter is accessible so as to be usable for a subsequent reference.


(1) Where any law provides that any document, record or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied—(a) the information contained therein remains accessible so as to be usable for a subsequent reference; (b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; (c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained: Provided that this sub-clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. (2) A person may satisfy the requirements referred to in sub-section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with. (3) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information.

11. No liability on Government to accept documents in electronic form.

Nothing contained in this Act shall by itself compel any Ministry or Department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Chapter III
ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS


(1) An electronic record shall be that of the originator it was sent by the originator himself. (2) As between the originator and the addressee, an electronic record shall be deemed to be that of the originator if it was sent—(a) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or (b) by an information system programmed by or on behalf of the originator to operate automatically. (3) As between the originator and the addressee, an addressee shall be entitled to regard an electronic record as being that of the originator and to act on that assumption if—(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or (b) the information as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify the electronic records as its own. (4) Sub-section (3) of this section shall not apply—(a) from the time when the addressee has received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;
(b) in such case as in clause (b) of section (3) of this section, at any time when the addressee knew or ought to have known, after using reasonable care or using agreed procedure, that the electronic record was not that of the originator; (c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the electronic record as being that of the originator or to act on that assumption.

(5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee shall be entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption.

(6) Whatever is there in sub-section (5) of this section, the addressee shall not be so entitled when the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the transmission resulted in any error in the electronic record as received.

(7) The addressee shall be entitled to regard each electronic record received as separate electronic record and to act on that assumption; however, it shall not be applicable for the following electronic records-- (a) duplicates of other electronic records created by the addressee; and (b) the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the electronic record was a duplicate.

15. Time and place of dispatch and receipt of electronic record.

(1) Save as otherwise agreed to between the originator and the addressee,-- (a) the time of dispatch of an electronic record shall be determined when it enters a computer or electronic machine or resource out side the control of the originator; (b) the time of receipt of an electronic record shall be determined as follows, namely:-- (i) if the addressee has designated an electronic device or resource for the purpose of receiving electronic records, receipt occurs,-- (a) at the time when the electronic record enters the designated electronic device or resource; (b) if the electronic record is sent to an electronic device or resource of the addressee that is not designated electronic device or resource, at the time when the electronic record is retrieved by addressee; (ii) if the addressee has not designated an electronic device or resource along with the specified timings, if any, receipt occurs when the electronic record enters the electronic device or resource. (c) An electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(2) The provision of sub-section (1) (b) of this section shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (1) (c) of this section.

(3) For the purposes of this section,-- (a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business; (b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.

Chapter V CONTROLLER & CERTIFYING AUTHORITIES


(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may, with the previous approval of the Government, and by notification in the Official Gazette and additionally optionally in Electronic Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1) of this section, the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) of this section, for reasons to be recorded in writing, by notification in the Official Gazette and additionally optionally in Electronic Gazette, revoke such recognition.

30. Access to computers and data

(1) Without prejudice to the provisions of section 45 of this Act the Controller or any officer authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or rules and
(2) For the purpose of sub-section (1) of this section the Controller or any officer authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

(3) If authorization has been given to a person, the authorized person shall oblige to assist as instructed under sub-section (1) of this section.

31. Certifying Authority to follow certain procedures.—Every Certifying Authority shall—

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;
(b) provide a reasonable level of reliability in its services which are reasonable suited to the performance of intended function under this Act;
(c) adhere to security procedures to ensure that the secrecy and privacy of digital signatures are assured; and
(d) observe such other standards as may be specified by regulations.

35. Disclosures.

(1) Every Certifying Authority shall disclose in the manner specified by regulations—

(a) Digital Signature Certificate used by the Certifying Authority to digitally sign another Digital Signature Certificate;
(b) any certification practice statement relevant thereto;
(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
(d) any other fact the materially and adversely affects either the reliability of a Digital Signature Certificate, which the Certifying Authority has issued, or the Certifying Authority's ability to perform its service.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then the Certifying Authority shall use reasonable efforts to notify any person who is likely to affected by the occurrence, or act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Part-2 Establishment of Cyber Tribunal, Investigation of Offences, Adjudication, Appeal Etc. (...)

72. Time limit to deliver verdict.

(1) The Judge of Cyber Tribunal shall give the verdict within ten days from the date of completing of taking evidence or debate, what happened later, unless he extends the time limit no more than ten days with having written reasons.

(2) If the verdict is given by the Cyber Tribunal under sub-section (1) of this section or any appeal is lodged against the verdict to the Cyber Appellate Tribunal then Cyber Tribunal or Cyber Appellate Tribunal concerned shall forward the copy of the verdict of the appeal to the Controller for preserving it in the electronic records repository room established under section 18 (7) of this Act.

87. Augmented use of few definitions used in few acts.

For the purpose of this Act,

(a) The definition of “document” in section 29 of Penal Code, 1860 (Act XLV of 1860) also includes the document generated or prepared by electronic machine or technology;

(b) The definition of “document” in section 3 of Evidence Act, 1872 (Act I of 1872) also includes the document generated or prepared by electronic machine or technology)
69. Trial procedure of Cyber Tribunal.

(1) Without written report of a police officer not below the rank of Sub-Inspector or the prior approval of the Controller or any other officer authorized by the Controller the special Tribunal shall not accept any offence trial.

2) The Tribunal shall follow the rules mentioned in the Chapter 23 of the Code of Criminal Procedure, if they are not inconsistent with the rules of this Act, which is used in Session Court.

(3) Any Tribunal shall not suspend any prosecution without having written reasons and unless it is required for the sake of just adjudication.

(4) If the Tribunal is in the opinion that the accused person has been absconded and for that it is not possible to arrest him and produce him before the Tribunal and there is no possibility to arrest him immediately, in that case the Tribunal can order the accused person to appear before the Tribunal by publishing such order in two mass circulated national Bengali dailies and if the accused person fails to do so, the prosecution shall take place in his absence.

(5) The rules mentioned in sub-section (4) of this section shall not be applicable if the accused person fails to appear before the Tribunal or absconded after getting bail.

(6) The Tribunal can order any police officer, or the Controller, or any officer authorized by the Controller, as the case may be, to reinvestigate the case and submit the report within the stipulated time of its own initiative or any application lodged to the Tribunal.

70. Application of code of criminal procedure in the activities of Tribunal.

(1) Rules of Code of Criminal Procedure, as far as, are not inconsistent with the rules of this Act shall be applicable in the activities of this Tribunal and it will have all the power as exercised by the Session Court.

2) The person prosecuting the case on behalf of the Government in this tribunal to be known as public prosecutor.

75. Prosecution procedure followed by the Session Court.

(1) To prosecute any offence committed under this Act, which is trialed in Session Court, Session Court shall follow the rules mentioned in section 23 of the Code of Criminal Procedure which is applicable in Session Court trial.

2) Any Session Court shall not accept any prosecution/trial of any offence committed under this Act without any written report from the police officer not below the rank of Sub-Inspector of the Police and prior approval of the Controller or any officer authorized by the Controller, whatever is contained in the Code of Criminal Procedure.

76. Investigation of crime, etc.

(1) Whatever is contained in the Code of Criminal Procedure, the Controller or any officer authorized by the Controller, or any police officer not below the rank of Sub-Inspector of the Police shall investigate any offence committed under this Act.

2) Offence committed under this Act shall be non-cognizable offence.

2009 Anti-Terrorism Act

(2012 and 2013)

2. Definitions

(14) "property" means, whether in or outside the country, -

i) any type of funds or assets, corporeal or incorporeal, moveable or immovable, tangible or intangible, how-
ever acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets or funds and any interest, dividends or other income on or value accruing from or generated by such funds or assets.

ii) cash, any other type of financial assets, economic resources, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travelers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

21. Special provisions with regard to examination of witnesses by police

(1) If any police officer, while investigating any case under this Act, finds it necessary to examine any person acquainted with the facts and circumstances of the case and, if the police officer has knowledge or reasonable grounds to believe that the said person is capable of giving a description of the facts in writing, the police officer with consent of the person, may take a written description of the facts from that person.

2) The said person shall make his statement or description of the facts in writing under his hand and shall sign the same.

3) Notwithstanding contained in the Evidence Act, any discussion and conversation through Facebook, Skype, Twitter or any other internet site by the terrorist person or entity or still picture or video involving their offence are presented by the police or law enforcement agency to the Court for the purpose of investigation, the presented information by the police or law enforcement agency shall be treated as evidence to the Court.

24. Time-limit for investigation.

(1) Any police officer shall complete the investigation of any case under this Act within [60 (sixty) days] of the date on which information was received or recorded under section 154 of the Code of Criminal Procedure.

2) If any police officer fails to complete investigation within the time-limit mentioned in sub-section (1), he may extend the time for investigation for a period not exceeding [30 (thirty) days], by recording the reasons in writing in the case diary.

3) If the said police officer fails to complete the investigation within the time-limit mentioned in sub-section (2), the said investigation officer may, with the written authorization of the Police Superintendent of the relevant district or, as the case may be, the relevant Deputy Police Commissioner of the Metropolitan area, may extend the time for a further period not exceeding 30 (thirty) days [: Provided that the time-limit mentioned in sub-sections (1) to (3) shall not be applicable, if the evidence is required to be collected from outside of Bangladesh for investigation purpose.]

4) If the said police officer fails to complete the investigation within the time-limit mentioned in sub-section (3), he shall, without any delay, inform the matter with reasons, to the Police Superintendent of the relevant district or, as the case may be, the relevant Deputy Police Commissioner of the Metropolitan area, and if the reasons given are not satisfactory, the said investigation officer shall be [accused for negligence in performing his duties].

25. Extension of time-limit with regard to investigation of certain cases.

(1) If any police officer fails to complete investigations within the extended time-limit specified in sub-section (3) of [section 24] due to the identity of the offender mentioned in the first information report (FIR) being not discovered and the inability to identify the said offender, it shall not be deemed to be a bar to submit any police report or a new police report or an additional police report at any time following the extended time-limit mentioned in [section 24].

2) If any police officer fails to complete investigation within the extended time-limit to provide offence related evidence or any report specified in sub-section (3) of [section 24] due to the inability to collect a medical, forensic, fingerprint, chemical or other expert witness, over which the police officer has no control and without which no effective report of the case may be possible to prepare, it shall not be deemed to be a bar to submit the police report at any time following the said extended time-limit.
26. Remand.

(1) Where any person is arrested and detained for purposes of investigation, the investigation officer may make an application to the competent Magistrate for remand of the accused in police custody.

2) On consideration of the application made under sub-section (1), the Magistrate may remand the accused in police custody and the duration of such remand shall not exceed an aggregate or consecutive period of 10 (ten) days: Provided that if the investigation officer is able to satisfactorily prove before the Magistrate that additional evidence may be gathered if the accused is remanded for an extended period, the Magistrate may extend the period of further remand for a term not exceeding 5 (five) days.


(1) The Government may, by notification in the official Gazette, constitute one or more Anti-terrorism Special Tribunals for speedy and effective trial of the offences committed under this Act.

2) A Special Tribunal constituted under sub-section (1) shall consist of a Sessions Judge or an Additional Sessions Judge appointed by the Government in consultation with the Supreme Court; and a Judge so appointed shall be designated as the “Judge, Anti-terrorism Special Tribunal”.

3) A Special Tribunal constituted under this section may be assigned to the local jurisdiction over the whole of Bangladesh, or of one or more Sessions Divisions; and the said Tribunal shall only try the cases of offences under this Act, which are filed or transferred to the Tribunal.

4) On account of assigning to a Special Tribunal the jurisdiction for the whole of Bangladesh, or any part thereof consisting of one or more Sessions Divisions by the Government, a Sessions Judge or an Additional Sessions Judge of that territorial jurisdiction shall not cease to have jurisdiction in respect of trial of offences under this Act, and the cases of offences pending before the Court of Sessions under this Act, shall not be transferred to any Special Tribunal having territorial jurisdiction, unless the Government, by notification in the official Gazette, so directs.

5) There shall not be any bar for a Special Tribunal, unless it otherwise decides to recall or rehear any witness whose evidence has already been recorded or to reopen the proceedings already held under sub-section (4), but may act on the evidence already recorded or produced and continue the trial from the stage the case has reached.

6) A Special Tribunal may sit and conduct its proceedings at such times and places as the Government may, by order, specify.

41. Transfer of cases to and from Special Tribunal.

The Government may, at any stage of trial before conclusion of evidence, transfer any case or cases involving any offence under this Act from a Court of Sessions to a Special Tribunal or from a Special Tribunal to a Court of Sessions on reasonable grounds.

2018 DIGITAL SECURITY ACT

27. Punishment for committing Cyber-terrorism:

(1) If any person –

a. With the intention to breach the national security or to endanger the sovereignty of the Nation and to instill terror within the public or a part of them creates obstruction in the authorized access to any computer, computer network or internet network or illegally accesses the said computer, computer network or internet network or cause the act of obstruction of access or illegal entry through someone, or

b. Creates such pollution within any digital device or inserts malware which causes in the death of a person or results in serious injury to a person or raises a possibility of it, or

c. Damages or destroys the supply of daily necessities of public or adversely affects any critical information infrastructure. d. Intentionally or knowingly enters or penetrates any computer, computer network, internet network,
any secured data information or computer database or such secured data information or computer database which can be used to damage friendly relations with another foreign country or can be used for acts against public order or which can be used for the benefit any foreign country or any foreign person or any group. Then that activity of that person will be considered as cyber security crime.

2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 14 (fourteen) years or with fine not exceeding 1(one) crore taka or with both.

3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with lifetime imprisonment or with fine not exceeding 5(five) crore taka or with both.

42. Search and Seizure through Warrant:

If any police office has reason to believe that,

a. An offence has been committed or there is possibility of commission of an offence under this Act, or-

b. Any computer, computer system, computer network, data-information relating to an offence under this Act, or any evidence-proof thereof is being kept in some place or with a person, Then, he/she can after recording the reason for such belief, apply to the tribunal or as the case may be, to the Chief Judicial Magistrate or Chief Metropolitan Magistrate to obtain search warrant and do the below mentioned tasks:

c. To seize any traffic data which is under possession of any service provider, At any level of communication create obstruction to any telegraph or electronic communication containing recipient information and any data traffic including data-information.

43. Search, Seizure and Arrest without Warrant:

(1) If a police officer has a reason to believe that an offence under this Act has been or is being or will be committed in any place, or there is a possibility of it happening, or if there is a possibility of evidence being lost, destroyed, deleted or altered or possibility of it being made scarce in some other way, then the officer, upon recording the reason for his/her belief, can undertake the following tasks:

a. Enter and search the said place and, if interrupted, take necessary action in accordance with the Code of Criminal Procedure;

b. Seize the computer, computer systems, computer network, data-information or other objects which were used in committing the offence or documents that can aid in proving the offence that are found in that place while conducting the search;;

c. Conduct physical search of any person present in that place; d. Arrest anyone present in the said place if suspected of committing or having committed an offence under this Act.

d. (2) After conducting a search under subsection (1), the police officer will submit a search report to the Tribunal.

44) Data Preservation:

(1) If the Director General on his own accord or on the basis of an application by the investigation officer believes that, any data-information stored in a computer should be preserved for the interest of an investigation under this Act or there is possibility that such information could be harmed, destroyed, altered or lost , then, he/she can order the person or institution responsible for that computer or computer system to preserve such data-information for 90(ninety) days.

2) Tribunal may, on application, extend the period of preservation of such data-information but it should not be for more than a total of 180 (one hundred and eighty) days.

58) Testimonial value:

Notwithstanding anything contained in the Evidence Act 1972 (Act I of 1872), or any other law, any forensic evidence obtained or collected under this Act shall be treated as evidence in the trial proceedings.
3. Evidence means all types of proof or probative matter presented and permitted by the Court at a legal proceeding by the act of the parties or required by the Court on its own through the medium of witnesses, documents inclusive of electronic records and physical evidence in relation to matters under inquiry.

### Types of evidence

4. Evidence shall be categorized into the following types:

- (a) Testimonial;
- (b) Documentary including electronic records;
- (c) Physical; and
- (d) Expert opinion.

5. Evidence may be:

- (a) Direct; or
- (b) Circumstantial or indirect.

### Examination of evidence

6. Evidence may be examined by the:
   - (a) Plaintiff or prosecutor;
   - (b) Defendant or victim;
   - (c) Witnesses; and
   - (c) Court.

### Objections to evidence

7. If a party believes that any evidence, including oral, physical, or documentary is improper under the Evidence Act, then that party shall at the time the evidence is given or sought to be given, state the grounds why the evidence is improper with specific reference to the applicable section of the Evidence Act.

8. When a party objects to evidence, the Court shall rule whether the evidence can be given or not and may hear arguments from either party on whether the evidence is admissible or not.
### Waiver of objections to evidence

9. If a party fails to object to evidence at the time it is introduced, then that party shall be deemed to have waived the right to object to the admission of that evidence thereafter and on any appeal.

### Offer of proof

10. If a party believes that the Court wrongfully refused to admit evidence, then that party shall at the time the Court rules against admissibility, state the type of evidence excluded and what the evidence consisted and would have proved.

### Limited admissibility of evidence

11. When evidence that is admissible as to one party or for one purpose but not admissible as to another party or for another purpose is admitted, the Court, upon request of a party or on its own, shall have the discretion to restrict the evidence to its proper scope and instruct the parties accordingly.

### Evidence that may be given

14. Evidence may be given in any legal proceeding of every fact in issue (i.e., the points of facts for determination in a case) and of every other fact and circumstance which does the following:
   a) Proves a fact in issue;
   b) Disproves a fact in issue; or
   c) Rationally renders the existence of a fact in issue probable or improbable.

### Relevant facts

15. Evidence may be given in a legal proceeding of facts that are connected with a fact in issue.
6. A fact though not in issue is relevant, if it forms part of the same transaction as the fact in issue.
7. A fact that is the cause and effect of a fact in issue or a relevant fact is relevant.
8. A fact that is necessary to explain or introduce a fact in issue or a relevant fact is relevant.

### Relevancy of the prior judgments and Court orders

19. The existence of any judgment or order from a Court about the same subject matter is a relevant fact, when it:
   d) Helps the Court to arrive at a correct conclusion as to a fact in issue or relevant fact; or
   e) The existence of the judgment or order is a fact in issue or relevant fact
20. Any party to a legal proceeding may challenge any judgment or order of a Court which is relevant or which is relied upon by showing that the judgment or order:
   a) Was delivered by a Court not competent to deliver it;
   b) Was obtained by fraud or collusion; or
   c) Is against the laws of the country.
1. Any judgment or order from a Court in the criminal proceeding shall not be relevant in the civil proceeding.
Expert reports

22. An expert report shall be admissible as evidence in a legal proceeding, if the expert, who wrote the report, gives oral evidence in the proceeding.
3. If the expert, who wrote the report does not give oral evidence at the legal proceeding, then that expert's report shall be admissible with leave of Court after the Court examines:
   a) The content of the report;
   b) The reasons why the expert, who wrote the report is not giving oral evidence at the legal proceeding; and any other circumstances that appear to the Court to be relevant and need to be considered in the interest of justice.

Motive

24. Any fact that establish the requisite intention or motive for any fact in issue or relevant fact are relevant and admissible.

Preparation and Conduct

25. Any fact, which shows preparation or conduct of the defendant for any fact in issue or relevant fact, is relevant and admissible.

Subsequent remedial measures

29. Evidence tendered after an injury or harm occurred that a party took certain actions to prevent the same injury or harm from occurring in the future shall not be admissible to show that the party is liable for the injury or harm originally caused.

Settlement

30. Evidence about failed attempts to resolve a legal proceeding, all non accepted offers of settlement and statements made during negotiations are not admissible in a legal proceeding.

Evidence taken in another legal proceeding

31. The evidence given in one legal proceeding upon the issues raised in that proceeding may be relevant and be taken into consideration in another legal proceeding in which the same issues arise.

Exclusion of relevant evidence

32. Although relevant, evidence may be excluded if:
   a) Its probative value is substantially outweighed by the danger of unfair prejudice;
   b) It could cause undue confusion of the issues;
   c) It could mislead the Court;
   d) It could cause undue delay or a waste of time; or
   e) It is cumulative.
3. No person’s identification shall be revealed, if the person is the source of evidence or a witness to the issue and the Court believes that his identification needs to be protected.

**Oral evidence as to the contents of a document**

41. Oral evidence as to the contents of a document that is or could be produced in Court is not admissible unless and until the party proposing to prove the contents shows that the genuineness of the document is in question and the Court determines that oral evidence about the content of the document is not unduly prejudicial to a party and is in the interest of justice.

**Duplicate documents**

42. A duplicate document is admissible to the same extent as an original unless:
   a) A genuine question is raised as to the authenticity of the original; or
   b) Under the circumstances, it would be unfair and prejudicial to a party to admit the duplicate in lieu of the original.

**Electronic documents**

43. An electronic document, including an electronic signature, is admissible to the same extent as a non-electronic document unless a genuine question is raised as to the security or integrity of the electronic document system by or in which the electronic document or electronic signature was recorded or stored.

**Content of official records**

45. The contents of an official record, including data compilations in any form, if otherwise admissible, may be proved by a copy certified as correct.

2004 PENAL CODE OF BHUTAN

PART ONE GENERAL PROVISION

Chapter 3

*Sentencing*

6. A defendant convicted of a criminal offence shall not be sentenced otherwise than in accordance with this Penal Code.

7. Life imprisonment shall be awarded to the defendant:
   a) In case of a felony of the first degree comprising of murder, treason or terrorism;
   b) For the offence against the Ku, Sung, Thuk-ten and Zung; or
   c) For the offence of illegal manufacturing of weapon of mass destruction

8. A defendant convicted of a felony of the first degree shall be sentenced to a term of imprisonment, a minimum of which shall be fifteen years and a maximum of which shall be life imprisonment. (…).
PART FOUR
COMMERCIAL CRIME, FRAUD, CORRUPTION AND RELATED OFFENCES

Chapter 22
Defamation and Related Offences

Grading of Defamation.

319. The offence of defamation shall be: (a) A felony of the fourth degree and pay compensation for a minimum of one month and a maximum of three years to the aggrieved party calculated in accordance with the daily minimum national wage rate, if the defamation includes murder, armed robbery, terrorism or treason; or (b) A petty misdemeanour and pay compensation to the aggrieved party for a minimum of one month and maximum of three years calculated in accordance with the daily minimum national wage rate, if the defamation includes any matter other than murder, armed robbery, terrorism or treason.

Grading of Libel.

321. The offence of libel shall be:
- A felony of the fourth degree and pay compensation for a minimum of one month and a maximum of three years to the aggrieved party calculated in accordance with the daily minimum national wage rate, if the libel includes murder, armed robbery, terrorism or treason;
- A petty misdemeanour and pay compensation to the aggrieved party for a minimum of one month and maximum of three years calculated in accordance with the daily minimum national wage rate, if the libel includes any matter other than murder, armed robbery, terrorism or treason.

PART 5 OFFENCES AGAINST STATE AND PUBLIC ORDER
CHAPTER 23 TREASON, TERRORISM AND RELATED OFFENCES

Terrorism 329.

A defendant shall be guilty of the offence of terrorism, if the defendant:
- With intent to subvert the state, uses or assists, recruits, or trains another person to use a bomb, dynamite, fire-arm, or other lethal weapon against Bhutan;
- Participate in financing, planning, or preparation of terrorists acts or in supporting terrorists acts directly; or
- Engages in a violent act or insurrection against Bhutan that is designed primarily to generate fear in a community or a substantial section of the society.

Grading of Terrorism.

330. The offence of terrorism shall be a felony of the first degree.
Eavesdropping

468. A defendant shall be guilty of the offence of eavesdropping, if the defendant unlawfully engages in wiretapping, mechanical overhearing of conversation, or intercepting or accessing of an electronic communication.

Unauthorized opening of mail or parcel.

470. A defendant shall be guilty of the offence of an unauthorized opening of mail or parcel, if the defendant without lawful warrant intercepts and opens any mail or parcel not addressed to the defendant.

Grading of Unauthorized opening of mail or parcel.

471. The offence of the unauthorized opening of mail or parcel shall be a felony of the fourth degree.

CHAPTER 31 COMPUTER OFFENCES

Tampering with computer materials.

472. A defendant shall be guilty of the offence of tampering with computer materials, if the defendant interferes, alters, or destroys any data or hacks in a computer system or computer program of another person or plants a virus in a computer without the right to do so.

Grading of Tampering with computer materials.

473. The offence of tampering with computer materials shall be a felony of the fourth degree.

Unlawful possession of computer materials.

474. A defendant shall be guilty of the offence of unlawful possession of computer materials, if the defendant knowingly possesses in any form any copy, reproduction, or duplicate of any computer data procured by someone else with intent to benefit the defendant or a person other than the owner thereof.

Grading of Unlawful possession of computer materials.

475. The offence of unlawful possession of computer materials shall be a petty misdemeanour.
2018 INFORMATION COMMUNICATION AND MEDIA ACT

Power to require information

53. The Authority may, by notice in writing direct any person of ICT and Media Facilities or ICT and Media Services:
   To produce, at a time and place specified in the notice, any document, or information specified in the notice which is in that person's custody or control;
   To appear, at a hearing, before the Authority at a time and place specified in the notice to give any evidence, either orally or in writing; and
   carrying on any business to furnish estimates, returns or other information as may be specified in the notice, and specify the time, the manner and the form in which any such estimates, returns or information are to be furnished.
4. A person shall not be compelled to produce a document under section 53 of this Act, which the person could not be compelled to be produced in a civil proceeding or civil court or give any information which the person could not be compelled to give in evidence in such proceedings.

Admissibility and evidential weight of data messages

299. In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
   1) On the sole ground that it is an electronic document or data message; or
   2) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the sole grounds that it is not in its original form.
05. Section 304 of this Act, does not limit the ability of any person to adduce evidence of non-reliability of an electronic signature.

Cyber terrorism

431. A person shall be guilty of the offence of cyber terrorism, if the person with intent to threaten sovereignty, security and harmony of Bhutan, or the interests of friendly relations with foreign states, disrupt public order, or to strike terror in the people:
   1) Deny access to any person authorised to access any computer or computer network;
   2) Attempt to penetrate or access any computer or computer network without authorisation or exceeding authorised access; or
   3) Introduces or causes to introduce any computer contaminant.
32. A person who commits or conspires to commit an act in section 431 of this Act shall be liable for offence of felony of first degree.

Entry and search of premises

443. Where a Court is satisfied upon application that there is reasonable ground for suspecting that an offence under this Act or under the Rules and Regulations made thereunder, has been or is being committed, and that evidence of the commission of the offence is likely to be found on any premises; it shall, in accordance with the provisions of the Civil and Criminal Procedure Code of Bhutan, issue a search warrant.
454. The Ministry may, for the purpose of providing expert opinion on computer evidence before any court, specify by directive to a department, body or agency of the Government or any third party to act as an Examiner of Electronic Evidence.

55. For the purposes of section 454 of this Act, “computer evidence” means any information of probative value that is either stored or transmitted in electronic form which include among others, computer evidence, cell phones, audio, and video devices.


**BRUNEI DARUSSALAM**

**1982 INTERNAL SECURITY ACT**

**PART I PRELIMINARY**

---

### Interpretation.

2. In this Act, unless the context otherwise requires

Terrorist means any person who —

a) by the use of any firearm, explosive or ammunition acts in a manner prejudicial to the public safety or to the maintenance of public order or incites to violence or counsels disobedience to the law or to any lawful order;

b) carries or has in his possession or under his control any firearm, ammunition or explosive without lawful authority therefor; or

c) demands, collects or receives any supplies for the use of any person who intends or is about to act, or has recently acted, in a manner prejudicial to public safety or the maintenance of public order.

### Powers of seizure.

19. Any officer or person authorised to exercise the powers of entry or investigation under section 17 may seize any document or other thing in respect of which he reasonably believes an offence to have been committed under this Chapter or any order made thereunder or which he reasonably believes to be or to contain evidence relating to such an offence: Provided that nothing in this section shall be deemed to affect the powers of a police officer under the provisions of the Criminal Procedure Code (Chapter 7).

### Powers of search.

47. (1) When on duty any police officer or any member of any other security force or any person who is authorised in writing so to do by the officer commanding a Police District, may without warrant and with or without assistance stop and search any vehicle, vessel, aircraft or individual, whether in a public place or not, if he suspects that any article or material being evidence of the commission of an offence against this Part as likely to be found in such vehicle, vessel or aircraft or on such individual, and may seize any article or material so found.

2) When on duty any police officer of or above the rank of corporal or any member of any other security force of or above the rating or rank of leading rate or non-commissioned officer (as the case may be) or any person authorised in writing so to do by the officer commanding a Police District may without warrant and with or without assistance enter and search any premises or place if he suspects that any article or material being evidence of the commission of any offence against this Part is likely to be found on such premises or place and may seize any article or material so found.

3) No woman shall be searched under this section except by a woman.

### Admission of statements in evidence.

57. (1) Where any person is charged with any offence against this Act or against any written law for the time being specified in Schedule 3 any statement, whether such statement amounts to a confession or not or is oral or in writing, made at any time, whether before or after such person is charged and whether in the course of a police investigation or not and whether or not wholly or partly in answer to questions, by such person to or in the hearing of any police officer of or above the rank of inspector and whether or not interpreted to him by any other police officer or any other person concerned or not, in the arrest, shall notwithstanding anything to the
Contrary contained in any written law be admissible at his trial in evidence and, if such person tenders himself as a witness, any statement may be used in cross examination and for the purpose of impeaching his credit.

2) Notwithstanding subsection (1), no statement shall be admissible or used as aforesaid under that subsection —

a) if the making of the statement appears to the court to have been caused by any inducement, threat or promise having reference to the charge against such person, proceeding from a person in authority and sufficient in the opinion of the court to give such person grounds which would appear to him reasonable for supposing that by making it he would gain any advantage or avoid any evil of a temporal nature in reference to the proceeding against him; or

b) in the case of a statement made by such person after his arrest, unless the court is satisfied that a caution was administered to him in the following words or words to the like effect: “It is my duty to warn you that you are not obliged to say anything or to answer any question, but anything you say, whether in answer to a question or not, may be given in evidence”. Provided that a statement made by any person before there is time to caution him shall not be rendered inadmissible in evidence merely by reason of no such caution having been given if it has been given as soon as possible.

3) Notwithstanding anything to the contrary contained in any written law a person accused of an offence to which subsection (1) applies shall not be bound to answer any question relating to such case after a caution has been administered to him under subsection 2(b).

### Inspection of banker’s books.

58. The Minister may, if he is satisfied that any evidence of the commission of an offence against this Act or against any written law for the time being specified in Schedule 3 is likely to be found in any banker’s book, by order authorise any police officer to inspect any such book, and a police officer so authorised may, at all reasonable times, enter the bank specified in the order and inspect the banker’s books kept therein, and may take copies of any entry in any such book.

# 2000 COMPUTER MISUSE ACT

(Revised Edition 2007)

## PART I PRELIMINARY

### Citation. 1.

This Act may be cited as the Computer Misuse Act.

### Interpretation. 2.

(1) In this Act, unless the context otherwise requires —

- “computer” means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include — (a) a similar device which is non-programmable or which does not contain any data storage facility; or (b) such other device as the Minister may, by notification in the Gazette, prescribe;

- “computer service” includes computer time, data processing and the storage or retrieval of data; “damage” means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that — (a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may by notification in the Gazette prescribe, except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account; (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons; (c) causes or threatens physical injury or death to any person; or (d) threatens public health or public safety;

- “data” means representations of information or of concepts that are being prepared or have been prepared in a
form suitable for use in a computer; electronic, acoustic, mechanical or other device” means any device or apparatus that is used or is capable of being used to intercept any function of a computer; function” includes logic, control, arithmetic, deletion, storage and retrieval, read and write, and communication or telecommunication to, from or within a computer; intercept”, in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof; Minister” means the Minister of Finance; “output” means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact — (a) produced by a computer; or (b) accurately translated from a statement or representation so produced; “program” means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he — (a) alters or erases the program or data; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c) uses it; or (d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

3) For the purposes of subsection (2)(c), a person uses a program if the function he causes the computer to perform — (a) causes the program to be executed; or (b) is itself a function of the program.

4) For the purposes of subsection (2)(d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if — (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

6) A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of that computer or any other computer — (a) any program or data held in that computer is altered or erased; (b) any program or data is added to its contents; or (c) any act which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as causing it.

8) Any modification referred to in subsection (7) is unauthorised if — (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and (b) he does not have consent to the modification from any person who is so entitled.

9) A reference in this Act to a program includes a reference to part of a program.

Evidence from computer records.

15. (1) Notwithstanding sections 35A and 35B of the Evidence Act (Chapter 108), in any proceedings under this Act any relevant output shall be admissible as evidence of any fact stated therein if it is shown — a) that there is no reasonable ground for believing that the output is inaccurate because of improper use of the computer and that no reason exists to doubt the truth or reliability of the output; or b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the output or the accuracy of its contents.

2) For the purpose of deciding whether or not such output is admissible, the court may draw any reasonable inference from the circumstances in which the output was made or otherwise came into being.

3) The Minister may, with the approval of His Majesty the Sultan and Yang Di-P pertuan, make rules requiring that, in any proceedings where it is desired to give a statement in evidence by virtue of this section, such information concerning the statement shall be provided in such form and at such time as may be so required.

Supplementary provisions on evidence

16. (1) In any proceedings where it is desired to admit output in evidence in accordance with section 15, a certificate —
a) identifying the output and describing the manner in which it was produced;
b) giving such particulars of any device involved in the production of that output as may be appropriate for the purpose of showing that the output was produced by a computer;
c) dealing with any of the matters mentioned in section 15(1); and
d) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer at all relevant times, shall be admitted in those proceedings as evidence of anything stated in the certificate.

2) If the person referred to in subsection (1)(d) who occupies a responsible position in relation to the operation of the computer did not have control or access over any relevant records and facts in relation to the production by the computer of the output, a supplementary certificate signed by another person who had such control or access and made in accordance with subsections (1)(a) to (c) shall be evidence of anything stated in the certificate.

3) For the purposes of subsections (1) and (2), it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

4) Notwithstanding subsections (1) and (2), a court may require oral evidence to be given of anything of which evidence could be given by a certificate under that subsection.

5) Any person who in a certificate tendered in a court under subsections (1) or (2) makes a statement which he knows to be false or does not believe to be true is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 2 years or both.

6) In estimating the weight, if any, of any admissible output, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output and, in particular —
a) to the question whether the information which the output reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and
b) the question whether any person concerned with the supply of information to that computer, or with the operation of that computer or any equipment by means of which the admissible output was produced by it, had any incentive to conceal or misrepresent the facts.

7) For the purposes of subsection (6), information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment.

---

**Proof of document or copy thereof.**

17. Notwithstanding the provisions of the Evidence Act (Chapter 108), where in any proceedings any output is admissible in evidence in accordance with section 15, it may be proved —
a) by the production of that output; or
b) (whether or not that output is still in evidence) by the production of a copy of that output, or the material part of it, authenticated in such manner as the court may approve.

---

**Power of police officer to access computer and data.**

18. (1) A police officer or any person authorised in writing by the Commissioner of Police shall —
a) be entitled at any time to —
i) have access to and inspect and check the operation of any computer to which this section applies;
ii) use or cause to be used any such computer to search any data contained in or available to such computer; or
iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;
b) be entitled to require —
i) the person by who or on whose behalf the police officer or investigation officer has reasonable cause to suspect any computer to which this section applies is or has been used; or
ii) any person having charge of, or otherwise concerned with the operation of, such computer, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or
iii) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

2) This section applies to a computer which a police officer or any person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.
3) The powers referred to in subsections (1)(a)(ii) and (iii) and in subsection (1)(c) shall not be exercised except with the consent of the Public Prosecutor.

4) Any person who obstructs the lawful exercise of the powers under subsection (1)(a) or who fails to comply with a request under subsections (1)(b) or (c) is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both.

5) For the purposes of this section — “decryption information” means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version; “encrypted data” means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; “plain text version” means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

PART VI. Offences and penalties

37. Powers of search and seizure

(1). Any police officer not below the rank of Inspector may, if he has reasonable grounds for believing that a telecommunication system or service has been established, installed, maintained, operated or provided in contravention of this Order or any regulations made thereunder or in breach of any licence granted by the Authority or that any telecommunication equipment used is of a type that is not approved by the Authority under section 9 or that the telecommunication equipment is imported in contravention of any of the provisions of this Order or any regulations made thereunder —

a) in the case of any telecommunication equipment or any telecommunication system or service, other than any radio-communication system or service, enter and inspect any place in which the telecommunication equipment is located or the telecommunication system or service is established, installed, maintained, operated or provided, and may seize any telecommunication system or equipment found therein which appears to be used for or in connection with telecommunications; and

b) in the case of any radio-communication system or service, enter any place in Brunei Darussalam or stop or board any vessel, aircraft or vehicle and inspect any place therein and may seize any radio-communication system or equipment found therein which appears to be used or is capable of being used for or in connection with radio-communications.

2) Where any police officer not below the rank of Inspector has reasonable grounds for believing that an offence has been or is being committed under section 33, 34, 35, 39 or 42, he may seize any telecommunication system or equipment or any radio-communication system or equipment, or any other thing used in the commission of the offence.

3) If there is no prosecution with regard to any equipment or system seized under this section, the equipment or system shall be taken and deemed to be forfeited to the Authority unless a claim is made within 2 months from the date of seizure.

4) Any person asserting that he is the owner of the equipment or system may personally or by his authorised agent give written notice to the Authority that he claims the same.

5) On receipt of this notice, the Authority may direct that the equipment or system be released or may refer the matter to a Magistrate’s Court.

6) The Magistrate’s Court may proceed to the examination of the matter and upon examination shall order that the equipment or system be forfeited or released.

PART VIII Enforcement Powers and Procedures

62. Power to require information etc

(1) The Authority or any officer authorised by the Authority in that behalf may, for the purpose of discharging its functions under this Order, by order —
a) require any person to furnish the Authority with any information in his possession which relates to any tele
communication service or telecommunication system; and
b) require any person who has in his custody or under his control any document which relates to any telecommu
nication service or telecommunication system —
   i) to furnish the Authority with a copy of or extract from the document; or
   ii) unless the document forms part of the records or other documents of a court or public authority, to transmit
       the document itself to the Authority for inspection.
2) The Authority or such duly authorised officer shall be entitled without payment to keep any copy or extract
   furnished to him under subsection (1).
3) The Authority or any officer authorised by the Authority in that behalf shall at all reasonable times in the
day have full and free access to all buildings, places, books, documents and other papers for the purpose of
discharging its functions under this Order, and may, without payment, inspect, copy or make extracts from any
such books, documents or papers.
4) The Authority may take possession of any equipment, books, documents or papers where in its opinion —
   a) the equipment, books documents or papers may be interfered with or destroyed unless possession is taken; or
   b) the equipment, books documents or papers may be required as evidence in proceedings for an offence under
       this Order or any regulations made thereunder.
5) The rights conferred by this section shall, in relation to information recorded otherwise than in legible form
   include the right to require the information to be made available in legible form for inspection or for a copy or
   extract to be made of or from it.
6) Any person who —
   a) fails to comply with any requirement specified in any order under subsection (1);
   b) intentionally alters, suppresses or destroys any document or information which he has been required by any
      order under subsection (1) to furnish or transmit to; or
   c) in furnishing any information required of him under any order under subsection (1), makes any statement
      which he knows to be false in a material particular, or recklessly makes any statement which is false in a ma
      terial particular, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000,
      imprisonment for a term not exceeding 12 months or both and, in the case of a continuing offence, to a further
      fine not exceeding $50 for every day or part thereof during which the offence continues after conviction.
7) No person shall by virtue of this section be obliged to disclose any particulars as to which he is under any
   statutory obligation to observe secrecy.

63. Power of arrest and search in respect of seizable offence

(1) Any police officer may arrest without warrant —
a) any person found committing or attempting to commit or employing or aiding any person to commit a seiz
able offence under this Order, or
b) any person against whom a reasonable suspicion exists that he has been guilty of a seizable offence under
this Order, and may search any person so arrested, except that no female shall be searched except by a female.
2) Every person so arrested shall, together with any article as to which an offence may have been committed or
   attempted to be committed, be taken to a police station.
3) For the purposes of this section, offences punishable under sections 33, 41, 42, 43, 44, 45, 46, 49 and 52 shall
   be deemed to be seizable offences within the meaning of the Criminal Procedure Code (Chapter 7)

64. Powers of search and arrest in respect of offences under sections 33 and 44

(1) Whenever it appears to any police officer that an offence under section 33 or 44 is being committed or is
about to be committed or attempted, or that any article is concealed or deposited or contained in or on any
vessel, aircraft, vehicle or premises in contravention of either of those sections, the police officer may, if he has
reasonable grounds for believing that by reason of the delay in obtaining a search warrant the article is likely to be
removed —
a) stop and examine the vessel, aircraft or vehicle or enter the premises and there search for and take posses
   sion of any article and of any book or document which is reasonably believed to have a bearing on the case; and
b) arrest any person being in the vessel, aircraft, vehicle or premises in whose possession the article may be
   found or whom the police officer may reasonably suspect to have concealed or deposited the article and may
search any person so arrested, except that no female shall be searched except by a female.
2) Every person so arrested shall, together with any such article, be taken to a police station.

**2001 AUTHORITY FOR INFO-COMMUNICATIONS TECHNOLOGY INDUSTRY ORDER**

(Amended in 2003)

### Powers of enforcement.

18. In addition to the powers conferred on him by any written law, an officer or employee of the Authority may, on declaration of his office and production to the person against whom he is acting such identification card as the Chief Executive may direct to be carried by officers or employees of the Authority, in relation to any offence under any such written law –

a) require any person whom he reasonably believes to have committed an offence under any such written law to furnish evidence of the person's identity;

b) require any person, for the purposes of any such written law, to furnish any information or produce any book, document or copy thereof in the possession of that person, and may, without fee or reward, inspect, copy or make extracts from such book or document; and

c) when conducting any investigation under such written law the power to require, by order in writing, the attendance before the officer or employee of any person being within the limits of Brunei Darussalam who from the information given or otherwise appears to be acquainted with the circumstances of the case, and the person so ordered shall attend as so required.

2) A person who-

a) refuses to give access to, or assaults, obstructs, hinders or delays, an officer or employee of the Authority in the discharge of his duties;

b) wilfully mis-states or without lawful excuse refuses to give any information or without lawful excuse refuses to produce any book, document or copy thereof required of him by an officer or employee of the Authority under subsection (1); or

c) fails to comply with a lawful demand of an officer or employee of the Authority in the discharge of his duties, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000, to imprisonment for a term not exceeding 12 months or both.

### Sealing of documents.

12. {1} All deeds, documents and other instruments requiring the seal of the Authority shall be sealed with the common seal of the Authority in the presence of any 2 officers of the Authority duly authorised by the Authority to act in that behalf and shall be signed by those officers and such signing shall be sufficient evidence that the common seal of the Authority has been duly and properly affixed and that the seal is the lawful common seal of the Authority.

2) The Authority may by resolution or otherwise appoint an officer or employee of the Authority or any other agent, either generally or in a particular case, to execute or sign on behalf of the Authority any agreement or other instrument not under seal in relation to any matter coming within the powers of the Authority.
PART I PRELIMINARY PROVISIONS OF ORDER

Objects of Order.

3. The objects of this Order are to facilitate the provision and obtaining by Brunei Darussalam of international assistance in criminal matters, including:
   i) the obtaining of evidence, documents, articles or other things;
   ii) the making of arrangements for persons, including detained persons, to give evidence or assist an investigation;
   iii) the confiscation of property in respect of an offence;
   iv) the service of documents;
   v) the identification and location of persons;
   vi) the execution of requests for search and seizure;
   vii) the provision of originals or certified copies of relevant documents and records, including Government, bank, financial, corporate or business records; and
   viii) any other type of assistance that is not contrary to the laws of Brunei Darussalam.

Application of Order. 4.

(1) This Order applies to any foreign country, subject to -
   a) any mutual assistance treaty between that country and Brunei Darussalam; and
   b) any multilateral mutual assistance treaty being a treaty to which that country and Brunei Darussalam are parties.
   2) This Order does not prevent the provision or obtaining of international assistance in criminal matters to or from the International Criminal Police (Interpol) or any other international organisation.
   3) This Order does not prevent the provision or obtaining of international assistance in a criminal matter to or from any foreign country other than assistance of a kind that may be provided or obtained under this Order.

PART II
REQUESTS BY BRUNEI DARUSSALAM
PRELIMINARY PROVISIONS OF PART

Application of Part.

6. A request for assistance pursuant to this Part may be made to any foreign country.

Requests to be made by Attorney General.

7. Requests by Brunei Darussalam for assistance under this Part shall be made by the Attorney General.
Requests for taking of article, thing or evidence.

8. (1) The Attorney General may request a foreign country to arrange for:
   a) any article, thing or evidence to be taken in that foreign country; and
   b) that article, thing or evidence to be sent to him.
(2) The Attorney General may request a foreign country:
   a) to assist in obtaining, by search and seizure if necessary, any article or thing in that foreign country or a photograph or copy thereof; and
   b) to arrange for that article, thing, photograph or copy thereof to be sent to him.

Immunities and privileges.

14. (1) Subject to subsection (3), where a person is in Brunei Darussalam pursuant to a request made under section 10, he shall not -
   a) be detained, prosecuted or punished in Brunei Darussalam for any offence that is alleged to have been committed, or that was committed, before his departure from the foreign country pursuant to that request;
   b) be subject to any civil proceedings in Brunei Darussalam for any act or omission that is alleged to have occurred, or that did occur, before his departure from that country pursuant to the request, being civil proceedings to which he could not be subject if he were not in Brunei Darussalam;
   c) be required to give or provide evidence or assistance in relation to any criminal matter in Brunei Darussalam, other than the criminal matter to which the request relates;
   d) be required, in the proceedings or investigation to which the request relates, to answer any question that he would not be required to answer if those proceedings or that investigation were taking place in that foreign country; and
   e) be required, in such proceedings or investigation, to produce any document, article or thing that he would not be required to produce if those proceedings or that investigation were taking place in that foreign country.
2) Subsection (1) does not apply in relation to any person where:
   a) he has left Brunei Darussalam and has subsequently returned otherwise than pursuant to the same or another such request; or
   b) he has had the opportunity to leave Brunei Darussalam and has remained in Brunei Darussalam otherwise than for -
   i) the purpose to which the request relates;
   ii) the purpose of giving evidence in any criminal proceedings in Brunei Darussalam declared by the Attorney General in writing to be proceedings in which it is desirable that he gives evidence; or
   iii) the purpose of providing assistance in relation to an investigation in Brunei Darussalam declared by the Attorney General in writing to be an investigation in relation to which it is desirable that he gives assistance.
3) A declaration in writing by the Attorney General under sub-paragraph (ii) or (iii) of paragraph (b) of subsection (2) has effect from the date specified in the declaration (which may be a day earlier than the day on which that declaration is signed).

Limitation on use of evidence.

15. Where -
   a) a person is in Brunei Darussalam pursuant to a request made under section 10; and
   b) he has given evidence in any criminal proceedings, being -
   i) the criminal proceedings to which the request relates or any criminal proceedings consequent on the investigation to which the request relates; or
   ii) criminal proceedings declared by the Attorney General pursuant to sub-paragraph (ii) of paragraph (b) of subsection (2) of section 14 in relation to that person, that evidence shall be inadmissible and not otherwise used in any prosecution of the person for any offence against the law of Brunei Darussalam, except on the prosecution of that person for the offence of perjury or contempt of court in relation to the giving of that evidence, unless the foreign country concerned has consented to it being so used.
ENFORCEMENT OF CONFISCATION ETC.

Request for enforcement of orders. 16.

(1) The Attorney General may request a foreign country to make arrangements for the enforcement of a confiscation order, a charging order or a restraint order where there are grounds for believing that some or all of the property in respect of which any such order is made is located in that country. (2) In this section, a confiscation order, charging order or restraint order means respectively a confiscation order, restraint order or charging order made by a court in Brunei Darussalam under the Drug Trafficking (Recovery of Proceeds) Act (Chapter 1781, the Criminal Conduct (Recovery of Proceeds) Order, 2000 (S 52100) or any other similar written law.

SERVICE OF PROCESS

Assistance in service of process.

17. The Attorney General may request a foreign country to assist in effecting service of any process where the Attorney General is satisfied that, for the purposes of or in connection with any criminal matter in Brunei Darussalam, it is necessary or desirable to serve that process on any person in that country.

MISCELLANEOUS

Restriction on use of evidence.

19. Any evidence, information, document, article or thing that is obtained, provided or produced pursuant to a request made under this Part shall be used by Brunei Darussalam only for the purposes of or in connection with the criminal matter to which that request relates, unless -

a) the foreign country to which the request was made; and

b) in the case of any evidence, information, document, article or thing obtained from, or provided or produced by a person while he is in Brunei Darussalam pursuant to a request made under section 10, that person, consents to the use of that evidence, information, document, article or thing for any other purpose.

PART III
REQUESTS TO BRUNEI DARUSSALAM
PRELIMINARY PROVISIONS OF PART

Application of this Part. 20.

Assistance under this Part may be provided to any foreign country.

Requests to be made to Attorney General. 21.

(1) Every request by a foreign country for assistance in a criminal matter pursuant to this Part shall be made to the Attorney General. (2) If a foreign country makes a request to a court in Brunei Darussalam for assistance in a criminal matter - (a) that court must refer that request to the Attorney General; and (b) that request is then deemed, for the purposes of this Order, to have been made to the Attorney General.
Requests for assistance 22.

(1) If a foreign country requests assistance under this Part, the Attorney General shall consider the following matters in order to decide whether that request should be dealt with - (a) if there is in force a treaty, memorandum of understanding or other agreement between Brunei Darussalam and that country under which that country has agreed to provide assistance in criminal matters in Brunei Darussalam; (b) if the request is made in accordance with a convention to which Brunei Darussalam and that country are parties which provides for the convention to be used as a basis of providing assistance in criminal matters; (c) if paragraphs (a) and (b) are not applicable - (i) any assurances given by that country that it will entertain a similar request by Brunei Darussalam for assistance in criminal matters; (ii) the seriousness of the offence to which the request relates; (iii) the objects of this Order as specified in section 3; and (iv) any other matters that the Attorney General considers relevant. (2) If, after considering those matters, the Attorney General decides that the request should be dealt with under this Part, he may deal with that request accordingly.

Form of request. 23.

Every request by a foreign country for assistance under this Part shall - (a) be made in writing or by any other means capable of producing a written record, in the English language; (b) be made orally only in urgent circumstances but shall subsequently be confirmed in writing in the English language; (c) specify the purpose of the request and the nature of the assistance being sought; (d) identify the person who initiated the request; and (e) be accompanied by - (i) a statement from that country that the request is made in respect of a criminal matter; (ii) a description of the nature of that criminal matter and a statement setting out a summary of the relevant facts and law; (iii) where the request relates to - (A) the location of a person who is suspected to be involved in or has benefited from the commission of an offence; or (B) the tracing of property that is connected with a criminal matter, the name, identity, nationality, location or description of that person, or the location and description of the property, if known, and a statement setting out the basis for suspecting the matter referred to in sub-paragraph (A) or (B); (iv) a description of the offence to which the criminal matter relates, including its maximum penalty; (v) details of the procedure that that country wishes to be followed by Brunei Darussalam in giving effect to the request, including details of the manner and form in which any information, article or thing is to be supplied to that country pursuant to that request; (vi) a statement setting out the wishes of that country concerning the confidentiality of the request and the reason for those wishes; (vii) details of the period within which that country wishes the request to be met; (viii) if the request involves a person travelling from Brunei Darussalam to that country, details of allowances to which the person will be entitled, and of the arrangements his accommodation while he is in that country pursuant to that request; (ix) any other information required to be forwarded with the request under any treaty, memorandum of understanding or other agreement between Brunei Darussalam and that country; and (x) any other information that may assist in giving effect to the request or which is required under the provisions of this Order.

Refusal of assistance.

24. (1) A request by a foreign country for assistance under this Part shall be refused if, in the opinion of the Attorney General – (...) (h) in the case of a request for assistance in obtaining evidence and in search and seizure, that country has failed to undertake to return to the Attorney General, upon his request, anything obtained pursuant to that request upon completion of the criminal matter in respect of which the request was made; (...)
27. (1) Where, on receipt of a request made under section 26 by a foreign country, the Attorney General is satisfied that -
   a) the request relates to a criminal matter in that country; and
   b) there are reasonable grounds for believing that the evidence can be taken or, as the case may be, the documents, articles or other things can be produced in Brunei Darussalam, he may in writing authorise a Magistrate to take the evidence before transmitting it to that country.

2) Upon receipt of an authorisation under subsection (1), the Magistrate shall -
   a) take the evidence of each witness appearing before him;
   b) cause such evidence to be reduced in writing and certify at the end of that writing that the evidence was taken by him; and
   c) cause the writing, so certified, to be sent to the Attorney General.

3) The proceedings may be conducted in the presence or absence of the person to whom the criminal matter in the foreign country relates or of his legal representative (if any).

4) If the foreign country has so requested, the Magistrate conducting proceedings under subsection (2) may permit -
   a) any person to whom the proceedings in that country relates or that person’s legal representative; or
   b) the legal representative of the relevant person of that country, to examine or cross-examine, including through a live television link, from that country, any person giving evidence or producing a document, article or other thing at those proceedings.

5) The certificate referred to in subsection (2) shall state whether the person to whom the criminal matter in the foreign country relates or his legal representative (if any) was present at the proceedings.

6) The law with respect to the compelling of persons to attend before a Magistrate, and to give evidence, answer questions and produce documents, upon the hearing of a charge against any person for an offence against the law of Brunei Darussalam shall apply, so far as they are capable of application, with respect to the compelling of persons to attend before a Magistrate, and to give evidence, answer questions and produce documents, for the purposes of this section:
   Provided that the Magistrate conducting proceedings under subsection (2) shall record any objection as to whether any evidence should be taken under the laws of that foreign country, but shall not rule on the matter.

7) For the purpose of this section, the person to whom a criminal matter in a foreign country relates is competent but not compellable to give evidence.

8) Evidence taken under this section shall not be admissible in evidence or otherwise used, for the purposes of any judicial proceedings, disciplinary proceedings or other proceedings in Brunei Darussalam, except in the prosecution of the person who gave that evidence for the offence of perjury or contempt of court in relation to the giving of that evidence.

30. Notwithstanding section 29 or any other written law, if the documents, articles or other things are in the possession of a financial institution, the Attorney General may in writing order that that financial institution provide an authorised officer within such period and in such form and manner as may be specified in the order, the information, documents, articles or other things, including those relevant to any one or more of the following -
   a) whether an account is held by a specified person with that financial institution;
   b) whether a particular person is a signatory to an account;
   c) whether any person holds an account with that financial institution, and the current balance of that account;
   d) details of transactions on such an account over a specified period;
   e) details of any related accounts (including the names of those who hold those accounts);
   f) any transaction conducted by the financial institution on behalf of a specified person.

31. (1) Where a court orders any person under section 29 to give an authorised officer access to any document, article or other thing on any premises, it may, on the same or a subsequent application of an authorised officer, order any person who appears to the court to be entitled to grant entry to the premises, to allow an authorised officer to enter those premises to obtain access to that document, article or other thing.

2) Where any material to which an order under section 29 relates consists of information contained in or acces-
sible by means of any data equipment -
a) an order under section 29 shall have effect as an order to produce the material in a form which can be taken away and which is visible and legible; and
b) an order under section 29 shall have effect as an order to give access to the material in a form which is visible and legible.

3) A person is not excused from producing or making available any document, article or other thing by an order under section 29 only on the ground that-
a) the production or making available of that document, article or other thing will incriminate him or make him liable to any penalty; or
b) the production or making available of the document, article or other thing would be in breach of an obligation (whether imposed by law or otherwise) on him not to disclose the existence of the contents of that document, article or other thing.

4) An order under section 29 shall have effect notwithstanding any obligation as to secrecy or other restriction upon the disclosure of information imposed by any written law or otherwise.

5) An authorised officer may photograph or make copies of any document, article or other thing produced or to which access is granted pursuant to an order made under section 29.

6) Where an authorised officer takes possession of any document, article or other thing under an order made under section 29, takes any photograph or makes any copy of that document, article or other thing under subsection (5), he may retain that document, article or other thing, photograph or copy for a period not exceeding one month pending a written direction from the Attorney General as to the manner in which it is to be dealt with (which may include a direction that the document, article, thing, photograph or copy be sent to the appropriate authority of the foreign country concerned).

7) Rules of Court made under section 57 may provide for-
a) the discharge and variation of an order under section 29; and
b) proceedings relating to such an order.

8) In this section, “data equipment” means any equipment which-
a) automatically processes information;
b) automatically records or stores information;
c) can be used to cause information to be automatically recorded, stored or otherwise processed on other equipment (wherever situated);
d) can be used to retrieve information whether information is recorded or stored in the equipment itself or in other equipment (wherever situated).

ASSISTANCE IN OBTAINING ATTENDANCE OF PERSONS IN FOREIGN COUNTRY

Assistance in arranging attendance of person to give or provide evidence or assistance in relation to criminal matter in foreign country. 35.

(1) A foreign country may request the Attorney General to assist in arranging the attendance in that country of a person in Brunei Darussalam (not being a person to whom section 36 applies) for the purposes of giving or providing evidence or assistance in relation to a criminal matter in that country. (2) Where, on receipt of a request made under subsection (1), the Attorney General is satisfied that - (a) the request relates to a criminal matter in that country; (b) there are reasonable grounds for believing that the person concerned could give or provide evidence or assistance relevant to that criminal matter; (c) the person concerned has freely consented to attend as requested; and (d) the country concerned has given adequate undertakings in respect of the matters specified in paragraphs (a), (b), (c) and (e) of section 37, he may in writing authorise assistance in accordance with this section, and may assist in the making of arrangements to facilitate that attendance.

Assistance in arranging attendance of a prisoner in foreign country for specified purposes. 36.

(1) A foreign country may request the Attorney General to assist in arranging the attendance in that country for either or both of the purposes specified in subsection (2), of a person in Brunei Darussalam who is a prisoner. (2) The purposes referred to in subsection (1) are - (a) for giving evidence in relation to any criminal proceedings in that country; (b) for assistance in relation to a criminal matter in respect of an offence in that country. (3) The Attorney General may in writing authorise assistance in accordance with this section if, on receipt of a request
made under subsection (l), he is satisfied that –
a) the request relates to the attendance of the person concerned in connection with a criminal matter in that
country; (b) there are reasonable grounds for believing that the person concerned could give or provide evi-
dence or assistance relevant to that criminal matter; (c) the person concerned has freely consented to attend
as requested; (d) the foreign country has given an adequate undertaking in respect of the matters specified in
section 37. (4) Where assistance is authorised in accordance with subsection (3), the Attorney General may direct
that the prisoner be released from the prison in which he is detained for the purpose of travelling to that foreign
country to give evidence at the hearing, and may make arrangements for the prisoner to travel to that country
in the custody of a police officer or of a prison officer as defined in section 2 of the Prisons Act (Chapter 51). (5)
A direction given pursuant to subsection (4) by the Attorney General in respect of a prisoner shall be sufficient
authority for the release of the prisoner from the prison for the purposes of the direction. (6) Where a person
has been transferred to a foreign country in accordance with subsection (3), he shall be deemed or continue to
be in legal custody when, being in Brunei Darussalam or on board a Brunei Darussalam aircraft or hovercraft or
a Brunei Darussalam ship, he is being taken to or from any place or being kept in custody under the direction
made by the Attorney General under subsection (4). (7) A person authorised by or for the purposes of any such
direction to take the prisoner to or from any place or to keep him in custody shall have all the powers, author-
ity, protection and privileges of a police officer in Brunei Darussalam. (8) If the prisoner escapes or is unlawfully
at large, he may be arrested without warrant by a police officer and taken to any place directed by the Attorney
General. (9) This section applies to a person in custody awaiting trial or sentence and a person committed to
prison for default in paying fines as it applies to a prisoner.

ASSISTANCE IN SEARCH AND SEIZURE

Request for search and seizure. 42.

(1) A foreign country may request the Attorney General to assist in obtaining any article or thing by search or
seizure. (2) Where, on receipt of a request made under subsection (l), the Attorney General is satisfied that - (a)
the request relates to a criminal matter in that country; and (b) there are reasonable grounds for believing that
the article or thing to which the request relates is relevant to the criminal matter and is located in Brunei Da-
russalam, the Attorney General, or an authorised officer directed by him, may apply to the court for a warrant
referred to in section 43 in respect of specified premises.

Search warrants. 43.

(1) On an application referred to in section 42, the court may issue a warrant authorising an authorised officer to
enter and search the specified premises if the court is satisfied that - (a) an order made under section 29 in rela-
tion to anything on the premises has not been complied with; or (b) it is necessary or desirable for the purposes
of the foreign criminal matter to which the application relates. (2) A warrant issued under this section shall be
subject to such conditions as the court may specify.

Additional powers of person executing search warrant. 44.

(1) Where an authorised officer has entered premises in the execution of a warrant issued under section 43, he
may seize and retain any article or thing that is specified in the warrant.
2) An authorised officer may photograph or make a copy of any article or thing seized under subsection ( 1). (3)
Where an authorised officer seizes a photograph or makes a copy of any article or thing under a warrant, he
may retain that article, thing, photograph or copy for a period not exceeding one month pending a direction in
writing from the Attorney General as to the manner in which it is to be dealt with (which may include a direc-
tion that the article, thing, photograph or copy be sent to the foreign country concerned.). (4) Any person who
hinders or obstructs an authorised officer in the execution of a warrant issued under section 43 is guilty of an
offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 2 years
or both.
PART IV MISCELLANEOUS PROVISIONS

Authentication of documents etc. 52.

(1) Subject to the law relating to the admissibility of evidence, any document or record that is obtained, provided or produced pursuant to a request made under this Order which is duly authenticated is admissible in evidence in any criminal proceedings. (2) A document or record duly authenticated for the purposes of subsection (1) if it purports to be signed or certified by a Judge, Magistrate or other judicial officer in or of that foreign country. (3) For the purposes of subsection (2), a document or record is deemed to be duly authenticated if an electronic signature (as defined in subsection (3) of section 54) is used. (4) Nothing in this section prevents the proof of any matter, or the admission in evidence of any document, in accordance with any other provision of this Order or of any other written law.

Legal recognition of electronic document or record. 53.

It is hereby declared for the purposes of this Order that any document or record shall not be denied legal effect, validity or enforceability solely on the ground that it is in electronic form.

Legal recognition of electronic signature. 54.

(1) For the avoidance of doubt, in respect of any provision in this Order that requires a signature or provides for certain consequences if a document or record is not signed, an electronic signature satisfies that requirement. 2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record or document is that of such party. 3) In this section, «electronic signature» means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving that record.

2006 EVIDENCE ACT

PART I RELEVANCY OF FACTS

Chapter I

Preliminary

Interpretation.

3. In this Act, unless there is something repugnant in the subject or context —
1) by deleting the definition of “document” and by substituting the following new definition therefor - "document" means any matter expressed, described or howsoever represented upon any substance, material, thing or article, including any matter embodied in a disc, tape, film, soundtrack or other device whatsoever, by means of -
   a) letters, figures, marks, symbols, signals or other forms of expression, description or representation whatsoever;
   b) any visual recording (whether of still or moving images);
   c) any sound recording or any electronic, magnetic, mechanical or other recording, whatsoever and howsoever made, or any sound, electronic impulse or other data whatsoever;
   d) a recording or transmission of the means mentioned in paragraph (a), (b) or (c), or by more than one of the
means mentioned in paragraph (a), (b), (c) or (d), intended to be used or which may be used for the purpose of expressing, describing or howsoever representing that matter; 

Illustrations (...)

A writing is a document. 
Words printed, lithographed or photographed are documents. 
A map, plan, graph or sketch is a document. 
An inscription on wood, metal, stone or any other substance, material or thing is a document. A photograph or a negative is a document. 
A tape recording of a telephonic communication, including a recording of such communication transmitted over distance is a document. 
A photographic or other visual recording, including a recording of photographic or other visual transmission over a distance is a document. 
A matter recorded, stored, processed, retrieved or produced by a computer is a document."

“evidence” includes —
a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence; 
b) all documents produced for the inspection of the court: such documents are called documentary evidence. 
“film” includes a microfilm and any negative; 
“microfilm” means any transparent material bearing a visual image in reduced size either singly or as a series, and includes microfiche; 
“negative” means a transparent negative photograph on any substance or material, and includes any transparent negative photograph made from the original negative photograph. 
A fact is said to be “proved” when, after considering the matters before it, the court either believes it to exist or considers its existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it exists. A fact is said to be “disproved” when, after considering the matters before it, the court either believes that it does not exist or considers its non-existence so probable that a prudent man ought, under the circumstances of the particular case, to act upon the supposition that it does not exist. A fact is said to be “not proved” when it is neither proved nor disproved

«Certificate in criminal proceedings in respect of foreign documents.

78A. (1) Any document purporting to be signed by the Attorney General certifying that any foreign document attached thereto has been received by him in connection with any criminal proceedings shall be admitted in evidence in those proceedings together with the document attached thereto on production, without further proof, as prima facie evidence of the facts contained in such documents. 
2) In this section, “foreign document” means a document purporting to be-
a) a true copy or extract from-
 i) any record, book or document of a public nature kept or maintained in any place outside Brunei Darussalam; or
 ii) any document filed in or issued out of an office kept or maintained in any place outside Brunei Darussalam for the purpose (whether the sole purpose or not) of registering companies or business names or the ownership of property; and
 b) signed and certified as a true copy of or extract from any such record, book or document by a person having custody or control thereof. 
3) In relation to a document tendered in evidence under this section and purporting to be signed and certified as a true copy of or extract from any record, book or document by a person having custody or control thereof, it shall be presumed, unless the contrary is proved, that such record, book or document is –
a) a record, book or document of a public nature kept or maintained in a place outside Brunei Darussalam; or 
b) a document filed in or issued out of an office kept or maintained in a place outside Brunei Darussalam for the purpose of registering companies or business names or the ownership of property, if there is endorsed on the document a statement purporting to be signed by that person to that effect. 
4) Unless the court otherwise orders, a document shall not be admitted in evidence under this section unless 14 days notice in writing of the intention to tender such document in evidence, together with a copy thereof and of the certificate under subsection (1) of the Attorney General in respect thereof, has been served-
a) where the document is tendered by the prosecution, on the defendant (or, if more than one, on each defendant) or his counsel;
b) where the document is tendered by a defendant, on the Public Prosecutor, but nothing in this subsection shall affect the admissibility of a document in respect of which notice has not been served in accordance with the requirements of this subsection if no person entitled to be so served objects to its being so admitted.”
123. Notwithstanding any other law on the contrary, no one shall be permitted to produce any unpublished official records relating to affairs of State or any document in the possession of a Ministry or of a department of Government, or to give any evidence derived therefrom, except with the permission of the Permanent Secretary of the Ministry or the head of the department concerned, who shall give or withhold such permission as he thinks fit, subject however to the control of the Minister concerned, and no court shall order the production of any such record or document until such permission has been obtained.”

**ANTI-TERRORISM (FINANCIAL AND OTHER MEASURES) (REVISED EDITION 2008)**

**8. Duty to provide information.**

Any person who in Brunei Darussalam, and any citizen of Brunei Darussalam and any company incorporated or registered under the Companies Act (Chapter 39) who or which outside Brunei Darussalam, has —

a) possession, custody or control of any property belonging to any terrorist or any person owned or controlled by any terrorist; or

b) information about any transaction or proposed transaction in respect of any property belonging to any terrorist or any person owned or controlled by any terrorist, shall immediately inform the Commissioner of Police and any such other person as the Minister may designate of that fact or information and provide such further information relating to the property, transaction or proposed transaction as the Commissioner of Police or such designated person may require.

**9. Immunity from proceedings.**

No action, suit or other legal proceedings shall lie against any —

a) party to a contract for failing, neglecting or refusing to carry out any act required by that contract; or

b) person for failing, neglecting or refusing to carry out any act under any written law, where such failure, neglect or refusal is solely attributable to, or occasioned by, the provisions of this Act or any regulations made thereunder.

Protection of persons for acts done under Act. 10. No person shall be liable in respect of any act done by him in the execution or purported execution of this Act or any regulations made thereunder if he did it in the honest belief that his duty under this Act or any regulations made thereunder required or entitled him to do it.

**2011 ANTI-TERRORISM ORDER**

**Power to search.**

23. (1) Any police officer may without warrant stop and search any vehicle, vessel, aircraft or individual, whether in a public place or not, if he suspects that any article or material being evidence of the commission of an offence against this Order is likely to be found in such vehicle, vessel or aircraft or on such individual, and may seize any article or material so found.

2) Any police officer of or above the rank of corporal may without warrant enter and search any premises or place if he suspects that any article or material being evidence of the commission of any offence against this Order is likely to be found on such premises or place and may seize any article or material so found.
Inspection of banker's books.

24. (1) The Public Prosecutor may, if he is satisfied that any evidence of the commission of an offence against this Order is likely to be found in any banker's book, by order authorise any police officer to inspect any such book, and a police officer so authorised may, at all reasonable times, enter the bank specified in the order and inspect the banker's book kept therein, and may take copies of any entry in any such book.

2) In this section, “banker’s books” include ledgers, day books, cash books, account books and all other books used in the ordinary business of a bank, whether these records are in written form or are kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval system.

Power to intercept communications.

25. (1) Notwithstanding the provisions of any other written law, the Public Prosecutor, if he considers that it is likely to contain any information which is relevant for the purpose of any investigation into an offence under this Order, may, on the application of an officer of or above the rank of Superintendent of Police, authorise any police officer –

a) to intercept, detain and open any postal article in the course of transmission by post;

b) to intercept any message transmitted or received by any telecommunication; or

c) to intercept, listen to and record any conversation by any telecommunication, and listen to the recording of the intercepted conversation.

2) When any person is charged with an offence under this Order, any information obtained by a police officer under subsection (1), whether before or after such person is charged, shall be admissible at his trial in evidence.

3) An authorisation by the Public Prosecutor under subsection (1) may be given either orally or in writing; but if an oral authorisation is given, the Public Prosecutor shall, as soon as practicable, reduce the authorisation into writing.

4) A certificate by the Public Prosecutor stating that the action taken by the police officer under subsection (1) had been authorised by him under that subsection shall be conclusive evidence that it had been so authorised, and such certificate shall be admissible in evidence without proof of signature thereof.

5) No person shall be under any duty, obligation or liability, or be in any manner compelled, to disclose in any proceedings the procedure, method, manner or means, or any matter related thereto, of anything done under subsection (1)(a), (b) or (c).

6) In this section -

postal article” has the same meaning as in the Post Office Act (Chapter 52);

Public Prosecutor” means the Public Prosecutor personally; “telecommunication” has the same meaning as in the Telecommunications Order, 2001 (S 38/2001).

Application by interested person to revoke or vary warrant or order.

35. (1) Any person who has an interest in the property that was seized under a warrant issued under section 27(1)(a) or in respect of which a restraint order was issued under section 27(1)(b) may, at any time, apply to a Judge –

a) for an order under subsection (4); or

b) for permission to examine the property.

2) Where an application is made under subsection (1)(a) -

a) the application shall not, without the consent of the Attorney General, be heard by a Judge unless the applicant has given to the Attorney General at least 2 clear days notice in writing of the application; and

b) the Judge may require notice of the application to be given to and may hear any person who, in the opinion of the Judge, appears to have a valid interest in the property.

3) The Judge may, on an application made to him under subsection (1)(b), order that the applicant be permitted to examine the property subject to such conditions as appear to the Judge to be necessary or desirable to ensure that the property is safeguarded and preserved for any purpose for which it may subsequently be required.

4) On an application made under subsection (1)(a) in respect of any property and after hearing the applicant and the Attorney General and any other that a warrant should not have been issued under section 27(1)(a) or a restraint order should not have been issued under section 27(1)(b) in respect of the property; or (b) in any other case, that the applicant is the lawful owner of or lawfully entitled to possession of the property and appears innocent of any complicity in any terrorism financing offence or of any collusion in relation to such an offence, and that no other person appears to be the lawful owner of or lawfully entitled to possession of the property, and
that the property will no longer be required for the purpose of any investigation or as evidence in any proceed-
ing.

### Expiration of warrants and restraint orders.

36. (1) Subject to this section, where property has been seized under a warrant issued under section 27(1)(a) or
is the subject of a restraint order issued under section 27(l)(b), the property may be detained or the order may
continue in force, as the case may be, for a period not exceeding one year from the seizure or the issuance of
the order, as the case may be.
2) The property may continue to be detained, or the order may continue in force, for a period exceeding one
year if proceedings are instituted in respect of which the property detained may be forfeited.
3) The property may continue to be detained or the order may continue in force for a period or periods exceed-
ing one year if the continuation is, on application made by the Attorney General, ordered by a Judge, where the
Judge is satisfied that the property is required, after the expiration of the period or periods, for the purpose of
this Order or any other written law respecting forfeiture or for the purpose of any investigation or as evidence in
any proceedings.

### Sharing of information with foreign counterpart agencies.

54. (1) The Financial Intelligence Unit may share information with any foreign counterpart agency that performs
similar functions based upon reciprocity or mutual agreement on the basis of cooperation arrangements en-
tered into between the Financial Intelligence Unit and such foreign counterpart agency.
2) The Financial Intelligence Unit may make inquiries on behalf of a foreign counterpart agency where the
inquiry may be relevant to the foreign counterpart agency's analysis of a matter involving suspected terrorist
property or potential financing of terrorism.
3) Without prejudice to the generality of subsection (2), the Financial Intelligence Unit may -
a) search its own databases, including information related to reports of suspicious transactions, and other data-
bases to which the Financial Intelligence Unit had direct or indirect access, including law enforcement databases,
public databases, administrative databases and commercially available databases;
b) obtain from financial institutions and designated non-financial businesses and professions that is relevant in
connection with such request;
c) obtain from competent authorities' information that is relevant in connection with such request to the extent
the Financial Intelligence Unit could obtain such information in a domestic matter; and
d) take any other action in support of the request of the foreign counterpart agency that is consistent with the
authority of the Financial Intelligence Unit in a domestic matter.

### BROADCASTING ACT (CHAPTER 180) BROADCASTING
(CLASS LICENCE) NOTIFICATION, 2001

**Interpretation. 2.**

For the purposes of this Notification
Internet Content Provider» means (a) any individual in Brunei Darussalam who provides any programme, for
business, political or religious purposes, on the World Wide Web through the Internet; or (b) any corporation or
group of individuals (including any association, business, club, company, society, organisation or partnership,
whether registrable or incorporated under the laws of Brunei Darussalam or not) who provides any programme
on the World Wide Web through the Internet, and includes any web publisher and any web server administrator;
Internet Service Provider» means any of the following persons - (a) an Internet Access Service Provider licensed
under section 3 of the Telecommunications Act (Chapter 54); (b) a Localised Internet Service Reseller; or (c) a
Non-localised Internet Service Reseller;
Localised Internet Service Reseller» means a person - (a) who obtains Internet access from an Internet Access
Service Provider or from a Non-localised Internet Service Reseller; and (b) who provides Internet services ob-
tained from the Internet Access Service Provider, or the Non-localised Internet Service Reseller, to all or part
of the public; and (c) whose Internet services are available for reception only within a single building, dwelling-
house, hospital, educational institution, residential, commercial or industrial complex, or any other single tem-
porary or permanent structure, but does not include a person who provides Internet services to that person’s
own employees for use solely within that person’s firm or corporation;
Non-localised Internet Service Reseller» means a person who - (a} obtains Internet access from an Internet Ac-
cess Service Provider; and (b) provides Internet services obtained from the Internet Access Service Provider to all
or part of the public by leased telecommunication lines, integrated services digital networks, modems or by any
other wired or wireless means, but does not include a person who provides Internet services to that person’s
own employees for use solely within that person’s firm or corporation;
«VAN computer on-line service» means a computer on-line service that is licensed as a Value Added Network
service under section 3 of the Telecommunications Act (Chapter 54).
SECTION 2 - The Rules of Evidence

Article 321. Evaluation of Evidence by the Court

Unless otherwise required by a law, any evidence in criminal cases is freely admissible. The court shall have a free choice to determine the value of the evidence submitted to the court on the ground of its true belief. The decision of the court shall be based only on the evidence which it has in the file or which has been presented at the hearing. A confession shall be submitted to the court for consideration in the same manner as other evidence. Answers given under the physical or mental duress shall have no evidentiary value. Communications between the accused person and his/her lawyers is not admissible as evidence.

CHAPTER 5 - Rules of Investigation on Flagrant Offenses

Article 105. Prohibition to non-Permitted Listening Primarily:

Judicial police officers shall have no authority to allow the listening to or record any telephone conversations. Judicial Police Officers shall have no authority to allow the interception or record any correspondences by telecommunications, such as facsimiles or internet messages.

SECTION 7 – Listening to telephone Conversation

Art. 172. Listening to Telephone Conversation

Article 172. Listening to Telephone Conversation Ordered by an Investigating Judge When it is necessary to reveal the truth, an investigating judge can issue an order authorizing the listening to and recording telephone conversations. The investigating judge can also order the intercept and record of all telecommunications, such as messages through facsimile or Internet. The investigating judge can request every qualified public institution or specialist civil servant to install technical instruments and make recordings. The investigating judge shall indicate in his/her order the type of communications that are authorized to be monitored and the duration of the mission. The appointed public institutions or civil servants shall perform their duties according to the order of the investigating judge. During the mission, the appointed public institutions or civil servants shall report to the investigating judge on the progress of the mission, particularly concerning the eventual difficulties. When the mission is completed, the public institutions or civil servants shall transcribe all recorded voices into written transcripts. The transcriptions shall accurately reflect the substance of the recorded communication. The recorded voice shall be given to the investigating judge and sealed. The investigating judge can have access to the place where the interception or recording is being carried out at any time. The investigating judge may not be prohibited from accessing the place for any reasons, even the place is a military location. An investigating judge can authorize this assignment by way of a rogatory commission.

Article 183. Listening to telephone conversation primarily under Rogatory Commission

When a rogatory commission allows the listening or recording telephone conversations or monitoring and recording conversations through means of telecommunications such as facsimiles or internet messages, the
judicial police officer shall apply the authorities provided to the investigating judge by the second phrase of the paragraph 1, and paragraph 2 of Article 172 (Listening to Telephone Conversations Ordered by an Investigating Judge) of this Code.

2007 LAW ON COUNTER TERRORISM

Article 3 Definitions

(...) 4. property means:
   a) assets and economic resources of every kind, whether tangible or intangible, movable or immovable, however acquired; and
   b) legal documents and instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including bank credits, travellers cheques, money orders, shares, securities, bonds, drafts and letters of credit.

Chapter 12. Part 3 Mutual assistance

Article 103 - Requests of a foreign State to Cambodia for assistance in investigations or court proceedings in a foreign State
1) This article applies if the Royal Government of Cambodia receives a request from a foreign State for assistance in relation to:
a) an investigation into an offence under a law of that State that corresponds to an offence under this Law; or
b) court proceedings for such an offence; or
c) investigations relating to tainted property; or
d) proceedings for the freezing or forfeiture of tainted property in the requesting State; or
e) the freezing or forfeiture of tainted property in the Kingdom of Cambodia.
2) The Royal Government of Cambodia, through the courts or other relevant competent authorities, may provide assistance in any of the following ways:
a) taking statements or evidence in written or oral form from persons;
b) assisting in making persons including persons held in detention available, with their consent, to give evidence or to assist in investigations;
c) serving judicial documents;
d) executing searches;
e) assisting in tracing tainted property;
f) investigating financial dealings;
g) obtaining information or evidence which may assist in the recovery of tainted property for forfeiture;
h) freezing of tainted property so as to prevent any dealing in, or transfer or disposal of, the property pending a determination on forfeiture;
i) seizing tainted property, including documents;
j) implementing a final decision of the foreign State to forfeit tainted property;
k) examining objects and sites;
l) providing information and evidentiary items to the foreign State;
m) providing the originals, or certified copies, of relevant documents or records including bank, financial, corporate or business records to the foreign State.
3) Information and evidentiary items that may be provided to the foreign State in accordance with subparagraph (2) (l) include all lawfully obtained material including material obtained by the interception of telecommunications or by the use of listening devices.
4) For the purposes of executing a request for assistance from a foreign State, the procedures and processes in the Kingdom of Cambodia for the investigation or prosecution of an offence against the laws of Cambodia may be used for the provision of assistance to the foreign State.
Article 107 – Requests for giving of evidence at hearings in foreign States

(1) This article applies if:
   a) a proceeding relating to:
      i) an offence under the law of a foreign State that corresponds to an offence under this Law; or
      ii) freezing or forfeiture of tainted property has commenced in a foreign State; and
   b) the foreign State requests the attendance of a person who is in the Kingdom of Cambodia at a hearing in connection with the proceeding; and
   c) there are reasonable grounds to believe that the person is capable of giving evidence relevant to the proceeding; and
   d) the person has consented to giving evidence in the foreign State.

(2) The foreign State must give the following undertakings:
   a) that the person will not:
      i) be detained, prosecuted or punished for any offence against the law of the foreign State that is alleged to have been committed, or that was committed, before the person's departure from the Kingdom of Cambodia; or
      ii) be subjected to any civil suit in respect of any act or omission of the person that is alleged to have occurred, or that occurred, before the person's departure from the Kingdom of Cambodia, if the person could not be subjected to the civil suit if the person were not in the foreign State; or
      iii) be required to give evidence in any proceeding in the foreign State other than the proceeding to which the request relates; unless the person has left the foreign State or the person has had the opportunity of leaving the foreign State and has remained in that State otherwise than for the purpose of giving evidence in the proceeding to which the request relates;
   b) that any evidence given by the person in the proceeding to which the request relates will be inadmissible or otherwise disqualified from use in the prosecution of the person for an offence against a law of the foreign State other than the offence of perjury in relation to the giving of that evidence;
   c) that the person will be returned to Cambodia in accordance with arrangements agreed by the Royal Government of Cambodia;
   d) if the person is being held in custody in Cambodia and the Royal Government of Cambodia requests the foreign State to make arrangements for the keeping of the person in custody:
      i) that the State will make appropriate arrangements for that purpose; and
      ii) that the person will not be released from custody in the foreign State unless the Royal Government of Cambodia notifies an appropriate authority of the foreign State that the person is entitled to be released from custody under Cambodian law; and
      iii) if the person is released in the foreign State as mentioned in subparagraph (ii), that the foreign State will pay the costs of the person's accommodation and expenses until the proceeding to which the request relates is completed.

Article 108 - Request by Cambodia to a foreign State for assistance in investigations or court proceedings

(1) The Royal Government of Cambodia may request a foreign State to provide assistance in relation to:
   a) an investigation into an offence under this Law; or
   b) court proceedings for such an offence; or
   c) investigations relating to tainted property; or
   d) proceedings for the freezing or forfeiture of tainted property in the Kingdom of Cambodia; or
   e) the freezing or forfeiture of tainted property in the requested State.

2) The request may be for assistance in any matter listed in paragraph 2 of article 103 of this Law.

3) Evidence lawfully obtained in the foreign State may be used in evidence in proceedings in the Kingdom of Cambodia.

4) If a person who was being held in custody in the foreign State is made available to give evidence in the Kingdom of Cambodia and the foreign State requests the Royal Government of Cambodia to make arrangements for the keeping of the person in custody while the person is in the Kingdom of Cambodia, the Royal Government of Cambodia:
   a) must make appropriate arrangements for that purpose; and
   b) must not release the person from custody in the Kingdom of Cambodia unless the foreign State notifies an appropriate authority of the Royal Government of Cambodia that the person is entitled to be released from custody under the law of the foreign State; and
   c) must, if the person is released in the Kingdom of Cambodia as mentioned in subparagraph (b), pay the costs
of the person’s accommodation and expenses until the proceeding to which the request relates is completed.
5) A person made available by a foreign State to give evidence in the Kingdom of Cambodia must be returned to
that foreign State, without the need for extradition proceedings, in accordance with arrangements agreed with
that foreign State.

**Article 109 - International Cooperation**

The provisions of Part 3 of this law do not limit or prevent the giving or receiving of information or international
cooperation in relation to an offence under this Law, or a corresponding offence under the law of a foreign
State, by any other means.

---

**2007 LAW ON ANTI-MONEY LAUNDERING AND
COMBATING THE FINANCING OF TERRORISM**

*(updated 27 June 2020)*

**CHAPTER I
GENERAL PROVISIONS**

**Article 1 - Purpose**

The present Law has the purpose to set up measures against money laundering and financing of terrorism as
well as the organization and the control of those measures enforcement.

**Article 2 - Scope of Application**

The present Law and other regulations set forth for it implementation are to be used for the prevention and the
control of money laundering and financing of terrorism.

**Article 3 – Definitions**

For the purposes of the present law, the term:
(a) “Money laundering” shall mean: (i) The conversion or transfer of property, knowing that such property is the
proceeds of offence, for the purpose of concealing or disguising the illicit origin of the property or of helping any
person who is involved in the commission of the offence to evade the legal consequences of his or her action;
(b) (c) “Property” shall mean assets of every kind, whether movable or immovable, tangible or intangible, and
legal documents or instruments evidencing title to, or interest in, such assets.
(c) (f) “Financing of terrorism” shall mean the willful provision of financial or other services with the intention that
such services be used or in the knowledge that they are or may be used, in full or in part, for the purpose of sup-
porting terrorism, terrorist acts or terrorist organizations.
(d) (h) “Financial Intelligence Unit” shall mean a central body responsible for receiving, analyzing and disseminat-
ing reports on suspicious transactions, as defined in Article 3(g) of the present law, cash transactions as defined
in Article 12(1) of the present Law and other information regarding money laundering or financing of terrorism.
CHAPTER III MEASURES TO BE TAKEN BY BANKING AND FINANCIAL INSTITUTIONS AND NON-BANK FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND FINANCING OF TERRORISM

Article 8 – Customer Due Diligence Measures

1. Reporting entities referred in Article 4 of the present Law shall take customer due diligence measures, including the identification of their customers and the verification of their customers’ identity:
   a) prior to establishing business relations, such as opening accounts, taking stocks, bonds or other securities into safe custody, granting safe-deposit facilities or engaging in any other business dealings;
   b) prior to carrying out occasional or one-off transactions, including wire-transfers, that involve a sum in excess of amount as defined by the supervisory authority; identification information accompanying wire transfers shall contain the name and address of the originator, and where an account exists, the number of that account. In the absence of an account, a unique reference number shall be included;
   c) if the reporting entity has a suspicion of money laundering or financing of terrorism irrespective of the sum involved in the transaction;
   d) if the reporting entity has any doubts about the veracity or adequacy of previously obtained customer identification data.

2. The following customer due diligence measures shall be taken by reporting entities:
   a) identifying the customer by obtaining at the minimum name, birth date, and address, for natural persons and name, articles of incorporation or registration, tax identification number, address, telephone number, for legal persons as defined by the supervisory authority and verifying that customer’s identity using reliable, independent source documents, data or information by using a national ID card, a passport or any other official photo ID document. (b) identifying the ultimate beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, the reporting entities should take reasonable measures to understand the ownership and control structure of the customer.
   c) obtaining information on the purpose and intended nature of the business relationship.
   d) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting entities, knowledge of the customer, their business and risk profile including, where necessary, the source of funds.

3. Where the reporting entity is unable to comply with paragraphs 2 (a) to (c) above, it should not open the account, commence business relations or perform the transaction, or in case of existing business relations with the customer, it should terminate such business relations, unless instructed to the contrary by the FIU. In any such cases, the reporting entity should consider making a suspicious transaction report in relation to the customer.

4. The requirements set forth by this Article shall apply to all new customers as well as to existing customers on the basis of materiality and risk. Reporting entities shall conduct due diligence on such existing relationships retrospectively.

Article 10 – Special Monitoring of Certain Transactions

1. A reporting entity shall pay special attention to:
   a) any complex, unusual or large amount transactions;
   b) any unusual patterns of transactions; that have no apparent or visible economic or lawful purpose;
   c) business relations and transactions with institutions or persons in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or financing of terrorism; (d) wire transfers that do not contain complete originator information;
   e) business relations and transactions with persons with whom the reporting entity has had no face-to-face contact during the implementation of identification procedure;
   f) business relations and transactions with politically exposed persons;
   g) business relations and transactions conducted by means of cross-border correspondent banking or other similar relationships.

2. In cases referred to under paragraph 1 of this Article, the reporting entity shall seek additional information
as to the origin and destination of the money, the purpose of the transaction and the identity of the transacting parties.

**Article 11 – Record-keeping by Reporting Entities**

Reporting entities referred to at Article 4 of the present Law shall maintain, at least for 5 years after the account has been closed or the business relations with the customer have ended, and shall hold at the disposal of the competent authorities any records of customer identification and records of transactions conducted by customers in a manner that they are sufficient to permit the reconstruction of individual transactions, including the amounts and types of currency involved if any, so as to provide, if appropriate, evidence for the prosecution of offense.

**Article 13 – Contents of Suspicious Transaction Reports**

The suspicious transaction reports submitted to the FIU shall at a minimum contain:
- a) the identity and identifying particulars of the reporting entity, including the name and contact details of the reporting officer;
- b) the identity and identifying particulars of the customer and of the beneficiary involved in the transaction;
- c) the type and details such as amount, currency, date, parties involved of the transaction that is reported as suspicious, including the account number and particulars of the account holder;
- d) a short description of the circumstances and reasons that justify the suspicion.

**Article 16 – Internal Controls and Compliance at Reporting Entities**

Reporting entities referred to at Article 4 of the present Law shall develop programs for the prevention of money laundering and the financing of terrorism in accordance with the guidelines of the supervisory authority as stipulated in article 31 of the present Law. Such programs shall include the following:
- a) Development of internal policy procedures and controls, including appropriate compliance arrangements and adequate screening procedures to ensure high standards when hiring employees;
- b) Designation of compliance officers at management level;
- c) Ongoing training for officials or employees;
- d) Internal audit function to check compliance with and effectiveness of the measures taken to apply the present law.

**CHAPTER IV FINANCIAL INTELLIGENCE UNIT**

**Article 19 - Organization**

1. A financial intelligence unit hereinafter referred to as the FIU shall be established as a unit under the control of the National Bank of Cambodia.
2. The FIU shall have adequate financial resources and independent decision-making authority on matters coming within its sphere of responsibility.

**Article 20 - FIU Board and Staff**

1. The FIU shall have a permanent secretariat, which shall be headed by a senior official appointed by the Prime Minister proposed by the National Bank of Cambodia. The permanent secretariat shall work under the authority of a Board of Directors, composed of the senior representatives of the following agencies:
   a) Office of the Council of Minister;
b) Ministry of Justice;
c) Ministry of the Interior;
d) Ministry of the Economy and Finance;
e) National Bank of Cambodia
2. The head of the Board shall be appointed by the Prime Minister proposed by the National Bank of Cambodia selected from amongst the representatives of the above agencies for a period of 2 years. The first head of the Board shall be the representative of the National Bank of Cambodia. The board members shall be appointed by the Royal Sub-decree with reference to the proposal of the National Bank of Cambodia.
3. The permanent secretariat of FIU shall have adequate staff selected by the head of FIU and approved by the Board. Staff shall meet high standards of integrity and shall be screened by the relevant authorities before employment by the FIU.

### Article 21 - Functions

The FIU shall:

a) receive suspicious and cash transaction reports made in pursuance of Article 12 of the present Law and information provided to the FIU about suspicions of money laundering or financing of terrorism;
b) collect information that the FIU considers relevant to its activities with regard to money laundering or financing of terrorism and that is publicly available, including commercially available databases, as well as other information necessary to carry out its functions, such as information collected maintained and stored in the database by the reporting entity;
c) have access on a timely basis to financial, administrative and law enforcement information as authorized by law that is necessary to undertake its functions set forth by this Article, including information collected and maintained by, or stored in the databases of, any public agency;
d) analyze and assess a suspicious transaction reports and related information in order to determine whether there are reasonable grounds to believe that a money laundering offense or an offense of financing of terrorism has been committed and in such cases refer the matter to the relevant law enforcement authority for criminal investigation;
e) compile statistics and records on suspicious and cash transaction reports received, analyzed and forwarded to the law enforcement authorities and disseminate information to other public agencies on related matters as required;
f) provide feedback to reporting entities and other relevant agencies regarding the outcome of suspicious transaction reports or information provided to it under the present Law;
g) ensure that personal information under its control is protected from unauthorized disclosure;
h) act to enhance public awareness and understanding of matters related to money laundering and financing of terrorism.

### Article 22 – Supervision by the FIU

1. The FIU shall issue guidelines to reporting entities in relation to customer identification, record keeping, reporting of suspicious transactions and other obligations established pursuant to the present Law. The FIU shall consult with supervisory agencies in those sectors where such supervision is already in place.
2. The FIU shall be responsible for ensuring compliance of reporting entities with the requirements set forth by the present Law through off-site monitoring and by conducting on-site inspections in accordance with the relevant legislation. The FIU shall coordinate its supervision of compliance under the present Law with the existing supervisory agencies.
3. If during its supervision of compliance with the present Law, the FIU discovers non-compliance with any of its provisions, it may:
   a) instruct the reporting entity to take remedial action as determined by the FIU to rectify non-compliance;
   b) inform the other supervisory agencies of such noncompliance and propose that they implement control measures, including the imposition of sanctions or the revocation of license, within their competence, as appropriate;
   c) initiate administrative sanctions under the present Law.
Article 25 – Relationship with Foreign FIU

1. The FIU may, subject to a reciprocal arrangement, exchange information with foreign FIU, provided that they are subject to similar requirements of confidentiality and irrespective of the nature of those units. It may, for that purpose, conclude cooperation agreements with such units. 2. Upon receipt of a request for information or transmission from a counterpart foreign FIU, it shall comply with that request within the scope of the powers conferred upon it by the present Law.

CHAPTER VI SANCTIONS

Article 30 – Freezing and confiscation of property

In case of a proceeding on the violation of money laundering or financing terrorism as stipulated in the existing Penal Code all relating or suspicious to be related property may be frozen or restrained from transferring until the court decision becomes definitive. In case where the court has decided to penalize the offence of money laundering or financing terrorism, the property shall be confiscated as state property.

Article 35 – Freezing of funds Associated with Financing of Terrorism

Notwithstanding any other provision of law, funds of terrorists, of those who finance terrorism and of organizations designated by the United Nations Security Council Resolutions 1267, 1373 and successor Resolutions shall be frozen without delay pursuant to mechanism and procedures defined by a legislative regulation.

Article 44- Financing of Terrorism Offence

1. A penalty of imprisonment for a period between 10 (ten) and 20 (twenty) years shall be applied to a person who provides and collects property, funds or other services with the intention that such property, funds or other services to be used or in the knowledge that they are or may be used, in full or in part, to support directly or indirectly any activities of terrorists or terrorist organizations including but not limited to the financing of travel, training, planning or preparation of, participation in, or perpetration of the terrorism, for the benefit of: a) A person who commits an offence under Law on Counter Terrorism or a corresponding offence under a law of a foreign State; b) An entity owned or controlled, directly or indirectly, by the person mentioned in (a) above; or c) A person or entity acting on behalf of, or at the order of, the person mentioned in (a) above. i. An act mentioned under paragraph 1 of this Article constitutes an offence although the property, resources or services have not been used to carry out an offence mentioned in the Law on Counter Terrorism or a corresponding offence under a law of a foreign State. ii. The legal entity may be declared as being criminally responsible under conditions as stipulated in Article 42 (Criminal Responsibility of a Legal Entity) of the Criminal Code for the offence committed in paragraph 1 of this Article. iii. The legal entity shall be subject to a fine from 1,000,000,000 (one billion) riels up to 2,000,000,000 (two billion) riels and any one or more additional sanctions as stipulated in Article 43 (Additional Penalties Applicable to Legal Entities) of the present Law.
CHAPTER IX
FINAL PROVISION

Article 46 – Repeal of the previous laws

The Law of Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0607/014 dated 24 June 2007 and the Law on Amendment of Article 3, Article29, Article 30 of Law on Anti-Money Laundering and Combating Terrorism promulgated by Royal Kram No. NS/RKM/0613/066 dated 3 June 2013 shall have no more effect and be replaced by the present Law after being in force.

PRAKAS ON ANTI-MONEY LAUNDERING AND
COMBATING THE FINANCING OF TERRORISM

Article 5 – Customer Due Diligence

5.1 Banks and financial institutions must conduct customer due diligence and obtain satisfactory evidence and properly establish in its records the identity and legal existence of persons applying to do business with them. Such evidence must be substantiated by reliable documents.
5.2 The customer due diligence should be conducted, when:
- establishing business relationship with the customer such as opening an account, granting a safe deposit facility or engaging in any other business dealings;
- carrying out an occasional or one off transaction, that involves a sum in excess of USD 10,000 (or 40 million Riel or foreign currency equivalent) or wire-transfer in excess of USD 1,000 (or 4 million Riel or foreign currency equivalent);
- banks and financial institutions have any suspicion of money laundering or financing of terrorism; or
- banks and financial institutions have any doubts about the veracity or adequacy of previously obtained information.
5.3 The customer due diligence undertaken by banks and financial institutions should at least comprise the following:
identify the customer and verify the identity of the customer using reliable, independent source documents, data or information referred to in articles 6 or 7;
- determine if the customer conducting business is acting on behalf of another person or beneficial owner;
- understanding the beneficial ownership and control structure of the customer. Beneficial owner is defined in article 8;
- obtain information on the purpose and intended nature of the business relationship; and conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant and ensure that the transactions being conducted are consistent with the bank's or financial institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.
5.4 Unwillingness of the customer to provide the information requested and to cooperate with banks and financial institution.

Article 10 - Trust and Nominee Accounts

10.1 Banks and financial institutions need to establish whether the customer is acting on behalf of another person as trustee, nominee or agent.
10.2 Banks and financial institutions should take reasonable measures to understand the ownership and control structures and the relationship among the relevant parties in handling a trust or nominee account and obtain evidence of the identity of the settler, trustee, nominee, authorised signatories, persons exercising effective control and the beneficiaries.
10.3 Banks and financial institutions should ensure customer due diligence requirements are completed for beneficial owners, when the trust or nominee account is established.
10.4 Banks and financial institutions require a written assurance from the trust or nominee that evidence of the identity of the beneficiaries has been obtained, recorded and retained, and that the trust or nominee is satisfied regarding the source of funds. In addition, identification information must be immediately available to banks and financial institutions upon requests’ customer due diligence process may itself be a factor of suspicion.

5.5 Banks and financial institutions should not open the account, commence business relations or perform transaction, or in the case of existing business relations with customers, it should terminate such business relations if the customer fails to comply with the customer due diligence requirements. Such situation warrants a suspicious transaction report to be submitted to the Financial Intelligence Unit.

2010 PRAKAS ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM RELATING TO ALL REPORTING ENTITIES NOT REGULATED BY THE NATIONAL BANK OF CAMBODIA

Article 6 – Customer Due Diligence

6.1 Reporting entities must conduct customer due diligence and obtain satisfactory evidence and properly establish in its records the identity and legal existence of persons applying to do business with them. Such evidence must be substantiated by reliable documents.

6.2 The customer due diligence should be conducted, when: - establishing business relationship with the customer such as opening an account, granting a safe deposit facility or engaging in any other business dealings; - carrying out an occasional or one off transaction, that involves a sum in excess of 40 million Riel (40,000,000KHR) or Ten thousand USD (USD10,000 or foreign currency equivalent) or wire-transfer in excess of 4 million Riel (4,000,000KHR) or One thousand USD (USD1,000 or foreign currency equivalent) Cashing out the winnings in gambling in excess of 40 million Riel (40,000,000KHR) or Ten thousand USD (USD10,000 or foreign currency equivalent). - reporting entities have any suspicion of money laundering or financing of terrorism; or - reporting entities have any doubts about the veracity or adequacy of previously obtained information.

6.3 The customer due diligence undertaken by reporting entities should at least comprise the following: - identify the customer and verify the identity of the customer using reliable, independent source documents, data or information referred to in articles 8 or 9; - determine if the customer conducting business is acting on behalf of another person or beneficial owner; - understanding the beneficial ownership and control structure of the customer. Beneficial owner is defined in article 09 of the present Prakas; - conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant and ensure that the transactions being conducted are consistent with the reporting entity’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

6.4 Unwillingness of the customer to provide the information requested and to cooperate with reporting entities’ customer due diligence process may itself be a factor of suspicion.

6.5 Reporting entities should not open the account, commence business relations or perform transaction, or in the case of existing business relations with customers, it should terminate such business relations if the customer fails to comply with the customer due diligence requirements. Such situation warrants a suspicious transaction report to be submitted to the CAFIU.

Article 11 – Trust and Nominee Accounts

11.1 Reporting entities need to establish whether the customer is acting on behalf of another person as trustee, nominee or agent.

1.2 Reporting entities should take reasonable measures to understand the ownership and control structures and the relationship among the relevant parties in handling a trust or nominee account and obtain evidence of the identity of the settler, trustee, nominee, authorised signatories, persons exercising effective control and the beneficiaries.

1.3 Reporting entities should ensure customer due diligence requirements are completed for beneficial owners, when the trust or nominee account is established.

1.4 Reporting entities require a written assurance from the trust or nominee that evidence of the identity of the
beneficiaries has been obtained, recorded and retained, and that the trust or nominee is satisfied regarding the source of funds. In addition, identification information must be immediately available to reporting entities upon request.
Section 66F – Punishment for cyber terrorism

(1) Whoever,--
A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--
   i) denying or cause the denial of access to any person authorised to access computer resource; or
   ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
   iii) introducing or causing to introduce any computer contaminant,
   and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or
B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 3 – Authentication of electronic records

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.--For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible--
   a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm; 
b) that two electronic records can produce the same hash result using the algorithm.

3) Any person by the use of a public key of the subscriber can verify the electronic record.

4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Section 3A – Electronic signature

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which--
   (a) is considered reliable; and
   b) may be specified in the Second Schedule.

2) For the purposes of this section any electronic signature or electronic authentication technique shall be con-
sidered reliable if--
a) the signature creation data or the authentication data are, within the context in which they are used, linked to
the signatory or, as the case may be, the authenticator and to no other person;
b) the signature creation data or the authentication data were, at the time of signing, under the control of the
signatory or, as the case may be, the authenticator and of no other person;
c) any alteration to the electronic signature made after affixing such signature is detectable;
d) any alteration to the information made after its authentication by electronic signature is detectable; and
e) it fulfils such other conditions which may be prescribed
3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic
signature is that of the person by whom it is purported to have been affixed or authenticated.
4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or
electronic authentication technique and the procedure for affixing such signature from the Second Schedule:
Provided that no electronic signature or authentication technique shall be specified in the Second Schedule un-
less such signature or technique is reliable.
5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.]

4 – Legal recognition of electronic records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed
form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been
satisfied if such information or matter is:
a) rendered or made available in an electronic form; and
b) accessible so as to be usable for a subsequent reference.

Section 5 – Legal recognition of [electronic signature]

Where any law provides that information or any other matter shall be authenticated by affixing the signature or
any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in
such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenti-
cated by means of 1 [electronic signature] affixed in such manner as may be prescribed by the Central Govern-
ment.

Explanation.--For the purposes of this section, “signed”, with its grammatical variations and cognate expressions,
shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and
the expression “signature” shall be construed accordingly.

Section 7 – Retention of electronic records

1) Where any law provides that documents, records or information shall be retained for any specific period,
then, that requirement shall be deemed to have been satisfied if such documents, records or information are
retained in the electronic form, if--
a) the information contained therein remains accessible so as to be usable for a subsequent reference;
b) the electronic record is retained in the format in which it was originally generated, sent or received or in
a format which can be demonstrated to represent accurately the information originally generated, sent or
received;(c) the details which will facilitate the identification of the origin, destination, date and time of despatch
or receipt of such electronic record are available in the electronic record:
Provided that this clause does not apply to any information which is automatically generated solely for the pur-
pose of enabling an electronic record to be despatched or received.
2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records
or information in the form of electronic records.
Section 7A – Audit of documents, etc., maintained in electronic form

[7A. Audit of documents, etc., maintained in electronic form.--Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in the electronic form.]

Section 10 – Power to make rules by Central Government in respect of electronic signature

- The Central Government may, for the purposes of this Act, by rules, prescribe--
  a) the type of [electronic signature];
  b) the manner and format in which the [electronic signature] shall be affixed;
  c) the manner or procedure which facilitates identification of the person affixing the [electronic signature];
  d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
  e) any other matter which is necessary to give legal effect to [electronic signatures].

Section 11 – Attribution of electronic records

An electronic record shall be attributed to the originator--
  a) if it was sent by the originator himself;
  b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
  c) by an information system programmed by or on behalf of the originator to operate automatically

Article 13 – Time and place of dispatch and receipt of electronic record.

1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:--
   i) receipt occurs at the time when the electronic record enters the designated computer resource; or
   ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;
3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
5) For the purposes of this section,--
   a) if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business;
   b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
   c) “usual place of residence”, in relation to a body corporate, means the place where it is registered.
Section 14 – Secure electronic record

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 15 – Secure electronic signature

An electronic signature shall be deemed to be a secure electronic signature if--
(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.—In case of digital signature, the “signature creation data” means the private key of the subscriber.

Section 21 – Licence to issue electronic signature Certificates

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue electronic signature Certificates.

(2) No licence shall be issued under sub-section (1), unless the applicant fulfils such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue electronic signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this section shall--
a) be valid for such period as may be prescribed by the Central Government;
b) not be transferable or heritable;
c) be subject to such terms and conditions as may be specified by the regulations.

Section 35 – Certifying authority to issue electronic signature Certificate

(1) Any person may make an application to the Certifying Authority for the issue of an electronic signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:
Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the electronic signature Certificate or for reasons to be recorded in writing, reject the application:
Provided] that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Section 40A – Duties of subscriber of Electronic Signature Certificate

In respect of Electronic Signature Certificate the subscriber shall perform such duties as may be prescribed.
Section 73 – Penalty for publishing electronic signature Certificate false in certain particulars

(1) No person shall publish a electronic signature Certificate or otherwise make it available to any other person with the knowledge that—
   a) the Certifying Authority listed in the certificate has not issued it; or
   b) the subscriber listed in the certificate has not accepted it; or
   c) the certificate has been revoked or suspended,
Unless such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation.

2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 79A- Central Government to notify Examiner of Electronic Evidence

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation. For the purposes of this section, “electronic form evidence” means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

1984 THE TERRORIST AFFECTED AREAS ACT (SPECIAL COURTS)

7. Jurisdiction of Special Court.

(1) Notwithstanding anything contained in the Code or in any other law, a scheduled offence committed in a judicial zone in a State at any time during the period during which such judicial zone is, or is part of, a terrorist affected area shall be triable, whether during or after the expiry of such period, only by the Special Court established for such judicial zone in the State:
Provided that where the period specified under sub-section (2) of section 3 as the period during which an area declared by notification under sub-section (1) of that section to be a terrorist affected area commences from a date earlier than the date on which such notification is issued, then—
e) nothing in the foregoing provisions of this sub-section shall apply to a scheduled offence committed in such area in which the whole of the evidence for the prosecution has been taken before the date of issue of such notification; and
f) all other cases involving scheduled offences committed in such area and pending before any court immediately before the date of issue of such notification shall stand transferred to the Special Court having jurisdiction under this section and the Special Court to which such proceedings stand transferred shall proceed with such cases from the stage at which they were pending at that time. (…)

10. Procedure and powers of Special Courts.

(1) A Special Court may take cognizance of any scheduled offence, without the accused being committed to it for trial, upon receiving a complaint of facts which constitute such offence or upon a police report of such facts. (…) 
3) A Special Court may, with a view to obtaining the evidence of any person supposed to have been directly or indirectly concerned in, or privy to, an offence, tender a pardon to such person on condition of his making a full and true disclosure of the whole circumstances within his knowledge relative to the offence and to every other
person concerned whether as principal or abettor in the commission thereof, and any pardon so tendered shall, for the purposes of section 308 of the Code, be deemed to have been tendered under section 307 thereof.

2000 THE INFORMATION TECHNOLOGY ACT

CHAPTER X THE 2 [APPELLATE TRIBUNAL]

58. Procedure and powers of the Appellate Tribunal].

(1) The 1[Appellate Tribunal] shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908) but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the 1[Appellate Tribunal] shall have powers to regulate its own procedure including the place at which it shall have its sittings.
2) The 1[Appellate Tribunal] shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:-
a) summoning and enforcing the attendance of any person and examining him on oath;
b) requiring the discovery and production of documents or other electronic records;
c) receiving evidence on affidavits;
d) issuing commissions for the examination of witnesses or documents;
e) reviewing its decisions;
f) dismissing an application for default or deciding it ex parte;
g) any other matter which may be prescribed.
3) Every proceeding before the 1[Appellate Tribunal] shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code (45 of 1860) and the 1[Appellate Tribunal] shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

CHAPTER XI OFFENCES

68. Power of Controller to give directions.

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. 1[(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.]

69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried
out, shall be such as may be prescribed.

3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to—
a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
b) intercept, monitor, or decrypt the information, as the case may be; or (c) provide information stored in computer resource.

4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

69A. Power to issue directions for blocking for public access of any information through any computer resource.

(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.

(1) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which any extend to three years and shall also be liable to fine.

Explanation.–For the purposes of this section,— (i) ―computer contaminant shall have the meaning assigned to it in section 43; (ii) ―traffic data means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.]

66F. Punishment for cyber terrorism.

(1) Whoever,–
A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—
i) denying or cause the denial of access to any person authorised to access computer resource; or
ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is
likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

CHAPTER XII INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

79. Exemption from liability of intermediary in certain cases.

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

2) The provisions of sub-section (1) shall apply if—

a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

b) the intermediary does not—

i) initiate the transmission,

ii) select the receiver of the transmission, and

iii) select or modify the information contained in the transmission;

c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

3) The provisions of sub-section (1) shall not apply if—

a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.—For the purposes of this section, the expression —third party information means any information dealt with by an intermediary in his capacity as an intermediary.

Chapter XIIA Examiner of Electronic Evidence

79A. Central Government to notify Examiner of Electronic Evidence

Central Government to notify Examiner of Electronic Evidence.—The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. Explanation.—For the purposes of this section, —electronic form evidence means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.]
16. Procedure and powers of Special Courts

(1) A Special Court may take cognizance of any offence, without the accused being committed to it for trial, upon receiving a complaint of facts that constitute such offence or upon a police report of such facts.
2) Where an offence triable by a Special Court is punishable with imprisonment for a term not exceeding three years or with fine or with both, the Special Court may, notwithstanding anything contained in sub-section (1) of section 260 or section 262 of the Code, try the offence in a summary way in accordance with the procedure prescribed in the Code and the provisions of sections 263 to 265 of the Code shall, so far as may be, apply to such trial: Provided that when, in the course of a summary trial under this sub-section, it appears to the Special Court that the nature of the case is such that it is not desirable to try it in a summary way, the Special Court shall recall any witnesses who may have been examined and proceed to re-hear the case in the manner provided by the provisions of the Code for the trial of such offence and the said provisions shall apply to, and in relation to, a Special Court as they apply to and in relation to a Magistrate: Provided further that in the case of any conviction in a summary trial under this section, it shall be lawful for a Special Court to pass a sentence of imprisonment for a term not exceeding one year and with fine which may extend to five lakh rupees.
3) Subject to the other provisions of this Act, a Special Court shall, for the purpose of trial of any offence, have all the powers of a Court of Session and shall try such offence as if it were a Court of Session so far as may be in accordance with the procedure prescribed in the Code for the trial before a Court of Session.
4) Subject to the other provisions of this Act, every case transferred to a Special Court under sub-section (2) of section 13 shall be dealt with as if such case had been transferred under section 406 of the Code to such Special Court.
5) Notwithstanding anything contained in the Code, but subject to the provisions of section 299 of the Code, a Special Court may, if it thinks fit and for reasons to be recorded by it, proceed with the trial in the absence of the accused or his pleader and record the evidence of any witness, subject to the right of the accused to recall the witness for cross-examination.

THE INDIAN PENAL CODE

196. Using evidence known to be false

Whoever corruptly uses or attempts to use as true or genuine evidence any evidence which he knows to be false or fabricated, shall be punished in the same manner as if he gave or fabricated false evidence.

197. Issuing or signing false certificate

Whoever issues or signs any certificate required by law to be given or signed, or relating to any fact of which such certificate is by law admissible in evidence, knowing or believing that such certificate is false in any material point, shall be punished in the same manner as if he gave false evidence.

198. Using as true a certificate known to be false

Whoever corruptly uses or attempts to use any such certificate as a true certificate, knowing the same to be false in any material point, shall be punished in the same manner as if he gave false evidence.
199. False statement made in declaration which is by law receivable as evidence

Whoever, in any declaration made or subscribed by him, which declaration any Court of Justice, or any public servant or other person, is bound or authorised by law to receive as evidence of any fact, makes any statement which is false, and which he either knows or believes to be false or does not believe to be true, touching any point material to the object for which the declaration is made or used, shall be punished in the same manner as if he gave false evidence.

200. Using as true such declaration knowing it to be false

Whoever corruptly uses or attempts to use as true any such declaration, knowing the same to be false in any material point, shall be punished in the same manner as if he gave false evidence. Explanation- A declaration which is inadmissible merely upon the ground of some informality, is a declaration within the meaning of sections 199 to 200.

201. Causing disappearance of evidence of offence, or giving false information to screen offender

Whoever, knowing or having reason to believe that an offence has been committed, causes any evidence of the commission of that offence to disappear, with the intention of screening the offender from legal punishment, or with that intention gives any information respecting the offence which he knows or believes to be false; if a capital offence- shall, if the offence which he knows or believes to have been committed is punishable with death, be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine; if punishable with imprisonment for life- and if the offence is punishable with 104[imprisonment for life], or with imprisonment which may extend to ten years, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; if punishable with less than ten years' imprisonment- and if the offence is punishable with imprisonment for any term not extending to ten years, shall be punished with imprisonment of the description provided for the offence, for a term which may extend to one-fourth part of the longest term of the imprisonment provided for the offence, or with fine, or with both.

Illustration
A, knowing that B has murdered Z, assists B to hide the body with the intention of screening B from punishment. A is liable to imprisonment of either description for seven years, and also to fine.

201. Causing disappearance of evidence of offence, or giving false information to screen offender

Whoever, knowing or having reason to believe that an offence has been committed, causes any evidence of the commission of that offence to disappear, with the intention of screening the offender from legal punishment, or with that intention gives any information respecting the offence which he knows or believes to be false; if a capital offence- shall, if the offence which he knows or believes to have been committed is punishable with death, be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine; if punishable with imprisonment for life- and if the offence is punishable with 104[imprisonment for life], or with imprisonment which may extend to ten years, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; if punishable with less than ten years' imprisonment- and if the offence is punishable with imprisonment for any term not extending to ten years, shall be punished with imprisonment of the description provided for the offence, for a term which may extend to one-fourth part of the longest term of the imprisonment provided for the offence, or with fine, or with both.

Illustration
A, knowing that B has murdered Z, assists B to hide the body with the intention of screening B from punishment. A is liable to imprisonment of either description for seven years, and also to fine.
202. Intentional omission to give information of offence by person bound to inform

Whoever, knowing or having reason to believe that an offence has been committed, intentionally omits to give any information respecting that offence which he is legally bound to give, shall be punished with imprisonment of either description for a term which may extend to six months, or with fine, or with both.

204. Destruction of document to prevent its production as evidence

Whoever secretes or destroys any document which he may be lawfully compelled to produce as evidence in a Court of Justice, or in any proceeding lawfully held before a public servant, as such, or obligates or renders illegible the whole or any part of such document with the intention of prevention the same from being produced or used as evidence before such Court or public servant as aforesaid, or after he shall have been lawfully summoned or required to produce the same for that purpose, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

205. False personation for purpose of act or proceeding in suit or prosecution.

Whoever falsely personates another, and in such assumed character makes any admission or statement, or confesses judgement, or causes any process to be issued or becomes bail or security, or does any other act in any suit or criminal prosecution, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.
CHAPTER I GENERAL PROVISIONS

Article 1.

[...] Documents shall be evidence in the form of data, recordings or information that can be seen, read and/or heard, with or without the assistance of an instrumentality on paper or any physical material other than paper, or electronically, including and not limited to:

a. writings, voice, or images;
b. maps, designs, photographs, or the like;
c. letters, signs, numbers, symbols, or perforations which have meaning or are understandable by those able to read or understand them.

CHAPTER II THE REQUEST FROM INDONESIAN GOVERNMENT
Part Four Assistance for Obtaining Evidence

Article 12.

(1) if it is believed that there are legal means of proof related with an investigation, prosecution and examination before the court in Indonesia, the Minister may ask for Assistance to the Foreign State to endeavor: a. the taking of a Deposition in the Foreign State; or b. the surrender of Documents or other legal means of proof located in the Foreign State.

2) Deposition received from Foreign States based on the Request for Assistance as referred to in paragraph (1) subparagraph (a) may be accepted as legal means of proof in an investigation, prosecution, and examination before the court related to said request insofar as it has been acknowledged and/or signed by the Person making Depositions and by the competent official taking said Depositions.

3) Documents or other legal means of proof originating from Foreign States based on the request for Assistance as referred to in paragraph (1) subparagraph b may be accepted as legal means of proof in an investigation, prosecution and examination before the court pursuant to said request for Assistance.

Part Five Assistance for Arranging the Attendance of Persons in Indonesia

Article 17.

– (...) (3) For the purposes provided for in paragraph (2), legal immunity assurance by virtue of law of the Foreign State shall be admissible in examination before the court, unless proven otherwise. (...)
Article 19.

The Minister may convey the request for Assistance to Foreign States to issue the following orders: a. freezing; b. search warrant; c. seizure; or d. other necessary orders in accordance with the provisions of laws and regulations in relation with criminal proceedings in Indonesia.

Part Nine Limitation on the Use of Depositions, Documents and Evidence

Article 24.

Any deposition, document or other legal means of proof obtained or provided upon request as referred to in Article 12 up to Article 14 may only be used by Indonesian competent officials for the purpose of an investigation, prosecution and examination before the court related with said request for Assistance.

Article 28. (...) the Request for Assistance, to the extent that it is necessary and possible, must also contain the following:

a. identity, citizenship, and domicile of the Person deemed able to provide statement or depositions related with the investigation, prosecution and examination before the court;

b. a description concerning the requested statement or deposition;

c. description concerning required documents or other legal means of proof articles to be submitted, including a description concerning the Person deemed able to provide such evidence; and

d. information concerning expenses and accommodations required from the Person requested to be present in said Foreign State.

3) the Minister may ask for additional information if the information contained in the request for Assistance is not sufficient to approve such request for Assistance.

4) A conveyance of the request for Assistance, information or other communications drawn up hereunder may be drawn up in the language of the Requesting State and/or in English and the Indonesian translation thereof shall be made.

CHAPTER III REQUEST TO THE GOVERNMENT OF THE REPUBLIC OF INDONESIA

Part Three Assistance for Deriving Depositions, Documents and Other Evidences Voluntarily

Article 32.

(1) A Requesting State may convey the request for Assistance to the Minister for: a. Taking a Deposition from a person in Indonesia; or b. Delivering Documents and other legal means of proof located in Indonesia.

2) In addition to requirements as referred to in Article 28, the request for Assistance must also include the following:

a. explanation that the request for Assistance is related with an investigation, prosecution and examination before the court in the Requesting State and the status of the person is as a suspect or a witness;

b. the matters to be questioned in the form of a list of questions; and/or

c. description of deposition can be taken in Indonesia or documents or other legal means of proof being requested are in Indonesia.

3) In the event the request for Assistance has met requirements as referred to in paragraph (2), the Minister may ask the Kapolri or the Attorney General in accordance with the phrases of case examination in the Requesting State to follow up the same.
4) In the event that the Kapolri or the Attorney General has taken measures as referred to in paragraph (3), the Kapolri or the Attorney General shall deliver the results to the Minister. (5) In the event that the provision of Assistance is approved pursuant to the provisions as referred to in paragraph (2), and the Requesting state requests that copies of documents be legalized, the Minister shall order a competent official in relevant jurisdiction to legalize the same and return them to the Minister.

**Article 33.**

A person involved in the process of investigation, prosecution and examination before the court in the Requesting State may not be forced to give a Deposition in Indonesia. (2) Any person related to the request for Assistance as referred to in Article 32 paragraph (1) may not be forced to give a Deposition, to deliver documents or other legal means of proof in an investigation, prosecution and examination before the court in the Requesting State if Indonesian Law restricts the person in the same position to do so.  

3) the Person as referred to in Article 33 paragraphs (1) and (2) shall have the right for not being:  
   a. detained, prosecuted, adjudicated and convicted based on domestic laws of the Requesting State for any crime alleged to have committed, or that was committed before his/her departure from Indonesia to fulfill said request;  
   b. sued in any civil proceeding in the Requesting State with respect with any act or omission, that occurred before the person's departure from Indonesia to fulfill said request; or  
   c. required to provide a statement or other Assistance in relation with any criminal matter in Indonesia other than the criminal matter to which the request related; or  
   d. required, in the process of investigation, prosecution, or examination before the court related with said request for Assistance, to answer any question that the Person would not be required to answer under the law of his/her state.  

4) For the purposes as set forth in paragraph (2), an immunity certificate authenticated based on the law of the Requesting State shall be acknowledged as authenticated evidence, unless proved otherwise with regard to the matters mentioned in a Deposition.  

5) Any person related to the request for Assistance as set forth in Article 30, shall have the same privileges with respect to provision of a Deposition and delivery of Documents and other legal means of proof as if the investigation, prosecution and examination before the court on such person had not yet obtained a binding court decision in Indonesia.

**Part Six Assistance for Conducting Search and Seizure of Goods, Articles or Assets**

**Article 42 –**

The Head of the Local District Court may issue search and seizure warrants with respect to the object if it is believed that in or at a certain place there are goods, articles or assets that are:  

a. allegedly obtained from or the proceeds of crime under the law of the Requesting State that have been or allegedly have been committed;  

b. used to commit or prepare such crime;  

c. particularly designed or allocated to commit such crime;  

d. related to such crime;  

e. that is believed to be evidence in such crime; or  

f. that was used to hamper the investigation, prosecution and examination before the court of such crime.

**Article 47 –**

In the event that the Requesting State asks that goods, objects, assets or evidence of seizure of goods, objects or assets be sent to the Requesting State for the purpose of criminal proceeding and the Minister considers that such request can be granted and there is a guarantee that the Requesting State will return the aforementioned goods, objects or assets, the Minister shall send goods, objects or assets to the Requesting State.

**Article 58 –**

the Minister may require the Requesting State to keep secret a request for Assistance, the content of the request and any of its supporting documents, as well as the provision of assistance based on the aforementioned request.  

2) In the event that the request for Assistance cannot be approved by the Requesting State without violating the confidentiality, the Minister may determine whether such request will stand although it violates the requested
What is meant in this law by:
1. Investigator is a state police official of the Republic of Indonesia or a certain civil service official who is granted special authority by law to conduct an investigation.
2. Investigation is a series of acts by the investigator in matters and according to ways regulated by this law to seek and gather evidence with which to make clear a criminal act committed and to find the suspect.
9. Administering justice is a series of acts by the judge of accepting, examining, and deciding a criminal case on the basis of the principles of freedom, honesty and impartiality at a court session in matters and according to ways as regulated by this law.
10. Pre-trial is the competence of the court of justice to conduct an investigation and decide in ways which are regulated by this law, on: a. whether or not an arrest and/or detention is legal at the request of the suspect or his family or other party on behalf of the suspect; b. whether or not the termination of investigation or prosecution upon request is valid for the sake of upholding law and justice; c. a request for indemnity or rehabilitation from a suspect or his family or another party on his behalf whose case has not been brought before the court.
14. Suspect is a person who because of his act or condition, on the basis of initial proof can reasonably be suspected of being a perpetrator of a criminal act.
15. Defendant is a suspect who is prosecuted, examined and tried at a court session.
16. Confiscation is a series of acts by an investigator of taking over and/or placing under his control moveables or immovables, tangibles or intangibles to be used as evidence in investigations, prosecutions and trials.
17. House search is an act by an investigator of entering a residential house or other closed place to carry out an investigation and/or confiscation and/or arrest in matters and according to ways as regulated by this law.
20. Arrest is an act by an investigator of temporarily restricting the freedom of a suspect or defendant if there is enough evidence for purposes of investigation or prosecution and/or trial in matters and according to ways regulated by this law.
27. Testimony is one of the means of providing evidence in a criminal case in the form of information from a witness concerning a criminal event which he himself has heard of, witnessed or experienced by mentioning the reasons for his knowledge.
28. Expert information is information provided by a person who has special expert knowledge on a subject needed to throw light on a criminal case in the interest of investigation.

CHAPTER III TRIAL BASIS

Article 3

Trial shall be conducted in ways as regulated by this law.
### Article 4

An interrogator can be any police officer of the Republic of Indonesia.

### Article 5

(1) An interrogator as intended in section 4
a. because of his duties has the authority
   1. to accept a report or complaint from a person about the presence of a criminal act;
   2. to seek information and evidence material;
   3. to order a suspected person to stop and to ask for and inspect his identification card;
   4. to take other responsible legal measures.
b. on order of an investigator can take measures in the form of
   1. arrest, restriction of movement, search and confiscation;
   2. inspection and confiscation of letters;
   3. taking the fingerprints and a photograph of a person
   4. taking and bringing a person before an investigator.

An interrogator prepares and submits a report on the results of measures as mentioned in section (1) letters a and b to the investigator.

### Article 17

An order of arrest shall be carried out against a person who is strongly presumed to have committed a criminal act on the basis of enough initial evidence.

### Article 18

(1) The task of making an arrest shall be executed by state police officers of the Republic of Indonesia by showing their assignment letters and handing over to the suspect the arrest warrant which contains the suspect's identity and mentions the reasons for his arrest, and explains in brief the criminal case of which he is suspect and his place of examination.

2) If a person is caught in-the-act the arrest shall be made without a warrant, with the stipulation that the arresting officer must immediately hand over the arrested and available evidence materials to the nearest investigator or assistant investigator.

3) A copy of the arrest warrant as intended in section (1) shall be delivered to the family of the arrested immediately after his arrest.
**Article 21**

(1) A detention order or further detention order shall be applied to a suspect or defendant who is strongly presumed to have committed a criminal act on the basis of sufficient evidence, in case there are circumstances which give reason for concern that the suspect or defendant will get away, damage or destroy evidence materials and/or repeat the criminal act.

**Part Four Confiscation**

**Article 40**

In a caught in-the-act case, an investigator can confiscate goods and equipment which obviously or which can reasonably be presumed to have been used for committing the criminal act or other goods which can be used as evidence materials.

**Article 41**

In a caught in-the-act case, an investigator is authorized to confiscate packages or letters or goods transported or sent by the post and telecommunication office, a communication or transportation agency or enterprise, provided said packages, letters or goods are meant for the suspect or have originated from him and for this, the suspect and/or the official at the post and telecommunication office, communication or transportation agency or enterprise concerned, shall be provided with a receipt.

**Article 42**

(1) An investigator is authorized to order a person in control of goods which can be confiscated, to hand over the goods to him in the interest of investigation and the person delivering the goods shall be given a receipt.

2) Letters or other written materials can only be ordered for delivery to an investigator if the letters or written materials originate from a suspect or defendant or are addressed to him or are his own or are meant for him or if the goods mentioned are means for committing a criminal offense.

**Article 44**

(1) In case the confiscated goods consist of easily damaged or dangerous materials, making it impossible to keep them until the court’s decision on the case concerned has attained permanent legal force or if the cost of keeping the goods will become too high, as far as possible with the agreement of the suspect or his proxy the following measures can be taken:

a. if the case is still in the hands of the investigator or public prosecutor, the goods mentioned can be sold in an auction or taken for safekeeping by the investigator or public prosecutor, with suspect or his proxy as witness;

b. if the case is already in the hands of the court, the goods mentioned can be taken for safekeeping or sold in an auction by the public prosecutor with the permission of the judge who is handling the case, with the suspect or his proxy as witness.

2) The proceeds of the auction sale of the goods concerned in the form of cash shall be used as evidence material.

3) In the interest of providing proof a small portion of the goods as intended in section (1) should as far as possible be set aside.

4) Confiscated goods which are contraband in nature or are banned from circulation shall be excluded from the provision as intended in section (1) and seized for use in the interest of the state or in order to be destroyed.
Article 46

(1) Goods which are confiscated shall be returned to the person or to those from whom they have been confiscated, or to the person or those who are the most entitled to them, if,
a. they are no longer needed in the interest of investigation and prosecution;
b. the case in question has been dropped because of the lack of sufficient proof or it having turned out to be no criminal offence. c. the case in question has been put aside in the public interest or closed for the sake of law, except when the goods have resulted from a criminal act or have been used for committing a criminal offense.
2) If the case has been decided, the goods confiscated shall be returned to the person or to those mentioned in the decision, except when according to the decision of the judge the goods shall be seized for the state, in order to be destroyed or damaged in such a way as to be no longer usable -or if the goods concerned are still needed, to be used as evidence material; for another case.

Part Five
Examination of Letters

Article 47

(1) An investigator has the right to open, examine and confiscate letters and other written materials sent through the post and telecommunication office, a communication or transport agency or enterprise, if the materials in question are strongly suspected of having connection with a criminal case being investigated, with a special warrant issued for that purpose by the chairman of the district court.
2) In said interest the investigator can ask the head of the post and telecommunication office, the head of the communication or other transport agency or enterprise concerned to hand over to him the intended letters, for which he shall give a receipt.
3) The measure as intended in section (1) and section (2) of this article can be taken at all levels of examination in the trial process in accordance with the provision arranged in the section concerned.

Article 48

(1) If after it has been opened and examined, a letter proves to have some connection with the case being examined, the latter shall be enclosed in the dossier of the case.
2) If after it has been examined, a letter proves to have no connection whatsoever with said case, it shall be neatly closed again and send back immediately to the post and telecommunication office, the communication and other transport agency or enterprise concerned after being marked «opened by investigator» and provided with a date, and the signature and identity of the investigator,
3) The investigator and the officials at all levels of examination in the trial process are obliged to really keep the content of the returned letter a secret by strength of their oath of office.

Article 49

(1) The investigator shall make a report about the measures as intended in article 48 and article 75.
2) Copies of the report shall be sent by the investigator to the head of the post and telecommunication office, the head of the communication or transport agency or enterprise concerned.
CHAPTER VI SUSPECT AND DEFENDANT

Article 57

(1) A suspect or defendant who is detained has the right to contact his legal adviser in accordance with the provisions of this law.
3) A suspect or defendant of foreign nationality who is detained has the right to contact and speak with a representative of his country in facing the process of his case.

CHAPTER X COURT’S AUTHORITY TO JUDGE
Part One Pre-trial hearing

Article 82

(1) The procedure of pre-trial examination for such cases as intended in article 79, article 80 and article 81 shall be as follows
a. within three days after receipt of the request, the appointed judge shall determine the day for the session;
b. in examining and in order of decide whether or not an arrest or detention is legal, whether or not the termination of an examination or prosecution, a request for compensation; and/or rehabilitation as the consequence of an illegal arrest or detention, as the result of the legal termination of an examination or prosecution and the presence of confiscated goods which do not belong to materials of evidence are valid, the judge shall hear information both from the suspect or petitioner and the competent official concerned;
c. said examination shall be carried out speedily and within seven days at the latest the judge must have passed his verdict
d. in the event the trial of a case has already been started by the court of first instance (district court), while the examination of the motion for a pre-trial hearing has not yet been completed, the motion shall be dropped. e. the decision of the pre-trial hearing at the level of Investigation does not preclude the possibility of another pre-trial examination being held at the level of examination by the public prosecutor, if a new motion is filed for this purpose.
2) The decision of the judge in the pre-trial examination of the matters intended in article 19, article 80 and article 81, shall be clearly explained as to its basis and reason.
3) The decision shall not only meet the provision as intended in section (2) but shall also provide for the following:
a. in case the decision determines that an arrest or detention is illegal, the investigator or the public prosecutor at their respective levels of examination shall immediately release the suspect;
b. in case the decision determines that the termination of an investigation or prosecution is not valid, the investigation and prosecution of the suspect shall be continued:
c. in case the decision determines that an arrest or detention is illegal, then it shall mention the amount of compensation and rehabilitation to be given, while in case the termination of an investigation or prosecution is valid and the suspect is not detained, the decision shall mention his rehabilitation.
d. in case the decision determines that the goods confiscated do not all consist of evidence materials, it shall also provide for the immediate return of the goods concerned to the suspect or the person from whom they have been confiscated.
4) Compensation can be demanded, to cover matters as intended in article 77 and article 95.

Part Four Conviction and Verdict in Normal Trial Procedure.

Article 183

A judge shall not penalize a person except when with two legal evidence materials he has come to the conviction that a criminal act has really been committed and that it is the defendant who is guilty of perpetrating it.
Article 184

(1) Legal evidence materials are:
a. the testimony of a witness;
b. information by an expert;
c. a letter;
d. an indication;
e. the statement of a defendant.
2) Matters which are generally known need not be proved.

Article 185

(1) The testimony of a witness as evidence material is what the witness has stated in a court session.
2) The testimony of one witness alone is not sufficient to prove that a defendant is guilty of the act, of which he is charged of having committed.
3) The provision as intended in section (2) shall not apply if accompanied by another legal evidence material.
4) Separate testimonies by several witnesses on an event or situation can be used as legal evidence material if they are connected with one another in such a way as to confirm the occurrence of an event or the presence of a certain situation.
5) An opinion or an assumption, as the mere product of a thought process does not constitute witness testimony.
6) In judging the truth of a testimony by a witness, a judge must seriously take into account:
a. the concurrence between the testimony of one witness with that of another;
b. the concurrence between the testimony of a witness with another evidence material;
c. the reason which might have motivated a witness to give a certain testimony.
d. the way of life and morality of a witness and any other things which can be of influence for determining whether or not the information he has given can be trusted.
7) Testimonies made by witnesses not under oath despite their concurrence, make no evidence material; however if they concur with the testimony made by a witness under oath, they can be used as an additional legal evidence material.

Article 187

The letter as intended in article 184 section (1) letter c, made under an oath of office or strengthened by an oath, can be:
a. a record and other letter made in official form by or in front of a competent public official, which contains information about an event or a situation he himself has heard of, witnessed or experienced, accompanied by a clear and firm reason for the information;
b. a letter made in accordance with the provision of a law regulation or a letter which is made by an official concerning a matter coming under his responsible management and which is meant as a proof for something or a situation;
c. a statement by an expert which contains an opinion based on his expertise it something or about a situation, officially asked from him; d. another letter which is only useful if it has some connection with the content of another evidence material.

Article 188

(1) Indication is an act, event or situation which because of its concurrence whether between one and the other, or with the criminal act itself, indicates the occurrence of a criminal act and the person committing it.
2) An indication as intended in section (1) can only be obtained from a. the testimony of witness; b. a letter; c. a statement by a defendant.
3) Evaluation by the judge of the proving strength of an indication in every definite situation shall be wise and prudent, after he has accurately and carefully conducted an examination on the basis of his conscience.
Article 189

(1) In case the verdict is for release or acquittal of all legal charges, the court shall decide that confiscated evidence materials be handed over to the party most entitled to receive them back whose name shall be mentioned in said decision except when law regulations provide that the evidence materials must be seized in the interest of the state or destroyed or damaged so that they can no longer be used.
2) Except when there is a valid reason, the court shall decide that the evidence materials be handed over immediately after the session is over.
3) The order for, the handing over of the evidence materials shall be carried out without any conditions except when the court’s decision has not yet attained permanent legal force.

CHAPTER XIX IMPLEMENTATION OF A COURT’S DECISION

Article 273

(1) If a court's verdict provides for a fine penalty, the Convicted person shall be given one month's time to pay the fine except in a quick trial decision when the fine must be paid immediately.
2) In case there is a strong reason, the time limit as intended in section (1) can be extended for at most one month.
3) If a court's decision also provides for the seizure of evidence materials for the state, with the exception mentioned in article 46, the attorney shall entrust the goods to the state auction office in order to be sold by auction within three months, the proceeds of which shall be delivered to the state treasury for and on behalf of the attorney.
4) The time limit as intended in section (3) can be extended for at most one month

LAW NUMBER 8 YEAR 2010 ON THE PREVENTION OF CRIME OF MONEY LAUNDERING

CHAPTER I GENERAL PROVISIONS

Article 1.

16. Documents shall be data, recordings, or information that can be seen, read, and/or heard, which can be exhibited with or without the aid of equipment, whether shown on paper or any physical object whatsoever other than paper or that has been recorded electronically, including but not limited to:
- written text, sound, or drawings;
- maps, designs, photos, or anything similar;
- Alphanumeric characters, marks, numbers, symbols, or perforations that have a meaning or that may be understood by a person capable of reading or understanding them.

Article 2.

(1) Proceeds of criminal acts shall be Assets acquired from the following criminal acts:

...)
. terrorism;
...
Assets known or reasonably suspected to be used and/or being used, directly or indirectly, for acts of terrorism,
organized terrorism or individual terrorism, shall be considered equal to proceeds from criminal acts as referred to in paragraph (1) sub-paragraph n.

SECTION TWO
APPLICATION OF KNOW YOUR CUSTOMER PRINCIPLE

Article 18.

(1) The Regulating and Monitoring Institution establishes provisions regarding know your customer principles.
2) The Reporting Party must implement know your customer principles as referred to in paragraph (1).
3) The mandatory implementation of Know Your Customer Principles as referred to in paragraph (2) is applied when:
   a. establishing a business relationship with a Services User;
   b. there is a Financial Transaction using Rupiah currency and/or other foreign currency minimum in the amount of or in equivalent with Rp100,000,000.00 (one hundred million rupiah);
   c. there is a Suspicious Financial Transaction related to the crime of money laundering and financing of terrorism; or d. The Reporting Party doubts the accuracy of Information reported by the Services User.
4) The Regulating and Monitoring Institution must perform monitoring on the Reporting Party’s compliance in implementing Know Your Customer Principles.
5) Know Your Customer Principles shall at least comprise of:
   a. the identification of the Services User;
   b. verification of the Services User; and
   c. monitoring transactions of the Services User.
6) In the event that a Regulating and Monitoring Institution does not yet exist, provisions regarding know your customer principles and its monitoring shall be stipulated in a Regulation issued by the Head of PPATK.

Article 73

Valid evidence in proving the crime of money laundering shall be:
   a. evidence as referred to in the Criminal Procedures Code; and/or
   b. other evidence in the form of information spoken, transmitted, received, or electronically stored with optical equipment or similar to those and Documents.

LAW NUMBER 11 YEAR 2008 CONCERNING ELECTRONIC INFORMATION AND TRANSACTION

CHAPTER I GENERAL PROVISIONS

Article 1 in this Law:

“Electronic Information” means one cluster or clusters of electronic data, including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them.
Electronic Transaction” means a legal act that is committed by the use of Computers, Computer networks, and/or other electronic media.
Information Technology” means a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.
Electronic Record” means any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via Computers or
Electronic Systems, including but not limited to writings, sounds, images, maps, drafts, photographs or the like, letters, signs, figures, Access Codes, symbols or perforations having certain meaning or definition or understandable to persons qualified to understand them. 

Electronic System means a set of electronic devices and procedures that functions to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information. 

Provision of Electronic System means an Electronic System usage by the state administrators, Persons, Business Entities, and/or the public. 

Electronic System Network means a closed or open connection of two Electronic Systems or more. 

Electronic Agent means an automated electronic means that is used to initiate an action to certain Electronic Information, which is operated by Persons. 

Electronic Certificate means a certificate in electronic nature that bears an Electronic Signature and identity, demonstrating a status of a legal subject of parties to an Electronic Transaction issued by Certification Service Providers. 

Electronic Certification Service Provider means a legal entity that acts as a reliable party, issues and audits Electronic Certificates. 

Trustworthiness Certification Body means an independent institution that is formed by professionals acknowledged, certified, and supervised by the Government, whose authority is to audit and issue trustworthiness certificates for Electronic Transactions. 

Electronic Signature means a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of verification and authentication. 

Computer means an electronic, magnetic, optical data processing device, or a system that performs logic, arithmetic, and storage functions. 

Access means an activity to make interaction with independent or network Electronic Systems. 

“Access Code” means a figure, letter, symbol, other character or a combination thereof, which is a key to enable Access to Computers and/or other Electronic Systems. 

Electronic Contract means an agreement of parties entered into by means of Electronic Systems. 

Sender/Originator means a legal subject that sends Electronic Information and/or Electronic Records. 

Recipient/Addressee means a legal subject that receives Electronic Information and/or Electronic Records from Senders/Originators. 

Domain Name means an internet address of a state administrator, Person, Business Entity, and/or the public that can be used for communication over the internet, in the form of unique character code or set to identify a certain location on the internet. 

Person means an individual, whether an Indonesian citizen, foreign citizen, or legal entity. 

Business Entity means a sole proprietorship or partnership of both legal entity and nonlegal entity. 

“Government” means a Minister(s) or other official(s) the President designates.

Article 2:

This Law shall apply to any Person who commits legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, having legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia.

Elucidation of Article 2:

Since Information Technology usage for Electronic Information and Electronic Transactions is cross-territorial or universal in nature, this law shall have jurisdiction over legal acts applicable not only in Indonesia and/or committed by Indonesian citizens, but also applicable to legal acts committed outside jurisdiction of Indonesia by both Indonesian citizens and foreign citizens or Indonesian legal entities and foreign legal entities having legal effect in Indonesia.

Detrimental to the interest of Indonesia shall include but not limited to detrimental to the interests of national economy, strategic data protection, nation's dignity and degree, state defense and security, sovereignty, citizens as well as Indonesian legal entities.

CHAPTER III ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES

Article 5:

(1) Electronic Information and/or Electronic Records and/or the printouts thereof shall be lawful means of proof. 

Elucidation of Article 5 Section (1): Sufficiently clear
2) Electronic Information and/or Electronic Records and/or the printouts thereof as intended by section (1) shall be the expansion of lawful means of proof in accordance with the Law of Procedure applicable in Indonesia.  
*Elucidation of Article 5 Section (2): Sufficiently clear*

3) Electronic Information and/or Electronic Records shall be declared to be lawful if using Electronic Systems in accordance with provisions as governed by this Law.  
*Elucidation of Article 5 Section (3): Sufficiently clear*

4) Provisions on Electronic Information and/or Electronic Records as intended by section (1) shall not apply to:

   a. certificates that under Laws must be made in writing form;  
   *Elucidation of Article 5 Section (4) Point a:*
   Certificates that under laws must be made in writing form shall include but not limited to negotiable instruments, valuable documents, and documents used in the process of law enforcement of civil procedure, criminal procedure, and state administration.

   b. certificates together with their papers that under Laws must be made in notarial deed or deed made by land conveyancers.  
   *Elucidation of Article 5 Section (4) Point b:*
   Sufficiently clear

---

**Article 6:**

Where other provisions are in place other than those regulated in Article 5 section (4) requiring that information must be in writing or original form, Electronic Information and/or Electronic Records shall be deemed to be lawful to the extent information contained therein is accessible, displayable, assured as to its integrity, and accountable in order to be explanatory.  
*Elucidation of Article 6:*
Until the present, a writing form is identical to information and/or records contained on paper only; in effect, information and/or records can essentially be inscribed on any medium, including electronic media. Within the context of Electronic Systems, it is no longer relevant to distinguish the original information from its copies in that Electronic Systems can typically generate copies that make the original information can no longer be distinguished from them.

---

**Article 7:**

Any Person who asserts rights, affirms existing rights, or denies other Persons’ rights with respect to the existence of Electronic Information and/or Electronic Records must ensure that Electronic Information and/or Electronic Records with him/her originate in Electronic Systems eligible under Laws and Regulations.  
*Elucidation of Article 7:*
His provision is intended that Electronic Information and/or Electronic Records may be used as grounds from which rights accrue.

---

**Article 8:**

(1) Unless agreed otherwise, time of sending of Electronic Information and/or Electronic Records shall be determined at the time the Electronic Information and/or Electronic Records have been sent to the proper address by the Senders/Originators to Electronic Systems the Recipients/Addressees designate or use, and have entered Electronic Systems outside the control of the Senders/Originators.  
2) Unless agreed otherwise, the time of receipt of Electronic Information and/or Electronic Records shall be determined at the time the Electronic Information and/or Electronic Records enter Electronic Systems under the control of the authorized Recipients/Addressees.  
3) Where Recipients/Addressees have designated certain Electronic Systems to receive Electronic Information, reception shall occur at the time Electronic Information and/or Electronic Records enter designated Electronic Systems.  
4) Where there are two or more information systems used in the sending or reception of Electronic Information and/or Electronic Records, then:
   a. the time of sending shall be the time when Electronic Information and/or Electronic Records enter a first information system outside the control of the Senders/Originators.
   b. the time of receipt shall be the time when Electronic Information and/or Electronic Records enter a last infor-
Article 9:

Business actors that offer products through Electronic Systems must make available full and true information about contractual conditions, producers, and offered products.

*Elucidation of Article 9:*

Full and true information” includes:

- Information that contains the identity as well as the status of legal subject and its competency, whether as producers, suppliers, providers or intermediaries;
- Other information that explains certain matters of requirements for validity of agreements, as well as explains offered goods and/or services, such as names, addresses, and descriptions of goods/services;

Article 10:

(1) Any business actor who conducts Electronic Transactions may be certified by Trustworthiness Certification Bodies.

*Elucidation of Article 10 section (1):*

Trustworthiness Certification is intended as proof that business actors conducting trade electronically are eligible to do business upon assessment and audits by authorized bodies. Proof that Trustworthiness Certification has been made shall be demonstrated by a trustmark certification logo on the homepage of the business actor.

2) Provisions on formation of Trustworthiness Certification Bodies as intended by section (1) shall be regulated by Government Regulation.

*Elucidation of Article 10 section (2):*

Sufficiently clear

Article 11:

(1) Electronic Signatures shall have lawful legal force and legal effect to the extent satisfying the following requirements:

- a. Electronic Signature-creation data shall be associated only with the Signatories/ Signers;
- b. Electronic Signature-creation data at the time the electronic signing process shall be only in the power of the Signatories/ Signers;
- c. Any alteration in Electronic Signatures that occur after the signing time is knowable;
- d. Any alteration in Electronic Information associated with the Electronic Signatures after the signing time is knowable;
- e. There are certain methods adopted to identify the identity of the Signatories/ Signers; and
- f. There are certain methods to demonstrate that the Signatories/Signers have given consent to the associated Electronic Information;

*Elucidation of Article 11 Section (1):*

This Law grants recognition definitely that despite codes, Electronic Signatures have an equal position to manual signatures in general, with legal force and legal effect. The requirements as intended by this Article shall be the requirements that minimally any Electronic Signature must satisfy. This provision gives as wide opportunities as possible to anyone to develop methods, techniques, or process for creating Electronic Signatures.

2) Further provisions on Electronic Signatures as intended by section (1) shall be regulated by Government Regulation.

*Elucidation of Article 11 Section (2):*

The Government Regulation concerned shall govern, inter alia, techniques, methods, means or process for creating Electronic Signatures.
Article 12:

(1) Any Person involved in electronic signing is required to provide security of Electronic Signatures he/she uses;
2) Security of Electronic Signatures as intended by section (1) shall include at least:
   a. the systems are not accessible to unauthorized Persons;
   b. the Signatories/Signers must apply the principle of prudence to avoid unauthorized uses of Electronic Signature-creation data;
   c. the Signatories/Signers must without delay adopt methods recommended by Electronic Signature providers, or other appropriate methods and should promptly notify Persons whom the Signatories/Signers consider to be relying on the Electronic Signatures or notify parties that support Electronic Signature services if
   5. the Signatories/Signers know that the Electronic Signature-creation data has been compromised; or
   6. circumstances known to the Signatories/Signers may pose considerable risks due likely to the compromised Electronic Signature creation data; and
   d. where Electronic Certificates are used to support Electronic Signatures, the Signatories/Signers must confirm the truth and integrity of all information in connection with the Electronic Certificates.
3) Any Person in violation of the provisions as intended by section (1) shall be responsible for 15 (1),

Elucidation of Article 12: Sufficiently clear

CHAPTER IV PROVISION OF ELECTRONIC CERTIFICATION AND ELECTRONIC SYSTEMS
Part One Provision of Electronic Certification

Article 13

(1) Any Person shall be entitled to engage the service of Electronic Certification Service Providers for creating Electronic Signatures.
2) Electronic Certification Service Providers must confirm the attribution of an Electronic Signature to the owner.
3) Electronic Certification Service Providers shall include:
   c. Indonesian Electronic Certification Service Providers; and
   d. foreign Electronic Certification Service Providers.
4) Indonesian Electronic Certification Service Providers shall be an Indonesian legal entity and domiciled in Indonesia.
5) Foreign Electronic Certification Service Providers that operate in Indonesia must be registered in Indonesia.
6) Further provisions on Electronic Certification Service Providers as intended by section (3) shall be regulated by Government Regulation.

Elucidation of Article 13: Sufficiently clear

Article 14 Electronic Certification Service Providers as intended by Article 13

section (1) through section (5) must make available to any service user accurate, clear, and definite information that includes:
   a. methods that are adopted to identify the Signatories/Signers;
   b. things that can be used to recognize Electronic Signature-creation personal data
   c. things that can demonstrate the validity and security of Electronic Signatures;

Elucidation of Article 14:
Information as intended by this Article shall be the information that minimally any Electronic Signature service provider must satisfy.
Part Two
Operation of Electronic Systems

Article 15:
(1) Any Electronic System Provider must provide Electronic Systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems.
2) Electronic System providers shall be responsible for their Operation of Electronic Systems.
3) The provision as intended by paragraph (2) shall not apply where it is verifiable that there occur compelling circumstances, fault, and/or negligence on the part of the Electronic System users.

Article 16:
(1) To the extent not provided otherwise by separate laws, any Electronic System Provider is required to operate Electronic Systems in compliance with the following minimal requirements:
   a. can redisplay Electronic Information and/or Electronic Documents in their entirety in accordance with the retention period as provided for by Rules;
   b. can protect the availability, entirety, authenticity, confidentiality, and accessibility of Electronic Information in the Provision of Electronic Systems;
   c. can operate in compliance with procedures or guidelines for the Provision of Electronic Systems;
   d. are furnished with procedures or guidelines that are announced with languages, information, or symbols that are understandable to parties attributed to the Provision of Electronic Systems; and
   e. adopt sustainable mechanism in order to maintain updates, clarity, and accountability for the procedures or guidelines;
2) Further provisions on Provision of Electronic Systems as intended by paragraph (1) shall be regulated by Government Regulation.

CHAPTER V
ELECTRONIC TRANSACTIONS

Article 17:
(1) Operator of Electronic Transactions may be carried out within a public or private scope.
2) Parties that conduct Electronic Transactions as intended by paragraph (1) must be in good faith in making interaction and/or exchange of Electronic Information and/or Electronic Documents during the transactions.
3) Further provisions on operation of Electronic Transactions as intended by paragraph (1) shall be regulated by Government Regulation.

Article 18:
(1) Electronic Transactions that are stated in Electronic Contracts shall bind on parties.
2) Parties shall have the power to choose law applicable to international Electronic Transactions they enter.
3) If parties do not make choice of law in international Electronic Transactions, the applicable law shall be under the principles of the Private International Law.
4) Parties shall have the powers to determine forums of court, arbitration, or other alternative dispute resolution institutions with jurisdiction to handle disputes that may arise from international Electronic Transactions they enter.
5) If parties do not make choice of forum as intended by paragraph (4), the jurisdiction of court, arbitration, or other alternative dispute resolution institution with jurisdiction to handle disputes that may arise from such transactions shall be determined under the principles of the Private International Law.
Article 19:

Parties that conduct Electronic Transactions must adopt agreed-on Electronic Systems.

Article 20:

(1) Unless provided otherwise by parties, Electronic Transactions shall occur at the time the transaction offers sent by Senders have been received and accepted by Recipients.
2) Acceptance on the Electronic Transaction offers as intended by paragraph (1) must be made with an electronic acknowledgement of receipt.

Article 21:

(1) Senders or Recipients may conduct Electronic Transactions in person, or by his/her proxy, or by Electronic Agents.
2) Parties responsible for any legal effect in the conduct of Electronic Transactions as intended by paragraph (1) shall be regulated as follows:
   a. if conducted in person, any legal effect in the conduct of Electronic Transactions shall become the responsibility of parties to a transaction;
   b. if conducted by proxy, any legal effect in the conduct of Electronic Transactions shall become the responsibility of the grantors of the proxy; or
   c. if conducted by Electronic Agents, any legal effect in the conduct of Electronic Transactions shall become the responsibility of Electronic Agent providers.
3) If damage of Electronic Transactions is occasioned by failure of the operation of Electronic Agents due to third parties’ direct measures against Electronic Systems, any legal effect shall become the responsibility of Electronic Agents providers.
4) If damage of Electronic Transactions is occasioned by failure of the operation of Electronic Agents due to negligence of service users, any legal effect shall become the responsibility of the service users.
5) The provision as intended by paragraph (2) shall not apply if provable that there occur compelling circumstances, fault and/or negligence on the part of the Electronic System users.

Article 22:

(1) Certain Electronic Agent Providers must provide features to Electronic Agents they operate to enable their users to alter information still in the process of transaction.
2) Further provisions on certain Electronic Agent providers as intended by paragraph (1) shall be regulated by Government Regulation.

Article 23:

(1) Any state administrator, Person, Business Entity, and/or the society shall be entitled to hold Domain Names on a first applicant principle basis.
2) Holding and use of Domain Names as intended by paragraph (1) must be on the basis of good faith, non-violation of fair business competition, and non-infringement of the rights of other Persons.
3) Any state administrator, Person, Business Entity, or the society damaged by other Persons’ unauthorized use of Domain Names shall be entitled to lodge a claim for cancelling such Domain Names.
CHAPTER VII
PROHIBITED ACTS

Article 27:

(1) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents with contents against propriety.
2) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents with contents of gambling.
3) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents with contents of affronts and/or defamation.
4) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Documents with contents of extortion and/or threats.

Article 28:

(1) Any Person who knowingly and without authority disseminates false and misleading information resulting in consumer loss in Electronic Transactions.
2) Any Person who knowingly and without authority disseminates information aimed at inflicting hatred or dis-sension on individuals and/or certain groups of community based on ethnic groups, religions, races, and inter-groups (SARA).

Article 29:

Any Person who knowingly and without authority sends Electronic Information and/or Electronic Documents that contain violence threats or scares aimed personally.

Article 30:

(1) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Sys-
tems of other Persons in any manner whatsoever.
2) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Sys-
tems in any manner whatsoever with the intent to obtain Electronic Information and/or Electronic Documents.
3) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Sys-
tems in any manner whatsoever by breaching, hacking into, trespassing into, or breaking through security systems.

Article 31:

(1) Any Person who knowingly and without authority or unlawfully carries out interception or wiretapping of Electronic Information and/or Electronic Documents in certain Computers and/or Electronic Systems of other Persons.
2) Any Person who knowingly and without authority or unlawfully carries out interception of the transmission of non-public Electronic Information and/or Electronic Documents from, to, and in certain Computers and/or Elec-tronic Systems of other Persons, whether or not causing alteration, deletion, and/or termination of Electronic Information and/or Electronic Documents in transmission.
3) Interception excepted from one as intended in paragraphs (1) and (2) shall be interception carried out in the framework of law enforcement at the request of the police, prosecutor’s office, and/or other law enforcement institutions as stated by laws.
4) Further provisions on procedures for interception as intended by paragraph (3) shall be regulated by Government Regulation.

**Article 32:**

(1) Any Person who knowingly and without authority or unlawfully in any manner whatsoever alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Documents of other Persons or of the public.
2) Any Person who knowingly and without authority or unlawfully in any manner whatsoever, moves or transfers Electronic Information and/or Electronic Documents to Electronic Systems of unauthorized Persons.
3) Acts as intended by paragraph (1) shall be acts that result in any confidential Electronic Information and/or Electronic Document being compromised such that the data becomes accessible to the public in its entirety in an improper manner.

**Article 33:**

Any Person who knowingly and without authority or unlawfully commits any act resulting in faults on Electronic Systems and/or resulting in Electronic Systems working improperly.

**Article 34:**

(1) Any Person who knowingly and without authority or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns:
   a. Computer hardware or software that is designed or specifically developed to facilitate acts as intended by Article 27 through Article 33;
   b. Computer passwords, Access Codes, or the like to make Electronic Systems accessible with the intent to facilitate acts as intended by Article 27 through Article 33;
2) Acts as intended by paragraph (1) are not criminal acts if aimed at carrying out research activities, testing of Electronic Systems, protection of Electronic Systems themselves in a legal and lawful manner.

**Article 35:**

Any Person who knowingly and without authority or unlawfully manipulates, creates, alters, deletes, tampers with Electronic Information and/or Electronic Documents with the intent that such Electronic Information and/or Electronic Documents would seem to be authentic data.

**Article 36:**

Any Person who knowingly and without authority or unlawfully commits acts as intended by Article 27 through Article 34 to other Persons’ detriment.

**Article 37:**

Any Person who knowingly commits prohibited acts as intended by Article 27 through Article 36 outside the territory of Indonesia towards Electronic Systems residing within jurisdiction of Indonesia.
CHAPTER VIII
DISPUTE RESOLUTION

Article 38:

(1) Any Person may institute actions against parties that provide Electronic Systems and/or using Information Technology to his/her detriment.
(2) The society in accordance with provisions of Rules may bring class action lawsuits against parties that provide Electronic Systems and/or using Information Technology to the society loss, in accordance with Rules.

CHAPTER IX
ROLE OF THE GOVERNMENT AND ROLE OF THE SOCIETY

Article 40:

(1) The Government shall facilitate the Information Technology and Electronic Transaction utilization in accordance with provisions of Rules.
(2) The Government shall protect the public interest from any type of threat as a result of misusing Electronic Information and Electronic Transactions that offends public order, in accordance with provisions of Rules.
(3) The Government shall specify agencies or institutions holding strategic electronic data that must be protected.
(4) Agencies or institutions as intended by paragraph (3) must create Electronic Documents and the electronic backups thereof, and connect them with specified data centers in the interest of data security.
(5) Other agencies or institutions other than those regulated by paragraph (3) shall create Electronic Documents and their electronic backups as necessary to protect data they hold.
(6) Further provisions on role of the Government as intended by paragraphs (1), (2), and (3) shall be regulated by Government Regulation.

Article 41:

(1) The society may play role in the improvement of the Information Technology utilization through the use and Operation of Electronic Systems and Electronic Transactions in accordance with the provisions of this Law.
(2) Role of the society as intended by paragraph (1) may be played through institutions formed by society.
(3) Institutions as intended by paragraph (2) may have the functions of consultation and mediation.

CHAPTER X
INVESTIGATION

Article 42:

Investigation of criminal acts as intended by this Law shall be made under the provisions of the Law of Criminal Procedure and the provisions of this Law.
**Article 43:**

(1) In addition to Investigators of the State Police of the Republic of Indonesia, certain Civil Service Officials within the Government whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions shall be granted special authority as investigators as intended by the Law of Criminal Procedure to make investigation of criminal acts of Information Technology and Electronic Transactions.  
2) Investigation of Information Technology and Electronic Transactions as intended by paragraph (1) shall be made with due regard to privacy protection, secrecy, smooth public services, data integrity, or data entirety in accordance with provisions of Rules.  
3) Searches and/or seizures of electronic systems suspiciously involved in criminal acts must be carried out with the permission of the local chief justice of the district court.  
4) In carrying out searches and/or seizures as intended by paragraph (3), investigators are required to maintain the public service interests.  
5) Civil Service Investigators as intended by paragraph (1) shall have the authority:  
   a. to receive reports or complaints from Persons of the occurrence of criminal acts under the provisions of this Law;  
   b. to summons any Person or other party for hearing and/or examination as suspects or witnesses in connection with suspected criminal acts in the field related to the provisions of this Law;  
   c. to make examination of the truth of reports or inquiries into criminal acts under the provisions of this Law;  
   d. to make examination of Persons and/or Business Entities that should be suspected of having committed criminal acts under this Law;  
   e. to make inspection of equipment and/or facilities in connection with the activities of Information Technology suspected of having been used to commit criminal acts under this Law;  
   f. to search certain places suspected of having been used as the place to commit criminal acts under the provisions of this Law;  
   g. to seal and seize equipment and/or facilities of Information Technology activities suspected of having been used in a manner departing from provisions of Rules;  
   h. to solicit assistance of experts necessary for investigation of criminal acts under this Law, and/or  
   i. to cease investigation of criminal acts under this Law in accordance with the provisions of the prevailing law of criminal procedure.  
6) To make arrest and detention, investigators through public prosecutors are required to seek order of the local chief justice of the district court within a period of twenty-four hours.  
7) Civil Service Investigators as intended by paragraph (1) shall coordinate with Investigators of the State Police of the Republic of Indonesia to notify the commencement of investigation and deliver the results thereof to public prosecutors.  
8) In the framework to uncover criminal acts of Electronic Information and Electronic Transactions, investigators may cooperate with investigators of other countries to share information and means of proof.

**Article 44:**

Means of proof on the investigation, prosecution and examination at court under the provisions of this Law shall be as follows:  
a. means of proof as intended by provisions of Laws; and  
b. other means of proof in the form of Electronic Information and/or Electronic Documents as intended by Article 1 paragraph 1 and paragraph 4 as well as Article 5 paragraphs (1), (2), and (3).

**CHAPTER XI**
**PENAL PROVISIONS**

**Article 52:**

(1) Criminal acts as intended by Article 27 paragraph (1) involving propriety or sexual exploitation of children shall be subject to an increase in the sentence by one third of the basic sentence.  
2) Criminal acts as intended by Article 30 through Article 37 aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents of the Government and/or used for public services
shall be sentenced to the basic sentence plus one third.
3) Criminal acts as intended by Article 30 through Article 37 aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents of the Government and/or strategic agencies including and not limited to defense institutions, the central bank, banking, finance, international institutions, aviation authority shall be subject to a sentence of maximally the basic sentence for the respective Articles plus two-thirds.
4) Criminal acts as intended by Article 27 through Article 37 committed by corporations shall be sentenced to the basic sentence plus two-thirds.
Article 157: Embezzlement of material evidence.

Any individual bearing the responsibility to safeguard properties or objects considered as material evidence, but selling, concealing, withdrawing, using, exchanging or damaging them, etc. in an illegal way is punishable of six months to three years of imprisonment or of correctional penalties without privation of liberty.


Any individual enrolled in an armed organization attacking and destroying factories, social organizations or sequestrating or killing officials, simple civilians or robbing the properties of the state Collectively, and individuals with the aim of destroying the basis of imprisonment; liable to the seizure of his properties and confinement to home custody or life imprisonment or death penalty. Preparation and attempt of such infractions are also punishable.

2004 CRIMINAL PROCEDURE LAW

Part III - Evidence in Criminal Proceedings – Chapter 1 - Evidence

Article 27 (modified). Evidence

Evidence in a criminal case is the factual information collecting from each proceeding in which the investigation organizations, public prosecutor, and the courts shall use it as the basis for considering the case, and for adjudicating whether the accused persons are guilt or innocent or endanger to the society. The behavior of a person shall be an important evidence to consider the case correctly and justly.

Article 28. Types of Evidence

Evidence in criminal proceedings consists of:
Physical evidence;
Documentary evidence;
Evidence from persons.

The evidence mentioned above includes evidence to prove guilt confirming that the accused person or defendant has committed the offence, and evidence to prove innocence that confirms that the accused person or defendant is innocent.

In criminal proceedings, concerned persons shall seek both evidence to prove guilt and evidence to prove innocence.
Chapter 2 - Physical Evidence –

Article 29 (new). Physical Evidence

Physical evidence is derived from material items relating to the offence, such as guns, knives, fingerprints, bloodstains, and other materials.

Article 30 (new). Gathering and Keeping Physical Evidence

Gathering of physical evidence should be immediately made at the time of discovering; collecting evidence must be thorough, recorded of the circumstances, and protecting the evidence as of the prescription in laws. In case that the evidence cannot be gathered materially, taking photo shall be recommended for collecting as electronic evidence.

Physical evidence should be protected by wrapping up, or kept in the bag.

Physical evidence should be protected from damaging, lost, changing, breaking, and mixing up with others.

Protection of physical evidence should follow:

iv. Physical evidence should be wrapped up and kept in the bag immediately after completing gathering process.

All items should be recorded documentarily in detail and kept in the case file;

v. Physical evidence which is money, bank note, gold, silver, diamond, and other valuable items should be deposited with the bank under the rules of laws;

vi. Chemical or addictive items must be identified before being kept;

iiv. Guns, exploded substance, inflaming substance, and other dangerous substances, must be delivered to concerned organizations for properly maintaining;

viii. Physical evidence which is about bloodstain, hair, fingerprint, footprint, bullet, and others, must be kept properly as prescribed by laws;

In case that all physical evidence mentioned above has been lost, changed, and damaged, without any reasonable explanation, authorities concerned must be legally responsible under the penal law.

Article 31 (new). The Resolution of Physical Evidence

Criminal proceeding organization has the rights and duties to deal with the evidence including:

1. All objects used or will be used into the productive process or any products which are prohibited to possess by laws, or use, will be seized and repossessed to the government;

2. Public belongings must be returned back to the government after gathering from physical evidence from the offenses;

3. Physical evidence which cannot be identified of the true owner will automatically be transferred to the government;

4. Substance which is fragile to be derogated and spoiled must be placed on auction, and then shall be brought to the court for further proceeding;

5. All priceless and useless items shall be destroyed after having been gone through case proceeding; or all disputes of criminal physical evidence should be resolved by laws.

Chapter 3 - Documentary Evidence - Article 32. Documentary Evidence

Documentary evidence is derived from letters, reports of the investigation, reports of the activities of the people's courts, account, drawings, sketches, photographs, and other documents relating to the offence.
Article 33 (new). Reports from Proceeding Authorities

The reports from proceeding authorities include the order of arrest, examination, confiscation or sequestration, inspection at the incident, verification of evidence, investigation, confirmation and testing of information, the activities of the people's courts, and other reports including letters, accounts, drawings, sketches, photographs, and other documents relating to the criminal offence.

Chapter 5 - Gathering Evidence –

Article 41 (new). Searching for Facts

In the time of investigation, the order of petition and adjudication, the criminal proceeding organization must provide the facts as follow:
7. The incident of the case (behavior, date, day, time, place, vehicles, tools, method, and others);
8. The offence of the accused person or defendant (intentionality, or carelessness) and reasons for the execution;
9. Conducts and level of the danger of the case which include behavior of the accused persons or defendants;
10. Conducts and level of the loss resulting from the offense;
11. The conditions to be discharged from all criminal responsibilities or taking liabilities;
12. The conditions to minimize or increase the criminal liabilities.

Article 42 (new). Impractical Evidence

Receiving information by breaching this law shall not be taken as criminal evidence. Impractical evidence shall not be bound by law and cannot be used into the criminal proceeding.

Article 43 (new). Gathering Evidence

The investigation organization shall have the rights and duties as follow:
5. Taking testimony from the suspects, the accused persons, defendants, civil claimants, civil responsibility takers, and witnesses;
6. Inspection at the incident, examining houses, vehicles, and individuals, retesting findings, sequestration or confiscation;
7. Call for all persons who have learned about the incident to give testimony, take part in face to face investigation, point out and confirm the offenders;
8. Appoint professionals or experts to give opinion;
9. Demand documents, or objects of criminal evidence from persons, or organizations;
10. Identification of evidence
11. To exercise such other rights and perform such other duties as provided by the laws.
Individuals and organizations concerned must obey the warrant, invitation, demand, or appointment of criminal proceeding organization.
Individuals and organizations can gather criminal evidence and then must handover them to the concerned authorities.

Article 44 (modified). Examination and Evaluation of Evidence

Existing evidence must be examined and evaluate the correctness based on a comprehensiveness, truth, and relationship in the case which can be used for further proceeding.
The criminal proceeding organizations must examine and evaluate the evidence comprehensively based on thorough and objective consideration with confidence.
In the examination and evaluation of evidence, if the evidence indicates doubt whether the accused person or defendant has committed the crime or not, such person must be released from charges. Criminal proceedings should not mainly take into account the admission of the accused person or defendant but should seek additional evidence to prove the guilt of such persons. Even if the accused person or defendant deny or does not admit such guilt, if there is strong and reliable evidence, he may be regarded as the wrong-doer.

**Article 54 (modified). Rights and Duties of Investigation Officers**

Investigation officers shall have the following rights and duties:
1. To receive and record complaints, reports or requests relating to offences;
2. To order warrants, invite, bring in suspects, detain, arrest, confiscate or seize, release the accused persons, suspend or dismiss the case;
3. To take testimony from the injured party, civil plaintiff, accused person, witness, and other concerned persons;
4. To inspect the site of the incident, to conduct inspections of dead body, to conduct searches of buildings, vehicles, and persons, and to collect evidence relating to the offence;
5. To bring, detain, and release the accused persons according to the order of the investigation organizations;
To search for, arrest and release the accused persons by following the order of the people's courts or public prosecutors;
6. To inform charges, rights, and duties to the suspect, and accused person;
7. To implement orders and to report on the circumstance in criminal proceedings to the head of the investigation organization;
8. To summarize, report, and organize a case file for the investigation organizations;
9. To exercise other rights and perform other duties according to the order of the head.
In the criminal proceeding, investigators shall have responsibilities to the laws, and the head of investigation organization.

**Article 55 (new). Rights and Duties of Assistants of Investigators**

Assistants of investigation officer have the rights and duties to exercise under article 54 of this law, and as of an assigned work, except for to open the investigation.

**Article 57 (new). Rights and Duties of Prosecutors**

Rights and duties of prosecutors consist of:
1. To open an investigation of criminal cases;
2. To inform charges, rights and duties, to the suspects and the accused persons;
3. To record the testimony from defendant, plaintiff, and other relevant people to the case;
4. To collect, and gather criminal evidence;
5. To study, summarize criminal case file, draft statement or resolution of the Office of the Public Prosecutor;
6. To participate in court hearing of criminal case;
7. To monitor and inspect adherence to the absolute court's decision;
8. To monitor and inspect detention areas, prisons, and re-education centers;
9. To exercise such other rights and performs such other duties as provided by the laws.

**Article 58 (new). Rights and Duties of Assistants of the public prosecutor**

Assistants have the rights and duties as follow:
1. To participate in and record the testimony of participants in criminal procedure;
2. To study, summarize criminal case, and draft statement or draft resolution made by the Office of the Public Prosecutors;
3. To mark case numbers, organize case files, list, keep and make a statistic of criminal cases;
4. To list and inspect protection of criminal evidence;
5. To list and make statistic of the suspects, and the accused persons;
6. To issue the warrants, and invitation;
7. To exercise such other rights and performs such other duties as provided by the laws.

**Article 60 (new). Rights and Duties of Judges**

Judges have the following rights and duties:
1. To study case files that are assigned to them;
2. To take the testimony of the plaintiff, defendant, and other persons in the court proceedings;
3. To collect the evidence of cases;
4. To mediate cases;
5. To preside over judicial tribunals; and
6. To exercise such other rights and perform such other duties as provided by the laws.

**Article 64 (new). The Suspect**

A suspect is a person who is doubted to commit crime, but the investigation organizations, and the Office of the Public Prosecutor still not opening an investigation yet. The suspect has the rights as follow:
1. Be informed the charges
2. Receive explanation on his/her rights and duties
3. Explain or provide information relevant to the charges
4. Provide evidence
5. Report the unacceptable behavior of the investigation organization, and the Office of the Public Prosecutors
6. Request to bail for the minor offense in which the sentence shall not exceed three years in jail

**Chapter 2 - Opening an Investigation –**

**Article 84 (new). Opening an Investigation**

The investigation organizations, or the Office of the Public Prosecutor, have to open an investigation immediately after finding out of comprehensive evidence indicating to the offenses prescribed in article 91 of this law. In the case that the offender has committed a number of offenses, concerned investigation authorities shall have to inform all charges to the lawbreakers with detail of sentencing prescribed in criminal law, and other laws.

Make a copy of an order to open an investigation, and summarize all circumstances which lead to an issuance of order to open an investigation, and report to the Office of the Public Prosecutor within 20 hours from a minute of issuing an order. Within 48 hours after receiving a report, the Office of the Public Prosecutor has to have a comment whether the concerned order should be continued or rejected, and then response back quickly to the investigation organization.

In the case that the Office of the Public Prosecutor found some involved persons of the case, and are still not being investigated, the Office of the Public Prosecutor shall request the investigation organization to open an additional investigation immediately.

**Article 89 (new). Discovery of Trace of Offenses**

The head of investigation organization, investigators, and the public prosecutor or prosecutors, must record all evidence and information founded in order that those items will be used for further investigation.
Article 126 (new). The Confiscation of Objects or Document at the Time of Search

At the time of searching building, work place, vehicles, and individuals, the investigators shall have the right to confiscate or seize objects or documents relevant to evidence, or trace of the offenses. The confiscation or seizure shall be followed an article 30, of this law.

The confiscation of objects or document at the time of search must be recorded, and provide clearly the date, time, place of search, name and surname, position and duties of the participants in the search, and items of confiscation. When finishing the record of the search, all detail shall be read out to participants, and give signatures with thumbprint on the record.

The confiscation of objects or document at the time of search must be recorded as prescribed in article 100 of this law.

Part XIV - International Cooperation in Criminal Proceedings

Article 270. Principle of International Cooperation in Criminal Proceedings

International cooperation in criminal proceedings between the competent organization conducting criminal proceedings in the Lao PDR and competent organs of foreign countries shall comply with principles of respect for the independence, territorial sovereignty of the States, non-interference in the domestic affairs, equality and mutual benefit, and be consistent with the Constitution of Lao PDR and the fundamental principles of international law.

Article 271. International Cooperation in Criminal Proceedings

International cooperation in criminal proceedings must carried out in compliance with agreements that the Lao PDR has signed with foreign countries or international conventions that it has entered into and in accordance to the laws of the Lao PDR. In the incident that the Lao PDR has not yet signed or not yet entered into international conventions relating to criminal proceedings, such co-operation shall be carried out on the basis of principles of mutual cooperation, but shall not be in conflict with the laws of the Lao PDR.

Article 272 (modified). Implementation of Judicial Assistance

In the provision of judicial assistance, the competent organization conducting criminal proceedings in the Lao PDR shall comply with the agreements that the Lao PDR has signed with foreign countries or international conventions that the Lao PDR is a party to and shall comply with this law. Provision of judicial assistance may have the objective of extradition, or exchange of prisoners, or seizure or sequestration of assets of an accused person or defendant, or enforcement of judgment, or cooperation in combating of cross-border crime and others.
2016 INFORMATION, COMMUNICATION AND TECHNOLOGY LAW

Pending submission.

2015 LAW ON PREVENTION AND COMBATING CYBER CRIME

Part I
General Provisions.

Article 3. Definitions

The terms used in this law have the following meaning:
1. Crime means any offence prescribed by the Penal Code and any other law prescribed criminal penalty;
2. Computer System means a piece of electronic equipment or sets of electronic equipment units is integrated together, for which contains an ordering, sets of ordering and other related process to enable the electronic equipment to perform the duty of processing data automatically in a computer or any interconnected computers through computer network or internet system;
3. Server System means a service system providing through the Computer System including Database Server, Web Server, Mall Server, File Server and other related components;
4. Computer's data and Information means data, message, program or database system, personal data and information, computer traffic data in for of data processing and enabling computer to perform a function;
5. Database System means a storage data system in form of electronic mean that being able to manage, modify and use;
6. Personal Data and Information means any data and information directly or indirectly relating and identifying individual, action of person, legal entity and organization;
7. Computer Traffic Data means data related to communication through computer system-based developed by a computer system as a part of communication chain showing sender, source of origin, intermediary, route, destination time, date as well as size and duration of communication, type of service and other service concerned relating to computer system communication;
8. Service Provider means a person providing of communication data information through computer system and/or a person providing of computer data storage;
9. Automatically Data Processing means a process of calculating and developing data in any computer system by computer program;
10. Program means an ordering system or sets of ordering for computer's operating and performing as manufactured design;
11. Virus means any specifically developed program for wide spreading virus, demanding and destroying computer system, computer network, computer's data and information;
12. Malicious Code means any developed set for ordering for destroying computer system or hacking computer's data information;
13. Fishing Website means any new creating website containing the same characters and components similar to the original website in order to achieve for obtaining consumer information;
14. Vulnerability means a weakness of any software or program which is not be accomplished or updated allowing an attacher to use for destroying computer system, hacking or changing data, information and others in computer system;
15. Consumer Information means any information on consumer’s address such as postal address, electronic address, geographical address, internet protocol, telephone number and other related code applying into any computer;
16. Specific Access prevention Measure means an applying of any specific tool and/or program into any computers for prevention and combating others from unauthorized computer access;
17. Online Social Media means an internet system disseminating and providing data and information to public by means of computer equipment and communication devices;
18. Animation means ant created image moving as live action which can be visible through an electronic device such as cartoon movies.
Article 4. State Policy on Campaining of Prevention and Combating Cyber Crime

The state supports using of computer system with safe, convenient, fast and farness usage, and protects the legitimate rights and benefits of service provider, consumer of computer system service, computer's data and information in according to the laws and regulations. The state develops conditions and provides facilities for campaign of prevention and combating cyber crime by contribution of budget, developing and supplying of person, technical equipment and vehicle, researching and applying modern technology, developing of related infrastructure for the effective implementation of mentioned campaign. The state takes the camping of prevention and combating cyber crime as the main task and regards the dealing with cyber crime the important task. The state supports and encourage person, legal entity and organization from both domestic and foreign country to invest in technical production and modern technology as well participating in the campaign of prevention and combating cyber crime.

5. Principle of Prevention and Combating Cyber Crime

The campaign of prevention and combating cyber crime shall ensure the following main principles:
1. Compliance with stat's policy, laws, strategic plan and national socio-economic plan;
2. National security, peace and society order as well as national culture and fine tradition of the nation;
3. Protection of national and official secret confidence, secret person, legal entity and organization;
4. Unity, safety, convenience, fast and fairness;
5. Protection of legitimate rights and benefits of service provider, consumer of computer system service, computer's data and information in according to laws and regulations;
6. Participation of society;
7. Implementation of the international agreements and treaties which the Lao PDR is party to.

Article 6. Scope of the Law Enforcement

This law applies to person, legal entity and organizations, both domestic and foreign country, living and researching and operating computer system and computer's data and information in the Lao PDR.

Article 7. International Cooperation

The state opens and encourage the relations and cooperation with foreign countries, regional and international community in campaign of prevention and combating cyber crime through exchange of lessons, information, experiences, upgrade of technical knowledge and capacity building of technical staffs concerned as well as identifying and certifying data and information in accordance with international agreements and treaties, which the Lao PDR is party to.

PART II
Offences Regarding as Cyber Crime

Article 8. Offence Regarding as Cyber Crime

The Offences regarding as cyber crime are following:
1. Disclosing of Specific Computer Access Prevention Measure;
2. Unauthorized Computer Access;
3. Unauthorized Editing Picture, Animation, Audio and Video;
4. Unauthorized Interception of Computer's Data and Information;
5. Causing Damages via Online Social Media;
6. Dissemination of Pornography;
7. Computer System Interference;
8. Computer's Data and information;

## Article 9. Disclosing of Specific Computer Access Prevention Measure

Disclosing of specific computer access prevention measure is an offence taking specific computer access prevention measure to reveal without any authorization causing damage to state, person, legal entity, organization and society.

## Article 10. Unauthorized Computer Access

Unauthorized computer access is an offence applying an electronic equipment or device to access any computer having specific computer access prevention measure or steal any commercial, financing data information as well as secret confidence, other related information of person, legal entity and organization.

## Article 11. Unauthorized Editing Picture, Animation, Audio and Video

Unauthorized editing, picture, animation, audio and video is an offence of editing picture or image, adding or modifying the original version by mean of electronic process or other means in order to disseminate the outcome through computer system causing damage to state, person, legal entity and organization concerned.

## Article 12. Unauthorized Interception of Computer's Data Information

Unauthorized interception of computer's data and information is an offence of interception if computer's data and information by mean of applying any electronic equipment or device receiver is receiving, or the sender is sending, data and information via computer system.

## Article 13. Causing Damages via Online Social Media

Causing Damages via Online Social Media are offences in the action of following:
1. Posting of computer's data and information containing of context on sending, blaspheming, using impolite words through computer system;
2. Applying of violence, false, misleading and deception information into computer system;
3. Bringing the computer's data and information destroying national security, peace, order in society, national culture and fine tradition of the nation to apply into computer system;
4. Bringing the computer's data in information containing of aspects of convening, persuading and encouraging people to resist the government or separate the national solidarity;
5. Advertising of drug, weapon of war, chemical weapon selling as well as human, prostitute, prostitution trafficking and other illegal products concerned;
6. Disseminating and sending of computer's data and information prescribed in Article 11 and 14 of this law including the title number 1,2,3,4, and 5 in this Article.
Article 15. Computer System Interference

Computer system interference are offences in the actions of following:
1. Using of comport program, virus or other tools to interrupt or destroy the performance of computing;
2. Sending of computer system data and information or electronic mail message with concealing of address, source and sender or distribute and/or destroy the performance of computing.

Article 16. Computer’s Data and Information Forgery

Computer data and information forgery is an offence of using the computer, computer system and electronic equipment or device by means of action of following:
1. Intentionally inputting and changing data information, forgery of electronic address or deleting of data and information in any computer consequently causing outcome of changing from the original data and information,
2. Inputting and changing data and information of financial and commercial transaction, secrete confidence as well as other data and information of person, legal entity, organization without any authorization;
3. Developing of fake website to mislead, device other persons using computer system or internet to input data and information of bank account, credit card codes, internet usage card codes as well as the other data and information concerned.

Article 17. Destroying computer’s Data and information

Destroying Computer's data and information is an offence of deleting, editing and/or modifying of computer's data and information or data and information in computer system in order to cause data information in computer system being damage and different from original aspects.

Article 18. Operating Business of Tools and Equipments for Cyber Crime

Operating business of tools and equipment for cyber crime is an offence of developing of any new specific program, producing, importing, possessing, selling and buying, distributing, advertising, disseminating or distributing of the tools and equipment such as computer program or designing of computer's data and information for combatting any cyber crime.

PART III
Campaign of Prevention and Combating Cyber Crime

CHAPTER I
Campaign of Prevention Cyber Crime

Article 19. Campaign of prevention cyber crime

The Campaign of prevention cyber crime are activities following:
1. Warning Notice;
2. Consultation Providing;
3. Emergency Notification;
4. Incident Response.
Article 20. Warning Notice

Ministry of Post and Telecommunications is an organization issuing the notice of risk and hazardous incident occurring in computer system and internet such as the warning notice of fake website, malicious software, notification of vulnerability, misleading and deceiving via electronic mail and message and other risks concerned. Service provider of computer system must issues the warning notice and set conditions for computer access in order to limit or disallow some user categories to access.

Article 21. Consultations Providing

Sector of Post and Telecommunications is an organization providing of consultation and advice on methodology for protection and technical process dealing with risk and hazardous incident for person, legal entity and organization in order to reduce losing and interrupting of data and information, stop suspending of computer system operation, anti wide spreading of computer system operation, anti wide spreading of computer virus and accessing to destroy data and information in any computer system.

Article 22. Emergency Notification

Person, legal entity and organization, in both domestic and foreign, living involving and using of computer system and/or computer's data and information in the LAO PDR must notify the existing of emergency incident relating to cyber crime occurring in their computer system to the Sector of Postal and Telecommunication as prescribed in the Article 50 and 51 of this law. The emergency notification for general incidents should be conducted by means of following:
1. Submission of specific provided Application Form;
2. Informing via telephone, fax or hotline;
3. Sending of electronic email or message;
4. Notifying through other means.

Article 23. Incident Response

After receiving the warning notice on emergency incident relating to computer system, Ministry of Post and Telecommunication should bring it into consideration and reply with suggestion of dealing methodology to address the incident within five official working days. In case of necessary and urgent incident, Ministry of Post and Telecommunication should immediately take action technical response and addressing in accordance with the incident notification concerned. In case of receiving of incident notification relating to the acts prescribed in the Article 11 and 13 of this law affecting national security or dignity of any person, sectors concerned of both central and local levels should bring it into consideration and respond basing on situations of case by case.

Chapter II
Campaign of Combating Cyber Crime

Article 24. Campaign of Combating Cyber Crime

The campaign of combating cyber crime are activities following:
1. Organizing Dissemination;
2. Training;
3. Providing Knowledge on computer System Safety;
4. Developing of Activities for Data and Information Protection;
5. Surveillance of Emerging incident;  

**Article 25. Organizing Dissemination**

Ministry of Post and Telecommunications is an organization developing of handbook, sticker, poster, printing matter and video on surveillance, prevention of risk and hazard incident for computer system, also according with other relating sectors and local administration authorities concerned for organizing dissemination throughout nationwide.

**Article 26. Training**

Sector of Post Telecommunications should coordinate with other relating sectors and local administration authorities concerned to organize the training for officials and authorities on prevention and combating cyber crime as well as process of investigating operation.

**Article 27. Providing Knowledge on Computer System Safety**

Ministry of Post and Telecommunication is the leading organization for coordination with sector concerned to constitute the specific measure for society.

**Article 28. Developing of Activities for Data and Information Protection**

In order to secure the computer system security and protection of computer's data and information, the Sector of Post and Telecommunication and Sector of National Security, service providers as well as computer's data and information storage person should develop activities to provide knowledge and lessons on security, using of computer system for acknowledgment and awareness of techniques and methodologies to protect computer's data and information in the state organizations, private sectors and education facilities.

**Article 29. Surveillance of Emergency Incident**

Sector of Post and Telecommunications is an organization taking responsibility of surveillance of emergency incident by means of tracking, monitoring, advising, preventing and responding the risk and hazard incidents occurring in computer system.

**Article 30. Collection of Statistics**

Sector of post and Telecommunications and Sector of National Security should collect statistics and develop database system on cyber crime as well as take the responsibility of periodically searching and reviewing in order to find out the conditions and causes of cyber crime.
Chapter III
Lao Computer Emergency Response Center

**Article 31. Lao Computer Emergency Response Center**

In order to ensure the managing, monitoring, inspecting, preventing, combating, restricting and suppressing of crime, protection of database system, server system, computer's data information, and the capacity of integration with regional and interregional community; state establish the Lao Computer Emergency Response Team which is written in the abbreviation form of “Lao CERT”.

Lao computer emergency response team is an organization having role at the relevant level of department of ministry including in the organization structure of Ministry of Post and Telecommunication, having responsibility roles of chief of operation for above prescribed ministry in this article in responsibilities of preventing addressing of risk and hazard incidents for computer system.

**Article 32. Rights and Duties of Lao Computer Emergency Response team**

The Lao computer emergency response team has the following rights and duties:

1. Study and elaborate strategic plan, policies into its work plans programs and projects as well as take them into account of effective implementation;
2. Study and develop the regulations on management of campaign of prevention and combating cyber crime with submission to Ministry of Post and Telecommunications for consideration;
3. Disseminate laws and regulations regarding to campaign of prevention and combating cyber crime;
4. Develop, train and upgrade personnel working on security of computer system;
5. Oversee, track, monitor, inspect, advise, notify and respond risk and hazard incidents for computer system as assigning;
6. Receive the warning notification and reporting of cyber crime to the sector concerned;
7. Coordinate and cooperate with sectors concerned in case procedure process of cyber crime;
8. Inform the service providers, data information storage persons to provide facilities and information relating to cyber crime;
9. Carry out relations and coordination with foreign countries, regional and international community related to campaign of prevention and combating cyber crime as assigning;
10. Summarize and report on its activities regarding to campaign of prevention and combating cyber crime Ministry of Postal and Telecommunication on a regular basis;
11. Perform rights ad duties as prescribed in the laws and regulations concerned.

Part IV
International Cooperation in Campaign of Prevention and Combating Cyber Crime

**Article 33. Principle of International Cooperation**

International cooperation in campaign of prevention and combating cyber crime between organizations having authorities concerned of Lao PDR and foreign organizations should follow the principle of respecting of independence, sovereignty and territorial integrity, non-interference in each other's domestic affairs, mutual obtaining benefits and conformity with international agreements and treaties which Lao PDR is party to.

**Article 34. Technical Subjects Cooperation**

Technical subjects cooperation in campaign of prevention and combating cyber crime should be included as follow:
1. Exchanging of technical information including studying measures on prevention and combating of computer system emergency incidents;
2. Suspension or notification to stop computer system destruction;
3. Coordinating with service providers in foreign countries on using of online social media containing contents defined in the Article 12 of this law;
4. Providing mutual assistance on surveillance, combating and responding the computer system emergency incidents in any significant events such as meeting or convention of national, regional and international levels as well as other fairs and festival.

### Article 35 Mutual Legal Assistance

Move dual legal assessment shall be aimed at the request for conducting of investigation applying of counting measures issuing of ordinance for storage and protection of computers data and information as well as computer traffic data searching diagnosing and identifying of offenders sizing or confiscating equipments or tools use in and related to offences requests for additional information and evidence related to offences as well as requests to extradition the mechanism and procedures of mutual legal assistance shall follow the related laws and regulation of the law PDR international agreements and treaties which the Lao PDR is party to.

### Article 36 Content of the request for Mutual Legal Assistance

Request for mutual legal assistance shell include the following contents:
1. Purpose, necessity reason and *de facto* condition of the request;
2. any important information necessary for identifying and tracing and diagnosing of cyber crime offenders;
3. brief summarizing of computer system's data and information or computer traffic data wanting to protect and storage ;
4. legislative reference and visits of the accused and suspect;
5. Information of organization or authorities concerned for the case of asking for any additional information from the requesting state.

### Article 37 Requirement of Confidentiality

The competent authority of the Lao PDR must ensure the confidentiality of requests from the related states.

### Article 38 Request Refusal.

The competent authority of the Lao PDR may refuse the request of mutual legal assistance while the requests are not consistent with the basic principle of international cooperation defined in article 33 of this law as well as the other related the laws of the Lao PDR.

### Part 5 Prohibitions

### Article 39 General Prohibitions

Persons, legal entity and organizations are prohibited from the following behaviors:
1. Committing of offensive divine in articulate of this law;
2. Propagating to destroy or against the political regime in order to cause in trouble in society;
3. This triangle or causing damages to any electronic equipment computer and other relating facilities or exchanging and transmitting data and information to through computer system;
4. Colluding with any person to disseminate pornography content through online social media;
5. Asking requesting providing and receiving bribes;
6. Committing other activities contravening laws and regulations.

**Article 40. Prohibitionists for service Providers**

Service providers are prohibited from the following behaviors:
1. Deleting computer traffic data before ninety days in case of having connection system and three hundred sixty five days of having no connection system;
2. Deleting that and information of any user causing damages before 90 days;
3. Supplying incorrect data and information to officials and authorities concerned;
4. Disclosing of data and information of service consumers without any authorizing;
5. Providing conditions or facilitates for activities of cyber crime;
6. Committing other activities contravening laws and regulations.

**Article 41. Prohibition for Official and Competent Authorities**

Official and competent authorities are prohibited from the following:
1. Disclosing of confidential data and information of state, official affairs, person, legal entity, organization through computer system;
2. Reveal computer system access code and specific access prevention measures of their working sector;
3. Sending or transferring computer data or consumer's the data and information except the sending of transferring for the purpose of cyber crime case procedure such as implementation of ordinance so or in case of authorizing of the case procedure organization;
4. Postponing holding and falsifying emphasis documents relating to cyber crime data and information;
5. Abusing duties, functions and positions for personal, family and group of friends benefit and interests;
6. Leaving off duties and responsibilities assigned by their working organizations;
7. Committing other activities contravening laws and regulations.

**Part 6**

**Investigation of Cyber Crime Case**

**Article 42. Causes for Opening of Investigation**

Causes for opening by cyber crime case are following:
1. Having a claim, reporting or complaint of person, legal entity or organization concerning of any offense regarding cyber crime;
2. Capitulating cyber crime perpetrators;
3. Discovery of cyber crime trees evidence as well as that and information concerned for the fences prescribed in articulate in this law.

**Article 43 Process of Investigation of Cyber Crime Case**

The investigation of cybercrime cases should be conducted as follows:
1. Claiming reporting or complaining;
2. Opening investigation;
3. Conducting of investigation;
Article 44 Claiming Reporting or Complaining

The claiming, reporting or complaining and offence regarding a cyber crime shall be brought to notify or submit to the investigation organization of police or officer of public prosecutor. The organization of police or office of public prosecutors should study and consider the claiming reporting or complaining within five official working days from the day of receiving the claiming reporting or complaining. In case of having any difficulty the study and consideration. Shall not be more than ten official working days.

Article 45. Opening of Investigation

In case of having sufficient information and evidence of any fans regarding as a cyber crime, the head of investigation organization of police or public prosecutors shall issue in the ordinance of opening of investigation basing on the scope of rights and duties of the issuing thr ordinance in according to the law on criminal procedure. In case of emergency, necessity and having sufficient information and evidence providing that there is a preparation of committing of cyber crime, the head of investigation organization of police or public prosecutors shall issue an ordinance for production and storage computer’s data and information as well as computer traffic data. Service providers or sectors having duties of data and information management have obligations of protection and storage the prescribed that and information in good condition till the final process of cyber crime case procedure in order to ensure that they are not being lost or damaged.

Article 46 Conducting of Investigation

The investigation organization of police or office of public prosecutor shall coordinate with sector of post and telecommunication and other sectors concerned in order to search and trace information and evidence as well as source of cyber crime for regarding as the basis of investigation conducting. The conducting of cyber crime case investigation shall apply the investigation procedures and the prevention measures as prescribed under the law not criminal procedures.

Article 47. Summarizing of Investigation and Preparation of Case File

After completion of an investigation, in case of having sufficient information and evidence supporting that such violation easy cyber crime, the investigation organization shall conclude and summarize investigation with perpetration is cyber crime case file and then forward to the public prosecutor for consideration to submit the prosecution of the court. In case of the competent office of public prosecutor conducts the investigation, the office of the public prosecutor shall conclude and summarise the investigation with preparation a cyber crime case file and then submit the prosecution to the court.

Part VII
Management and inspection

Chapter one
Management

Article 48. Management Organization

The government is taking a official role as managing organization to centrally and uniformly manage the campaign of preventing and combating cyber crime by assigning Ministry of Post and Telecommunication to directly take responsibilities and coordinate with the National Defence Ministry, Public Security Ministry, Information, Culture and Tourism, Science and Technology as well as other ministries and local administration authorities
The management organizations of the campaign of preventing and combating cyber crime are comprised of:
1. Ministry of Post and Telecommunication;
2. Provincial and the Capital Department of Post and Telecommunication;
3. District and Municipal Offenses of Post and Telecommunication.

**Article 49. Rights and Duties of the Ministry of Post and Telecommunication**

In the management of the campaign of preventing and combating cyber crime, the Ministry of Post and Telecommunication as the following rights and duties:
1. Study, develop and strategy, policies, law on campaign of preventing and combating cyber crime to propose the government for consideration;
2. Disseminate, popularize and educate laws and regulations relating to preventing and combating cybercrime throughout nationwide;
3. Take supervising role of managing, developing, training, upgrading the knowledge, capacity and expertise of the personnel and staff working on computer system security;
4. Take leading role of surveillance, tracking, monitoring, advice, notification and responding computer system emergency incident;
5. Coordinate with other ministers, relevant organization on campaign of preventing and combating cyber crime;
6. Collaborate and cooperate with other countries, regional and international on campaign of preventing and combating cyber crime;
7. Summarize, consolidate of its activities on campaigning of preventing and combating cyber crime, then report to the government;
8. Perform other rights and duties as defined in the laws and regulations.

**Article 50. Rights and Duties of the Provincial and the Capital Department of Post and Telecommunication**

In the management of the campaign of preventing and combating cyber crime the provincial end the capital departments of post and telecommunication have the following rights and duties:
1. Disseminate, popularize and educate laws and regulations relating to preventing and combating cyber crime and bring them to implement effectively;
2. Develop plan managing, developing, training, upgrading the knowledge, capacity and expertise to the personal and stuff working on preventing and combating cyber crime and then propose the plan to upper administration authority;
3. Received the emergency notification of computer system emergency incident and report to the Lao Computer Emergency Response Team;
4. Claim and report on cyber crime offences to Provincial and the Capital Office of the Public Prosecutor;
5. Coordinate collaborate with the investigation organization and the Provincial and the Capital Office of Public Prosecutor in terms of cyber crime case procedure;
6. Notify the service providers, data and the information storage persons to facilitate and supply data and information on cyber crime;
7. Coordinate with the other provincial and the capital sector is concerned on campaign of preventing and combating cyber crime;
8. Coordinate collaborate with the Lao Computer Emergency Response Team, Ministry of Post and Telecommunications;
9. Collect data and statistic on cyber crime;
10. Collaborate and cooperate with the other countries regional and international on campaigning of preventing and combating crime in accordance with the assigning;
11. Summarize, consolidate of its activities on campaign or preventing and combating cyber crime, then report to Ministry of Post Telecommunication and the provincial and the capital administration authorities;
12. Perform on the rights and duties as defined in the laws regulations.
Article 51 Rights and Duties of the District and Municipal Offices of Post and Telecommunication.

In the management of the campaign of preventing and combating cyber crime the district and municipal offices of Boston telecommunication have the following rights and duties:
1. Disseminate and popularize police, strategic plans, laws and regulations relating to preventing and combating cyber crime and bringing them to implement effectively;
2. Develop plan managing, developing, training, upgrading the knowledge, capacity and expertise to the personal and staff working on preventing and combating cyber crime and then purpose they plan to upper administration authority;
3. Receive them urgency notification of computer system emergency incident and report to the Provincial and the Capital Department of Post and Telecommunication of reporting to the Lao Computer Emergency Response Team;
4. Claim and report on cyber crime offenses to the investigation organization or the Regional Office of Public Prosecutor;
5. Coordinate collaborate with investigation organization and the Region Office of Public Prosecutor in terms of cyber crime case procedure;
6. Coordinate with the other district and municipal offenses on campaign of preventing and combating cyber crime;
7. Collect data insert cyber crime;
8. summarize consolidate of its activities on campaign of preventing and combating cyber crime, then report to Provincial and the capital department of Post and Telecommunication and district municipal administration authorities;
9. Perform other rights and duties as defined in the laws and regulations.

Article 52. Rights and Duties of Other Sectors and Local Administration Authority Concerned

In the management of the campaign of preventing and convening cyber crime, the other sectors and local administration authority concerned such as sectors of national defense, public security, information, culture and tourism, science and technology and local administration authorities concerned have rights and duties of participation, collaboration on prevention and combating cyber crime with reporting and supplying of data and information on the existing cyber crime in accordance with respective scope of responsibilities.

Chapter 2
Inspection

Article 53. Inspection Authorities

Inspection authorities for the campaign of preventing and combating cyber crime shall include the following:
1. Internal inspection authorities which are the same organizations of management organization as defined in article 48 of this law;
2. External inspection authorities which are the National Assembly, State Audit Authority, Governmental Inspection and Anti-Corruption Authority, Lao Front for National Construction and Mass Organizations.

Article 54. Contents of Inspection

The content of his passion of the campaign of preventing and combating cyber crime include:
1. The implementation of policies strategic plan laws and regulations on the campaign of preventing and combating cyber crime;
2. Organization and activities of the campaign of preventing and combating cyber crime;
3. The implementation of international agreements and treaties which the Lao PDR is party to.
Article 55. Forms of Inspection

These factions should be conducting in the forms as follows:
. Regular inspection;
. Inspection of their notification;
. Emergency section.

Regular inspection is an inspection that follows the regular plan with certain timeframe or schedule.
Inspection of their notification is an inspection that is not included in the plan but it shall be carried out by informing their audited person in advance.
Emergency inspection is an urgent inspection without any performing the inspected person in advance.
The operation and conducting of each defined inspection shall comply with laws and regulations strictly.
1950 EVIDENCE ACT
(Incorporating all amendments up to 1 January 2006)

PART I RELEVANCY
CHAPTER I PRELIMINARY

Interpretation

3. In this Act, unless the context otherwise requires—“computer” means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

...) “court” means a court established by or under Part IX of the Federal Constitution and includes—

a) a Judge;
b) a Sessions Court Judge;
c) a Magistrate; and

d) except an arbitrator, every person legally authorized to take evidence;

document” means any matter expressed, described, or howsoever represented, upon any substance, material, thing or article, including any matter embodied in a disc, tape, film, sound-track or other device whatsoever, by means of—

a) letters, figures, marks, symbols, signals, signs, or other forms of expression, description, or representation whatsoever;
b) any visual recording (whether of still or moving images);
c) any sound recording, or any electronic, magnetic, mechanical or other recording whatsoever and howsoever made, or any sounds, electronic impulses, or other data whatsoever;
d) a recording, or transmission, over a distance of any matter by any, or any combination, of the means mentioned in paragraph (a), (b) or (c), or by more than one of the means mentioned in paragraphs (a), (b), (c) and (d), intended to be used or which may be used for the purpose of expressing, describing, or howsoever representing, that matter.

Illustrations
A writing is a document. Words printed, lithographed or photographed are documents. A map, plan, graph or sketch is a document. An inscription on wood, metal, stone or any other substance, material or thing is a document. A drawing, painting, picture or caricature is a document. A photograph or a negative is a document. A tape recording of a telephonic communication, including a recording of such communication transmitted over distance, is a document. A photographic or other visual recording, including a recording of a photographic or other visual transmission over a distance, is a document. A matter recorded, stored, processed, retrieved or produced by a computer is a document;

evidence” includes—

a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence; (b) all documents produced for the inspection of the court:

uch documents are called documentary evidence;

...
CHAPTER V - DOCUMENTARY EVIDENCE

61. Proof of contents of documents

The contents of documents may be proved either by primary or by secondary evidence.

62. Primary evidence

Primary evidence means the document itself produced for the inspection of the court.

Explanation 1—Where a document is executed in several parts, each part is primary evidence of the document. Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, each counterpart is primary evidence as against the parties executing it. Explanation 2—Where a number of documents are all made by one uniform process, as in the case of printing, lithography or photography, each is primary evidence of the contents of the rest; but where they are all copies of a common original they are not primary evidence of the contents of the original. Explanation 3—A document produced by a computer is primary evidence.

ILLUSTRATIONS
A person is shown to have been in possession of a number of placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original.

63. Secondary evidence

Secondary evidence includes— (a) certified copies given under the provisions hereinafter contained; (b) copies made from the original by mechanical processes, which in themselves ensure the accuracy of the copy, and copies compared with such copies; (c) copies made from or compared with the original; (d) counterparts of documents as against the parties who did not execute them; (e) oral accounts of the contents of a document given by some person who has himself seen or heard it or perceived it by whatever means.

ILLUSTRATIONS
(a) A photograph of an original is secondary evidence of its contents, though the two have not been compared, if it is proved that the thing photographed was the original. (b) A copy compared with a copy of a letter made by a copying machine is secondary evidence of the contents of the letter if it is shown that the copy made by the copying machine was made from the original. (c) A copy transcribed from a copy but afterwards compared with the original is secondary evidence, but the copy not so compared is not secondary evidence of the original, although the copy from which it was transcribed was compared with the original. (d) Neither an oral account of a copy compared with the original nor an oral account of a photograph or machine copy of the original is secondary evidence of the original.

64. Proof of documents by primary evidence

Documents must be proved by primary evidence except in the cases hereinafter mentioned.

65. Cases in which secondary evidence relating to documents may be given

(1) Secondary evidence may be given of the existence, condition or contents of a document admissible in evidence in the following cases:
   a) when the original is shown or appears to be in the possession or power—
      i) of the person against whom the document is sought to be proved;
      ii) of any person out of reach of or not subject to the process of the court; or
      iii) of any person legally bound to produce it, and when after the notice mentioned in section 66 such person does not produce it;
b) when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;
c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot for any other reason not arising from his own default or neglect produce it in reasonable time;
d) when the original is of such a nature as not to be easily movable;
e) when the original is a public document within the meaning of section 74;
f) when the original is a document of which a certified copy is permitted by this Act or by any other law in force for the time being in Malaysia to be given in evidence;
g) when the originals consist of numerous accounts or other documents which cannot conveniently be examined in court, and the fact to be proved is the general result of the whole collection.

2) (a) In the cases referred to in paragraphs (1)(a), (c) and (d) any secondary evidence of the contents of the document is admissible.
b) In the case referred to in paragraph (1)(b) the written admission is admissible.
c) In the case referred to in paragraph (1)(e) or (f) a certified copy of the document but no other kind of secondary evidence is admissible.
d) In the case referred to in paragraph (1)(g) evidence may be given as to the general result of the documents by any person who has examined them and who is skilled in the examination of such documents.

66. Rules as to notice to produce

Secondary evidence of the contents of the documents referred to in paragraph 65(1)(a) shall not be given unless the party proposing to give such secondary evidence has previously given to the party in whose possession or power the document is, or to his advocate, such notice to produce it as is prescribed by law; and if no notice is prescribed by law, then such notice as the court considers reasonable under the circumstances of the case: Provided that such notice shall not be required in order to render secondary evidence admissible in any of the following cases or in any other case in which the court thinks fit to dispense with it:
a) when the document to be proved is itself a notice;
b) when from the nature of the case the adverse party must know that he will be required to produce it;
c) when it appears or is proved that the adverse party has obtained possession of the original by fraud or force;
d) when the adverse party or his agent has the original in court;
e) when the adverse party or his agent has admitted the loss of the document; or
f) when the person in possession of the document is out of reach of or not subject to the process of the court.

67. Proof of signature and handwriting of person alleged to have signed or written document produced

If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting shall be proved to be in his handwriting.

68. Proof of execution of document required by law to be attested

If a document is required by law to be attested, it shall not be used as evidence until one attesting witness at least has been called for the purpose of proving its execution, if there is an attesting witness alive and subject to the process of the court and capable of giving evidence.

69. Proof where no attesting witness found

If no such attesting witness can be found, or if the document purports to have been executed in the United Kingdom, it must be proved that the attestation of one attesting witness at least is in his handwriting, and that the signature of the person executing the document is in the handwriting of that person.
70. Admission of execution by party to attested document

The admission of a party to an attested document of its execution by himself shall be sufficient proof of its execution as against him, though it is a document required by law to be attested.

71. Proof when attesting witness denies the execution

If the attesting witness denies or does not recollect the execution of the document, its execution may be proved by other evidence.

72. Proof of document not required by law to be attested

An attested document not required by law to be attested may be proved as if it was unattested.

73. Comparison of signature, writing or seal with others admitted or proved

(1) In order to ascertain whether a signature, writing or seal is that of the person by whom it purports to have been written or made, any signature, writing or seal, admitted or proved to the satisfaction of the court to have been written or made by that person, may be compared by a witness or by the court with the one which is to be proved, although that signature, writing or seal has not been produced or proved for any other purpose. (2) The court may direct any person present in court to write any words or figures for the purpose of enabling the court to compare the words or figures so written with any words or figures alleged to have been written by that person. (3) This section applies also, with any necessary modifications, to finger impressions.

73A. Admissibility of documentary evidence in civil cases, etc.

(1) Notwithstanding anything contained in this Chapter, in any civil proceedings where direct oral evidence of a fact would be admissible, any statement made by a person in a document and tending to establish that fact shall, on production of the original document, be admissible as evidence of that fact if the following conditions are satisfied:
   a) if the maker of the statement either—
      i) had personal knowledge of the matters dealt with by the statement; or
      ii) where the document in question is or forms part of a record purporting to be a continuous record, made the statement (so far as the matters dealt with thereby are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had, or might reasonably be supposed to have had, personal knowledge of those matters; and
   b) if the maker of the statement is called as a witness in the proceedings: Provided that the condition that the maker of the statement shall be called as a witness need not be satisfied if he is dead, or unfit by reason of his bodily or mental condition to attend as a witness, or if he is beyond the seas and it is not reasonably practicable to secure his attendance, or if all reasonable efforts to find him have been made without success.

2) In any civil proceedings, the court may at any stage of the proceedings, if having regard to all the circumstances of the case it is satisfied that undue delay or expense would otherwise be caused, order that such a statement as is mentioned in subsection (1) shall be admissible as evidence or may, without any such order having been made, admit such a statement in evidence—
   a) notwithstanding that the maker of the statement is available but is not called as a witness; and
   b) notwithstanding that the original document is not produced, if, in lieu thereof, there is produced a copy of the original document or of the material part thereof certified to be a true copy in such manner as may be specified in the order or as the court may approve, as the case may be.

3) Nothing in this section shall render admissible as evidence any statement made by a person interested at a time when proceedings were pending or anticipated, involving a dispute as to any fact which the statement might tend to establish.
4) For the purposes of this section, a statement in a document shall not be deemed to have been made by a person unless the document, or the material part thereof, was written, made or produced by him with his own hand, or was signed or initialled by him, or otherwise recognized by him in writing as one for the accuracy of which he is responsible.

5) For the purpose of deciding whether or not a statement is admissible as evidence by virtue of subsections (1) to (4), the court may draw any reasonable inference from the form or contents of the document in which the statement is contained, or from any other circumstances, and may, in deciding whether or not a person is fit to attend as a witness, act on a certificate purporting to be the certificate of a registered medical practitioner, and, where the proceedings are with assessors, the court may in its discretion reject the statement notwithstanding that the requirements of this section are satisfied with respect thereto, if for any reason, it appears to it to be inexpedient in the interests of justice that the statement should be admitted.

6) In estimating the weight, if any, to be attached to a statement rendered admissible as evidence by this Act, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement, and, in particular, to the question whether or not the statement was made contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not the maker of the statement had any incentive to conceal or misrepresent facts.

7) For the purpose of any rule of law or practice requiring evidence to be corroborated, or regulating the manner in which uncorroborated evidence is to be treated, a statement rendered admissible as evidence by this Act shall not be treated as corroboration of evidence given by the maker of the statement.

### Public Documents

#### 74. Public documents

The following documents are public documents: (a) documents forming the acts or records of the acts of— (i) the sovereign authority; (ii) official bodies and tribunals; and (iii) public officers, legislative, judicial and executive, whether Federal or State or of any other part of the Commonwealth or of a foreign country; and (b) public records kept in Malaysia of private documents.

#### 75. Private documents

All documents other than those mentioned in section 74 are private.

#### 76. Certified copies of public documents

Every public officer having the custody of a public document which any person has a right to inspect shall give that person on demand a copy of it on payment of the legal fees therefor, together with a certificate, written at the foot of the copy, that it is a true copy of the document or part thereof, as the case may be, and the certificate shall be dated and subscribed by the officer with his name and his official title, and shall be sealed whenever the officer is authorized by law to make use of a seal, and the copies so certified shall be called certified copies. Explanation—Any officer who by the ordinary course of official duty is authorized to deliver the copies shall be deemed to have the custody of the documents within the meaning of this section.

#### 77. Proof of documents by production of certified copies

Copies certified in the manner set out in section 76 may be produced in proof of the contents of the public documents or parts of the public documents of which they purport to be copies.
78. Proof of certain official documents

(1) The following public documents may be proved as follows:
   a) acts, orders or notifications of the Government of Malaysia or of any State in any of its departments—
      i) by the records of the departments certified by the heads of those departments respectively; (ii) by a Minister
         in the case of the Government of Malaysia, and by the Chief Minister, a State Minister (if any), the State Secretary
         or the Permanent Secretary to the Chief Minister in the case of a State Government; or
      iii) by any document purporting to be printed by the authority of the Government concerned; (b) the proceed-
   b) ings of Parliament or of any of the federal legislatures that existed in Malaysia before Parliament was consti-
   tuted or of the legislature of any State— by the minutes of the body or by the published Acts of Parliament,
   Ordinances, Enactments or abstracts or by copies purporting to be printed by the authority of the Government
   concerned;
   c) proclamations, orders or regulations issued by the Crown in the United Kingdom or by the Privy Council or
      by any Minister or department of the Crown— by copies or extracts contained in the London Gazette or in the
      Gazette or in any State Gazette or purporting to be printed by Her Britannic Majesty's Printer;
   d) the acts of the Executive or the proceedings of the legislature of a foreign country— by journals published by
      their authority or commonly received in that country as such, by a copy certified under the seal of the country or
      sovereign or by a recognition thereof in some Act, Ordinance or Enactment of Malaysia or of any State;
   e) the proceedings of a municipal body, town board or other local authority in Malaysia— by a copy of the pro-
      ceedings certified by the lawful keeper thereof, or by a printed book purporting to be published by the authority
      of that body;
   f) public documents of any other class in a foreign country— by the original or by a copy certified by the lawful
      keeper thereof, with a certificate under the seal of a notary public or of a consular officer of Malaysia that the
      copy is duly certified by the officer having the lawful custody of the original and upon proof of the character of
      the document according to the law of the foreign country.

2) Copies of Acts, Ordinances and Statutes passed by the legislature of any part of the Commonwealth and of
   orders, regulations and other instruments issued or made under the authority of any such Act, Ordinance or
   Statute, if purporting to be printed by the Government Printer, shall be received in evidence by all courts in Ma-

3) In this section “Government Printer” means, as respects any part of the Commonwealth, the printer purport-
   ing to be the printer authorized to print the Acts, Ordinances or Statutes of the legislature of that territory, or
   otherwise to be the Government Printer of that territory.

78A. Proof of public documents produced by computers

Notwithstanding anything contained in sections 77 and 78, the provisions of sections 90A, 90B and 90C shall ap-

79. Presumption as to genuineness of certified copies

(1) The court shall presume to be genuine every document purporting to be a certificate, certified copy or other
   document which is by law declared to be admissible as evidence of any particular fact, and which purports to be
   duly certified by any officer in Malaysia who is duly authorized thereto: Provided that the document is substan-
   tially in the form and purports to be executed in the manner directed by law in that behalf.

2) The court shall also presume that any officer by whom any such document purports to be signed or certified
   held, when he signed it, the official character which he claims in the document.

80. Presumption as to documents produced as record of evidence

Whenever any document is produced before any court purporting to be a record or memorandum of the evi-

dence or of any part of the evidence given by a witness in a judicial proceeding or before any officer authorized
by law to take such evidence, or to be a statement or confession by any prisoner or accused person, taken in accordance with law and purporting to be signed by any Judge, Sessions Court Judge or Magistrate or by any such officer as aforesaid, the court shall presume that—

a) the document is genuine;
b) any statements as to the circumstances under which it was taken, purporting to be made by the person signing it, are true; and

c) such evidence, statement or confession was duly taken.

81. Presumption as to Gazettes, newspapers, etc.

The court shall presume the genuineness of every document purporting to be the Gazette, a State Gazette or the London Gazette, or the Government Gazette of any part of the Commonwealth, or to be the Gazette issued by the local Government of any part of the Commonwealth, or to be a newspaper or journal, or to be a copy of a private Act of Parliament printed by Her Britannic Majesty's Printer, and of every document purporting to be a document directed by any law to be kept by any person, if the document is kept substantially in the form required by law and is produced from proper custody.

Explanation—see explanation to section 90.

82. Presumption as to document admissible in England without proof of seal or signature

When any document is produced before any court, purporting to be a document which by the law in force for the time being in England or Northern Ireland would be admissible in proof of any particular in any Court of Justice in England or Northern Ireland, without proof of the seal or stamp or signature authenticating it, or of the judicial or official character claimed by the person by whom it purports to be signed—

a) the court shall presume that such seal, stamp or signature is genuine, and that the person signing it held at the time when he signed it the judicial or official character which he claims;
b) the document shall be admissible for the same purpose for which it would be admissible in England or Northern Ireland.

83. Presumption as to maps or plans made by authority of Government

(1) The court shall presume that maps or plans purporting to be made by the authority of the Government of Malaysia or the Government of any State were so made and are accurate.

84. Presumption as to collections of laws and reports of decisions

The court shall presume the genuineness of every book purporting—

a) to be printed or published under the authority of the Government of any country and to contain any of the laws of that country; or
b) to contain reports of decisions of the courts of that country.

85. Presumption as to powers of attorney

The court shall presume that every document purporting to be a power of attorney, and to have been executed before and authenticated by a Notary Public or Commissioner for Oaths, or any court, Judge, Magistrate, or consular officer of Malaysia was so executed and authenticated.
86. Presumption as to certified copies of foreign judicial records

The court may presume that any document purporting to be a certified copy of any judicial record of any country not being a part of the Commonwealth is genuine and accurate if the document purports to be certified in any manner which is certified by any representative of the Yang di-Pertuan Agong in or for such country to be the manner commonly in use in that country for the certification of copies of judicial records.

87. Presumption as to books, maps and charts

The court may presume that any book to which it may refer for information on matters of public or general interest, and that any published map or chart the statements of which are relevant facts and which is produced for its inspection, was written and published by the person and at the time and place by whom or at which it purports to have been written or published.

88. Presumption as to telegraphic messages

The court may presume that a message forwarded from a telegraph office to the person to whom it purports to be addressed corresponds with a message delivered for transmission at the office from which the message purports to be sent; but the court shall not make any presumption as to the person by whom the message was delivered for transmission.

89. Presumption as to due execution, etc., of documents not produced

The court shall presume that every document called for and not produced, after notice to produce given under section 66, was attested, stamped and executed in the manner required by law.

90. Presumption as to documents twenty years old

Where any document purporting or proved to be twenty years old is produced from any custody which the court in the particular case considers proper, the court may presume that the signature and every other part of that document which purports to be in the handwriting of any particular person is in that person's handwriting, and in the case of a document executed or attested, that it was duly executed and attested by the persons by whom it purports to be executed and attested. Explanation—Documents are said to be in proper custody if they are in the place in which and under the care of the person with whom they would naturally be; but no custody is improper if it is proved to have had a legitimate origin, or if the circumstances of the particular case are such as to render such an origin probable.

His explanation applies also to section 81.

ILLUSTRATION

a) A has been in possession of landed property for a long time. He produces from his custody documents relating to the land, showing his title to it. The custody is proper.
b) A produces documents relating to landed property of which he is the chargee. The chargor is in possession. The custody is proper.
c) A, a connection of B, produces documents relating to lands in B's possession, which were deposited with him by B for safe custody. The custody is proper.
90A. Admissibility of documents produced by computers, and of statements contained therein

(1) In any criminal or civil proceeding a document produced by a computer, or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.

2) For the purposes of this section it may be proved that a document was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who either before or after the production of the document by the computer is responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.

3) (a) It shall be sufficient, in a certificate given under subsection (2), for a matter to be stated to the best of the knowledge and belief of the person stating it.

b) A certificate given under subsection (2) shall be admissible in evidence as prima facie proof of all matters stated in it without proof of signature of the person who gave the certificate.

4) Where a certificate is given under subsection (2), it shall be presumed that the computer referred to in the certificate was in good working order and was operating properly in all respects throughout the material part of the period during which the document was produced.

5) A document shall be deemed to have been produced by a computer whether it was produced by it directly or by means of any appropriate equipment, and whether or not there was any direct or indirect human intervention.

6) A document produced by a computer, or a statement contained in such document, shall be admissible in evidence whether or not it was produced by the computer after the commencement of the criminal or civil proceeding or after the commencement of any investigation or inquiry in relation to the criminal or civil proceeding or such investigation or inquiry, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.

7) Notwithstanding anything contained in this section, a document produced by a computer, or a statement contained in such document, shall not be admissible in evidence in any criminal proceeding, where it is given in evidence by or on behalf of the person who was— (a) responsible for the management of the operation of that computer or for the conduct of the activities for which that computer was used; or

b) in any manner or to any extent involved, directly or indirectly, in the production of the document by the computer.

90B. Weight to be attached to document, or statement contained in document, admitted by virtue of section 90A

In estimating the weight, if any, to be attached to a document, or a statement contained in a document, admitted by virtue of section 90A, the court—

a) may draw any reasonable inference from circumstances relating to the document or the statement, including the manner and purpose of its creation, or its accuracy or otherwise:

b) shall have regard to—

i) the interval of time between the occurrence or existence of the facts stated in the document or statement, and the supply of the relevant information or matter into the computer; and

ii) whether or not the person who supplies, or any person concerned with the supply of, such information or the custody of the document, or the document containing the statement, had any incentive to conceal or misrepresent all or any of the facts stated in the document or statement.

90C. Sections 90A and 90B to prevail over other provisions of this Act, the Bankers’ Books (Evidence) Act 1949, and any written law

The provisions of sections 90A and 90B shall prevail and have full force and effect notwithstanding anything inconsistent therewith, or contrary thereto, contained in any other provision of this Act, or in the Bankers’ Books
(Evidence) Act 1949 [Act 33], or in any provision of any written law relating to certification, production or extraction of documents or in any rule of law or practice relating to production, admission, or proof, of evidence in any criminal or civil proceeding.

CHAPTER VA- ADMISSIBILITY OF EVIDENCE OBTAINED UNDER MUTUAL ASSISTANCE IN CRIMINAL MATTERS REQUESTS
CHAPTER VI - EXCLUSION OF ORAL BY DOCUMENTARY EVIDENCE

91. Evidence of terms of contracts, grants and other dispositions of property reduced to form of document

When the terms of a contract or of a grant or of any other disposition of property have been reduced by or by consent of the parties to the form of a document, and in all cases in which any matter is required by law to be reduced to the form of a document, no evidence shall be given in proof of the terms of the contract, grant or other disposition of property or of the matter except the document itself, or secondary evidence of its contents in cases in which secondary evidence is admissible under the provisions hereinafter contained.

Exception 1—When a public officer is required by law to be appointed in writing, and when it is shown that any particular person has acted as such officer, the writing by which he is appointed need not be proved.

Exception 2—Wills admitted to probate in Malaysia may be proved by the probate. Explanation 1—This section applies equally to cases in which the contracts, grants or dispositions of property referred to are contained in one document and to cases in which they are contained in more documents than one.

Explanation 2—Where there are more originals than one, one original only need be proved. Explanation 3—The statement in any document whatever of a fact, other than the facts referred to in this section, shall not preclude the admission of oral evidence as to the same fact.

ILLUSTRATION

a) If a contract is contained in several letters, all the letters in which it is contained must be proved.
b) If a contract is contained in a bill of exchange, the bill of exchange must be proved.
c) If a bill of exchange is drawn in a set of three, one only need be proved.
d) A contracts in writing with B for the delivery of pepper upon certain terms. The contract mentions the fact that B had paid A the price of other pepper contracted for verbally on another occasion. Oral evidence is offered that no payment was made for the other pepper. The evidence is admissible.
e) A gives B a receipt for money paid by B. Oral evidence is offered of the payment. The evidence is admissible.

92. Exclusion of evidence of oral agreement

When the terms of any such contract, grant or other disposition of property, or any matter required by law to be reduced to the form of a document, have been proved according to section 91, no evidence of any oral agreement or statement shall be admitted as between the parties to any such instrument or their representatives for the purpose of contradicting, varying, adding to, or subtracting from its terms:

Provided that—

a) any fact may be proved which would invalidate any document or which would entitle any person to any decree or order relating thereto, such as fraud, intimidation, illegality, want of due execution, want of capacity in any contracting party, the fact that it is wrongly dated, want or failure of consideration, or mistake in fact or law;
b) the existence of any separate oral agreement, as to any matter on which a document is silent and which is not inconsistent with its terms, may be proved, and in considering whether or not this proviso applies, the court shall have regard to the degree of formality of the document;
c) the existence of any separate oral agreement constituting a condition precedent to the attaching of any obligation under any such contract, grant or disposition of property, may be proved;
d) the existence of any distinct subsequent oral agreement, to rescind or modify any such contract, grant or disposition of property, may be proved except in cases in which the contract, grant or disposition of property is by law required to be in writing, or has been registered according to the law in force for the time being as to the registration of documents;
e) any usage or custom by which incidents not expressly mentioned in any contract are usually annexed to contracts of that description may be proved if the annexing of any such incident would not be repugnant to or inconsistent with the express terms of the contract; and
f) any fact may be proved which shows in what manner the language of a document is related to existing facts.

**ILLUSTRATION**

a) A policy of insurance is effected on goods “in ships from Penang to London.” The goods are shipped in a particular ship, which is lost. The fact that that particular ship was orally excepted from the policy cannot be proved.

b) fact that at the same time an oral agreement was made that the money should not be paid till 31 March cannot be proved.

c) An estate called “the Kranji Tea Estate” is sold by a document which contains a map of the property sold. The fact that land not included in the map had always been regarded as part of the estate and was meant to pass by the document cannot be proved.

d) A enters into a written contract with B to work certain mines, the property of B, upon certain terms. A was induced to do so by a misrepresentation of B as to their value. This fact may be proved.

e) A institutes a suit against B for the specific performance of a contract, and also prays that the contract may be reformed as to one of its provisions on the ground that that provision was inserted in it by mistake. A may prove that such a mistake was made as would by law entitle him to have the contract reformed.

f) A orders goods of B by a letter in which nothing is said as to the time of payment, and accepts the goods on delivery. B sues A for the price. A may show that the goods were supplied on credit for a term still unexpired.

g) A sells B a horse and verbally warrants him sound. A gives B a paper in these words: “ Bought of A a horse for RM300.” B may prove the verbal warranty.

h) A hires lodgings of B and gives B a card on which is written: “Rooms RM80 a month.” A may prove a verbal agreement that these terms were to include partial board. A hires lodgings of B for a year, and a regularly stamped agreement drawn up by an attorney is made between them. It is silent on the subject of board. A may not prove that board was included in the terms verbally.

i) A applies to B for a debt due to A by sending a receipt for the money. B keeps the receipt and does not send the money. In a suit for the amount A may prove this.

j) A and B make a contract in writing to take effect upon the happening of a certain contingency. The writing is left with B, who sues A upon it. A may show the circumstances under which it was delivered

93. **Exclusion of evidence to explain or amend ambiguous document**

When the language used in a document is on its face ambiguous or defective, evidence may not be given of facts which would show its meaning or supply its defects.

**ILLUSTRATION**

a) A agrees in writing to sell a horse to B for RM500 or RM600. Evidence cannot be given to show which price was to be given.

b) A document contains blanks. Evidence cannot be given of facts which would show how they were meant to be filled.

94. **Exclusion of evidence against application of document to existing facts**

When language used in a document is plain in itself and when it applies accurately to existing facts, evidence may not be given to show that it was not meant to apply to such facts.

**ILLUSTRATION**

A conveys to B by memorandum of transfer “my estate at Kranji containing 100 acres.” A has an estate at Kranji containing 100 acres. Evidence may not be given of the fact that the estate meant was one situated at a different place and of a different size.

95. **Evidence as to document unmeaning in reference to existing facts**

When language used in a document is plain in itself, but is unmeaning in reference to existing facts, evidence may be given to show that it was used in a peculiar sense.

**ILLUSTRATION**

A conveys to B by memorandum of transfer “my plantation in Penang.” A had no plantation in Penang, but it appears that he had a plantation in Province Wellesley of which B had been in possession since the execution of the memorandum. These facts may be proved to show that the memorandum related to the plantation in Province Wellesley.
96. Evidence as to application of language which can apply to one only of several persons

When the facts are such that the language used might have been meant to apply to any one, and could not have been meant to apply to more than one of several persons or things, evidence may be given of facts which show to which of those persons or things it was intended to apply.

ILLUSTRATION
a) A agrees to sell to B for RM500 “my white horse.” A has two white horses. Evidence may be given of facts which show which of them was meant.
b) A agrees to accompany B to Halifax. Evidence may be given of facts showing whether Halifax in Yorkshire or Halifax in Nova Scotia was meant.

97. Evidence as to application of language to one of two sets of facts to neither of which the whole correctly applies

When the language used applies partly to one set of existing facts and partly to another set of existing facts, but the whole of it does not apply correctly to either, evidence may be given to show to which of the two it was meant to apply.

ILLUSTRATION
A agrees to sell to B “my land at X in the occupation of Y.” A has land at X, but not in the occupation of Y, and he has land in the occupation of Y, but it is not at X. Evidence may be given of facts showing which he meant to sell.

98. Evidence as to meaning of illegible characters, etc.

Evidence may be given to show the meaning of illegible or not commonly intelligible characters, of foreign, obsolete, technical, local and provincial expressions, of abbreviations and of words used in a peculiar sense.

ILLUSTRATION
A, a sculptor, agrees to sell to B, “all my mods.” A has both models and modelling tools. Evidence may be given to show which he meant to sell.

99. Who may give evidence of agreement varying terms of document

Persons who are not parties to a document or their representatives in interest may give evidence of any facts tending to show a contemporaneous agreement varying the terms of the document.

ILLUSTRATION
A and B make a contract in writing that B shall sell A certain tin to be paid for on delivery. At the same time they make an oral agreement that three months' credit shall be given to A. This could not be shown as between A and B, but it might be shown by C if it affected his interests.
munications and Multimedia Act 1998 [Act 588]; and
b) “publication” means a statement or a representation, whether in written, printed, pictorial, film, graphical, acoustic or other form displayed on the screen of a computer.

CHAPTER XI - IMPROPER ADMISSION AND REJECTION OF EVIDENCE

No new trial for improper admission or rejection of evidence

167. The improper admission or rejection of evidence shall not be ground of itself for a new trial or reversal of any decision in any case if it appears to the court before which the objection is raised that, independently of the evidence objected to and admitted, there was sufficient evidence to justify the decision, or that, if the rejected evidence had been received, it ought not to have varied the decision.

1960 INTERNAL SECURITY ACT

(Incorporating all amendments up to 1 January 2006)

PART I PRELIMINARY

Interpretation

2. In this Act, unless the context otherwise requires—

...)
terrorist” means any person who—
a) by the use of any firearm, explosive or ammunition acts in a manner prejudicial to the public safety or to the maintenance of public order or incites to violence or counsels disobedience to the law or to any lawful order;
b) carries or has in his possession or under his control any firearm, ammunition or explosive without lawful authority therefor; or
c) demands, collects or receives any supplies for the use of any person who intends or is about to act, or has recently acted, in a manner prejudicial to public safety or the maintenance of public order.

PART II GENERAL PROVISIONS RELATING TO INTERNAL SECURITY

CHAPTER I Prohibition of Organizations and Associations of a Political or Quasi-Military Character and Uniforms, etc.

Prohibition of quasi-military organisations

5. (1) If the members or adherents of any association of persons, whether incorporated or not, are—
a) organized or trained or equipped for the purpose of enabling them to be employed in usurping the functions of the police or of the armed forces; or
b) organized or trained or equipped either for the purpose of enabling them to be employed for the use or display of physical force in promoting any political or other object, or in such a manner as to arouse reasonable apprehension that they are organized or trained or equipped for that purpose,

4) In any criminal or civil proceeding under this section proof of things done or of words written, spoken or published (whether or not in the presence of any party to the proceedings) by any person taking part in the control or management of an association or in organising, training or equipping members or adherents of an association shall be admissible as evidence of the purposes for which, or the manner in which, members or adherents of the association were organized or trained or equipped.

5) If a Magistrate or Chief Police Officer is satisfied by information that there is reasonable ground for suspect-
ing that an offence under this section has been committed, and that evidence of the commission thereof is to be found at any premises or place specified in the information, he may, on an application made by a police officer not below the rank of Inspector, grant a search warrant authorizing any such officer with or without assistance to enter the premises or place at any time within one month from the date of the warrant, if necessary by force, and to search the premises or place and every person found therein, and to seize anything found on the premises or place or on any such person which the officer has reasonable ground for suspecting to be evidence of the commission of such an offence as aforesaid.

Chapter III Special Powers Relating to Subversive Publications, etc

Powers of search and seizure of documents

30. (1) Any police officer not below the rank of Inspector may, without warrant and with or without assistance—
a) enter and search any premises; or 
b) stop and search any vehicle, vessel, train, aircraft or individual, whether in a public place or not, if he suspects that any document, publication, material or article being evidence of the commission of an offence against this Chapter is likely to be found in that vehicle, vessel, train, aircraft or on that individual, and may seize any document, publication, material or article so found.

CHAPTER IV Control of Entertainments and Exhibitions

Powers of seizure

38. Any officer or person authorized to exercise the powers of entry or investigation under section 36 may seize any document or other thing in respect of which he reasonably believes an offence to have been committed under this Chapter or any order made thereunder or which he reasonably believes to be or to contain evidence relating to such an offence: Provided that nothing in this section shall be deemed to affect the powers of a police officer under the Criminal Procedure Code [Act 593].

PART III SPECIAL PROVISIONS RELATING TO SECURITY AREAS

CHAPTER IV Powers of Police and Others

Powers of search

65. (1) When on duty any police officer or any member of the security forces or any person who is authorized in writing so to do by the Officer in Charge of a Police District, may without warrant and with or without assistance stop and search any vehicle, vessel, train, aircraft or individual, whether in a public place or not, if he suspects that any article or material being evidence of the commission of an offence against this Part is likely to be found in the vehicle, vessel, train, aircraft or on the individual, and may seize any article or material so found.
2) When on duty any police officer of or above the rank of Corporal or any member of the security forces of or above the rating or rank of leading rate or non-commissioned officer, as the case may be, or any person authorized in writing so to do by the Officer in Charge of a Police District may without warrant and with or without assistance enter and search any premises or place if he suspects that any article or material being evidence of the commission of any offence against this Part is likely to be found on the premises or place and may seize any article or material so found.
3) No woman shall be searched under this section except by a woman.
Part IV. – MISCELLANEOUS PROVISIONS

75. Admission of statements in evidence

75. Where any person is charged with any offence against this Act or against any written law for the time being specified in the Second Schedule any statement, whether the statement amounts to a confession or not or is oral or in writing, made at any time, whether before or after the person is charged and whether in the course of a police investigation or not and whether or not wholly or partly in answer to questions, by the person to or in the hearing of any police officer of or above the rank of Inspector and whether or not interpreted to him by any other police officer or any other person concerned, or not, in the arrest, shall notwithstanding anything to the contrary contained in any written law, be admissible at his trial in evidence and, if the person tenders himself as a witness, any such statement may be used in cross-examination and for the purpose of impeaching his credit:

Provided that—

a) no such statement shall be admissible or used as aforesaid—

i) if the making of the statement appears to the court to have been caused by any inducement, threat or promise having reference to the charge against such person, proceeding from a person in authority and sufficient in the opinion of the court to give such person grounds which would appear to him reasonable for supposing that by making it he would gain any advantage or avoid any evil of a temporal nature in reference to the proceeding against him; or

ii) in the case of a statement made by such person after his arrest, unless the court is satisfied that a caution was administered to him in the following words or words to the like effect: “It is my duty to warn you that you are not obliged to say anything or to answer any question, but anything you say, whether in answer to a question or not, may be given in evidence”;

b) a statement made by any person before there is time to caution him shall not be rendered inadmissible in evidence merely by reason of no such caution having been administered if it has been administered as soon as possible.

2) Notwithstanding anything to the contrary contained in any written law a person accused of an offence to which subsection (1) applies shall not be bound to answer any questions relating to the case after any such caution as aforesaid has been administered to him.

3) This section shall apply in relation to any person tried after the commencement of this Act, whether or not the proceedings against the person were instituted and whether or not the relevant statement was made before such commencement.

Disposal of property

77. (1) Subject to subsection (2) the provisions of the Criminal Procedure Code relating to the disposal of property the subject of an offence shall apply to any article coming into the possession of a police officer or any other person having any functions in connection with the operation of this Act which the officer or person has reasonable ground for believing to be evidence of the commission of an offence against this Act; and in relation to any such article any reference therein to a police officer shall have effect as if it included a reference to any such person.

2) Any article or material coming into the possession of a police officer under section 65 may be disposed of in such manner as the Minister may order.

3) Nothing in this section shall be taken to prejudice any right to retain or dispose of property which may exist in law apart from the provisions of this section.
Powers of search, seizure and arrest

10. (1) Whenever it appears to any Magistrate upon information and after such inquiry as he thinks necessary that there is reasonable cause to believe that in any premises there is evidence of the commission of an offence under this Act, he may, by warrant directed to any police officer of or above the rank of Inspector, empower the officer to enter the premises, by force if necessary, and there to search for, seize and detain any such evidence and he shall be entitled to—
a) have access to any program or data held in any computer, or have access to, inspect or check the operation of, any computer and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act;
b) require—
i) the person by whom or on whose behalf the police officer has reasonable cause to suspect the computer is or has been so used; or
ii) any person having charge of or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable assistance as he may require for the purposes of paragraph (a); and
c) require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible.

(2) Whenever it appears to any police officer of or above the rank of Inspector that there is reasonable cause to believe that in any premises there is concealed or deposited any evidence of the commission of an offence under this Act, and the police officer has reasonable grounds for believing that by reason of the delay in obtaining a search warrant the object of the search is likely to be frustrated, he may exercise in and in respect of the premises all the powers mentioned in subsection (1) in as full and ample a measure as if he were empowered to do so by warrant issued under that subsection.

3) Any police officer may arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against this Act, and every offence against this Act shall be deemed to be sizable offence for the purposes of the law for the time being in force relating to criminal procedure.

1998 COMMUNICATIONS AND MULTIMEDIA ACT

PART I PRELIMINARY

Interpretation

6. In this Act, unless the context otherwise requires—
“access” means access to a network facility or network service listed under Chapter 3 of Part VI;
“access code” means a voluntary industry code prepared under section 153;
“access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other network service, applications service or content applications service, equipment, or facility identifier, or other means of access that can be used, alone or in conjunction with another access device, for the purposes of any communications;
aplications service provider” means a person who provides an applications service “access forum” means a forum designated under section 152;
“access list” means the list of facilities or services established under Chapter 3 of Part VI;
“agreement” means an agreement, whether formal or informal, oral or written, express or implied;
apparatus assignment” means an assignment issued under section 164;
“Appeal Tribunal” means the Appeal Tribunal established under Part III;
aplications service” means a service provided by means of, but not solely by means of, one or more network services;
aplications service provider” means a person who provides an applications service;
“appointed date” means the date on which this Act comes into operation;
“arrangement” means an arrangement, whether formal or informal, oral or written, express or implied;
“assignment” means the assignment by the Commission of rights to use the spectrum, numbers or electronic
addresses and may include conditions to which the exercise of those rights shall be subject;
“authorized interception” means interception by the licensee of any network facilities, network service or applica-
tions service permitted under section 265;
“authorized officer” means any public officer or officer appointed by the Commission and authorized in writing
by the Minister for the purposes of this Act;
certifying agency” means a certifying agency registered under section 186;
“class assignment” means an assignment issued under section 169;
“class licence” means a licence for any or all persons to conduct a specified activity and may include conditions
to which the conduct of that activity shall be subject;
“communications” means any communication, whether between persons and persons, things and things, or
persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination
of those forms;
“communications market” means an economic market for a network service, or an applications service, or for
goods or services used in conjunction with a network service or an applications service, or for access to facilities
used in conjunction with either a network service or an applications service;
“Commission” means the Malaysian Communications and Multimedia Commission established under the
Malaysian Communications and Multimedia Commission Act 1998 [Act 589];
“conduit” means—
a) any conduit which, whether or not it is itself an electric line, is maintained by an electricity company for the
purpose of enclosing, surrounding or supporting such line, including, where such conduit is connected to any
box, chamber or other structure (including a building) maintained by an electricity supply company for purposes
connected with the conveyance, transmission or distribution of electricity, that box, chamber or structure;
b) a water main or any other conduit maintained by a water authority for the purpose of conveying water from
one place to another;
c) a public sewer;
d) a culvert or water course; or
e) any other underground facility for carrying, enclosing, surrounding or supporting any network facilities;
consumer code” means a voluntary industry code prepared under Chapter 1 of Part VIII;
“content” means any sound, text, still picture, moving picture or other audio-visual representation, tactile repre-
sentation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved
or communicated electronically;
“content applications service” means an applications service which provides content;
“content code” means a voluntary industry code prepared under Chapter 2 of Part IX;
“court” means a court of law of competent jurisdiction;
“customer equipment” means any equipment, whether hardware or software, or device, used on the customer
side of the network boundary;
“data processing device” means any article or device from which information is capable of being reproduced,
with or without the aid of any other article or device;
determination” means a determination made by the Minister under section 13;
direction” means a determination made by the Minister under section 10, or by the Commission under
section 55;
direction” means a direction issued by the Minister under
section 7, or by the Commission under section 51;
“director” has the meaning given to it in the Companies Act 1965 [Act 125];
“disaster plan” means a disaster plan which may be developed in accordance with section 267;
frequency band” means a continuous frequency range of spectrum;
“incident content” means a content which is incidental to the supply of an applications service because of—
a) it being related solely to the interface between an applications service and an end user; or
b) the reasons set out in a Ministerial determination made under section 10;
“individual licence” means a licence for a specified person to conduct a specified activity and may include condi-
tions to which the conduct of that activity shall be subject;
“industry forum” means a forum designated under section 94;
“instrument” includes a direction, determination or declaration;
“intercept” means the aural or other acquisition of the contents of any communications through the use of any
electronic, mechanical, or other equipment, device or apparatus;
“interception capability” means the capability of any network facilities or network service or applications service
to intercept communications under section 265;
“licensee” means a person who either holds an individual licence, or undertakes activities which are subject to a
class licence, granted under this Act;
“limited content applications service” means a content applications service the appeal of which is limited because of—
a) it being targeted to a special interest group;
b) it being available in a restricted geographical area;
c) it being available for a short time;
d) it being based on content of limited appeal; or (e) the reasons set out in a Ministerial determination made under section 10;
“mail” includes the postal service;
“mandatory standard” means a mandatory standard established under Chapter 10 of Part V;
“Minister” means the Minister for the time being charged with the responsibility for communications and multimedia;
“multimedia information and content” means digitized content;
“network boundary” means the network boundary provided under section 128;
“network facilities” means any element or combination of elements of physical infrastructure used principally for, or in connection with, the provision of network services, but does not include customer equipment;
“network facilities provider” means a person who owns or provides any network facilities;
“network service provider” means a person who provides network services;
“nominated facilities provider” means a person, other than the owner of the network facilities, declared by the Minister to be a nominated facilities provider;
“number” means a number, letter or symbol;
“numbering and electronic addressing plan” means the numbering and electronic addressing plan developed under section 180;
“owner” means the legal or beneficial owner;
“post” means a post, pole, tower, standard, stay, strut or other above-ground facility for carrying, suspending or supporting any network facilities;
“public utility” means a body that provides to the public—
a) reticulated products or services, such as electricity, gas, water, sewerage or drainage;
b) telecommunications services;
c) transport services; or
d) a product or service of a kind that is similar to a product or service covered by paragraph (a), (b) or (c);
“register” means any one of the registers established or maintained by the Commission for the purposes of this Act;
“register of opinions” means the register of opinions maintained under section 97 or 210, or any other relevant section;
“required applications service” means an applications service which is in a list determined by the Minister under section 192;
“spectrum” means the continuous range of electromagnetic wave frequencies up to and including a frequency of 420 terahertz;
“spectrum assignment” means the assignment issued under section 159;
“spectrum plan” means the spectrum plan developed under section 172;
“technical code” means a voluntary industry code prepared under Chapter 3 of Part VII;
“technical standards forum” means a forum designated under section 184;
“transmit” or “transmission” means to cause any emission of unguided electromagnetic energy in any part of the spectrum;
“voluntary industry code” means a voluntary industry code prepared under Chapter 9 of Part V.

PART III APPEAL TRIBUNAL

Powers of Appeal Tribunal

24A. The Appeal Tribunal shall have the power—
i) to summon parties to the proceedings or any other person to attend before it to give evidence in respect of an appeal;
ii) to procure and receive evidence on oath or affirmation, whether written or oral, and examine all such persons as witnesses as the Appeal Tribunal thinks necessary to procure, receive or examine;
iii) where a person is so summoned, to require the production of any book, paper, document, record or other thing in his possession or under his control and which the Appeal Tribunal may consider necessary for the purposes of the appeal;
iv) to administer any oath, affirmation or statutory declaration, as the case may require;
v) where a person is so summoned, to allow the payment for any reasonable expenses incurred in connection
with his attendance;
vi) of a subordinate court with regard to the enforcement of attendance of witnesses, hearing evidence on oath or affirmation and punishment for contempt;
vii) to admit evidence or reject evidence adduced, whether oral or documentary, and whether admissible or inadmissible under the provisions of any written law for the time being in force relating to the admissibility of evidence;
viii) to adjourn the hearing of an appeal from time to time, including the power to adjourn to consider its decision; and
ix) to generally direct and do all such things as may be necessary or expedient for the expeditious decision of the appeal.

PART V POWERS AND PROCEDURES OF THE MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION

Chapter 3 Inquiry

Confidential material not to be disclosed

63. (1) If an inquiry takes place in public and the Commission is of the opinion that—
a) the evidence or other material presented to the inquiry; or
b) the material in written submissions lodged with the Commission, of a confidential nature, the Commission may direct that—
(aa) the evidence or material should not be published; or
(bb) its disclosure be restricted.
2) A person shall not without reasonable excuse fail to comply with a direction under subsection (1).

Directions about an inquiry

64. (1) If an inquiry or part of an inquiry takes place in private, the Commission—
a) shall give a direction as to the persons who may be present at the inquiry or part of the inquiry; and
b) may give a direction restricting the disclosure of evidence or other material presented at the inquiry or part of the inquiry.
(2) Notwithstanding section 53, a person who without reasonable excuse fails to comply with a direction given under subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding twenty thousand ringgit or to imprisonment for a term not exceeding six months or to both.

Chapter 5 - Information-gathering Powers

Provision of information

73. (1) This section applies to any person if the Commission has reason to believe that the person—
a) has any information (including but not limited to accounts and records) or any document that is relevant to the performance of the Commission’s powers and functions under this Act or its subsidiary legislation; or
b) is capable of giving any evidence which the Commission has reason to believe is relevant to the performance of the Commission’s powers and functions under this Act or its subsidiary legislation.
2) Notwithstanding the provisions of any other written law, the Commission may, by a written notice, direct any person—
a) to give the Commission, within the period and in the manner and form specified in the notice, any such information;
b) to produce to the Commission, within the period and in the manner specified in the notice, any such documents, whether in a physical form or in an electronic media;
c) to make copies of any such documents and to produce those copies to the Commission within the period and in the manner specified in the notice;
d) if the person is an individual, to appear, at a private hearing, before the Commission at a time and place
specified in the notice to give any such evidence, either orally or in writing, and produce any such documents, whether in a physical form or in an electronic media;
e) if the person is a body corporate or a public body, to cause a competent officer of the body to appear, at a private hearing, before the Commission at a time and place specified in the notice to give any such evidence, either orally or in writing, and produce any such documents, whether in a physical form or in an electronic media; or
f) if the person is a partnership, to cause an individual who is a partner in the partnership or an employee of the partnership to appear, at a private hearing, before the Commission at a time and place specified in the notice to give any such evidence, either orally or in writing, and produce any such documents, whether in a physical form or in an electronic media.
3) The Commission shall allow the person so directed under subsection (2) a reasonable time to give and to produce any information and/or documents specified in the notice.
4) Any person required to provide information under subsection (2) shall ensure that the information provided is true, accurate and complete and such person shall provide a representation to that effect, including a representation that he is not aware of any other information which would make the information provided untrue or misleading.

Offence for giving false or misleading information, evidence or document, etc.

75. Notwithstanding section 53, a person who fails to disclose or omits to give any relevant information or evidence or document, or provides information or evidence or document that he knows or has reason to believe is false or misleading, in response to a direction issued by the Commission commits an offence and shall, on conviction, be liable to a fine not exceeding twenty thousand ringgit.

Proof of compliance

76. (1) A person shall, if at any time called upon in writing by the Commission to do so, produce to the Commission all such evidence and provide all such information as the person may have relating to his compliance with any of the provisions of this Act or its subsidiary legislation, as the Commission may generally, or in relation to any particular case, require.
(2) Subsection (1) shall not affect any other power conferred on the Commission under this Act.

Commission may retain documents

77. (1) The Commission may take, and retain for as long as is necessary, possession of a document produced under this Chapter.
2) The person otherwise entitled to possession of the document is entitled to be supplied, as soon as practicable, with a copy certified by the Commission to be a true copy.
3) Notwithstanding the provisions of any other written law, the certified copy shall be received by all courts and tribunals as evidence as if it were the original.
4) Until a certified copy is supplied, the Commission shall, at such times and places as the Commission thinks appropriate, permit the person otherwise entitled to possession of the document, or a person authorized by that person, to inspect and make copies of, or take extracts from, the document.

Incorrect record

78. A person shall not, in purported compliance with a requirement imposed by the record-keeping rules made under section 268, make a record of any matter or thing in such manner that it does not correctly record the matter or thing.
Record of information

79. (1) The Commission shall maintain a record of all information, evidence or documents received pursuant to the directions given under subsection 73(2). (2) The record shall be made available to the public.

Publication of information

80. (1) The Commission may publish information received in the course of exercising its powers and functions under this Chapter if it is satisfied that the publication is consistent with the objects of this Act. 
2) The Commission shall consider the commercial interest of the parties to whom the information relates before publishing the information. 
3) The Commission shall not publish any information or any part of any information disclosed to it if the publication would—
   a) disclose a matter of a confidential character; 
   b) be likely to prejudice the fair trial of a person; or 
   c) involve the unreasonable disclosure of personal information about any individual (including a deceased person), but the Commission may publish an abstract relating to such information provided that the particulars in the abstract shall not be arranged in any way which would compromise or prejudice the person providing such information.

Chapter 15 - Monitoring and Reporting –

Report to the Minister on industry performance

123. (1) The Commission shall monitor all significant matters relating to the performance of network facilities providers, network service providers, applications service providers and content applications service providers and report to the Minister at the end of each financial year. (2) In performing its functions under subsection (1), the Commission shall have regard to such industry performance indicators as the Commission considers appropriate.

PART VI ECONOMIC REGULATION

Chapter 1 Licensing

Definition of network boundary

128. (1) The Minister may determine the network boundary for the purposes of this Act. 
2) In the absence of such determination, the network boundary shall be—
   a) the first equipment socket in a private residence; 
   b) the main distribution frame in a building; or 
   c) a point agreed to by the customer and the network facilities provider. 
3) The ownership of any network facilities and the provision of any network services or applications services, solely on the customer side of the network boundary, are exempted from the provisions of this Part.

Exemption for applications service provider not subject to a class licence

129. An applications service provider who is not subject to a class licence under section 126 shall be deemed to be exempted from the provisions of this Chapter, but not from the provisions of Part VII regarding technical regulation.
Nominated facilities provider

130. (1) The Minister may, on the recommendation of the Commission, determine that a licensed network facilities provider, other than the owner of any network facilities, be a nominated facilities provider for the network facilities for the purposes of this Act, if the Minister is satisfied that the nomination will not impede—

a) the achievement of the objects of this Act; and
b) the administration of this Act.

2) Upon the determination of the nominated facilities provider under subsection (1), the owner shall then be deemed to be exempted from the provisions of this Chapter.

Providers under a class licence shall register

131. A person shall not operate under a class licence in respect of any network facilities or network service or applications service unless that person is registered by the Commission.

Separate licence

132. A licence obtained under this Chapter does not exempt any person from the obligation to obtain a licence under any other relevant section of this Act.

Chapter 2 General Competition Practices

Minister may make rules

144. (1) Subject to subsection (2), the Minister may make rules, to be published in the Gazette, in respect of agreements between licensees, under this Act, and foreign network facilities providers and/or network service providers.

(2) The Minister shall only make the rules, under subsection (1), which are intended to prevent or mitigate—

a) any conduct by foreign network facilities providers and/or network service providers which will, or is likely to lead to, a substantial lessening of competition in a communications market; or
b) the misuse of market power in a communications market.

PART X GENERAL

Chapter 3 - Powers of Entry, Investigation into Offences and Prosecution

Authorized officer

245. (1) The Minister may in writing authorize any public officer or officer of the Commission to exercise the powers of enforcement under this Act.

2) Any such officer shall be deemed to be a public servant within the meaning of the Penal Code.

3) In exercising any of the powers of enforcement under this Act, an authorized officer shall on demand produce to the person against whom he is acting the authority issued to him by the Minister.

4) For the purposes of subsection (1), the Commission may issue directions to a licensee or other person to secure compliance with this Act or its subsidiary legislation.
246. (1) The Commission may investigate the activities of a licensee or other person material to his compliance with this Act or its subsidiary legislation.

2) In any case relating to the commission of an offence under this Act or its subsidiary legislation, any authorized officer carrying out an investigation may exercise all or any of the special powers in relation to police investigation in seizable cases given by the Criminal Procedure Code.

247. (1) If it appears to a Magistrate, upon written information on oath and after such inquiry as he considers necessary, that there is reasonable cause to believe that an offence under this Act or its subsidiary legislation is being or has been committed on any premises, or that any evidence or thing which is necessary to the conduct of an investigation into an offence may be found in any premises, the Magistrate may issue a warrant authorizing any police officer not below the rank of Inspector, or any authorized officer named in it, to enter the premises at any reasonable time by day or by night, with or without assistance and if need be by force, and there to search for and seize any such evidence or thing.

2) Without affecting the generality of subsection (1), the warrant issued by the Magistrate may authorize the search and seizure of—

a) copies of any books, accounts or other documents, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed;

b) any signboard, card, letter, pamphlet, leaflet or notice representing or implying that the person has a licence granted or assignment issued under this Act; or

c) any other document, facility, apparatus, equipment, device or matter that is reasonably believed to furnish evidence of the commission of the offence.

3) A police officer or an authorized officer conducting a search under subsection (1) may, for the purpose of investigating into the offence, search any person who is in or on the premises. (4) A police officer or an authorized officer making a search of a person under subsection (3) may seize, or take possession of, and place in safe custody all things, other than the necessary clothing, found upon the person, and any other things, for which there is reason to believe that they are the instruments or other evidence of the crime, and they may be detained until the discharge or acquittal of the person.

5) Whenever it is necessary to cause a woman to be searched, the search shall be made by another woman with strict regard to decency.

6) If, by reason of its nature, size or amount, it is not practicable to remove any book, accounts, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, equipment, device, thing or matter seized under this section, the seizing officer shall, by any means, seal such book, accounts, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, equipment, device, thing or matter in the premises or container in which it is found.

7) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (6) or removes any book, accounts, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, equipment, device, thing or matter under seal or attempts to do so commits an offence.

8) If a search under this section indicates that there is any interference-causing equipment, radio apparatus or radio-sensitive equipment, the authorized officer may direct that necessary steps be taken to ensure an interference-free environment.

248. Search and seizure without warrant

If a police officer not below the rank of Inspector in any of the circumstances referred to in section 247 has reasonable cause to believe that by reason of delay in obtaining a search warrant under that section the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed, the officer may enter the premises and exercise in, upon and in respect of the premises all the powers referred to in section 247 in as full and ample a manner as if he were authorized to do so by a warrant issued under that section.
Access to computerized data

249. (1) A police officer conducting a search under section 247 or 248 or an authorized officer conducting a search under section 247 shall be given access to computerized data whether stored in a computer or otherwise.

2) For the purposes of this section, “access” includes—
a) being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerized data; and
b) the meaning assigned to it by subsections 2(2) and (5) of the Computer Crimes Act 1997.

List of things seized

250. (1) Except as provided in subsection (2), where any book, accounts, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, equipment, device, thing or matter is seized under section 247 or 248, the seizing officer shall prepare a list of the things seized and immediately deliver a copy of the list signed by him to the occupier of the premises which have been searched, or to his agent or servant, at those premises. (2) If the premises are unoccupied, the seizing officer shall whenever possible post a list of the things seized conspicuously on the premises.

Release of things seized

251. (1) If any thing has been seized under this Act, a designated police officer other than the police officer who effected the seizure, may at any time after that before it is forfeited under this Act release the thing to the person as he determines to be lawfully entitled to the thing if he is satisfied that the thing is not liable to forfeiture under this Act and is not otherwise required for the purpose of any proceedings under this Act, or for the purpose of any prosecution under any other law, and in such event neither the officer effecting the seizure, nor the Government or any person acting on behalf of the Government, shall be liable to any proceedings by any person if the seizure and the release of the thing had been effected in good faith.

2) A record in writing shall be made by the officer effecting the release of anything under subsection (1) specifying in detail the circumstances of, and the reason for, the release, and he shall send a copy of the record to the Public Prosecutor and to the Inspector-General of Police within seven days of the release.

Power to intercept communications

252. (1) Notwithstanding the provisions of any other written law, the Public Prosecutor, if he considers that any communications is likely to contain any information which is relevant for the purpose of any investigation into an offence under this Act or its subsidiary legislation, may, on the application of an authorized officer or a police officer of or above the rank of Superintendent, authorize the officer to intercept or to listen to any communication transmitted or received by any communications.

2) When any person is charged with an offence under this Act or its subsidiary legislation, any information obtained by an authorized officer or a police officer under subsection (1), whether before or after the person is charged, shall be admissible at his trial in evidence.

3) An authorization by the Public Prosecutor under subsection (1) may be given either orally or in writing; but if an oral authorization is given, the Public Prosecutor shall, as soon as practicable, reduce the authorization into writing.

4) A certificate by the Public Prosecutor stating that the action taken by an authorized officer or a police officer under subsection (1) had been authorized by him under that subsection shall be conclusive evidence that it had been so authorized, and the certificate shall be admissible in evidence without proof of his signature there. (5) No person shall be under any duty, obligation or liability, or be in any manner compelled, to disclose in any proceedings the procedure, method, manner or means, or any matter related to it, of anything done under subsection (1).
Obstruction to search

253. A person who assaults, impedes, obstructs or interferes with, or refuses access to any premises to, an authorized officer in the performance of his duties under this Act or its subsidiary legislation commits an offence and shall, on conviction, be liable to a fine not exceeding twenty thousand ringgit or to imprisonment for a term not exceeding six months or to both.

Additional powers

254. An authorized officer shall, for the purposes of the execution of this Act or its subsidiary legislation, have power to do all or any of the following:
   a) to require the production of records, accounts, computerized data and documents kept by a licensee or other person and to inspect, examine and to download from them, make copies of them or take extracts from them;
   b) to require the production of any identification document from any person in relation to any case or offence under this Act or its subsidiary legislation; and
   c) to make such inquiry as may be necessary to ascertain whether the provisions of this Act or its subsidiary legislation have been complied with.

Power to require attendance of person acquainted with case

255. (1) An authorized officer making an investigation under this Act may by order in writing require the attendance before himself of a person who appears to the authorized officer to be acquainted with the circumstances of the case, and the person shall attend as so required.
   2) If the person fails to attend as required, the authorized officer may report the failure to a Magistrate who shall issue a warrant to secure the attendance of the person.

Examination of person acquainted with case

256. (1) An authorized officer making an investigation under this Act may examine orally a person supposed to be acquainted with the facts and circumstances of the case.
   2) The person shall be legally bound to answer all questions relating to the case put to him by the authorized officer, but the person may refuse to answer any question the answer to which would have a tendency to expose him to a criminal charge or penalty or forfeiture.
   (3) A person making a statement under this section shall be legally bound to state the truth, whether or not the statement is made wholly or partly in answer to questions.
   4) The authorized officer obtaining information from a person shall first inform that person of the provisions of subsections (2) and (3).
   5) A statement made by a person under this section shall, whenever possible, be reduced into writing and signed by the person making it or affixed with his thumb print, as the case may be, after it has been read to him in the language in which he made it and after he has been given an opportunity to make any corrections he may wish.

Admissibility of statements in evidence

257. (1) If any person is charged with an offence under this Act, any statement, whether the statement amounts to a confession or not or whether it is oral or in writing, made at any time, whether before or after the person is charged and whether in the course of an investigation under this Act or not and whether or not wholly or partly in answer to questions, by that person to or in the hearing of an authorized officer and whether or not interpreted to him by another officer or other person, shall be admissible in evidence at his trial and, if the person charged tenders himself as a witness, any such statement may be used in cross-examination and for the purpose of impeaching his credit.
2) No statement under subsection (1) shall be admissible or used—
a) if the making of the statement appears to the court to have been caused by any inducement, threat or promise having reference to the charge against such person proceeding from a person in authority and sufficient in the opinion of the court to give the person charged grounds which would appear to him reasonable for supposing that by making it he would gain any advantage or avoid any evil of a temporal nature in reference to the proceedings against him; or
b) in the case of a statement made by the person after his arrest, unless the court is satisfied that he was cautioned in the following words or words to the like effect: “It is my duty to warn you that you are not obliged to say anything or to answer any question, but anything you say, whether in answer to a question or not, may be given in evidence”.
3) A statement made by a person before there is time to caution him shall not be rendered inadmissible in evidence merely by reason of his not having been cautioned if he is cautioned as soon as possible after that.

**Authorized officer to complete investigation and hand over to police**

258. Upon completion of his investigation into an offence under this Act or its subsidiary legislation, the authorized officer shall immediately give all information relating to the commission of the offence to an officer in charge of a police station and a police officer may, by warrant, arrest a person who may have committed an offence under this Act or its subsidiary legislation.

**Prosecution**

259. No prosecution shall be instituted for an offence under this Act without the consent in writing of the Public Prosecutor.

**Forfeiture**

260. (1) Any facility, apparatus, equipment, device, thing or matter seized under this Act may be liable to forfeiture.
2) An order for the forfeiture or for the release of any facility, apparatus, equipment, device, thing or matter liable to forfeiture under this section shall be made by the court before which the prosecution with regard to it has been held and an order for the forfeiture of the facility, apparatus, equipment, device, thing or matter shall be made if it is proved to the satisfaction of the court that an offence under this Act or its subsidiary legislation, or any breach of the conditions subject to which a licence has been granted or an assignment has been issued, has been committed and that the facility, apparatus, equipment, device, thing or matter was used in the commission of the offence despite the fact that no person may have been convicted of the offence or breach.
3) If there is no prosecution with regard to any facility, apparatus, equipment, device, thing or matter seized in the exercise of any power conferred under this Act, the facility, apparatus, equipment, device, thing or matter was used in the commission of the offence despite the fact that no person may have been convicted of the offence or breach.
4) A person asserting that he is the owner of any facility, apparatus, equipment, device, thing or matter seized under this Act and that the facility, apparatus, equipment, device, thing or matter is not liable to forfeiture may personally or by his agent authorized in writing by him give written notice to the Commission or any authorized officer of his claim.
5) On receipt of a notice under subsection (4), the Commission or any authorized officer shall, after such enquiry as may be necessary, direct that the facility, apparatus, equipment, device, thing or matter be released or forfeited or refer the case to a Sessions Court Judge for decision. (6) The Sessions Court Judge to whom the case is referred shall issue a summons requiring the person asserting that he is the owner of the facility, apparatus, equipment, device, thing or matter and the person from whom they were seized to appear before him and upon his appearance or default to appear, due service of the summons being proved, the Sessions Court Judge shall proceed to the examination of the case and on proof that an offence under this Act has been committed and that the facility, apparatus, equipment, device, thing or matter was the subjectmatter or was used in the commission of the offence, shall order the facility, apparatus, equipment, device, thing or matter to be forfeited or may, in the absence of such proof, order the release of the facility, apparatus, equipment, device, thing or matter to the person entitled to it.
7) Any facility, apparatus, equipment, device, thing or matter forfeited or deemed to be forfeited shall be de-
livered to the Commission or an authorized officer who shall dispose of it in the manner as the Commission deems fit.

### Jurisdiction to try offences

261. Notwithstanding any written law to the contrary, a Sessions Court shall have jurisdiction to try any offence under this Act.

### Rewards

262. The Commission may order such rewards as it may deem fit to be paid to any police officer or other public officer or other person for services rendered in connection with the detection of any offence under this Act or its subsidiary legislation, or in relation to any forfeiture proceeding, or any seizure made, under this Act.

### Chapter 4 - National Interest Matters

#### 263. General duty of licensees

(1) A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia. (2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security.

#### 264. Persons not liable for act done in good faith

Any network facilities provider, network service provider, applications service provider or content applications service provider or any of his employees, shall not be liable in any criminal proceedings of any nature for any damage (including punitive damages), loss, cost, or expenditure suffered or to be suffered (whether directly or indirectly) for any act or omission done in good faith in the performance of the duty imposed under section 263.

### Network interception capability

265. (1) The Minister may determine that a licensee or class of licensees shall implement the capability to allow authorized interception of communications. 2) A determination, under subsection (1), may specify the technical requirements for authorized interception capability.

### Special powers in emergency

266. (1) On the occurrence of any public emergency or in the interest of public safety, the Yang di-Pertuan Agong or the Minister authorized by him in that behalf may—
a) suspend the licence of any licensee, take temporary control of any network facilities, network service, applications service and/or content applications service owned or provided by a licensee in any manner as he deems fit;
b) withdraw either totally or partially the use of any network facilities, network service, applications service and/or content applications service from any licensee, person or the general public;
c) order that any communication or class of communications to or from any licensee, person or the general public relating to any specified subject shall not be communicated or shall be intercepted or detained, or that any such communication or its records shall be disclosed to an authorized officer mentioned in the order; or
d) order the taking of possession of any customer equipment.

2) If any doubt arises as to the existence of a public emergency or whether any act done under subsection (1) was in the interest of public safety, a certificate signed by the Yang di-Pertuan Agong and exhibited at such places as the Minister deems fit shall be conclusive proof on the point.

3) If the Minister takes possession of any network facilities, network service, applications service, content applications service or customer equipment under subsection (1), the person licensed under this Act with regard to the facilities, service or equipment shall be paid adequate compensation which shall be determined by the Minister after giving an opportunity to the licensee to be heard on the matter.

4) Nothing in this section shall prevent the use of any network facilities, network service, applications service, content applications service or customer equipment for the purpose of making a distress call.

Disaster plan

267. The Commission may direct a licensee or class of licensees to develop, in consultation with the authorities specified by the Commission, a disaster plan for the survivability and recovery of any network facilities, network service, applications service or content applications service in case of a disaster, crisis or civil emergency.

2002 MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT

(Incorporating all amendments up to 1 January 2006)

Object of Act

3. The object of this Act is for Malaysia to provide and obtain international assistance in criminal matters, including—
a) providing and obtaining of evidence and things;
b) the making of arrangements for persons to give evidence, or to assist in criminal investigations; (...)
b) whether the law of the foreign State concerned allowed the parties to the criminal proceedings to be legally represented when the evidence was being taken.

**Request for attendance of person in Malaysia**

9. (1) The Attorney General may request the appropriate authority of a foreign State to assist in arranging for the attendance in Malaysia of a person in the foreign State for the purpose of giving any evidence or assistance if he is satisfied that—
a) there are reasonable grounds to believe that the person is capable of giving such evidence or assistance relevant to a criminal matter involving a serious offence; and
b) the person consents to travel to Malaysia for the purpose of giving such evidence or assistance.

2) The Attorney General may make arrangements with the appropriate authority of the foreign State for the purpose of the attendance of that person in Malaysia, his return to the foreign State and other relevant matters.

**Immunities and privileges**

11. (1) A person who is in Malaysia pursuant to a request made under section 9 shall not—
a) be detained, prosecuted or punished in Malaysia for any offence that is alleged to have been committed, or that was committed, before his departure from the foreign State concerned pursuant to the request;
b) be subjected to any civil suit in respect of any act or omission that is alleged to have occurred, or that had occurred, before his departure from the foreign State pursuant to the request; or
c) be required to give evidence or assistance in relation to any criminal matter in Malaysia other than the criminal matter to which the request relates.

2) Subsection (1) ceases to apply if—
a) the person has left Malaysia; or
b) the person has had the opportunity of leaving Malaysia and has remained in Malaysia otherwise than for—
i) the purpose to which the request relates; or
ii) the purpose of giving evidence or assistance in a criminal matter in Malaysia certified by the Attorney General in writing to be a criminal matter in which it is desirable that the person gives evidence or assistance.

3) A certificate given by the Attorney General under subparagraph (2)(b)(ii) has effect from the day specified in the certificate, which may be a day before the day on which the certificate is given.

**Request for enforcement of forfeiture order**

13. (1) The Attorney General may, if he is satisfied that there are reasonable grounds for believing that some or all of the property concerned is located in a foreign State, request the appropriate authority of that foreign State to make arrangements—
a) for the enforcement and satisfaction of a forfeiture order; or
b) where a forfeiture order may be made in criminal proceedings which have been or are to be instituted in Malaysia, to restrain dealing in any property against which the order may be enforced or which may be available to satisfy the order.

2) A certificate purporting to be issued by or on behalf of the appropriate authority of a foreign State stating—
a) that property has been recovered in the foreign State pursuant to a request under subsection (1);
b) the value of the property; or
c) the date on which the property was recovered,
shall, in any judicial proceedings, be admissible as evidence of the matter so stated.

**Prescribed foreign State**

17. (1) The Minister may, for the purposes of this Part, by order declare a foreign State to be a prescribed foreign State if there is in force a treaty or other agreement between Malaysia and that foreign State under which that foreign State has agreed to provide assistance in criminal matters to Malaysia.

2) An order under subsection (1) may provide that the provisions of this Part shall apply to the foreign State sub-
ject to such restrictions, limitations, exceptions, modifications, adaptations, conditions or qualifications as are
specified in the order, and in that event the provisions of this Part shall apply accordingly.
3) An order made under subsection (1) shall be conclusive evidence that the arrangement referred to in the or-
der complies with this Act, and that this Act applies in the case of the foreign State referred to in the order, and
the validity of the order shall not be questioned in any legal proceedings.
4) The Minister may by a subsequent order vary or revoke any order previously made under this section.

Taking of evidence for criminal proceedings

22. (1) Where a request is made by the appropriate authority of a prescribed foreign State that evidence be
taken in Malaysia for the purpose of any criminal proceedings pending in a court in the prescribed foreign State,
the Attorney General may, subject to such conditions as the Attorney General may specify, authorize the taking
of such evidence.
2) If the Attorney General authorizes the taking of the evidence under subsection (1), a Sessions Court Judge
shall—
a) take the evidence on oath of each witness appearing before him to give evidence in relation to the criminal
matter as if the witness were giving evidence on a charge against a person for an offence against the laws of
Malaysia;
b) cause the evidence to be reduced into writing and certify at the end of that writing that the evidence was
taken by him; and
c) cause the evidence so certified to be sent to the Attorney General.
3) The proceedings may be conducted in the presence or absence of the person to whom the criminal proce-
dings in the prescribed foreign State relates or of his legal representative, if any.
4) The Sessions Court Judge conducting proceedings under subsection (2) shall allow the following persons to
have legal representation at the proceedings before the Sessions Court Judge:
a) the person to whom the proceedings in the prescribed foreign State relates;
b) any other person giving evidence or producing any materials or articles at the proceedings before the Ses-
sions Court Judge; and
c) the appropriate authority of the prescribed foreign State.
5) The certificate referred to in subsection (2) shall state whether the person to whom the criminal proceedings
in the prescribed foreign State relates or his legal representative, if any, was present at the proceedings.
6) The laws for the time being in force with respect to the compelling of persons to attend before a Sessions
Court Judge, and to give evidence, answer questions and produce materials or articles shall, in so far as they are
applicable, apply for the purposes of this section as if it were a hearing of a charge against a person for an of-
fence against the laws of Malaysia.
7) Notwithstanding subsection (6), for the purposes of this section, the person to whom the criminal proceed-
ings in the prescribed foreign State relates is competent, but not compellable, to give evidence.
8) Notwithstanding subsection (6), no person who is required under this section to give evidence for the purpos-
es of any criminal proceedings in a prescribed foreign State shall be required to answer any question that the
person could not be compelled to answer in those proceedings in that prescribed foreign State.
9) A duly certified foreign law immunity certificate is admissible in proceedings under this section as prima facie
evidence of the matters stated in the certificate.
10) Evidence taken under this section shall not be admissible in evidence or otherwise used for the purposes of
any judicial proceedings, disciplinary proceedings, or other proceedings in Malaysia except in a prosecution of
the person who gave that evidence for the offence of perjury or contempt of court in respect of that evidence.
11) Notwithstanding subsection (10), evidence taken under this section may be used for impeaching the cred-
ibility of the person who gave the evidence in any judicial proceedings for the purposes under the Evidence Act
1950.

Evidence in relation to proceedings and orders in prescribed foreign State

34. (1) For the purposes of sections 31 and 32 and the regulations made pursuant to section 44, a certificate
purporting to be issued by or on behalf of the appropriate authority of a prescribed foreign State stating that—
a) judicial proceedings have been instituted and have not been concluded, or that judicial proceedings are to be
instituted, in that prescribed foreign State;
b) a foreign forfeiture order is in force and is not subject to appeal;
c) all or a certain amount of the sum payable under a foreign forfeiture order remains unpaid in that prescribed
foreign State, or that other property recoverable under a foreign forfeiture order remains unrecovered in that
prescribed foreign State;
d) a person has been notified of any judicial proceedings in accordance with the law of that prescribed foreign State; or
e) an order, however described, made by a court of that prescribed foreign State has the purpose of—
   (i) recovering, forfeiting or confiscating—
      . payments or other rewards received in connection with an offence against the law of that prescribed foreign State that is a foreign serious offence, or the value of the payments or rewards; or
      . property derived or realized, directly or indirectly, from payments or other rewards received in connection with such an offence or the value of such property; or
   iii) forfeiting or destroying, or forfeiting or otherwise disposing of, any drugs or other substance in respect of which an offence against the corresponding drug law of that prescribed foreign State has been committed, or which was used in connection with the commission of such an offence, shall, in any proceedings in a court, be received in evidence without further proof.
2) In any such proceedings, a statement contained in a duly authenticated document, which purports to have been received in evidence or to be a copy of a document so received, or to set out or summarize evidence given in proceedings in a court in a prescribed foreign State, shall be admissible as evidence of any fact stated in the document.
3) A document is duly authenticated for the purposes of subsection (2) if it purports to be certified by any person in his capacity as a judge, magistrate or officer of the court in the prescribed foreign State, or by or on behalf of an appropriate authority of that prescribed foreign State.
4) Nothing in this section shall prejudice the admissibility of any evidence, whether contained in any document or otherwise, which is admissible apart from by virtue of this section.

PART IV - MISCELLANEOUS –

Authentication of documents

42. (1) Subject to sections 13, 33 and 34 and any law relating to the admissibility of evidence, any document that is obtained, provided or produced pursuant to a request made under this Act and that is duly authenticated is admissible in evidence without any further proof in any criminal proceedings (2) A document is duly authenticated for the purposes of subsection (1) if—
   a) it purports to be signed or certified by a judge, magistrate, or officer in or of that prescribed foreign State; and
   b) either—
      i) it is verified by the oath or affirmation of a witness, or of an officer of the government of that prescribed foreign State; or
      ii) it purports to be sealed with an official or public seal of that prescribed foreign State or of a Minister of State, or of a department or officer of the government, of that prescribed foreign State.
3) All courts in Malaysia shall take judicial notice of the official or public seal referred to in subsection (2).
4) Nothing in this section prevents the proof of any matter or the admission in evidence of any document in accordance with any other provision of this Act or any other law of Malaysia.

PENAL CODE (AS AT 1 FEBRUARY 2013)

“property” means—

(a) assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, however acquired; or
(b) legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including bank credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit;

terrorism financing offence” means any offence under section 130N, 130O, 130P or 130Q;
“terrorist” means any person who—

(a) commits, or attempts to commit, any terrorist act; or
(b) participates in or facilitates the commission of any terrorist act, and includes a specified entity under section 66B or 66C of the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 [Act 613];

“terrorist entity” means any entity owned or controlled by any terrorist or terrorist group and includes an association of such entities; “terrorist group” means—

(a) an entity that has as one of its activities and purposes the committing of, or the facilitation of the commission of, a terrorist act; or
(b) a specified entity under section 66B or 66C of the *Anti-Money Laundering and Anti-Terrorism Financing Act 2001;

“terrorist property” means—

(a) proceeds from the commission of a terrorist act;
(b) property that has been, is being, or is likely to be used to commit a terrorist act;
(c) property that has been, is being, or is likely to be used by a terrorist, terrorist entity or terrorist group;
(d) property owned or controlled by or on behalf of a terrorist, terrorist entity or terrorist group, including funds derived or generated from such property; or
(e) property that has been collected for the purpose of providing support to a terrorist, terrorist entity or terrorist group or funding a terrorist act.

(2) For the purposes of this Chapter, “terrorist act” means an act or threat of action within or beyond Malaysia where—

(a) the act or threat falls within subsection (3) and does not fall within subsection (4);
(b) the act is done or the threat is made with the intention of advancing a political, religious or ideological cause; and
(c) the act or threat is intended or may reasonably be regarded as being intended to—

(i) intimidate the public or a section of the public;

(ii) influence or compel the Government of Malaysia or the Government of any State in Malaysia, any other government, or any international organization to do or refrain from doing any act.

(3) An act or threat of action falls within this subsection if it—

(a) involves serious bodily injury to a person;
(b) endangers a person’s life;
(c) causes a person’s death;
(d) creates a serious risk to the health or the safety of the public or a section of the public;
(e) involves serious damage to property;
(f) involves the use of firearms, explosives or other lethal devices;
(g) involves releasing into the environment or any part of the environment or distributing or exposing the public or a section of the public to—

(i) any dangerous, hazardous, radioactive or harmful substance;
(ii) any toxic chemical; or
(iii) any microbial or other biological agent or toxin;

(h) is designed or intended to disrupt or seriously interfere with, any computer systems or the provision of any services directly related to communications infrastructure, banking or financial services, utilities, transportation or other essential infrastructure;

(i) is designed or intended to disrupt, or seriously interfere with, the provision of essential emergency services such as police, civil defence or medical services;

(j) involves prejudice to national security or public safety;

(k) involves any combination of any of the acts specified in paragraphs (a) to (j),

(l) and includes any act or omission constituting an offence under the Aviation Offences Act 1984 [Act 307].

(4) An act or threat of action falls within this subsection if it—

(a) is advocacy, protest, dissent or industrial action; and

(b) is not intended—

(i) to cause serious bodily injury to a person;

(ii) to endanger the life of a person;

(iii) to cause a person’s death; or

(iv) to create a serious risk to the health or safety of the public or a section of the public.

(5) For the purposes of subsection (2)—
29. (1) The word “document” means any matter expressed, described or howsoever represented, upon any substance, material, thing or article, including any matter embodied in a disc, tape, film, sound track or other device whatsoever, by means of—
   a) letters, figures, marks, symbols, signals, signs or other forms of expression, description or representation whatsoever;
   b) any visual recording (whether of still or moving images);
   c) any sound recording, or any electronic, magnetic, mechanical or other recording whatsoever and howsoever made, or any sounds, electronic impulses, or other data whatsoever;
   d) a recording, or transmission, over a distance of any matter by any, or any combination, of the means mentioned in paragraph (a), (b) or (c), or by more than one of the means mentioned in paragraphs (a), (b), (c) and (d), intended to be used or which may be used for the purpose of expressing, describing, or howsoever representing, that matter.
   
2) For the purposes of this section—
   a) “film” includes a microfilm and any negative;
   b) “microfilm” means any transparent material bearing a visual image in reduced size either singly or as a series and includes a microfiche;
   c) “negative” means a transparent negative photograph on any substance or material, and includes any transparent negative photograph made from the original negative photograph.

Suppression of terrorist acts and support for terrorist acts

Committing terrorist acts

130C. (1) Whoever, by any means, directly or indirectly, commits a terrorist act shall be punished—
   a) if the act results in death, with death; and
   b) in any other case, with imprisonment for a term of not less than seven years but not exceeding thirty years, and shall also be liable to fine.
   
2) Where in any criminal proceeding it is necessary to decide whether any item or substance is a weapon, a hazardous, radioactive or harmful substance, a toxic chemical or a microbial or other biological agent or toxin, a certificate purporting to be signed by an appropriate authority to the effect that the item or substance described in the certificate is a weapon, a hazardous, radioactive or harmful substance, a toxic chemical or a microbial or other biological agent or toxin shall be sufficient evidence of the facts stated in it

2015 PREVENTION OF TERRORISM ACT

Introduction.

An Act to provide for the prevention of the commission or support of terrorist acts involving listed terrorist organizations in a foreign country or any part of a foreign country and for the control of persons engaged in such act and for related matters.
WHEREAS action has been taken and further action is threatened by a substantial body of persons both inside and outside Malaysia which is prejudicial to the security of Malaysia or any part of Malaysia:
AND WHEREAS Parliament considers it necessary to stop and prevent such action:
NOW, THEREFORE pursuant to Article 149 of the Federal Constitution, IT IS ENACTED by the Parliament of Malaysia as follows:
Part I
PRELIMINARY

1. (1) This Act may be cited as the Prevention of Terrorism Act 2015.
(2) This Act comes into operation on a date to be appointed by the Minister by notification in the Gazette.

Interpretation

2. (1) In this Act, unless the context otherwise requires –
district, mukim, town or village" means the land included in any district, mukim, town or village under the provisions of any law for the time being in force relating to land;
Register” means the register kept by the Registrar under section 22;
Board” means the Minister charged with the responsibility for home affairs’
registered person” means a person whose name is entered in the Register;
listed terrorist organization” means any specified entity declared under sections 66b and 66c of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 [Act 613];
Inquiry Officer” means an officer appointed by the Minister under section 9;
Registrar” means the Registrar of Criminal appointed under section 3 of the Registration of Criminal and Undesirable Persons Act 1969 [Act 7];
terrorist act” has the same meaning assigned to it by the Penal Code [Act 574].
2) References to the supervision of the police shall be construed as reference to the obligations imposed upon persons subject to police supervision under section 296 of the Criminal Procedure Code [Act 593].

Part III
INQUIRIES

Article 8. Prevention of Terrorism Board.

(1) A Prevention of Terrorism Board is established which shall consist of the following members to be appointed by Yang di-Pertuan Agong:
. A Chairman, who shall be a legally qualified person with at least fifteen years experience in the legal field;
. A Deputy Chairman; and
. Not less than three and not more than six other members
2) Every member of the Board shall, unless he sooner resigns, hold office of a period not exceeding three years and is eligible for re-appointment once for another period of three years.
3) Every member of the Board may at any time resign his office by giving notice in writing to the Yang di-Pertuan Agong.
4) The appointment of any member of the Board may at any time be revoked by Yang di-Pertuan Agong
5) The quorum for any siting of the Board shall be three members
6) Subject to this Act, the Board shall determine its own procedure
7) Every member of the Board shall be deemed to be a public servant within the meaning of the Penal Code.
8. The word “Document” in this Law shall mean to include any matter expressed or described upon any substance by means of letters, figures or marks and is intended to be used or which may be used as evidence of that matter. Note: It is immaterial by what means or upon what substance the letters, figures or marks are formed. And items not intended for use as evidence are included within this definition if such item may be likely to be used as evidence.

2005 MALDIVES RULES OF CRIMINAL PROCEDURE

Rule 1.8 – Definitions

(…) (c) «Communicative evidence» means the content of a person’s written or oral communications and does not include physical evidence (…) (w) «Preponderance of the evidence» has the meaning given in Section 17(86) of the Penal Code. (…) (y) «Reason to believe” or “reasonable belief” means a standard that is higher than reason to suspect, but lower than preponderance of the evidence, and under which there are enough articulable facts to lead a reasonable person to believe that a condition exists or an event is occurring.

Rule 2.1 – Search and Seizure

(a) Property, Information, or Persons Subject to Search or Seizure. The following may be searched for and seized by law enforcement officers: evidence of an offense (…) (d) Definition. “Exigent circumstances” exist when there is a substantial risk: (…) (2) that evidence will be destroyed (…) (1) Restraint During Execution of a Warrant. The law enforcement officer or officers executing a warrant may restrain a person to prevent him from destroying evidence or interfering with the execution of a warrant (…)

Rule 2.10 – Preliminary Hearing

(a) Generally. A preliminary hearing must take place within 10 days from the filing of a charging document. The court must:
8) ensure that the defendant has a copy of the charging document,
9) explain the charge or charges to the defendant, and
10) request that the defendant enter a plea.
b) Determining Validity of Charge. During the hearing, the law enforcement officer assigned to the case or involved in the original arrest or summons shall testify regarding the factual basis of the charge or charges. If the court determines that the evidence, taken in the light most favorable to the prosecution, could not lead a reasonable person to believe that the defendant committed an offense, it must order dismissal of the charge. c) Plea. The defendant shall be asked to enter a plea of guilty, not convictable, no offense, or not guilty as to each charge. If the defendant does not enter a plea, the court must enter a plea of not guilty for him. (…)
Rule 4.1 – Pretrial Motions

(a) Generally. A party may raise by pretrial motion any defense, objection, or request that the court can determine without a trial.

b) Motions Waived If Not Made Before Trial. If the following issues are not raised by motion before trial, they are waived:
   1) a defect in instituting the prosecution;
   2) a defect in the charging document, except for a claim that the charging document fails to state an offense, which is a claim that the court may hear at any time while the case is pending;
   3) admissibility of evidence, unless the moving party was not aware of, or could not reasonably have been aware of, the evidence before trial (...)

PART V – DISCOVERY

Rule 5.1 – Disclosure of Evidence by the Prosecution

(a) Information Subject to Discovery. Except as provided in subdivision (b), the information in this subdivision must be disclosed or made available for inspection or both if:
   i) it is within the prosecution's possession, custody, or control; and
   ii) the prosecutor knows, or by exercising due diligence could know, of its existence.

1) Statement of Defendant. Upon written request by the defendant, the prosecution must disclose to the defendant and permit the defendant to inspect and copy or photograph any of the following:
   i) relevant written or recorded statements made by the defendant, and
   ii) the substance of any oral statement made by the defendant to a prosecutor or any law enforcement officer if the prosecution intends to use the statement at trial. The prosecution must disclose the statements in (i) and (ii) only if they were made in response to interrogation by a person the defendant knew was a government agent at the time of interrogation.

2) Defendant's Prior Record. Upon written request by the defendant, the prosecution must provide the defendant with a copy of the defendant's prior criminal record.

3) Documents and Objects. Upon written request by the defendant, the prosecution must permit the defendant to inspect and copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions thereof, that:
   i) are material to the preparation of his defense, or
   ii) are intended for use by the prosecution as evidence in its case-in-chief at trial, or
   iii) were obtained from or belong to the defendant.

4) Reports of Examinations and Tests. Upon written request by the defendant, the prosecution must permit the defendant to inspect and copy or photograph any results or reports of physical or mental examinations or scientific tests or experiments made in connection with the particular case if the item is material to preparing the defense or the prosecution intends to use the item in its case-in-chief at trial.

5) Evidence Favorable to Defendant. Upon written request by the defendant before trial, the prosecution must disclose to the defendant all evidence that is favourable to the defendant and material either to guilt or punishment.

6) Witness Names and Addresses. Upon written request by the defendant, the prosecution must furnish to the defendant a written list of the names and addresses of all witnesses whom the prosecution intends to call at trial.

b) Information Not Subject to Discovery. The information in subdivision (a) is not subject to disclosure and inspection obligations under the following circumstances.

1) Work Product. Except as provided in subdivisions (a)(1), (2), (4), and (5), reports, memoranda, or other internal documents made by attorneys or agents for the government in connection with the investigation or prosecution of the case are not subject to disclosure or inspection.

2) Witness Statements. Except as provided in subdivisions (a)(1) and (5), statements made by witnesses or prospective witnesses to attorneys or agents of the government are not subject to disclosure or inspection.

3) Protective Order. The prosecution may move for a protective order to deny, restrict, or defer disclosure or inspection of any information subject to discovery under subdivision (a).

4) Pending Motion for Protective Order.
If the prosecution moves for a protective order, pending the court's ruling on the motion, it may deny access to the information to the extent the prosecution reasonably believes the protective order will permit.

**Rule 5.2 – Disclosure of Evidence by a Defendant**

(a) Information Subject to Discovery. Except as provided in subdivision (b), the information in this subdivision must be disclosed or made available for inspection or both if:

i) it is within the defendant's possession, custody, or control; and

ii) the defendant intends to use it in his case-in-chief at trial.

1) Documents and Objects. If the defendant obtains discovery under Rule 5.1(a)(3) and the prosecution makes a written request, the defendant must permit the prosecution to inspect and copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions thereof.

2) Reports of Examinations and Tests. If the defendant obtains discovery under Rule 5.1(a)(4) and the prosecution makes a written request, the defendant must permit the prosecution to inspect and copy or photograph any results or reports of physical or mental examinations or scientific tests or experiments made by or on behalf of the defendant in connection with the particular case.

3) Witness Names and Addresses. If the defendant obtains discovery under Rule 5.1(a)(6) and the prosecution makes a written request, the defendant must furnish to the prosecution a list of the names and addresses of the witnesses he intends to call at trial.

(b) Information Not Subject to Discovery. The information in subdivision (a) is not subject to disclosure and inspection obligations under the following circumstances.

1) Work Product. Except as provided in subdivision (a)(2), reports, memoranda, or other internal documents made by the defendant, the defendant's attorney, or the defendant's agent in connection with the investigation or defense of the case are not subject to disclosure or inspection.

2) Witness Statements. Except as provided in subdivision (a)(2), statements made by the defendant, a witness, or a prospective witness to the defendant, the defendant's attorney, or the defendant's agent are not subject to disclosure or inspection.

3) Protective Order. The defendant may move for a protective order to deny, restrict, or defer disclosure or inspection of any information subject to discovery under subdivision (a).

   i) Pending Motion for Protective Order. If the defendant moves for a protective order, pending the court’s ruling on the motion, the defendant may deny access to the information to the extent the defendant's attorney reasonably believes the protective order will permit.

   ii) Granting a Protective Order. In the interest of justice, the court may deny, place reasonable conditions on, or defer discovery if allowing disclosure or inspection would:

      aa) subject any person to physical or substantial economic harm or coercion, or

      bb) destroy the evidentiary value of any matter.

**Rule 5.3 – Continuing Duty to Disclose**

A party who discovers additional evidence or material before or during:

1) the evidence or material is subject to discovery under Rule 5.1 (Disclosure of Evidence by the Prosecution) and Rule 5.2 (Disclosure of Evidence by a Defendant); and

2) a party previously requested, or the court ordered, production of that category of evidence or material.

**Rule 5.4 – Requirement of Prompt Response to Discovery**

(a) Prompt Response. A party must produce the evidence or material subject to discovery under Rule 5.1 (Disclosure of Evidence by the Prosecution) or Rule 5.2 (Disclosure of Evidence by a Defendant) within the time period set by the court. The court shall set the time period for responding to discovery so as to insure that discovery is completed in sufficient time before trial to prevent prejudice to the party or parties seeking discovery. (b) Failure to Comply with Discovery. If a party fails to timely comply with disclosure or inspection obligations under Rule 5.1 (Disclosure of Evidence by the Prosecution), Rule 5.2 (Disclosure of Evidence by a Defendant), and Rule 5.3 (Continuing Duty to Disclose), the court shall:

1) order the party to permit the discovery or inspection, specify its time, place, and manner, and prescribe other just terms and conditions; (2) grant a continuance;
3) prohibit that party from introducing the undisclosed evidence; or
4) enter any other order that is just under the circumstances.

**Rule 5.5 – Inadmissibility Not a Bar**

That information is inadmissible at trial under the [Rules of Evidence] does not bar a party from obtaining information otherwise subject to discovery under Rules 5.1 (Disclosure of Evidence by the Prosecution), Rule 5.2 (Disclosure of Evidence by a Defendant), and Rule 5.3 (Continuing Duty to Disclose) as long as the information is reasonably calculated to lead to the discovery of admissible evidence.

**PART VI – TRIAL**

**Rule 6.1 – Time of Trial**

(a) Time Limitation. A defendant must be brought to trial within:
1) [60 days] from the filing of the charging document if the defendant remains in custody awaiting trial, or trial must promptly disclose its existence to the other party or the court if:
2) [90 days] from the filing of the charging document if the defendant secures pretrial release under Part III (Release Before and During Trial).

b) Waiver. A defendant may waive the time limitations in subdivision (a).

c) Request for Extension. The prosecution may request the court to extend the time limitations in subdivision (a). The prosecution must provide specific reasons for the requested extension. The court shall grant the request if an extension is in the interest of justice.

**Rule 6.2 – Continuity of Trial**

Once a trial begins, it shall continue without undue interruption until it is complete. The court may suspend the proceedings briefly as necessary in the interest of justice.

**Rule 6.3 – Conducting Trial**

(a) Order of Proceeding. The court shall call the trial to order, after which the trial shall proceed in the following order, unless the court otherwise directs:
1) the prosecutor shall state to the court the nature of the charge and the evidence upon which the prosecutor relies to support it;
2) the defendant or the defendant's attorney may state the defense and the evidence upon which the defendant relies to support it or the defendant may reserve this opening statement until the conclusion of the evidence for the prosecution;
3) the prosecutor must offer the evidence in support of the charge;
4) the defendant or the defendant's attorney may make an opening statement, if reserved, and offer evidence in support of the defense;
5) the parties respectively may offer rebutting evidence, unless the court, in the interest of justice, permits them to offer evidence-in-chief; and
6) the parties may submit or argue the case to the court. In the argument, the prosecutor shall have the conclusion and the defendant or the defendant’s attorney the opening. If more than one counsel is to take part in the closing argument on either side, or if several defendants have separate defenses and appear by different counsel, the court shall arrange the order of argument, always giving the prosecutor the closing argument.

b) Taking of Testimony. After the parties have had an opportunity to question a witness, the court may question the witness. The testimony of witnesses must be taken in open court, unless the court determines that taking the witness’s testimony in private is necessary to protect the witness from intimidation or substantial physical or psychological harm.
Rule 6.4 – Right of Confrontation at Trial

(a) Defendant's Presence. A defendant must be permitted to attend every stage of his trial, unless he:
1) is voluntarily absent; or
2) persists in conduct that is so disruptive as to justify exclusion from the
courtroom after being warned by the court that disruptive conduct will cause his removal; or
3) intimidates a witness, in which case the defendant may be excluded only during the witness's testimony.
b) Cross-Examination. The defendant's attorney, or the defendant himself if he is not represented by counsel,
must be permitted to cross-examine all witnesses against the defendant during trial.

Rule 6.5 – Admission of Evidence

The court may only consider evidence that has been presented by the parties during trial. Admissibility of evi-
dence may be contested by any party. The court shall rule on all questions of admissibility in accordance with
the [Rules of Evidence].

Rule 6.6 – Judgments at Trial

(a) Generally. At the conclusion of a trial, the court must enter a judgment of “guilty,” “no offense,” or “not guilty”
for each offense charged or an offense consisting of elements necessarily established by proof of an offense
charged.
1) Guilty. The court must enter a judgment of “guilty” if it finds that the requirements for liability in Section 20 of
the Penal Code are fulfilled.
2) No Offense. The court must enter a judgment of “no offense” if it finds that the defendant does not satisfy the
requirements for liability in Section 20 of the Penal Code because of:
i) an absence of an objective element under Section 21(a)(1) of the Penal Code,
ii) a justification defense in Chapter 40 of the Penal Code, or
iii) any other exemption from liability vitiating the offense harm or wrong.
3) Not Guilty. The court must enter a judgment of “not guilty” if it finds that the
defendant does not satisfy the requirements for liability in Section 20 of the Penal Code but is not entitled to a
judgment of “no offense.”
b) Entering the Judgment. The judgment must be entered in open court. If a party
requests before the judgment, the court must state its specific findings of fact in open court or in a written deci-
sion or opinion.

Rule 6.7 – Trial Motion for Acquittal

After the prosecution closes its evidence, the court, on motion of the defendant or its own motion, must order
the entry of a judgment of no offense or not guilty, as defined in Rule 6.6 (Judgments at Trial), as to any offense
for which the evidence would not reasonably permit a finding of guilty beyond a reasonable doubt. The court
shall rule upon the motion for acquittal before calling upon the defendant to present his case. If the court de-
nies a motion for a judgment of acquittal, the defendant may offer evidence without having reserved the right to
do so.

Rule 6.8 – Mistrial

(a) Generally. On motion of a party, the court shall declare a mistrial at any time during trial if necessary in the
interest of justice.
1) For Prejudice to Defendant. The court shall declare a mistrial on a defendant's motion if there occurs during
the trial an error or legal defect in the proceedings, or conduct in or outside the courtroom, resulting in substan-
tial and irreparable prejudice to the defendant's case.
2) For Prejudice to the Prosecution. The court shall declare a mistrial on the prosecution's motion if there occurs during the trial, either in or outside the courtroom, misconduct by the defendant, the defendant's lawyer, or someone acting at the prosecution's case.

b) Opportunity to Be Heard. Before ordering a mistrial, the court must consider fairness to the parties and give each party an opportunity:
1) to comment on the propriety of the order,
2) to state whether that party consents or objects, and
3) to suggest alternatives.

**Rule 6.9 – Judge Unable to Proceed**

(a) During Trial. If the judge before whom a trial began cannot proceed with a trial because of absence, death, sickness, other disability, termination of office, or a conflict of interest that did not exist or was not known before trial, a judge regularly sitting in or assigned to the court shall grant a new trial.

b) After a Judgment of Guilty. After a judgment of guilty, if the judge who presided at trial cannot perform post-trial duties because of absence, death, sickness, other disability, termination of office, or a conflict of interest, a judge regularly sitting in or assigned to a court shall:
1) complete the court's duties, or
2) grant a new trial if a judge other than the one who presided at the trial cannot adequately perform the post-trial duties.

c) Conflict of Interest. A conflict of interest exists when one of the parties involved in the case is a close relative or a business associate of the judge.

**PART VII – POST-TRIAL PROCEEDINGS**

**Rule 7.6 – Post-trial Motions**

(a) Post-trial Motion for Acquittal.
1) Grounds. If a mistrial is declared any time after the close of the prosecution's evidence, the court, on motion of the defendant or its own motion, shall order the entry of a judgment of no offense or not guilty, as defined in Rule 6.6 (Judgments at Trial), as to any offense for which the evidence would not reasonably permit a finding of guilty beyond a reasonable doubt.

2) Time for Motion. Unless the court otherwise permits in the interest of justice, the motion for acquittal must be made within ten days after mistrial or within any further time the court allows during the ten-day period.

b) Motion for a New Trial.
1) Granting the Motion. On motion of the defendant, the court shall grant the defendant a new trial if an error occurred and a new trial is required in the interest of justice. The court shall not grant the motion if it appears beyond a reasonable doubt that the error did not impact the outcome of the case.

2) Entry of a New Judgment. In lieu of granting a new trial, the court may vacate any judgment entered, receive additional evidence from the parties, and direct the entry of a new judgment if the new judgment is supported by sufficient evidence.

3) Time for Motion.
   i) Motion Based on Newly Discovered Evidence. A motion for a new trial based on newly discovered evidence must be made with reasonable diligence, considering the nature of the allegations in the motion. The court may grant the motion even though an appeal is pending.
   ii) Motion Based on Other Ground. Unless otherwise permitted by the court in the interest of justice, a motion for a new trial based upon any ground other than newly discovered evidence must be made within ten days after the entry of a judgment of guilty or within any further time the court allows during the ten-day period.

**Rule 7.8 – Forfeiture**

(a) When Authorized. The court shall order that a defendant forfeit the proceeds of or contraband involved in an offense for which he has been convicted if it finds by a preponderance of the evidence that there is a connection between the property sought to be forfeited and the offense.
b) Forfeiture Not Part of Sentence. An order of forfeiture is not part of sentence and shall not be included in the calculation of the guideline sentence under Part III (Sentencing Guidelines) of the Penal Code.
c) Notice to the Defendant. A court must not enter an order of forfeiture unless the charging document contains notice to the defendant that the prosecution will seek the forfeiture of property.
d) Entering a Preliminary Order of Forfeiture.
1) In General. After acceptance of a plea of guilty or entry of a judgment of guilty on any count in the charging document regarding which criminal forfeiture is sought, the court shall determine what property is subject to forfeiture under subdivision
a) and the amount of any personal money judgment sought. The court's determination may be based on:
i) evidence already in the record, including any written plea agreement; or ii) if the forfeiture is contested, on evidence or information presented by the parties at a hearing after the finding of guilt.
2) Preliminary Order. If the court finds that property is subject to forfeiture, it must enter a preliminary order of forfeiture setting forth the amount of any money judgment and directing the forfeiture of specific property without regard to any third party's interest in all or part of it.
3) Seizing Property. The entry of a preliminary order of forfeiture authorizes the attorney General, or his designee, to:
i) seize the specific property subject to forfeiture;
ii) conduct any discovery the court considers proper in identifying, locating, or disposing of the property; and iii) commence proceedings that comply with any law governing third party rights.
e) Entering a Final Order of Forfeiture.
1) When No Third Party Claims an Interest in the Property. If no third party files a timely petition, the preliminary order becomes the final order of forfeiture at the time of sentencing and must be included in the execution of judgment. The order of forfeiture may include conditions reasonably necessary to preserve the property's value pending any appeal. The defendant may not object to the entry of the final order on the ground that the property belongs, in whole or in part, to a third party if no third party claims an interest in the property (…)

2015 ANTI-TERRORISM ACT
(Second amendment)
To bring the following amendments to Law No. 32/2015 (Anti-Terrorism Act)

1. To amend section 4 of the said Act as follows.
Definition of Terrorism

(a) For the purpose of this act, terrorism refers to any act stated in subsection b) carried out to achieve any of the following objectives.
1) To promote/advance a certain political or religious or extremist ideology; and
2) To coerce or unduly influence the state or the government, or to create fear amongst the public or a segment of the public.
b) For the purposes of achieving the objectives of subsection a) of this act, an act of terrorism refers to carrying out any of the following acts.
1) Causing serious bodily harm to a person;
2) The act of endangering the life of a person other than the offender;
3) The act of enforced disappearance or holding a person hostage;
4) The act of causing substantial damage to property;
5) The act of hijacking vessels carrying passengers or goods;
6) The act of creating a situation risking the health or safety of the public or a segment of the public;
7) Causing damage to critical infrastructure or seriously interfere with an essential service.
c) Notwithstanding subsections (a)(1) and (2), the use of weapons of war or explosives to carry out an act pursuant to subsection (b), will be considered as an act of terrorism for the purpose of subsection(a) of this act.
d) Notwithstanding subsection (b)(7), interferences with essential public services due to lawful demonstration, industrial action and peaceful assembly will not be considered acts of terrorism (e) For the purposes of this section, “Critical infrastructure” refers to any asset, system, network, or physical and infrastructural resources and conveniences, which if willfully damaged, can negatively impact the national security of the Maldives.
f) For the purposes of this section, “Essential service” refers to electricity, water and sewerage services, telecommunication services and transport services.
2. To amend section 5 of the said Act as follows
Carrying out an act of terrorism

Unless otherwise stated in this Act, “Carrying out an act of terrorism” refers to carrying out any act of terrorism including those stated in Chapter 2 of this Act.

3. To amend section 6 of the said Act as follows
The Offences of terrorism

(a) (1) It is an offence to commit an act of terrorism as stated in Section 4 of this Act. (2) It is an offence to attempt, aid and abet an act of terrorism as stated in Section 4 of this Act.

5. To amend the title of section 12 of the said Act as follows
The Production, Sale or Transportation on of weapons of war or Items Containing Explosive or Destructive Material

6. To amend section 12 (a) of the said Act as follows

12 (a) It is an offence to produce, possess, sell, provide to another person, transport to another location and trade weapons of war or items containing explosive or destructive material for the purposes of carrying out or aiding and abetting an act of terrorism.

7. To amend section 16 of the said Act as follows.
Going to war and entering war zones

16 (a) Except under express authorization of the Government of the Maldives, the following acts shall be deemed an offence.
1) Going to war;
2) Entering and remaining in a war zone.
b) It is an offence to carry out the following acts.
1) Sending a person to war;
2) Attempting to, or encouraging a person to go to war

c) It is an offence to attempt or aid and abet any of the offences stated in Section (a)(1) of this act.
d) It is an offence to attempt or aid and abet any of the offences stated in Section (a)(2) of this act.
e) For the purposes of this section, “Going to War” refers to leaving the Republic of Maldives to achieve any of the following objectives
1) To participate in a war led by a terrorist organization or terrorists not belonging to any organization;
2) To conspire or prepare for or aid or abet to carry out an act of terrorism;
3) To provide or receive training to carry out an act of terrorism.
f) For the purposes of this section, “A war zone” refers to areas outside the Republic of Maldives where there is an armed conflict led by a terrorist organization or terrorists not belonging to any organization as specified under section 18 of this Act.
g) Unless otherwise proven, and notwithstanding the provisions stated in subsection (h), it is presumed that a person enters a war zone to participate in war.
h) Notwithstanding the provision stated in subsection (a), it is not an offence to enter or remain in a war zone for or in connection with any of the purposes stated below.
1) To provide humanitarian aid to victims of the war;
2) To enforce a court order;
3) To carry out work for the government of a country other than the Republic of Maldives;
4) To carry out work for the United Nations or an agency of the United Nations;
5) To carry out work as a journalist;
6) To carry out work authorized by the government for an organization or association;
7) Any other work authorized by the government.
   i) For the purposes of subsections (h)(1), (5), (6) and (7), a person entering or remaining in a war zone must get authorization in writing from the ministry.
   j) Notwithstanding the provision stated in subsection (i) of this section, an Officer of Maldives National Defense Force or Maldives Police Service entering or remaining in a war zone in their official capacity, does not require authorization from the ministry.
   k) The penalty for the offence stated in subsection (a)(1) is imprisonment of 9 (nine) to 12 (twelve) years.
   l) The penalty for the offence stated in subsection (a)(2) is imprisonment of 5 (five) to 7 (seven) years.
   m) The penalty for the offence stated in subsection (b) is imprisonment of 10 (ten) to 15 (fifteen) years.
   n) The penalty for the offence stated in subsection (c) is imprisonment of 5 (five) to 7 (seven) years.
   o) The penalty for the offence stated in subsection (d) is imprisonment of 3 (three) to 5 (five) years.
p) Upon his return, measures stated in Chapter 8 of this act must be taken against a person who goes to war or enters a warzone as stated in subsection (a). In addition to this, measures stated in Chapter 6 of this act may be taken against such a person.

8. To insert a section subsequent to section 16 of the said Act as follows

Supporting a Terrorist Organization
16-1 (a) It is an offence to carry out the following acts under the following circumstances.
1) Support or invite support for a terrorist organization;
2) Defend or provide reasonable justifications for an act of terrorism, or expresses an opinion or belief that is supportive of a terrorist organization, and in doing so is reckless as to whether a person to whom the expression is directed will be encouraged to support a proscribed organization;
3) Arrange, manage or assist in arranging or managing a meeting which he knows is to support a terrorist organization, or to further the activities of a terrorist organization, or to be addressed by a person who belongs or professes to belong to a terrorist organization.
4) Address a meeting where the purpose of the meeting is to encourage support for a terrorist organization or to further its activities.
5) Wear any garment or possess or use any document, illustration or photograph expressing support for a terrorist organization or a member of such an organization.
b) The penalty for the offence stated in subsection (a)(1), (2), (3) and (4) of this section is imprisonment of 3 (three) to 5 (five) years.
c) The penalty for the offence stated in subsection (a)(5) of this section is imprisonment of 1 (one) to 3 (three) years.

9. To amend section 18 of the said Act as follows.

Declaration of terrorist organizations and warzones
18 (a) The President, on the advice of the national security council, shall determine terrorist organizations and warzones for the purposes of section 15(b)(3) and 16(f) of this Act.
b) The list of terrorist organizations and warzones declared by the President under subsection (a) must be reviewed once every 12 (twelve) months.
c) The President, on the advice of the national security council, has the authority to amend the list of terrorist organizations and warzones declared under subsection (a) and review under subsection (b).
d) The list of terrorist organizations and warzones declared by the President under subsection (a), and the amendments brought to the list shall be published in the gazette.
Chapter Three Disclosing information and sharing intelligence associated with terrorism

### Disclosing information associated with terrorism Counter terrorism Intelligence Bodies

19-1 Any person possessing information regarding a potential act of terrorism as stated in this Act, must disclose this information to the Maldives Police Service. Maldives Police Service must inform Intelligence Bodies regarding such a disclosure, where it is required under Section 19-3 of this Act.

9-2 For the purpose of this act, the following institutions will be considered as counter terrorism intelligence bodies.

a) Maldives National Defense Force;
b) Maldives Police Service;
c) Maldives Customs Service;
d) Maldives Immigration;
e) Maldives Monetary Authority Financial Intelligence Unit.

### Framework for exchanging information and intelligence associated with terrorism

19-3 (a) For the purposes of this Act, the Minister must draw up a framework for the safe exchange of information and intelligence, and ensure that such an exchange is done so within the margins of the said framework by regular monitoring.

b) The framework drawn under subsection (a) must include a mechanism by which, the intelligence bodies stated in Section 19-2 of this Act can share and disclose relevant information and intelligence with relevant foreign countries or international organizations.

c) The intelligence bodies stated in Section 19-2 of this act must exchange relevant terrorism related information within those bodies in accordance with the framework drawn under subsection (a).

d) The intelligence bodies stated in Section 19-2 of this act must build capacity to acquire and investigate intelligence associated with terrorism.

e) In addition to the intelligence bodies stated in Section 19-2 of this act, State Institutions must disclose any terrorism related information acquired within their official scope of work, to the relevant intelligence body stated in the aforementioned section without any delays.

Chapter 4 Counter-terrorism powers

12. To amend section 20 of the said Act as follows.

### The Suspension of Certain Rights Granted Under the Constitution

20 (a) If a person is detained or arrested on an allegation of any of the offences under Chapter 2 of this Act, the constitutional rights stated in this Chapter may be restricted or limited to the extent as defined in the relevant sections.

b) Any constitutional right restricted under this chapter, has been done so in accordance with Article 16 (a) of the Constitution.

c) In determining whether the rights guaranteed under the Constitution has been restricted in accordance with Article 16 (a) of the Constitution, the relevant courts must presume that Parliament has taken into consideration all 6 (six) factors stated in Article 16 (c) of the Constitution.
13. To repeal the following provision copied below from the said Act

**Situations where the Accused may be found guilty, upon exercising his Right to Silence**

21 (a) Notwithstanding the Constitutional Guarantee under Article 48 (c) of the Constitution on a person's right to remain silent, except to reveal his or her identity; a person's silence may be interpreted against the accused as corroborative evidence, provided there is reasonable evidence otherwise that establish the accused's guilt. A person has a duty to substantiate otherwise, whenever there is reasonable evidence potentially establishing the person's guilt. (b) The adverse inference mentioned under subsection (a) shall be subject to the following; (1) The person was notified of his right to remain silent and at the same time, was also informed of potential adverse inference against should such person exercise this right. (2) The evidence otherwise presented to trial against such person in general weight, establishes the person's guilt beyond reasonable doubt.

14. To amend section 22 of the said Act as follows.

**Arrest without a warrant**

22 (a) Notwithstanding other legislation, Maldives Police Service has the authority to arrest a person without a warrant, where there are probable and reasonable grounds to believe that any offences stated in Sections 6, 7, 11, 12 and 14 of this act is imminent unless immediate action is taken.

b) Any persons arrested pursuant to subsection (a), must be brought before a Judge within 24 (twenty four) hours of arrest to determine the validity of the arrest.

c) Arresting a person pursuant to subsection (a), must be authorized by a police officer ranking higher than sub-inspector level.

d) Maldives Police Service must follow the procedures stated in Section 40(e), 40(f), 42, 43, 44 and 45 of Criminal Procedure Code (Act No: 12/2016) when arresting and detaining a person pursuant to subsection (a). At the time of the arrest, Maldives Police Service has the discretion to take preventive measures in order to minimize the impact of the alleged, potential act of terrorism by the accused arrested pursuant to subsection(a) of this section.

f) Maldives Police Service has the authority to enter a private property for the purpose of arresting persons referred to in this section.

g) In entering private property pursuant to this section, Maldives Police Service must follow the relevant procedure stated in Criminal Procedure Code (Act No: 12/2016).

**To insert a Section subsequent to Section 22 of the said Act as follows**

22-1 (a) Notwithstanding other legislation, Maldives Police Service has the authority to search any persons suspected of an offence, and is believed to possess an instrument of crime or evidence of an offence stated in this act, without a search warrant.

b) Maldives Police Service has the authority to enforce the powers granted to them under Section 38 (f) of Criminal Procedure Code (Act No: 12/2016) when carrying out a search under subsection (a).

c) Maldives Police Service has the discretion to conduct a strip search of a person pursuant to subsection (a) without a warrant; where there is a reasonable ground to believe that the person possesses an article related to the alleged offence.

d) In conducting the search as stated in subsection (a), Maldives Police Service must follow the relevant procedure stated in Section 38(g), (h) and (i) of the Criminal Procedure Code (Act No: 12/2016).

20. To amend section 27(a) of the said Act as follows.

Admissible evidence

7 (a) The following shall be considered as admissible evidence in a trial of a person accused of an act of terrorism as stated in this Act.
3) The confession or admission made in court, verbally, in writing or otherwise;
4) Dying declaration;
5) Recorded confession in the presence of legal counsel, on his own volition, without any duress or undue influence.
6) Any information proving the person's intention to carry out a certain element of the offence or any act done in preparation for the offence;
7) Forensic evidence;
8) Official documents;
9) Intelligence reports satisfying the following requirements;
. Where the probability of one or more facts stated in the report is, more likely than not, to be accurate.
i. Where there is evidence supporting the information stated in the report.
10) A medical report confirming that the injuries sustained by the accused must have resulted from a weapon of war;
11) Published documents, illustrations, photographs; or documents, illustrations, photographs, audio or video sent via telecommunication devices;
12) A data analysis document or a report, which finds a document, audio or video that can be used as training material for the production or operation of a weapon or instrument of war;
13) Audio and video recording of the statement by a relative of the accused, stating that the accused has or is about to or is carrying out an offence stated in this Act.
14) An official document stating that the accused has traveled to a war zone;
15) Eye witnesses;
16) Other admissible evidence.

21. To amend section 27 (c) of the said Act as follows.

27 (c) 'Official Document' for the purposes of section (a)(6) refers to formal representations made or information disseminated by an enforcement agency of the Republic of Maldives or a foreign country by means of any of the following instruments.

22. To insert the following subsections to Section 27 (c) of the said Act as follows

27 (d) Evidence obtained by an investigatory body from the following sources can be used against a person accused of an act of terrorism as stated in this Act. The judge must consider such evidence admissible.
3) International intelligence or investigatory body;
4) Foreign intelligence or investigatory body; and
5) Family member, or relative or a friend of the accused.
e) Where there is no Mutual Legal Assistance treaty in force between the Maldivian Government and a foreign Government, this act does not restrict the enactment of an agreement stipulating the procedures to be followed in exchanging evidence between the foreign authorities stated in subsections (d)(1) and (2).
f) Notwithstanding other legislation, this act does not restrict the submission of new evidence not previously known, after a person has been charged of an offence of terrorism as stated in this Act.
3. To insert the following Section subsequent to Section 27 of the said Act as follows.

Evidential Requirement

27-1 Notwithstanding other legislation regarding evidential requirement, for the purposes of this Act or any charges submitted under this Act, in establishing guilt of an offence stated in Chapter 2, where a minimum of 4 (four) types of evidence as stated in Section 27 (a) is submitted, such evidence shall be deemed sufficient to establish the offence beyond a reasonable doubt as stated in Article 51 (a) of the Constitution.
4. To amend section 28 of the said Act as follows.
2015 MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS ACT

(m) “Document” means a record of information in any form, including the following:

17) A written or printed thing (including a map, plan, graph, or drawing);
18) A computer file accessible through an electronic device;
19) A photograph;
20) A disk, tape or film soundtrack or other thing in which sound or other data is embodied;
21) A film, negative, tape or other thing in which visual images or other data is embodied.

2. Object of Act

The object of this Act is to facilitate:

a) the provision of assistance in obtaining evidence and other articles; the making of arrangements for persons to give evidence or assist in criminal investigations or proceedings where Maldives receives requests for assistance from other States;
b) the obtaining of evidence and other articles in another State in relation to criminal investigations or proceedings in Maldives, or the making of arrangements for persons in another State to give evidence or assist in such criminal investigations or proceedings and matters connected therewith.

3. Scope of Assistance

(a) Mutual legal assistance to be provided under this Act includes the provision or obtaining of the following types of assistance in relation to a criminal proceeding or a criminal investigation:
6) taking of evidence or statements from persons; or
7) the making of arrangements for persons to give evidence or assist in criminal investigations or proceedings; or
8) the service of documents; or
9) the execution of search and seizure warrants; or
10) the freezing or seizure of assets; or
11) examining effects and sites; or
12) providing information and evidentiary items; or
13) providing originals or certified copies of relevant documents and records including bank, financial, corporate or business records;

CHAPTER THREE- ASSISTANCE WITH TAKING EVIDENCE AND PRODUCTION OF DOCUMENTS OR OTHER ARTICLES

10. Requests by the Maldives for assistance with Evidence

(a) The Prosecutor General may request the appropriate authority of a foreign State to make the following arrangements with regard to a criminal proceeding or investigation in the Maldives;
4) for evidence to be taken in the foreign State, in accordance with the laws of that State;
5) for a document or other article in the foreign state to be produced in accordance with the laws of that state;
6) the transmission of the evidence and documents or articles obtained under sub-section (1) and/or sub-section (2), to the Maldives.
b) Evidence may be taken, or any document or other article may be obtained in the foreign country pursuant to subsection (a) even though under Maldivian law the evidence could not have been taken, or the document or...
other article could not have been obtained by using in the circumstances processes similar to those used in the foreign country.
c) When making a request under subsection (a), the Prosecutor General may also request that an opportunity be given for the person giving the evidence, or producing the document or other article, to be examined or cross examined, through a video or internet link by:
1) In the case of a criminal proceeding, a party to the proceeding, or the party's legal representative;
2) In the case of a criminal investigation, a person being investigated, or the person's legal representative.

11. Request by Foreign States for Assistance with Evidence

(a) Where a foreign State makes a request for the following types of assistance relating to a proceeding or investigation relating to a criminal matter in that State, the Prosecutor General may authorize, at his or her discretion, the provision of such assistance.
8) The taking of evidence from a person in Maldives;
9) The production of a document or other article in the Maldives that may be required with respect to the criminal matter;
10) The transmitting of the evidence and documents or articles obtained under sub-section (1) and/or sub-section (2) to the foreign State.
b) The authorization by the Prosecutor General pursuant to this Section shall be made in writing in the form prescribed under the Regulations made under this Act.

12. Taking Evidence

(a) Where the Prosecutor General authorizes the taking of evidence pursuant to Subsection (a) (1) of Section 11 of this Act, an authorized officer of the police shall be directed to produce such person before a competent court and request the court to take the evidence.
b) In taking evidence of a witness pursuant to this Section, the Judge shall:
6) take evidence on oath or affirmation of the witness appearing before the Judge to give evidence in relation to the matter and cause the evidence to be put in writing;
7) certify that a witness referred to in subsection (e) of this Section or any other person made an appearance in court to give evidence;
8) once the evidence has been recorded in writing, sign and certify that the evidence was taken by the Judge, and send the document to the Commissioner of Police.
c) Notwithstanding Subsection (b), this Section does not prevent the taking of evidence of a witness via video conference if the witness is unable to appear before the Court.
d) The Commissioner of Police shall inform the Prosecutor General forthwith of the receipt of any evidence under subsection (b).
e) The proceeding to take evidence pursuant to this Section may be conducted in the presence of or in absentia of the person to whom the criminal proceeding or investigation in the foreign State relates, or his legal representative.
f) A person to whom a criminal proceeding or an investigation in a foreign State relates shall not be compelled to give evidence pursuant to this Section.

13. Conduct of Proceedings

The Regulations to be made under this Act shall prescribe the procedures to be followed in the taking of evidence under Section 11 of this Act.
CHAPTER-1 PRELIMINARY 1.

Short Title, Extent and Commencement: (1) This Act may be called the «Evidence Act, 2031». (2) This Act shall apply to all proceedings of a case before the Court. (3) This Act shall come into force on the first day of Baisakh, 2032.

CHAPTER-2 FACTS IN WHICH EVIDENCE MAY BE EXAMINED AND FACTS NOT REQUIRED TO EXAMINE THE EVIDENCE

3. Facts in which evidence may be examined

The court may examine evidence on the fact in issue which is to be decided by it and the relevant fact thereof. Explanation:- «Relevant fact» means a fact which helps to prove or disprove the fact in issue of the case to be decided.

4. Facts not required to examine the evidence:

It shall not be necessary to examine evidence on the following facts-

a) If the fact expressed by a party to the case is admitted by the other party in the written form, Provided that, the court, if thinks appropriate may examine evidence on such fact.
b) Facts to be taken as judicial notice by the court pursuant to Section 5

2) It shall not be necessary to the court to examine any evidence to presume any fact pursuant to Section 6 and 7. Provided that, the court may examine evidence, as required, before making presumption on the facts as mentioned in Section 7.

(5) Facts to be taken into judicial notice by the court:

(1) The court shall take judicial notice of the following facts-
d) Geographical position of Nepal
e) Constitution of Nepal and Nepal law
f) Notice published in Nepal Gazette

2) The court may take judicial notice of the undisputed facts of general knowledge. Provided that, if, pursuant to this Sub- section, a party to the case requests to take judicial notice of any fact, the court may issue an order to that party to submit required evidence regarding that fact and the court may deny to take the judicial notice of that fact unless evidence is produced to the satisfaction of the court.
3) The court may take the help of any book or document to take judicial notice pursuant to this Section.

(6) The court shall presume the facts:

Unless otherwise proved-
a) The property, in the name of any co-partner of a joint family, shall be presumed by the court that such property is a joint property.
b) The property, in the possession or use of two or more persons, shall be presumed by the court that all of them have equal right on that property.
c) The Court shall presume that the matters recorded in the accounts (sayha), Papers (shresta) or documents (kagajat) to be recorded in pursuance of law by any court or government office are correctly recorded.

d) The baby, born during the continuance of marriage of the husband and wife or within two hundred and seventy two days of the dissolution of the marriage or the death of the husband, shall be presumed by the court that the baby is the child of the same husband.

e) Any document, so indicated that it is published, prepared or attested (certified) by any court or government office or official or by a person so authorized by the Nepal law shall be presumed by the court that it has been published or prepared or attested (certified) by such court, office, official or person.

f) Any law or judicial decision printed in a book or journal and where it has been indicated that it is published by the government of a foreign country or by the official so authorized by such government, the court shall presume that such law or decision has been published correctly.

7. The court may presume:

Unless otherwise provides:-

a) If a person is holding a stolen property with him / her, the court may presume that the property is either stolen by him/her or purchased knowingly that it is a stolen property. Provided that, if such person shows any reasonable ground to remain that property in his / her possession or it seems reasonable to remain such property in his/her possession by virtue of his/her profession or trade and it is laying with him/her without knowing that it is a stolen property, the court may not presume on that way.

b) If the court issues an order to a person to submit a document which he / she holds and he/she does not submit accordingly, the court may presume that the document may have evidential value against such person.

c) If any incident, conduct of the persons or general trend of the acts transactions reasonably leads towards certain presumption, the court may presume other facts accordingly.

CHAPTER-3 FACTS TO BE TAKEN OR NOT TO BE TAKEN AS EVIDENCE

8. Facts to be taken as evidence:

The facts to be taken as evidence under this Chapter and other facts stated by the witness before the court may be taken as evidence in the course of examining evidence pursuant to Section 3.

9. Facts expressed by the party:

(1) Any fact expressed by the party to a case may be taken as evidence against him/her.

2) Notwithstanding anything contained in Sub- section (1),

a) The fact expressed by the accused of a criminal case, in a place other than the court regarding the charge made against him/her, may be taken as evidence, when the court finds it as following:

1) At the time of expression, the accused was conscious and in a position to understand what he/she did or expressed.

2) The fact was not expressed putting pressure on him/her or with torture to him/her or with a threat to torture to him/her or any other person or putting him/her in a condition to express the fact against his / her will.

3) The public official, while conducting a process had not given any threat or promise in relation to any charge, by which there was a possibility of expressing any untrue fact and he /she had reasonably believed that such official had a power and authority to implement the threat or the promise.

b) Any fact, mentioned in from Clause (a) to (d) of Section 12 and any other fact which may be taken as evidence under any of the Sections of this Chapter, may be taken as an evidence even in his/her favour although it was expressed by him/herself, if he/she so desires.

c) A fact accepted by a person for the purpose of reaching to a compromise, by giving up any claim as a whole or in part or agreeing to pay any amount or to provide any service to any other person, may not be taken as an evidence against that person.

3) For the purpose of this Section, the following facts expressed by the following persons shall be considered to have been expressed by the party him/herself:

a) The fact expressed by the attorney (waris) of the party or by the representative of the party to a case, in the capacity of an attorney or a representative, pursuant to prevailing law,
b) Any fact expressed by a person so authorized to act upon on behalf of the party till such authority remains valid and up to the scope of the authority,
c) Any fact expressed by a person on such matter he/she deserves ownership or economic interest till such ownership or interest is valid and before the party to the case gets any right in the subject matter of the case,
d) Any fact expressed by a person regarding the subject matter of the case on which there was a joint ownership or economic interest between such person and party to the case.

10. Immediately expressed fact:

(1) If any of the following persons express any fact immediately or immediate before or after, regarding any act, incident or condition/situation such fact may be taken as evidence:
a) The person who had done that act or who had directly seen or known the act, incident or condition/situation,  
b) The victim of the act, incident or condition/situation.
2) If any person expresses any fact clearly knowing his/her physical or mental condition till the continuation to such condition the fact so expressed may be taken as evidence.

16. Special types of Data, Index etc.:

Facts mentioned in the data (facts and figure), detail out index, particulars or articles, regularly published for the consumption of the specific professions may be taken as evidence.

18. Document prepared in the course of inquiry or examination:

The fact expressed by a person in the document prepared in the course of inquiry or examination of any act, incident or situation/ condition pursuant to the prevailing law, may be taken as evidence, in case he/she appears before the court and records his/her statement as an witness.
Provided that,
(a) In case, there is no issue between the parties to the case on the facts mentioned by the expert in the Post-mortem Report or the fact so mentioned is not inconsistent with the evidence if any, such fact may be taken, as evidence even if the expert does not appear before the court. (b) An opinion expressed by a person, in the deed of and deed of spot investigation sarjameen done bye the Investigating Officer in the course of investigation, may taken as evidence for the purpose of remand even such person does not appeal before the court as wit.

19. Note (Nissa) or Certificate:

A Note or Certificate, issued by a person having the duty of issuing such Note or Certificate, may be taken as evidence.

21. Other documents with evidential value:

In addition to the document mentioned from Section 9 to Section 20, any other document may be taken as evidence to prove that such document exists.

22. Material (Dashi) Evidence:

Any material or object related to the case and identified by the witness before the court may be taken as evidence.
24. Facts not be taken as evidence:

(1) Whether the character of the parties to the case is good or bad, shall not be taken as evidence. Provided that, if the court has to decide on the character of a party to the case, fact relating to the character may be taken as evidence.

2) In case, where a person is not permitted to express any fact pursuant to Section 41, 43 and 45 and even if that person expresses that fact, such fact may not be taken as evidence.

3) If the court issues order to produce a document to a party to the case and that party does not submit the same accordingly that evidence shall not be permitted to produce in that case without the permission of the other party or the court.

4) In addition to the facts specifically mentioned in this Section, any other facts which can not be taken as evidence pursuant to this Act or other prevailing Nepal laws, may not be taken as evidence.

CHAPTER-6 DOCUMENTARY EVIDENCE

35. Documentary Evidence:

(1) A document or fact mentioned in the document has to be proved by producing such document.

2) Notwithstanding contained in Sub-section (1), any document or any fact mentioned in the document may be proved with the help of the picture, photocopy or duplicate copy which has been duly received pursuant to the law or oral evidence in the following circumstances:

   a) When it has been proved that the document is in the custody of that person against whom that document has to be produced, or
   b) When the document is in the custody of such person against whom the court cannot issue Summon/Notice or such person did not produce the document even after the service of the Summon/Notice, or
   c) When it has been proved that the document has been lost or destroyed, or
   d) When it is not easily possible to lift the document and produce it before the court, or
   e) When that document does not lie with the intending party to produce such document by virtue of the nature of the document itself. Provided that, in the case of the document mentioned in this Clause, it shall be necessary to produce the certified copy in case it is possible to get such copy pursuant to the law.

3) Notwithstanding anything contained in any Sub-section of this Section, the decision made or order issued by His Majesty the King or the Government of Nepal may be proved upon producing a document certified by the concerned officer pursuant to the prevailing Nepal Law.

36. Conclusion of Signature or the Thumb impression:

(1) When there arises a question, whether a document was written or signed or not by a person, the court may cause such person to write or sign in a separate piece of paper and shall compare that signature or thumb impression with any other signature or finger impression and may reach to the conclusion accordingly.

2) When it is not possible to reach to a conclusion comparing the signature or finger impression pursuant to Sub-section (1), the Court may conclude it with the help of other evidence.

3) Nothing contained in this Section shall bar to the Court to take the opinion of a signature or finger impression expert as the evidence.

CHAPTER-9 MISCELLINIOUS

54. Consequence of improper admission or rejection of evidence:

The improper admission or rejection of evidence pursuant to this Act shall not be ground of itself from the reversal of any verdict (decision) or order of the court. Provided that, if the improper admission or rejection of evidence causes any effect in the decision such verdict (decision) or order shall be reversed.
55. Saving:

This Act shall not bar to pursue the proceedings and conclude a case using the evidence which has been already examined pursuant to the law in force before the commencement of this Act.

**MUTUAL LEGAL ASSISTANCE ACT, 2070 (2014)**

Chapter – 2 Conditions for Provision and Matters of Mutual Legal Assistance

3. Conditions for exchange of mutual legal assistance:

(1) Where there exists a bilateral treaty between Nepal and a foreign state on the exchange of mutual legal assistance, mutual legal assistance may be exchanged between Nepal and such a foreign state. (2) Notwithstanding anything contained in sub-section (1), if a foreign state makes a request, through the diplomatic channel, to the Government of Nepal for mutual legal assistance in respect of any particular legal proceedings and the request is accompanied by the assurance of affording mutual legal assistance in similar type of judicial proceedings in the future, nothing shall bar the extension of legal assistance on a basis of reciprocity.

4. Conditions of not exchanging mutual legal assistance:

Notwithstanding anything contained in Section 3, mutual legal assistance shall not be extended if- (a) in relation to a matter of civil nature, the judicial proceedings involve the amount in controversy of less than one hundred thousand rupees, (b) in relation to a matter of criminal matter, the offence is punishable by imprisonment for less than one year or a fine of less than fifty thousand rupees, (c) the extension of mutual legal assistance as requested by a foreign state undermines or results in the undermining of the public order (odre public) or sovereignty of Nepal.

5. Matters of mutual legal assistance:

Mutual legal assistance may be provided between Nepal and a foreign state in the following matters related with judicial proceedings:

a) taking, collecting or receiving document or evidence,
b) providing information and evidence by inspecting any relevant thing or place,
c) providing originals or certified copies of relevant documents including banking, financial or business records,
d) executing searches and seizures of objects, locating or identifying persons,
e) facilitating the appearance of persons who can assist in a matter of criminal nature,
f) serving summons,
g) freezing or confiscating movable or immovable property, (h) enforcing judgments.

6. Designation of Central Authority:

(1) The Government of Nepal shall, by notification in the Nepal Gazette, designate anybody or authority as the Central Authority of the Government of Nepal for carrying out acts of mutual legal assistance between Nepal and a foreign state.

2) The authority in accordance with sub-section (1) shall execute functions in accordance with the provisions of this Act.
Chapter – 3 Procedures for Obtaining Mutual Legal Assistance

7. Request for provision of evidence:

(1) If the authority competent to make investigation or prosecution in accordance with the prevailing law has adequate grounds to believe that any document, evidence, information or object, including any banking, financial or business records, which may be of assistance in the investigation or prosecution of any offence, is in a foreign state, the authority may request the Central Authority for the provision of such document, evidence, information or object.

2) If there are adequate grounds to believe that any document, evidence, information or object, including any banking, financial or business records, which may be of assistance in the judicial proceedings, is in a foreign state, the Court may make an order for that purpose.

3) If an order is made under sub-section (1), the Court shall request the Central Authority for the provision of such document, evidence, information or object.

4) If, in making a request for the provision of any document, evidence, information or object under sub-section (1) or (3), it appears necessary to search any place or object or freeze any object, the concerned authority or Court may make a request also for executing the search of such place or object or freezing any object.

9. Request for service of process or judicial document:

(1) If, in any case filed in the Court, it is necessary to serve any process or judicial document on any person who is residing or staying in a foreign state, the Court may make an order for that purpose.

2) If an order is made under sub-section (1), the Court shall request the Central Authority for the service of such process or judicial document on the person residing or staying in the foreign country.

10. Request for taking evidence:

(1) If, in respect of any case sub judice in the Court, it is necessary to take any evidence in a foreign country, the Court may make an order for that purpose.

2) If an order is made under sub-section (1), the Court shall write to the Central Authority to that end.

12. Request for freezing or confiscating property:

(1) If there are adequate grounds to believe that the whole or any part of property related with the judicial proceedings is located in a foreign state, the Court may make an order for the freezing or confiscation of such property.

2) If an order is made under sub-section (1), the Court shall communicate it to the central authority for the freezing or confiscation of such property.

13. Request for enforcement of judgment:

(1) If it appears that any judgment made by a Court of Nepal is to be enforced by a foreign court, the Court may make an order for that purpose.

2) If an order is made under sub-section (1), the Court shall communicate it to the Central Authority.
15. Request to be made to foreign state for obtaining mutual legal assistance:

(1) If the Central Authority receives a request for mutual legal assistance under Sections 7, 8, 9, 10, 11, 12 or 13, it must request, through the diplomatic channel, the foreign state for the provision of such mutual legal assistance.

2) In making a request in accordance with sub-section (1), the Central Authority must set out the following description, in addition to the documents mentioned in Section 14: (a) the name of requesting authority or Court, (b) if a certain process has to be adopted in executing the request in the foreign state and in providing information or object as per the request, description of that process, (c) if confidentiality of request is intended, the reasons and grounds for that, (d) if the request is for facilitating the attendance of a person, arrangement for security of that person and other facilities including accommodations of that person, (e) if the request is made under any treaty and a separate process is to be adopted in making such request under the treaty, description of that process, (f) such other description as specified by the Government of Nepal by notification in the Nepal Gazette.

3) In making a request pursuant to sub-section (2), the following documents must be attached: (a) if a request is for arranging the attendance of a person, undertaking that the person shall not be detained, prosecuted or punished for any offence against law that was committed prior to the request for the attendance of that person, and that such person shall be returned to the concerned country, (b) undertaking that the person shall not be compelled to give evidence or assistance in relation to any matter other than the matter to which the request relates, (c) undertaking that the person shall not be subjected to any legal act or punishment in relation to the judicial proceedings except for making false statement or contempt of court, (d) if a request is made for search, undertaking that the objects searched and seized shall be retained safely and be returned after such purpose is served, (e) if a request is made for any document, object or information, undertaking that it shall not be published without consent of the concerned country, (f) such other documents as specified by the Government of Nepal by notification in the Nepal Gazette.

4) If, in making a request for mutual legal assistance under this Section, any treaty has not been concluded with a country for that purpose and any undertaking has to be made that if such country makes a request for mutual legal assistance of similar nature in the future, the mutual legal assistance as requested shall be provided on the basis of reciprocity, the Central Authority may make such undertaking through the diplomatic channel.

16. To be admissible in evidence:

(1) An evidence taken by a foreign country in accordance with the law of that country pursuant to a request made under Section 15 and made available to the Court through the Central Authority may be taken in evidence as if it were taken in accordance with law.

2) Notwithstanding anything contained elsewhere in this Act, nothing shall bar the settlement of a case by examining the other available evidence for the sole reason that a foreign state has refused to take evidence or evidence has not been taken by the competent authority of such state.

3) A certificate issued on behalf of the competent authority of a foreign state indicating the value of the property confiscated in the foreign state, and the date of confiscation, pursuant to a request for mutual legal assistance under Section 15 may be taken in evidence for any judicial proceedings.

4) Notwithstanding anything contained in the laws in force, examination of witness or interrogatories executed in a foreign country pursuant to this Act may be taken in evidence as if such examination of witness or written interrogatories were executed in the Court of Nepal.

18. Process or judicial document deemed to have been duly served:

(1) If a foreign state gives information that a process or judicial document has been served on the concerned person on the basis of a request made for mutual legal assistance pursuant to Section 15, the process or judicial document is deemed to have been duly served on that person.

2) If a foreign state refuses to serve a process or judicial document on the basis of a request made for mutual legal assistance pursuant to Section 15 or such country gives information through the diplomatic channel to the Court through the Central Authority that the process or judicial document could not be served since such person was not found or identified, the contents of such process or judicial document shall be published in any national daily newspaper of the country where such person is residing or staying or of Nepal.

3) Where a process or judicial document is served under subsection (2), the process or judicial document is deemed to have been duly served.
Chapter-4 Process for Making Request by Foreign State for Mutual Legal Assistance

19. Request for provision of document, evidence, information or object:

(1) If there are adequate grounds to believe that any document, evidence, information or object, which may be of assistance in the investigation of any offence or in the judicial proceedings or enforcement of judgment in a foreign country, is in Nepal, the concerned foreign state may make a request, through the diplomatic channel, to the Government of Nepal for mutual assistance.

2) If, in making a request under sub-section (1), it appears necessary to search any place or object or seize any object, the foreign state may make a request also for executing search of such place or object or seizure of any object.

21. Request for service of process or judicial document:

If it is necessary to serve any process or judicial document on any person or body who is related with judicial proceeding sub judice in a foreign court and is staying in Nepal, the foreign state may, pursuant to the order of the court of the foreign state, make a request through the diplomatic channel to the Government of Nepal for the service of such process or judicial document issued by the foreign court.

22. Request for examining witness or taking evidence:

(1) [...]. (2) If, in relation to any case sub judice in a court or body under sub-section (1), it is necessary to examine any evidence in Nepal, the foreign state may, pursuant to the order of the court or body of the foreign state, make a request through the diplomatic channel to the Government of Nepal.

28. Refusal to provide mutual legal assistance:

Notwithstanding anything contained in Section 27, the Central Authority may refuse to provide mutual legal assistance if: (a) there exists a ground provided for in Section 4, (b) the request is not made in accordance with a bilateral treaty, (c) the request is for mutual legal assistance in matter of any offence and the offence is of a political nature, (d) the description, document or evidence required pursuant to sub-section (2) of Section 27 is not received from the concerned foreign country, (e) the request is related to an offence under the Military Act, (f) there are grounds for believing that the request was made for the purpose of investigating, prosecuting or punishing a person on account of the person’s race, religion, sex, ethnic origin, nationality or political opinion, (g) the matter requested for is of insufficient importance to the investigation or information in relation to that matter can be obtained by other means, (h) there is no undertaking that the matter requested for mutual legal assistance shall not be used for any action other than that in respect of which the request was made, (i) the provision of the mutual legal assistance would impair public order (odre public).

Chapter-5 Provision of Mutual Legal Assistance

32. Provision of evidence:

(1) If a foreign state makes a request for the provision of any document, evidence, information or object pursuant to Section 19 and such document, evidence, information or object can be provided in accordance with law, the concerned authority or Court shall make order for sending certified copies of such document, evidence, information or object.
2) If a foreign state makes a request for the provision of originals of the document, evidence, information or of the object itself as provided for in sub-section (1), the concerned authority or Court may order for sending the originals of such document, evidence, information or object upon retaining certified copies thereof and, in the case of the object, shall provide such object upon maintaining records of description thereof.

3) If a foreign state makes a request for search or seizure of any object, the concerned body must make search or seizure of the object in accordance with law.

4) Notwithstanding anything contained in sub-section (3), if a request is made for the search or seizure of any object in relation to any offence, the request for the search or seizure of such object may be refused if that act is not an offence under the laws of both Nepal and the requesting foreign state.

36. To freeze or confiscate property:

(1) If a foreign state has made a request to freeze or confiscate any property situated in Nepal pursuant to Section 23, the Court must order the concerned body to freeze or confiscate the property in accordance with the laws of Nepal in force.

2) Notwithstanding anything contained in sub-section (1), if the Court is satisfied that the concerned person whose property is subject to the order of confiscation in relation to the offence has already paid the amount payable by him or her or that in the event of inability to pay such amount, that person has already served the sentence of imprisonment equal to that amount, the Court shall not make order to confiscate the property. Provided that if the property involves the proceeds of crime or instruments of crime, such property must be confiscated.

3) If the value of the property liable to confiscation is indicated in a currency other than the Nepalese currency, that value shall be converted into the Nepalese currency on the basis of the foreign exchange rate as determined by the Nepal Rastra Bank on the day of filing of application in the Court pursuant to Section 29, for the purpose of determining the amount in controversy pursuant to this Act.

Chapter-6 Miscellaneous

39. Documents, evidence to be certified:

(1) The documents, evidence attached with a request made for mutual legal assistance pursuant to this Act must be certified by the judge or competent government officer and bear the seal of office. (2) The documents, evidence not certified in fulfillment of the procedures as provided in sub-section (1) shall not be recognized.

2006 ELECTRONIC TRANSACTION ACT 2063 (2008)

Preamble:

Whereas, it is expedient to make, legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured; and where as, for controlling the acts of unauthorized use of electronic records or of making alteration in such records through the illegal manner,

("Computer") means an electro-magnetic, optical or other high-speed data processing device or system, which performs logical, arithmetic and memory functions by manipulating electro-magnetic or optical impulses, and also includes all acts of input, output, processing, storage and computer software or communication facilities which are connected or related to the computer in any computer system or computer network. 

("Computer Database") means an information, knowledge and concept or presentation of instructions, which are being prepared or have already been prepared in word, image, voice or audio visual form in a formalized manner or which have been produced by a computer, computer system or computer network, with a view to use in a computer, computer system or computer network. 

("Computer Network") means an interrelationship between two or more than two computers having intercon-
Chapter 8 - Provisions Relating to Network Service

42. Liability of Network Service Providers:

Intermediaries providing their services as network service providers shall undertake the following liabilities in regard to such service provided by them:

a) Liabilities referred to in the agreement made with the subscriber in regard to service provision

b) Liabilities referred to in the license of network service providers, and,

c) Any such other liability as prescribed.

43. Network Service Provider not to be Liable:

Notwithstanding anything contained in Section 42, no network service provider shall be liable to bear any criminal or civil liability arising from any fact or statement mentioned or included in the information or data of the third party made available in electronic form by him/her merely on the ground that he/she has made available the access to such information or data. Provided that, such a person or institution providing network service...
shall not be relieved from such liability, if he/she has made available access to such information or data with the knowledge that any fact or statement mentioned or included in such information or data contravene this Act or Rules framed hereunder.

Explanation: For the purpose of this section, “Third Party” means a network service provider who provides service as intermediary and any person over whom there is no control of the network service provider.

2007 ELECTRONIC TRANSACTION RULES 2064

12. Application to be filed for the Licence for Certification:

(1) Any person, firm or company having the following qualification, desirous to act as a Certifying Authority, shall have to file an application along with the application fee of Five Hundred Rupees to the Controller in the format as referred to in Schedule-2:

a) One who has paid-up capital of at least Ten Million Rupees or the assets equivalent thereof;

b) One who has at least Ten years of experience in computer related works;

c) Where there is no person as a board of director who has been convicted by a court in any criminal offence.

2) The following documents shall be included in the application to be filed under Sub-rule (1):

a) Certificate of registration of the firm or company;

b) Other necessary documentary evidence certifying the paid-up capital and assets of the firm or company;

c) An original copy of bank guarantee equivalent to Two Million Five Hundred Thousand Rupees with a time period of Six months issued by any commercial bank within the Nepal as a warranty for commencing the act of certification within Six months from the date of receipt of such a licence where a licence is received as a Certifying Authority;

d) The details of joint venture, if any, in the computer related works with any foreign person, firm, company or institution;

e) The evidence of any agreement, if any, made in relation to the performance of computer-related works on a joint venture with any foreign person, firm, company or institution; and

f) Other details as may be requested by the Controller.
2. Definitions.

In this Act unless there is anything repugnant in the subject or context, —

a) «basic telephone service» means the provision of any telecommunication service which consists of— (i) two-way live voice telephone service, in digital form or otherwise, over any public fixed switched network or between base stations or switches or modes of any public mobile switched network; (ii) real-time transmission or reception of facsimile images over a public fixed switched network; (iii) international telephony service; and (iv) the lease of circuits for the provision of the services specified in sub-clauses (i), (ii) and (iii);
f) «intelligence» means any speech, sound, data, signal, writing, image or video;
g) «licence» means an authorization granted by the Authority for the establishment, operation or maintenance of any telecommunication system or provision of any telecommunication service;
h) «international telephony service» means any direct or indirect telecommunication service, whether or not in digital form, conveyed by any means between a point in Pakistan and a point in another country, other than radio/broadcasting or television broadcasting;
i) «licencsee» means the grantee or holder of a licence;
j) «network termination point» means any point of termination on a telecommunication system at which terminal equipment may be connected;
k) «National Telecommunication Corporation» means the corporation to be established under section 41;
(q) «telecommunication equipment» means switches, equipment, wires, cables, apparatus, poles, structures, ducts, man-holes and other tangible property, software and data, other than terminal equipment, comprising any telecommunication system or used in connection with any telecommunication service;
r) «terminal equipment» means any apparatus directly or indirectly connected to any network termination point and used for sending, processing or receiving intelligence; (s) «telecommunication employees» means the employees of the Corporation who are transferred to the employment of the company under this Act, other than those to whom sub-section (3) of section 36 applies, and all persons, who, on the effective date for the Company, were employees of the Corporation, the former Telegraph and Telephone Department of the Federal Government and are receiving, or are entitled to receive, pensionary benefits from the Corporation; (t) «telecommunication system» means any electrical, electro-magnetic, electronic, optical or optio-electronic system for the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan, whether or not that intelligence is subjected to rearrangement, computation or any other process in the course of operation of the system, and includes a cable transmission system, a cable television transmission system and terminal equipment; (u) «telecommunication service» means a service consisting in the emission, conveyance, switching or reception of any intelligence within, or into, or from, Pakistan, whether or not the intelligence is subjected to rearrangement, computation or any other process in the course of the service;

32. Warrants for search.

(1) Where on information furnished by the Authority or Board, the Court has reason to believe that any unlicenced telecommunication system, wireless telegraphy apparatus or unapproved terminal equipment [or unapproved crypto apparatus]50 is being kept or concealed or any unlicenced telecommunication service is provided, [or any licensed is being used against the interest of national security and public safety]51 it may issue a search warrant; and the person to whom such warrant is directed, may enter the premises, vessel, aircraft, or hovercraft where such telecommunication system, wireless telegraphy apparatus or terminal equipment [or crypto apparatus]52 is allegedly kept or concealed or unlicenced telecommunication service is provided, [or any licensed service is being used against the interest of national security and public safety]53 therefrom carry out search and inspection thereof and seize such telecommunication system, wireless telegraph apparatus or terminal equipment [or crypto apparatus]54 (2) Any telecommunication equipment, wireless telegraphy apparatus
or terminal equipment seized under sub-section (1) having no ostensible owner shall vest to the Authority, or as
the case may be, the Board.

1898 CODE OF CRIMINAL PROCEDURE
(Amendments to 16 February 2017)

CHAPTER VII OF PROCESSES TO COMPEL THE PRODUCTION OF DOCUMENTS AND OTHER MOVABLE PROPERTY AND FOR THE DISCOVERY OF PERSONS WRONGFULLY CONFINED

A—Summons to produce

94. Summons to produce document or other thing:

(1) Whenever any Court, or, any officer incharge of a police-station considers that the production of any docu-
ment or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other pro-
ceeding under this Code by or before such Court or officer, such Court may issue a summons, or such officer a
written order, to the person in whose possession or power such document or thing is believed to be, requiring
him to attend and produce it or to produce it, at the time and place stated in the summons or order:
Provided that no such officer shall issue any such order requiring the production of any document or other thing
which is in the custody of a bank or banker as defined in the Banker’s Books Evidence Act, 1891 (XVII of 1891),
and relates, or might disclose any information which relates to the bank account of any person except—
a) for the purpose of investigating an offence under Sections 403, 406, 408 and 409 and. Sections 421 to 424
(both inclusive) and Sections 465 to 477-A (both inclusive) of the Pakistan Penal Code, with prior permission in
writing of a Sessions Judge ; and
b) in other cases, with the prior permission in writing of the High Court.
2) Any person required under this section merely to produce a document or other thing shall be deemed to
have complied with the requisition if he causes such document or thing to be produced instead of attending
personally to produce the same.
3) Nothing in this section shall be deemed to affect the Evidence Act, 1872, Sections 123 and 124, or to apply to
a letter, postcard, telegram or other document or any parcel or thing in the custody of the Postal or Telegraph
Authorities.

95. Procedure as to letters and telegrams:

(1) If any document, parcel or thing in such custody is, in the opinion of any Magistrate, High Court or Court of
Session wanted for the purpose of any investigation, inquiry, trial or other proceeding under this Code, such
Magistrate or Court may require the Postal or Telegraph Authorities, as the case may be, to deliver such docu-
ment, parcel or thing to such person as such Magistrate or Court directs.
2) If any such document, parcel or thing is, in the opinion of any Other Magistrate, or District Superintendent of
Police wanted for any such purpose he may require the Postal or Telegraph Department, as the case may be, to
cause search to be made for and to detain such document, parcel or thing pending the orders of any such Court.

B. —Search-warrants

96. When search warrant may be issued:

(1) Where any Court has reason to believe that a person to whom a summons or order under Section 94 or a
requisition under Section 95, sub-section (1), has been or might be addressed, will not or would not produce the
document or thing as required by such summons or requisition, or where such document or thing is not known
to the Court to be in the possession of any person, or where the Court considers that the purposes of any in-
quiry, trial or other proceedings under this Code will be served by a general search or inspection, it may issue a
search-warrant; and the person to whom such warrant is directed, may Search or inspect in accordance there-
with and the provision hereinafter contained, [Omitted by the Ordinance XXXVII of 2001, dt. 13.8.2001]

97. Power to restrict warrant:

The Court may, if it thinks fit, specify in the warrant the particular place or part thereof to which only the search
or inspection shall extend; and the person charged with the execution of such warrant shall then search or in-
spect only the place or part so specified.

98. Search of house suspected to contain stolen property, forged documents, etc.:

(1) If a Magistrate of the First Class, upon information and after such inquiry as he thinks necessary, has reason

to believe that any place is used for the deposit or sale of stolen property, or for the deposit or sale or manu-
facture of forged documents, false seals or counterfeit stamps, [bank notes, currency notes] or coins or instru-
ments or materials for counterfeiting coin or stamps, [bank notes or currency notes] for forgery, or that any

forged documents, false seals or counterfeit stamps, [bank notes, currency notes] or coins, or instruments or

materials for counterfeiting coins or Stamps or [bank notes, currency notes] for forging, are kept or deposited

in any place, or for the deposit, sale, manufacture or production of any obscene object such as is referred to in

Section 292 of the Pakistan Penal Code or that any such obscene objects are kept or deposited in any place; he

may by his warrant authorize any police-officer above the rank of a constable-

a) to enter with such assistance as may he required, such place, and

b) to search the same in manner specified in the warrant, and

c) to take possession of any property, document, seals, stamps or [bank notes, currency notes] or coins therein

found which he reasonably suspects to be stolen, unlawfully obtained, forged, false or counterfeit and also of

any such instruments and material or of any such obscene objects as aforesaid, and

d) to convey such property, documents, seals, stamps, [bank notes, currency notes], coins, instruments or ma-

terials or such obscene objects before a Magistrate, or to guard the same on the spot until the offender is taken

before a Magistrate or, otherwise to dispose thereof in some place of safety and

e) to take into custody and carry before a Magistrate every person, found in such place or who appears, to have

been privy to the deposit, sale or manufacture or keeping of any such property, documents, seals, stamps,

3o[bank notes, currency notes], coins, instruments or materials or such obscene objects knowing or having

reasonable cause to suspect the said property to have been stolen or otherwise unlawfully obtained or the said

documents, seals, stamps, [bank notes, currency notes], coins, instruments or materials to have been forged,

falsified or counterfeited, or the said instruments or materials to have been or to be intended to be used for

counterfeiting coin or stamps, [bank notes, currency notes] or for forging or the said obscene objects to have

been or to be intended to be sold, let to hire, distributed, publicly exhibited, circulated, imported or exported.

2) The provisions of this section with respect to-

a) counterfeit coin,

b) coin suspected to be counterfeit, and

c) instruments or materials for counterfeiting coin,

shall so far as they can be made applicable, apply respectively to

a) pieces of metal made in contravention of the Metal Tokens Act, 1889, or brought into Pakistan in contraven-
tion of any notification for the time being in force under Section 16 of the Customs Act, 1969;

b) pieces of metal suspected to have been so made or to have been so brought, into Pakistan or to be intended
to be issued in contravention of the former of those Acts, and

c) instruments or materials for making pieces of metal in contravention of that Act.

99. Disposal of things found in search beyond jurisdiction:

When, in the execution of a search-warrant at any place beyond the local limits of the jurisdiction of the Court

which issued the same any of the things for which search is made are found, such things together with the list

of the same, prepared under the provisions hereinafter contained, shall be immediately taken before the Court

issuing the warrant unless such place is nearer to the Magistrate having jurisdiction herein than to such Court,
in which case the list and things shall be immediately taken before such Magistrate; and unless there be good cause to the contrary, such Magistrate shall make an order authorizing them to be taken to such Court.

99-A. Power to declare certain publications forfeited and to issue search-warrants for the same:

(1) Where-
   a) any newspaper, or book as defined in the [West Pakistan Press and Publications Ordinance, 1963, or any other law relating to press and publication for the time being in force],
   b) any document, wherever printed, appears to the Provincial Government to contain any treasonable or seditious matter or any matter which is prejudicial to national integration or any matter which promotes or is intended to promote, feelings of enmity or hatred between different classes of the citizens of Pakistan or which is deliberately and maliciously intended to outrage the religious feelings of any such class, by inputting the religion or religious belief of that class, [or any matter, of the nature referred to in clause (ii) of sub-section (1) of Section 24 of the West Pakistan Press and Publication Ordinance, 1963] that is to say, any matter the publication of which is punishable under Section 123-A or Section 124-A or Section 295-A or Section 298-A or Section 298-B or Section 298-C of the Pakistan Penal Code, the Provincial Government may, by notification in the official Gazette stating the grounds of its opinion, declare every copy of the issue of the newspaper containing such platter and every copy of such book or other document to be forfeited to Government, and thereupon any police-officer may seize the same wherever found in Pakistan and any Magistrate may by warrant authorize any police-officer not below the rank of sub-Inspector to enter upon and search for the same in any premises where any copy of such issue or any such book or other document may be reasonably suspected to be.

(2) In sub-section (1) «document» includes also any painting, drawing or photograph, or other visible representation.


99-E. Evidence to prove nature or tendency of newspaper:

On the hearing of any such application with reference to any newspaper, any copy of such newspaper may be given in evidence in aid of the proof of the nature or tendency of the words, signs or visible representations contained in such newspaper, in respect or which the order of forfeiture was made.

E. —Miscellaneous

104. Power to impound document, etc., produced:

Any Court may, if it thinks fit, impound any document or thing produced before it under this Code.

CHAPTER XXV OF THE MODE OF TAKING AND RECORDING EVIDENCE IN INQUIRIES AND TRIALS

353. Evidence to be taken in presence of accused:

Except as otherwise expressly provided, all evidence taken under Chapters XX, XXI, XXII and XXII-A shall be taken in the presence of the accused, or, when his personal attendance is dispensed with, in presence of his pleader.
354. Manner of recording evidence:

In inquiries and trials (other than summary trials) under the Code by or before a Magistrate or Sessions Judge, the evidence of the witnesses shall be recorded in the following manner.

---

1984 THE QANUN-E-SHAHADAT ORDER

ADMISSIONS

30. Admission defined:

An admission is a statement, oral or documentary which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons and under the circumstances, hereinafter mentioned.

---

CHAPTER V OF DOCUMENTARY EVIDENCE

72. Proof of contents of documents:

The contents of documents may be proved either by primary or by secondary evidence.

73. Primary evidence:

«Primary evidence» means the document itself produced for the inspection of the Court.

Explanation 1: Where a document is executed in several parts, each part is primary evidence of the document.

Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, counterpart is primary evidence as against the parties executing it.

Explanation 2: Where a number of documents are all made by one uniform process, as in the case of printing, Lithography or photography, each is primary evidence of the contents of the rest; but where they are all copies of a common original they are not primary evidence of the contents of the original.

Illustrations

A person is shown to have been in possession of a number of placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original.

74. Secondary evidence:

«Secondary evidence means and includes—

1) certified copies given under the provisions hereinafter contained; 2) copies made from the original by mechanical process which is themselves insure the Accuracy of the copy, and copies compared with such copies; 3) copies made from or compared with the original.

4) counterparts of documents as against the parties who did not execute them; 5) oral accounts of the contents of a document given by some person who has himself seen it.

Illustrations

a) A photograph of an original is secondary evidence of its contents though the two have not been compared if it is proved that the thing photographed was the original.
b) A copy, compared with a copy of a letter made by a copying machine is secondary evidence of the contents of the letter, if it is shown that the copy made by the copying machine was made from the original.
c) A copy transcribed from a copy, but afterwards compared with the original, is secondary evidence; but the copy not so compared is not secondary evidence of the original, although the copy from which it was transcribed was compared with the original.
d) Neither an oral account of a copy compared with the original, nor an oral account of a photograph or machine-copy of the original, is secondary evidence of the original.

75. Proof of documents by primary evidence:

Documents must be proved by primary evidence except in the cases hereinafter mentioned.

76. Cases in which secondary evidence relating to documents may be given:

Secondary evidence may be given of the existence, condition or contents of a document in the following cases:

i. when the original is shown or appears to be in the possession or power of the person against whom the document is sought to be proved, or of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when after the notice mentioned in Article 77 such person does not produce it;
ii. when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative-interest;
iii. when the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;
iv. when, due to the volume or bulk of the original, copies thereof have been made by means of microfilming or other modern devices;
v. when the original is of such a nature as not to be easily movable;
vii. when the original is public document within the meaning of Article 85;
viii. when the originals consist of numerous accounts or other documents which cannot conveniently be examined in Court, and the fact to be proved is the general result of the whole collection;
vii. when an original document forming part of a judicial record is not available and only a certified copy thereof is available, certified copy of that certified copy shall also be admissible as a secondary evidence.

In cases (a), (c), (d) and (e), any secondary evidence of the contents of the document is admissible. In case (b), the written admission is admissible.

In case (f) or (g), certified copy of the document, but no other kind of secondary evidence, is admissible.

In case (h), evidence may be given as to the general result of the documents by any person who has examined them and who is skilled in the examination of such document.

77. Rules as to notice to produce:

Secondary evidence of the contents of the documents referred to in Article 76, paragraph (a), shall not be given unless the party proposing to give such secondary evidence has previously given to the party in whose possession or power the document is, or to his advocate, such notice to produce it as is prescribed by Law and, if no notice is prescribed by law, then such notice as the Court considers reasonable under the circumstances of the case: Provided that such notice shall not be required in order to render secondary evidence admissible in any of the following cases, or in any other case in which the Court thinks fit to dispense with it:
1) when the document to be proved is itself a notice;
2) when, from the nature of the case, the adverse party must know that he will be required to produce it;
3) when it appears or is proved that the adverse party has obtained possession of the original by fraud or force;
4) when the adverse party or his agent has the original in Court;
5) when the adverse party or his agent has admitted the loss of the document;
6) when the person in possession of the document is out of reach of, or not subject to, the process of the Court.
**81. Admission of execution by party to attested document:**

The admission of a party to an attested document of its execution by himself shall be sufficient proof of its execution as against him, though it be a document required by law to be attested.

**PRESUMPTION AS TO DOCUMENTS**

**90. Presumption as to genuineness of certified copies:**

(1) The Court shall presume every document purporting to be a certificate, certified copy or other document, which is by law declared to be admissible as evidence of any particular fact and which purports to be duly certified by any officer of the Federal Government or a Provincial Government to be genuine: Provided that such document is substantially in the form and purports to be executed in the manner directed by law in that behalf.

2) The Court shall also presume that any officer by whom any such document purports to be signed or certified, held when he signed it, the official character which he claims in such document.

**91. Presumption as to documents produced as record of evidence:**

Whenever any document is produced before any Court, purporting to be a record or memorandum of the evidence, or of any part of the evidence, given by a witness in a judicial proceeding or before any officer authorized by law to take such evidence or to be a statement or confession by any prisoner or accused person, taken in accordance with law, and purporting to be signed by any Judge or Magistrate or by any such officer as aforesaid, the Court shall presume— that the document is genuine; that any statements as to the circumstances under which it was taken, purporting to be made by the person signing it are true and that such evidence, statement or confession was duly taken.

**92. Presumption as to genuineness of documents kept under any law:**

The Court shall presume the genuineness of every document purporting to be a document directed by any law to be kept by any person, if such document is kept substantially in the form required by law and is produced from proper custody.

**158. Production of documents:**

(1) A witness summoned to produce a document shall, if it is in his possession or power, bring it to Court, notwithstanding any objection which there may be to its production or to its admissibility. The validity of any objection shall be decided on by the Court.

2) The Court, if it sees fit may inspect the document unless it refers to matters of State, or take other evidence to enable it to determine on its admissibility.

3) If for such a purpose it is necessary to cause any document to be translated, the Court may, if it thinks fit, direct the translator to keep the contents secret, unless the document is to be given in evidence; and if the translator disobeys such direction, he shall be held to have committed an offence under Section 166 of the Pakistan Penal Code (Act XLV of 1860).
159. Giving, as evidence, of document called for and produced on notice:

When a party calls for a document which he has given the other party notice to produce and such document is produced and inspected by the party calling for its production, he is bound to give it as evidence if the party producing it requires him to do so 160. Using, as evidence, of document production of which was refused on notice:

When a party refuses to produce a document which he has had notice to produce; he cannot afterwards use the document as evidence without the consent of the other party or the order of the Court.

Illustrations

A sues C on an agreement and gives B, notice to produce it. At the trial A calls for the document and B refuses to produce it. A gives secondary evidence of its contents, B seeks to produce the document itself to contradict the secondary evidence given by A, or in order to show that the agreement is not stamped. He cannot do so.

1997 ANTI-TERRORISM ACT

5)

The [Anti-Terrorism Court][24] to which a case is transferred or recalled for trial under subs-s. (4), shall proceed with the case from the stage at which it was pending immediately before such transfer or recall and it shall not be bound to recall or re-hear any witness who has given evidence and may act on the evidence already recorded ]

4. Composition and appointment of presiding officers of [25](AntiTerrorism Court)- 1) (Anti-Terrorism Court) shall consist of a Judge, being a person who:-

) [26][is a Judge of High Court or is] is or has been Sessions Judge or an additional Sessions Judge; or

i) has exercised the power of a District Magistrate or an Additional District Magistrate or and has successfully completed an advance course in Shariah, (Islamic Law )conducted by the International Islamic University Islamabad; or

ii) Has for a period of not less than ten years been an advocate [27](of High Court) 2) Subject to the provisions of subs. (4) the Federal Government or the Provincial Government if directed by the Federal Government to establish a Court under this Act, shall after consultation with the Chief Justice of the High Court appoint a judge of each Court.

) A Judge shall hold office for a period of two and a half years but may be appointed for such further term or part of term or part of tem as the Government appointing the Judge may determine.

) Judge may be removed from his officer prior to the completion of the period for which he has been appoint-ed after consultation with the Chief Justice of High Court. Explanation. The qualification of being an advocate for a period of not less than ten years may be relaxed in the case of a suitable person who is a graduate from a Islamic University and has studied Islamic Shariah and Fiqah as a major subject.

) [28][In a case a judge is on leave or for any other temporarily unable to perform his duties the Government making appointment of such judge may , after consultation with the Chief justice of High Court authorize the Sessions judge, having jurisdiction at the principal seat of the Anti-Terrorism Court to conduct proceedings of urgent nature so long as such judge is unable to perform his duties].

19. Procedures and powers of the Anti-Terrorism Court

(...) 9)[41]( Anti-Terrorism Court) shall not, merely by reason of a change in its composition or transfer of a case under sub-section (3) of section 12, be bound to recall and re-hear any witness who has given evidence and may act on the evidence already recorded (...)

21. D. Bail

(...) 4) In exercising its powers in relation to a person seeking bail under this Act, the Court shall have regard to such of the following considerations (as well as to any others which it consider relevant)

a) The nature and seriousness of the offence with which the person is charged;
b) The character, antecedents, associations and community ties of the person;
c) The time which the person has already spent in custody and the time which he is likely to spend in custody if he is not admitted to bail; and
d) The strength of the evidence of his having committed the offence. (...)

21. E. Remand

(...)

2) No extension of the time of the remand of the accused in police custody [or custody of any other Investigating Agency joined in the investigation ] [59] shall be allowed, unless it can be shown by the Investigating Officer, to the satisfaction of the Court that further evidence may be available and the Court is satisfied that no bodily harm has been or will be caused to the accused; (...)


Notwithstanding anything contained in the Qanoon-e-Shahadat, 1984 (President's Order No.10 of 1984) or any other law for the time being in force, where in any Court proceeding held under this Act the evidence (which include's circumstantial proceedings held under this Act the evidence ) produced raises the presumption that there is a reasonable probability that the accused has committed the offence, any confession made by the accused during investigation without being compelled, before a police officer not below the rank of a District Superintendent of Police, may be admissible in evidence against him if the Court so deems fit; Provided that the District Superintendent of Police before recoding any such confession, had explained to the person making it that he is not bound to make a confession and that if he does so it may be used as evidence against his and that no District Superintendent of Police has recorded such confession unless, upon questioning the person making it the District Superintendent of Police had reason to believe that it was made voluntarily; and that when he recorded the confession, he made a memorandum at the foot of such record to the following effect. 'I have explained to (...name...) that he is not bound to make a confession and that if he does so any confession he may make may be used as evidence against him and I believes that this confession was voluntarily made. It was taken in my presence, and was read over to the person making it and admitted by him to be correct, and it contains a full and true account of the statement made by him.

2009 PREVENTION OF ELECTRONIC CRIMES ORDINANCE

2. DEFINITIONS

(1) In this Ordinance, unless there is anything repugnant in the subject or context:
a)«access» means gaining access to any electronic system or data held in an electronic system or by causing the electronic system to perform any function to achieve that objective;
b)«Authority» means the Pakistan Telecommunication Authority established under section 3 of the Pakistan Telecommunication (Reorganization) Act, 1996 (XCI of 1996)
c)«data» means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in an electronic system including but not limited to computer program, text, images, sounds, video and information within adatabase or electronic system;
d)«Electronic Certification Accreditation Council» means the council established under section 18 of Electronic Transaction Ordinance, 2002 (LI of 2002)
e)«electronic» includes but not limited to electrical, digital, analogue, magnetic, optical biochemical, electrochemical, electromagnetic, radio electric or wireless technology;
f)«electronic device» means hardware which performs one or more specific functions and operates on any form or combination electrical energy;
g)«electronic mail massage» means any data generated by an electronic system for a unique electronic mail adress;
h)«electronic mail address» means destination, commonly expressed as a string of characters, consistinf of a unique user or group name or mailbox, commonly referred to as the local part, and a reference to an internet or intranet domain, commonly referred to as the domain part, whether or not displayed, to which an electronic mail message can be sent or delivered or originated from and inclueds an electronic mail adress which may be...
permanent, removable or any other electronic storage medium;
m) «encrypt data» means data which has been transformed or scrambled from its plain version or text to an unreadable or incomprehensible format and is recoverable by an associated decryption or decoding technique, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium which such data occurs or can be found for the purpose of protection such data;
n) «function» includes, logic, control, arithmetic, deletion, storage and retrieval and communication and telecommunication to, from or within an electronic system;
p) «offence» includes:
i- any offences punishable under this Ordinance;
ii- any offence punishable under the laws mentioned in the Schedule; or
iii- any offence punishable under any other law for the time being in force if committed through or by using any computer, electronic system, electronic means or electronic device as a mean or tool;
t) «sensitive electronic system» means an electronic system used directly in connection with or necessary for:
i- the security, defence or international relations of Pakistan;
ii- the existence or identity of confidential source of information relating to the enforcement of criminal law;
iii- the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or commerce infrastructure;
v- the protection of public safety including system related to essential emergency services such as police, civil defence and medical services;
- the purpose declared as such by the Federal Government in accordance with the prescribed procedure; or
i- containing any data or database protected as such by any other law.
u) «service provider» includes but not limited to:
- person acting as a service provider in relation to sending, receiving, storing or processing of electronic communication or the provision of other services in relation to electronic communication through any electronic system;
- person who owns, possesses, operates, manages or controls a public-switched network or provides telecommunications services; or
- any other person who processes or stores data on behalf of such electronic communication service or users of such service;
v) «subscriber information» means any information contained in any form that is held by a service provider, relating to subscriber's services other than traffic data and by which can be established:
- the type of communication service used, the technical provisions taken thereto and the period of service;
- he subscriber's identity, postal, geographic electronic mail address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or
- any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;
w) «traffic data» means any data relating to a communication by means of an electronic system, generated by an electronic system that fanned a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;
x) «Tribunal» means the Information and Communication Technologies Tribunal constituted under section 31; and
y) «unauthorized access» means access of any kind by any person to any electronic system or data held in an electronic system or electronic device, without authority or in access of authority, if he is not himself entitled to control access of the kind in question to the electronic system or electronic device, or data and he does not have consent to such access from any person, so entitled.

CHAPTER - II
OFFENCES AND PUNISHMENTS

3. Criminal access.

Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or electronic device with or without infringing security measures, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees, or with both.
4. Criminal data access.

Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such unauthorized access shall be punished with imprisonment of either description for a term which may extend to ten years, or with fine or with both.

5. Data damage.

Whoever with intent to illegal gain or cause harm to the public or any person, damages any data shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both:

Explanation.- For the purpose of this section the expression “data damage” includes but not limited to modifying, altering, deleting, deterioration, erasing, suppressing, changing location of data or making data temporarily or permanently unavailable, halting electronic system, choking the networks or affecting the reliability or usefulness of data.

6. System damage.

Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstructs the functioning, reliability or usefulness of an electronic system or electronic device by inputting, transmitting, damaging, deleting, altering, tempering, deteriorating or destroying any data or services or halting electronic system or choking the networks shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or, with both:

Explanation.- For the purpose of this section the expression “services” include any kind of service provided through electronic system.

7. Electronic fraud.

Whoever for wrongful gain interferes with or uses any data, electronic system or electronic device or induces any person to enter into a relationship or with intent to deceive any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

8. Electronic forgery.

Whoever for wrongful gain interferes with data, electronic system or electronic device, with intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not Shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both.

9. Misuse of electronic system or electronic device.

(1) Whoever produces, possesses, sells, procures, transports, imports, distributes or otherwise makes available an electronic system or electronic device, including a computer program, designed or adapted primarily for the
purpose of committing any of the offences established under this Ordinance or a password, access code, or similar data by which the whole or any part of an electronic system or electronic device is capable of being accessed or its functionality compromised or reverse engineered, with the intent that it be used for the purpose of committing any of the offences established under this Ordinance, is said to commit offence of misuse of electronic system or electronic devices:
Provided that the provisions of this section shall not apply to the authorized testing or protection of an electronic system for any lawful purpose.
2) Whoever commits the offence described in sub-section (I) shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

10. Unauthorized access to code.

Whoever discloses or obtains any password, access as to code, system design or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain, do reverse engineering or cause wrongful loss to any person or for any other unlawful purpose shall be punished with imprisonment of either description for a term which may extend to three years, or with, or with both.


(I) Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be accessed a computer or computer network or electronic system or electronic device or by any available means, and thereby knowingly engages in or attempts to engage in a terroristic act commits the offence of cyber terrorism.
Explanation 1.-For the purposes of this section the expression «terroristic intent» means to act with the purpose to alarm, frighten, disrupt, harm, damage, or carry out an act of violence against any segment of the population, the Government or entity associated therewith.
Explanation 2.-For the purposes of this section the expression «terroristic act» includes, but is not limited to,-
 "a) altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness; or death to any segment of the population; 
 b) transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity; 
 c) aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the • commission of such act of violence is actually completed; or 
 d) stealing or copying, or attempting to steal or copy, or secure classified information or data necessary to manufacture any form of chemical, biological or nuclear weapon, or any other weapon of mass destruction.
2) Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life, and with fine and in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten million rupees, or with both.

17. Enhanced punishment for offences involving sensitive electronic system.

( I) Whoever causes criminal access to any sensitive electronic system in the course of the commission of any of the offences established under this Ordinance shall, in addition to the punishment prescribed for that offence, be punished with imprisonment of either description for a term which may extend to ten years, or with fine not exceeding one million rupees, or with both.
2) For the purposes of any prosecution under this section, it shall be presumed, until contrary is proved, that the accused had the requisite knowledge that it was a sensitive electronic system.
18. Of abetments, aids, or attempt to commits offence.

(I) Any person who knowingly and willfully abets the commission of or who aids to commit or does any act preparatory to or in furtherance of the commission of any offence under this Ordinance shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

2) Any person who attempts to commit an offence under this Ordinance, shall be punished for a term which may extend to one-half of the longest term of imprisonment provided for that offence.

Explanation.- For aiding or abetting an offence to be committed under this section, it is immaterial whether the offence has been committed or not.

CHAPTER - IV
ESTABLISHMENT OF INVESTIGATION AND PROSECUTION AGENCIES

24. Establishment of investigation agencies and prosecution.

The Federal Government shall establish a specialized investigation and prosecution cell within Federal Investigation Agency to investigate and prosecute the offences under this Ordinance:
Provided that till such time any agency is so established, the investigation and prosecution of an offence shall be conducted in accordance with the provisions of the Code:
Provided further that any police officer investigating an offence under this Ordinance may seek assistance of any special investigation agency for any technical in put, collection and preservation of evidence.


25. Powers of officer.- (1) Subject to obtaining search warrant an investigation officer shall be entitled to,-
   a) have access to and inspect the operation of any electronic system;
   b) use or cause to be used any such electronic system to search any data contained in or available to such electronic system;
   c) have access to or demand any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such electronic system into readable and comprehensible format or plain version;
   d) require any person by whom or on whose behalf, the investigating officer has reasonable cause to believe, any electronic system has been used;
   e) require any person having charge of, or otherwise concerned with the operation of such electronic system to provide him reasonable technical and other assistance as he may require for the purposes of clauses (a), (b) and (c); and
   f) require any person who is in possession of decryption information of under investigation electronic system, device or data to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

   Explanation.- Decryption information means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable form and from cipher text to its plain text.

2) The police officer may, subject to the proviso, require a service provider to submit subscriber information relating to such services in respect of a person under investigation in that service provider's possession or control necessary for the investigation of the offence:
Provided the investigating officer shall get prior permission to investigate any service provider from the licensing authority where prior permission of the licensing authority is required under any law to investigate the licensed service provider.

Any person who obstructs the lawful exercise of the powers under sub-sections (1) or (2) shall be liable to punishment with imprisonment of either description for a term, which may extend to one year, or with fine not exceeding one hundred thousand rupees, or with both.
26. Real-time collection of traffic data.

(1) The Federal Government may require a licensed service provider, within its existing or required technical capability, to collect or record through the application of technical means or to cooperate and assist any law enforcement or intelligence agency in the collection or recording of traffic data or data, in real-time, associated with specified communications transmitted by means of an electronic system.

2) The Federal Government may also require the service provider to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.

27. Retention of traffic data.

(1) A service provider shall, within its existing or required technical capability, retain its traffic data minimum for a period of ninety days and provide that data to the investigating agency or the investigating officer when required. The Federal Government may extend the period to retain such data as and when deemed appropriate.

2) The service providers shall retain the traffic data under sub section (1) by fulfilling all the requirements of data retention and its originality as provided under sections 5 and 6 of the Electronic Transaction Ordinance, 2002 (LI of 2002).

Any person who contravenes the provisions of this section shall be punished with imprisonment for a term of six months or with fine or with both.

28. Trans-border access.

For the purpose of investigation the Federal Government or the investigation agency may, without the permission of any foreign Government or international agency access publicly available electronic system or data notwithstanding the geographical location of such electronic system or data, or access or receive, through an electronic system, data located in foreign country or territory, if it obtains the lawful and voluntary consent of the person who has the lawful authority to disclose it:

Provided that such access is not prohibited under the law of the foreign Government or the international agency:

Provided further that the investigating agency shall inform in writing to the Ministry of Foreign Affairs of Government of Pakistan and other relevant agencies, as the case may be, about the investigation conducted under this section.

CHAPTER - V
INTERNATIONAL COOPERATION

29. International cooperation.

(1) The Federal Government may cooperate with any foreign Government, Interpol or any other international agency with whom it has or establishes reciprocal arrangements for the purposes of investigations or proceedings concerning offences related to the electronic system and data, or for the collection of evidence in electronic form of an offence or obtaining expedient preservation and disclosure of traffic data or data by means of an electronic system or real-time collection of traffic data associated with specified communications or interception of data.

2) The Federal Government may, without prior request, forward to such foreign Government, Interpol or other international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the other Government or agency in initiating or carrying out investigations or proceedings concerning any offence.

3) The Federal Government may require the foreign Government, Interpol or other international agency to keep the information provided confidential or use it subject to some conditions.

4) The investigating agency shall, subject to approval of the Federal Government, be responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authori-
ties competent for their execution.
5) The Federal Government may refuse to accede to any request made by such foreign Government, Interpol or international agency if the request concerns an offence which is likely to prejudice its sovereignty, security, public order or other essential interests.
6) The Federal Government may postpone action on a request if such action would prejudice investigations or proceedings conducted by its investigation agency.

CHAPTER - VI
INFORMATION AND COMMUNICATION TECHNOLOGIES TRIBUNAL

30. Information and Communication Technologies Tribunal

(1) As soon as possible after the commencement of this Ordinance, the Federal Government shall, by notification in the official Gazette, constitute the Information and Communication Technologies Tribunal whose principal seat shall be at Islamabad.
2) The Tribunal may hold its sittings at such place or places as the Federal Government may decide.
3) The Tribunal shall consist of a Chairman and as many members as the Federal Government may determine but not more than seven members.
4) The Chairman may constitute Benches of the Tribunal and unless otherwise directed by him a Bench shall consist of not less than two members. A Bench shall exercise such powers and discharge such functions as may be prescribed. There shall be established at least one Bench in each province.
5) The Federal Government shall appoint the Chairman and members of the Tribunal.

31. Qualification for appointment.

(1) A person shall not be qualified for appointment as Chairman unless he is, or has been, or is qualified for appointment as a judge of the High Court.
2) A person shall not be qualified for appointment as a Member unless he has for two years served as a District and Sessions Judge; as for a period of not less than ten years been an advocate of a High Court; or as special knowledge of legislation and professional experience of not less than ten years in the field of telecommunication and information technologies.

36. Right for legal representation.

The parties in appeal may either appear in person or authorize one or more legal practitioners, and in case of a corporate body any of its officers, to present the case before the Tribunal.

37. Amicus curiae.

The Tribunal may, if it so requires, be assisted in technical aspects in any case by an amicus curiae having knowledge and experience in information communication technologies, finance and economics.
2) The Federal Government shall maintain a list of amicus curiae having relevant qualifications and experience.
3) The Tribunal in consultation with the Federal Government shall determine the remuneration of the amicus curiae and the Tribunal may decide the party or parties to pay such remuneration, keeping in view the circumstances of each case.
38. Procedure and powers of Tribunal.

(1) Subject to the provision of this Ordinance and the rules made thereunder, the Tribunal,—
   i) may, where it deems necessary, apply the procedures as provided in the Codi:: or, as the case may be, in the Code of Civil Procedure, 1908 (Act V of 1908);
   ii) in the exercise of its civil jurisdiction, shall have powers vested in the civil court under the Code of Civil Procedure, 1908; and
   iii) in the exercise of its criminal jurisdiction, shall have the same powers as are vested in the Court of Session under the Code.

39. Appeals to Tribunals.

(1) Any person aggrieved by any of the following orders may, within fifteen days from the date of such order, prefer an appeal to the Tribunal, namely:-
   a) any decision of the Authority; or
   b) any decision of the Electronic Certification Accreditation Council:
   Provided that no appeal shall lie to the ICT Tribunal from an order passed by the Authority or the Electronic Certification Accreditation Council with the consent of the parties.

2) Any appeal against a decision of the Authority shall be accompanied by a court fee of,-
   a) ten thousand rupees where the valuation of the subject matter in issue is not more than five million rupees;
   b) fifty thousand rupees where the valuation of the subject matter in issue is more than five million rupees but not more than ten million rupees; and
   c) one hundred thousand rupees where the valuation of the subject matter in issue is more than ten million rupees.

3) The appeal filed before the Tribunal under sub-section (I) shall be dealt with by it as expeditiously as possible and the Tribunal shall dispose of the appeal finally within ninety days from the date of receipt of the appeal.

40. Power of Tribunal.

The Tribunal while hearing an appeal under section 40 shall have all the powers as are vested in the court of first appeal under the Code or in exercise of its civil jurisdiction under the Code of Civil Procedure, 1908 (Act V of 1908) in respect of appeal against any decision or order of the Authority or the Electronic Certification Accreditation Council.

STATEMENT OF OBJECTS AND REASONS

A wide array of new and complex Information and Communication Technologies (ICT) related crimes are not covered under any of the existing Legislation; therefore, to counter the spread of electronic crimes, there is an urgent need for having a legislation for prevention of electronic crimes in Pakistan to check electronic crimes ranging from damage to data and electronic system; electronic fraud and forgery, unauthorized access to code and misuse of encryption, cyber stalking, spamming, spoofing, unauthorized interception and cyber terrorism. This law also provides a comprehensive mechanism for investigation, prosecution and trial’s procedures for prevention of electronic crimes.

2. By establishing a proper mechanism of investigation, prosecution and trial for electronic crimes in the field of Information and Communication Technologies, inter alia:
   a) a sense of security, safety and protection will prevail in each and every segment of society that uses or deals with IT and Telecommunication;
   b) increasing rate of electronic crimes in the country will be curbed;
   c) soft image of Pakistan will be developed in the world;
   d) the confidence of Bankers and their customers in electronic transactions will be enhanced which consequent-ly will boost e-anking and e-Commerce in Pakistan;
   e) the IT entrepreneurs will have more secure cyberspace which will be friendly and congenial to their business;
   f) Pakistan will be able to take another step further towards paper free economy; and
   g) it will romote the whole ICT sector and build confidence in the society to accept the use of more and more
Definitions.-

(l) In this Act, unless there is anything repugnant in the subject or context,
a) “act” includes
i. a series of acts or omissions contrary to the provisions of this Act; or
ii. causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device and whether having temporary or permanent impact;
b) “access to data” means gaining control or ability to use, copy, modify or delete any data held in or generated by any device or information system;
c) “access to information system” means gaining control or ability to use any part or whole of an information system whether or not through infringing any security measure;
d) “Authority” means the Pakistan Telecommunication Authority established under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996);
e) “authorization” means authorization by law or the person empowered to make such authorization under the law:

Provided that where an information system or data is available for open access by the general public, access to or transmission of such information system or data shall be deemed to be authorized for the purposes of this Act;

“authorized officer” means an officer of the investigation agency authorized to perform any function on behalf of the investigation agency by or under this Act;

Code” means the: Code of Criminal Procedure, 1898 (Act V of 1898);

content data” means any representation of fact, information or concept for processing in an information system including source code or a program suitable to cause an information system to perform a function;

critical infrastructure” means critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in:
i. major detrimental impact on the availability, integrity or delivery of essential services - including those services, whose integrity, if compromised, could result in significant loss of life or casualties- taking into account significant economic or social impacts; or
ii. significant impact on national security, national defense, or the functioning of the state”.

Provided that the Government may designate any private or Government infrastructure in accordance with the objectives of sub-paragraphs (i) and (ii) above, as critical infrastructure as may be prescribed under this Act.
a) “critical infrastructure information system or data” means an information system, program or data that supports or performs a function with respect to a critical infrastructure;
b) “damage to an information system” means any unauthorized change in the ordinary working of an information system that impairs its performance, access, output or change in location whether temporary or permanent and with or without causing any change in the system;
c) Data includes content data and traffic data;
d) “data damage” means alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable;
e) “device” includes:

i. Physical device or article;
ii. Any electronic or virtual tool that is not in physical form;
iii. A password, access code or similar data, in electronic or other form, by which the whole or any part of an information system is capable of being accessed; or
iv. Automated, self-executing, adaptive or autonomous device, programs or information system;
f) “dishonest intention” means intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence;
g) “electronic” includes electrical, digital, magnetic, optical, biometric, electrochemical, electromechanically, wireless or electromagnetic technology;
h) “identity information” means an information which may authenticate or identify an individual or an information system and enable access to any data of information system;

i) “information” includes text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) and codes including object code and source code.

j) “information system” means an electronic system for creating, generating, sending, receiving, storing reproducing, displaying, recording or processing any information;

k) “integrity” means, in relation to an electronic document, electronic signature or advanced electronic signature, the electronic document, electronic signature or advanced electronic signature that has not been tampered with, altered or modified since particular point in time,

l) “interference with information system or data” means and includes an unauthorized act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data;

m) “investigation agency” means the law enforcement agency established by or designated under this Act;

n) “minor” means, notwithstanding anything contained in any other law, any person who has not completed the age of eighteen years;

o) “offence” means an offence punishable under this Act except when committed by a person under ten years of age or by a person above ten fourteen years of age, who has not attained sufficient maturity of understanding to judge the nature and consequences of his conduct on that occasion;

p) “rule” means rule made under this Act;

za) “seize” with respect to an information system or data includes taking possession of such system or data or making and retaining a copy of the data;

zb) “service provider” includes a person who:

i. Acts as a service provider in relation to sending, receiving, storing, processing or distributing of any electronic communication through an information system;

ii. Owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

iii. Processes or stores data on behalf of such electronic communication service or users of such service;

zc) “subscriber information” means any information held in any form by a service provider relating to a subscriber other than traffic data;

zd) “traffic data” includes data relating to a communication indicating its origin, destination, route, time, size, duration or type of service;

zf) “unauthorized interception” shall mean in relation to an information system or data, any interception without authorization or in violation of the terms and conditions of the authorization, and

zg) “unsolicited information “means the information which is sent for commercial and marketing purpose against explicit rejection of the recipient and does not include marketing authorized under the law.

nless the context provides otherwise, any other expression used in this Act or rules made thereunder but not defined in this act, shall have the same meanings assigned to the expressions in the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898) and the Qanoon-e-Shahadat Order, 1984 (P.O.No.X of 1984), as the case may be.

CHAPTER II
OFFENCES AND PUNISHMENTS

3. Unauthorized access to information system or data.

Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.

2. Unauthorized copying or transmission of data.

Whoever either dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for the term which may extend to six months, or with fine which may be extend to one thousand rupees or with both.
5. Interference with information system or data.

Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both.

6. Unauthorized access to critical infrastructure information system or data.

Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

7. Unauthorized copying or transmission of critical infrastructure data.

Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend to ten million rupees or with both.

8. Interference with critical infrastructure information system or data.

Whoever with dishonest intention interferes with or damages, or causes to be interfered with or damaged, any part or whole of a critical information system, or data, shall be punished with imprisonment which may extend to seven years or with fine which may extend too ten million rupees or with both.

9. Glorification of an offence:

Whoever prepares or disseminates information, through any information system or device, with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism, or activities of proscribed organizations or individuals or groups shall be punished with imprisonment for a term which may extend to seven years or with fine which may extend to ten million rupees or with both.

Explanation: “glorification” includes depiction of any form of praise or celebration in a desirable manner.

10. Cyber terrorism:

Whoever commits or threatens to commit any of the offences under section 6,7,8 or 9, where the commission or threat is with the intent to:
) Coerce, intimidate, create a sense of fear, panic or insecurity in the Government or the public or section of the public or community or sect or create a sense of fear and insecurity in society; or
) Advance inter-faith, sectarian or ethnic hatred; or advance the objectives of organizations or individuals or groups prescribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.
10A. Hate speech.

Whoever prepares or disseminates information, through any information system or device, that advances or is likely to advance inter-faith, secretariat or racial hatred, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

10B. Recruitment, founding, and planning of terrorism.

Whoever prepares or disseminates information, through any information system or device, that invites or motivated to found, or recruits people for terrorism or plan for terrorism shall be punished with imprisonment for a term which may extend to seven years or with fine or with both.

11. Electronic forgery.

(1) Whoever interferes with or uses any information system, device or data with the intent to cause damage or injury to the public or any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implicit contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in an authentic data with the intent that it be considered or acted for legal purposes as if it were authentic, regardless of the fact that the data is directly readable and intelligible or not, shall be punished with imprisonment of either description for a term which may extend to three years, or we define which may extend to two hundred and fifty thousand rupees or with both. Whoever commits offence under subsection 1 in relation to it critical infrastructure information system or data shall be banished with imprisonment for a term may extend so seven years or with fine which may extend to five million rupees or with both.

12. Electronic fraud.

Whoever with the intent for wrongful gain interferes with or uses information system, device or data or induces there is a blender into relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment end to two years or with extend to ten million rupees or with both.

13 Making, obtaining, or supplying device for use in offence.

Whoever produces, makes, generates, adapts, exports, supplies, offers to supply or import for use any information system, data or device, with intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act shell, without prejudice to any other liability that he may incur in this behalf, be punished with imprisonment for a term which may extend to six months work with fine which may extend to fifty thousand rupees or with both.

14 Unauthorized use of identity information

(1) Whoever obtains, sell, possesses, transmits or use another person’s information without authorization shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five million rupees, or with both.

Any person whose identity information is obtained, sold, possessed, used or transmitted may apply to the Authority for securing, destroying, blocking access or preventing transmission of identity information refereed to
sub-section (1) and the Authority on receipt of such application may take such measures as deemed appropriate for securing, destroying or preventing transmission of such identity information.

**15. Unauthorized issuance of SIM cards ect.**

Whoever sell or otherwise provides subscriber identity module (SIM) card, reusable identification module (R-IUM) or universal integrated circuit card (UICC) or other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices such as tablets, without obtaining and verification of the subscriber's antecedents in the mode and manner for the time being approved by the Authority shall be punished with imprisonment to three years or with fine which may extend to five hundred thousand rupees or with both.

**16. Tampering, ect. of communication equipment.**

Whoever unlawfully or without authorization changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and stats using or marketing such device for transmitting and receiving information on shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.

Explanation. A “unique device identifier” is an electronic equipment identifier which is unique to communication device.

**17. Unauthorized interception.**

Whoever with dishonest intention commits unauthorized interception by technical means of:

1. any transmission that is not tended to be and is not open to the public, from or withing an information system; or
2. Electromagnetic emission from an information system that are carrying data, shall be punished with imprisonment of either description for a term which may extend to five hundred thousand rupees or with both.

**18. Offences against dignity of a natural person.**

(1) Whoever intentionally and publicly exhibits or display or transmits any information through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of natural person, shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provided that nothing under this sub-section shall apply to anything aired by a broadcast media or distribution service licensed under Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (XIII of 2002).

2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licenses to secure such information including traffic data.

**19 Offences against modesty of a natural person and minor.**

(1) Whoever intentionally and public exhibits or displays or transmits any information which:

a. superimposes a photograph of the face of a natural person over any sexually explicit image or video; or
b. includes a photograph or a video of a natural person sexually explicit conduct; or

2. intimidates a natural person with any sexual act, or any sexually explicit image or video of a natural person; or

d. cultivates, entices or induces a natural person to engage in sexually explicit act,
Through an information system to harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail, shall be punished with imprisonment for a term which may extend to five years or with fine which may extend to five million rupees or with both.

2) Whoever commits an offence under sub-section (1) with respect to a minor shall be punished with imprisonment for a term which may extend to seven years and with fine which may extend to five million rupees:

Provided that of a person who has been previously convicted of an offence under sub-section(1) with respect to a minor shall be punished with imprisonment for a term of ten years and with fine.

3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in a sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licences to secure such information including traffic data.

**19A. Child pornography.**

(1) Whoever intentionally produces, offers or make available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts:

- a minor engaged in sexually explicit conduct;
- a person appearing to be a minor engaged in sexually explicit conduct; or
- realistic images representing a minor engaged in sexually explicit conduct; or
- discloses the identity of the minor, shall be punished with imprisonment for a term which may extend to seven years, or with fine which may extend to five million rupees or with both.

2) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

**20. Malicious code.**

Whoever wilfully and without authorization writes, offers, makes available, distributes or transmits malicious code through an information system or device, with intent to cause harm to any information system or data resulting in the corruption, destruction, alteration, suppression, theft or loss of the information system or data shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both.

Explanation: for the purpose of this section, the expression “malicious code” includes, a computer program or hidden function in a program that damages an information system or data or compromises the performance of such system or availability of data or uses it without proper authorization.

**21. Cyber stalking.**

(1) A person commits the offence of cyber stalking who, with the intent to coerce or intimidate or harass any person, uses information system, information network, the internet, website, electronic mail or any other similar means of communication to:

a. Follow a person or contracts to or attempts to contact such person to foster personal interaction repeatedly despite a clear indication of disinterest by such person;

b. Monitor the use by a person of the internet, electronic mail, text message or any other forms of electronic communications;

c. Watch or see upon a person in a manner that results in fear of violence or serious alarm or distress, in the mind of such person; or

take a photograph or make video of any person and displays or distributes it without his consent in a manner that harms the person.

2) Whoever commits the offence specified in sub-section (1) shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both:

Provides that if victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to five
years or with fine which may extend to ten million rupees or with both.
3) Any aggrieved person or his guardian, where such person is a minor, may apply to the Authority for removal, destruction of or blocking access to such information referred to in sub-section (1) and the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances including an order for removal, destruction, preventing transmission of or blocking access to such information and the Authority may also direct any of its licences to secure such information including traffic data.

### 22 Spamming

(1) A person commits the offence of spamming, who with intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain.
2) A person including an institution or an organization engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe for such marketing.
3) Whoever commits the offence of spamming as described in sub-section (1) by transmitting harmful, fraudulent, misleading or illegal information, shall be punished with imprisonment for a term which may extend to three months or with fine of rupees fifty thousand which may extend up to rupees five million or with both.
4) Whoever commits the offence of spamming as described in sub-section (1) by transmitting unsolicited information, or engages in direct marketing in violation of sub-section (2), for the first time, shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not exceeding fifty thousand rupees, and for every subsequent violation shall be punished with fine not less than fifty thousand rupees that may extend to up one million rupees.

### 23 Spoofing.

(1) Whoever with dishonest intention establish a website or send any information with a counterfeit source intended to be believed by the recipient or visitor of the website, to be authentic source commits spoofing.
2) Whoever commits spoofing shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to five hundred thousand rupees or with both.

### 24 Legal recognition of offences committed in relation to information system.

(1) Notwithstanding anything contained in any law for the time being in force, an offence under this Act or any other shall not be denied legal recognition and enforcement for the sole reason of such offence being committed in relation to or through the use of information system.
2) References to “property” in any law creating an offence in relation to or concerning property, shall include information system and data.

### 25. Pakistan Penal Code, 1860(Act XLV of 1860) to apply.

The provisions of the Pakistan Penal Code, 1860(Act XLV of 1860), to the extent not inconsistent with anything provided in this Act, shall apply to the offence provide in this Act.
CHAPTER III
ESTABLISHMENT OF INVESTIGATION AGENCY AND PROCEDURAL POWERS FOR INVESTIGATION

26. Establishment of investigation agency

(1) The Federal Government may establish or designate a law enforcement agency as the investigation agency for the purposes of investigation of offences under this Act.
(2) Unless otherwise provided for under this Act, the investigation agency and the authorised officer shall in all matters follow the procedure laid down in the Code to extent that it is not inconsistent with any provision of this Act.
(3) The investigation agency shall establish its own capacity for forensic analysis of the data or information systems and the forensic analysis reports generated by the investigation agency shall not be inadmissible in evidence before any court for the sole reason that such reports were generated by the investigation agency.

27 Power to investigate.

Only an authorized officer of the investigation agency shall have the powers to investigate an offence under this Act: Provided that the Federal Government or the Provincial Government may, as the case may be, constitute one or more joint investigation teams comprising of an authorized officer of the investigation agency and any other law enforcement agency for investigation of an offence under this Act and any other law for the time being in force.

28 Explicated preservation and acquisition of data

(1) If an authorized officer is satisfied that:
   . specific data stored in any information system or by means of information system is reasonable required for the purposes of a criminal investigation; and
   . there is a risk or vulnerability that the data may be notified, lost, destroyed or rendered inaccessible,
   he authorized officer may, by written notice given to the person in control of the information system, require that person to provide that data or to ensure that the data specified in the notice be preserved and the integrity thereof is maintained for a period not exceeding ninety days as specified in the notice:
   Provided that the authorized officer shall immediately but not later than twenty-four hours bring to notice of the Court, the fact of acquisition of such data and the Court on receipt of such information may pass such orders as deemed appropriate in the circumstances of the case including issuance of warrants for retention of such data or otherwise.
(2) The period provided in sub-section(1) for preservation of data may be extended by the Court if so deemed necessary upon receipt of an application from the authorized officer in this behalf.

29 Retention of traffic data

(1) A service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the court, provide that data to the investigation agency or the authorized officer whenever so required.
(2) The service providers shall retain the traffic data under sub-section (1) by fulfilling all the requirements of retention and its originally as provided under section 5 and 6 of the Electronic Transactions Ordinance, 2002 (LI of 2002).
(3) Any owner of the information system who is not licensee of the Authority and violates sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or
with fine or with both:
Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be
a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecom-

### 30 Warrant for search or seizure

(1) Upon an application by authorized officer that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that there may be in a specified place an information system, data, device or other articles that:
. may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in providing a specifically identified offence made out under this Act; or
. has been acquired by a person as a result of the commission of an offence, the Court may issue a warrant which shall authorize an officer of the investigation agency, which such assistance as may be necessary, to enter the specified place and to search the premises and any information system, data, device or storage medium reinvent to the offence identified in the application and access, seize or similarly secure an information system, data, device or other articles relevant to the offence identified in the application.
2) In circumstances involving an offence under section 10, under which a warrant may be issued but cannot be obtained without the apprehension of destruction, alteration or loss data information system, data, device or other articles required for investigation, the authorized officer, who shall be a Gazette officer of the investiga

### 31 Warrant for disclosure of content data.

(1) Upon an application by an authorized office that application by an authorized office that demonstrates to the satisfaction of the Court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required for the purpose of a criminal investigation or criminal proceedings with respect to an offence made out under this Act, the Court may, after recording reasons, order that the person in control of the data or information system, to provide such data or access to such data to the authorized officer.
2) The period of warrant issued under sub-section (1) may be extended beyond seven days if, on an application, a Court authorizes an extension for a further period of time as may be specified by the Court.

### 32 Powers of an authorized officer

(1) Subject to provision of this Act an authorized officer shall have the powers to:
  a. have access to and inspect the operation for any specified information system;
  b. use or cause to be used any specified information system to search any specified data contained in or available to such system;
  c. obtain and copy only relevant data, use equipment to make copies and obtain an intelligible output from an information system;
  d. have access to or demand any information in readable and comprehensible format or pain version;
  e. require any person by whom or on whose behalf, the authorized officer has reasonable cause to believe, any information system has been used to grant access to any data within an information system within the control of such person;
  f. require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence under this Act; and
  g. require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigation any such offence.
Explanation: Decryption information means information or technology that enables a person to readily retrans-
form or unscramble encrypted data from optics unreadable form and from ciphered data to intelligible data.

2) In exercise of the power of search and seizure of any information system, program or data the authorized officer at all time shall:
   a. act with proportionality;
   b. take all precautions to maintain integrity and secrecy of the information system and data in respect of which a warrant for search or seizure has been issued;
   c. not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences identified in the application for which a warrant for search and seizure has been issued;
   d. avoid disruption to the continued legitimate business operations and the premises subject to search and seizure under this Act; and
   e. avoid disruption to any information system, program or data not connected with the information system that is not the subject of the offences identified in the application for which a warrant has been issued or is not necessary for the investigation of the specific offence in respect of which a warrant has been issued.

3) When seizing or securing any data or information system, the authorized officer shall make all efforts to use technical measures to maintain its integrity and chain of custody. The authorized officer shall seize an information system, data, device or articles, in part or in whole, as a last resort only in the event where it is not possible under the circumstances to use such technical measures or where use of such technical measures by themselves shall not be sufficient to maintain the integrity an chain of custody of the data or information system being seized.

4) Where an authorized officer seizes or secures any data or information system, the authorized officer shall ensure that data or information system while in the possession or in the access of the authorized officer is not released to any other person including competitors or public at large and details including log of any action performed on the information system or data is maintained in a manner prescribed by the Act.

33 Dealing with seized data or information system.

1) If any data or information system has been seized or secure following a search or secured following a search or seizure under this Act, the authorized officer who undertook the search or seizure shall, at the time of the seizure:
   . make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and
   . give a copy of that list to:
     . the occupier of the premises; or
     i. the owner of the data or information system; or
     ii. The person from whose possession the data or information system has been seized, in a prescribed manner in the presence of two witnesses.

2) The authorized officer, upon an application of the owner of the data or information system or an authorizes agent of the owner and on payment of prescribed costs, shall provide forensic image of the data or information system to the owner or his authorized agent within time prescribed under this Act.

3) If the authorized officer has reasons to believe that providing forensic image of the data or information system to the owner under sub-section (2) may prejudice:
   . the investigation in connection with which the search was carried out; or
   . another ongoing investigation; or
   . any criminal proceedings that are pending or that may be brought in relation to any of those investigations, the authorized officer shall, within seven days of receipt of the application under sub-section (2), approach the Court for sicking an order not to provide copy of the seized data or information system.

a) The Court upon receipt of an application from an authorized officer under sub-section (3), may after recording reasons in writing pass such order as deemed appropriate in the circumstances of the case.

5) The costs associated with the exercise of rights under this section shall be borne by the person exercising these rights.

34 Unlawful on-line content

1) The Authority shall have the power to remove or block or issue directions for removal or blocking of access to an information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act.

2) The Authority shall, with the approval of the Federal Government, prescribe rules providing for, among other matters, safeguards, transparent process and effective oversight mechanism for exercise of power under sub-
section (1).
3) Until such rules are prescribed under sub-section (2), the Authority shall exercise its power under this Act or any other law for the time being in force in accordance with the directions issued by the Federal Government not inconsistent with the provision of this Act.
4) Any person aggrieved from any order passed by the Authority under sub-section (1), may file an application with the Authority for review of the order within thirty days from the date of passing of the order.
5) An appeal against the decision of the Authority in review shall lie before the High Court within thirty days of the order of the Authority in review.

35. Limitation of liability of service providers.

(1) No service provider shall be subject to any civil or criminal liability, unless it is established that the service providers had specific actual knowledge and willful intent to proactively and positively participate, and not merely through omission or failure to act, and thereby facilitated, aided or abetted the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider in connection with a contravention of this Act or rules made thereunder or any other law for the time being in force:
Provided that the burden to prove that a service provider had specific actual knowledge, and willful intent to proactively and positively part participate in any act that gave rise to any civil or criminal liability shall be upon the person alleging such facts and no interim or final orders, or directions shall be issued with respect to a service provider by any investigation agency or Court unless such facts have so been proved and determined:
Provided further that such allegation and its proof shall clearly identify with specificity the content, material or other aspect with respect to which civil or criminal liability is claimed including but not limited to unique identifiers such as the Account Identification (Account ID), Uniform Resource Locator (URL), Top Level Domain (TLD9, Internet Protocol Adresses (IP Adresses), or other unique identifier and clearly state the statutory provision and basis of the claim.
2) No service provider shall under any circumstance be liable under this Act, rules made thereunder or any other law for maintaining and making available the provision of their service in good faith.
3) No service provider shall be subject to any civil or criminal liability as a result of informing a subscriber, user or end-user affected by any claim, notice or exercise of any power under this Act, rules made thereunder or any other law:
Provided that the service provider, for a period of time not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon it by an authorized officer, which period of confidentiality may be extended beyond fourteen days if, on an application by authorized officer the Court authorizes an extension for a further pacified period upon being satisfied that reasonable cause for such extension exists.
4) No service provider shall be liable under this Act, rules made thereunder or any other law for the disclosure of any data or other information that the service provider discloses only to the extent of the provision of this Act.
5) No service provider shall be under any obligation to proactively monitor, make inquiries about material or content hosted, cached, routed, relayed, conduit, transmitted or made available by such intermediary or service provider.

36 Real-time collection and recording of information

(1) If a Court is satisfied on the basis of information furnished by an authorized officer that there are reasonable grounds to believe that the content of any information is reasonably required for the purpose of a specific criminal investigation, the Court may order, with respect to information held by or passing through a service provider, to a designated agency has notified under the Investigation for Fair Trial Act 2013 8Iof 2013) or any other law for the time being in force having capability to collect real time information, such information in real-time in coordination with the investigation agency for provision in the prescribed manner:
Provided that such a real-time collection or recording shall not be for a period beyond what is absolutely necessary and in any event for not more than seven days.
2) notwithstanding anything contained in any law to the contrary the information so clear sub-section (1) shall be admissible in evidence.
3) the period of real time collection recording may be extended beyond seven days if, on an application, the Court authorizes an extension for a further specified period.
4) The Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it.
5) The application under sub-section (1) and (2) shall in addition to substantive grounds and reasons also:
why it is believed that the data sought will be available with the person in control of an information system; identify and explain with specificity the type of information likely to be found on such information system; identify and explain with specificity the identified fans made out under this act in respect of which the warrant is sought; if authority to seek real time collection or recording on more than one occasion is needed, explain why and how many further disclosures are needed to achieve the purpose for which the warrant is to be issued; specify what measures shall be taken to prepare and ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information of any person not part of the investigation; explain why the investigation may be frustrated or a seriously prejudiced unless the real time collection or recording is permitted; and why, to achieve the purpose for which the warrant is being applied, real time collection or recording by the person in control of the information system is necessary.

37. Forensic laboratory.

The Federal Government shall establish or designate a forensic laboratory, independent of the investigation agency, to provide expert opinion before the court for the benefit of the investigation agency in relation to evidence collected for purposes of investigation and prosecution of offences under this Act.

38. Confidentiality of information

Notwithstanding immunity granted under any other law for the time being in forced, any person including a service provider while providing services under the terms of lawful contract or otherwise in accordance with the law, or an authorized officer who has secured access to any material or data containing personal information about another person, except when required by law, without the consent of the person concerned or in breach of lawful contract with the intent to cause or knowing that he is likely to cause harm, wrongful loss or gain to any person or compromise confidentiality of such material or data shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both: Provided that the burden of proof of any defense taken by an accused service provider or an authorized officer that he was acting in good faith, should be on such a service provider or the authorized officer, as the case may be.

CHAPTER IV
INTERNATIONAL COOPERATION

39. International cooperation

(1) The Federal Government may upon receipt of request, through the designated agency under this Act, extend such cooperation to any foreign government, 24 X 7 network, any foreign agency or any international organization or agency for the purpose of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offense or obtaining expeditious preservation and disclosure of data by means of an information system or real time collection of data associated with specified communications or interpretation of data under this Act.
2) The Federal Government may forward to a foreign government, 24 X 7 network, any foreign agency or any international organization any information obtained from its own investigations if it considers that the disclosure of such information might assist the other government, agency or organization etc., as the case be, in initiating or carrying out investigations or proceedings concerning any offence under this Act.
3) The Federal Government shall require the foreign government, 24 X 7 network, and if rain agency or any international organization or agency to keep the information provided confidential and use it strictly for the purpose it is provided.
4) The Federal Government may, through the designated agency, send and answer request for mutual assistance the execution of such requests or their transmission to the authorities competent for their execution.
5) The Federal Government may refuse to accede do I need request made by a foreign government, 24 X 7 net-
work, any foreign agency or any international organization or agency if:
. it is of the opinion that the request, if granted, would prejudice sovereignty, security, public order or other essential public interest of Pakistan;
. the offense is regarded by the Federal Government as being of a political nature;
. there are substantial grounds for believing that the request for assistance has been made for the purpose of prosecuting a person on account of that person’s race, sex, religion, nationality, ethnic, origin or political opinions or that that person’s position may be prejudicated for any of those reasons;
. the request relates to an offense the prosecution of which in the requesting state may be incompatible with the laws of Pakistan;
. the assistance requested requires the Federal Government to carry out compulsory measures that may be inconsistent with the laws or practices of Pakistan had the offence been the subject of investigation or prosecution under its own jurisdiction; or
. the request concerns and defense which may prejudice and ongoing investigation or trial or rights of its citizens guaranteed under the Constitution.
6) Where the Federal Government decides to provide the requested cooperation, the relevant requirements and safeguards provided under this Act and rules framed thereunder shall be followed.
7) The designated agency shall maintain a register of requests received from any foreign government, 24 X 7 network, any foreign agency or any international organization or agency under this Act and action taken thereon.

CHAPTER VI
PREVENTIVE MEASURES

45. Prevention of electronic crimes

(1) The Federal Government or the Authority, as the case may be, may issue directives to be followed by the owners of the designated information system or service providers in the interest of preventing any offence under this Act.
2) Any owner of information system who is not a licensee of the Authority and violates the directives issued under sub-section (1) shall be guilty of an offence punishable, if committed for the first time, with fine which may extend to ten million rupees and upon any subsequent conviction shall be punishable with imprisonment which may extend to six months or with fine or with both.
Provided that where the violation is committed by a licensee of the Authority, the same shall be deemed to be a violation of the terms and conditions of the licensee and shall be treated as such under the Pakistan Telecommunication (Re-organization) Act, 1996.

46 Computer emergency response team

(1) The Federal Government may constitute one or more computer emergency response teams to respond to any threat against or attack on any critical infrastructure information system or critical infrastructed data, or widespread attack on information system in Pakistan.
2) A computer emergency response team constituted under sub-section (1) may comprise of technical experts of known expertise of any intelligence or agency or any sub-set thereof.
3) A computer emergency response team shall respond to a threat or attack without causing any undue hindrance or inconvenience to the use and access of the information system or data may be prescribed.
2. Definitions.

— In this Act, unless there is anything repugnant in the subject or context,—

a) “agreement” means a treaty, agreement, convention in force, or memorandum of understanding to which the Islamic Republic of Pakistan is a party and which contains provisions relating to mutual legal assistance in criminal matters;

b) “appropriate authority” in relation to a foreign country, means a person or body in that country referred to in the agreement or reciprocal agreement with the Islamic Republic of Pakistan as the authority responsible for administering mutual legal assistance to and from such country;

c) “central authority” means the office of the secretary to the Ministry of Interior, Government of the Islamic Republic of Pakistan and the powers of such office shall be exercised by an executive committee comprising the secretary to the Ministry of Interior, Government of the Islamic Republic of Pakistan, the secretary to the Ministry of Law and Justice, Government of the Islamic Republic of Pakistan, the secretary to the Ministry of Foreign Affairs, Government of the Islamic Republic of Pakistan and the home secretaries of all the four Provinces, namely Balochistan, Khyber Pakhtunkhwa, Punjab and Sindh, while the secretary to the Ministry of Interior, Government of the Islamic Republic of Pakistan shall be its convener. 

Explanation— The decision of the central authority shall be by majority of the members presents;

d) “information system” includes an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing any information;

e) “data” means content data and traffic data;

f) “electronic” means electrical, digital, magnetic, Optical, biometric, electrochemical, Electromechanical, wireless or electromagnetic technology;

g) “computer system” means any device or a group of interconnected or related devices one or more of which, pursuant to a programme, performs automatic processing or recording data, and includes a mobile telephone and other telecommunication devices;

h) “confiscation” means deprivation of property by order of a court;

i) “confiscation order” means an order made by a court in the Islamic Republic of Pakistan or a court of a country with whom the Islamic Republic of Pakistan has entered into reciprocal agreement for the confiscation of proceeds or instrumentalities of crime or terrorist property after criminal conviction;

j) “court” means the court which has jurisdiction to try an offence for which a request has been made under this Act;

k) “criminal matter” includes any investigation, prosecution or judicial proceedings relating to,—

i) a criminal offence;

ii) identification or tracing of proceeds or instrumentalities of crime or other related articles for evidentiary process;

iii) the determination as to whether a property is proceeds or instrumentalities of money laundering or terrorist property;

iv) a confiscation order; or

v) the freezing or seizure of proceeds or instrumentalities of crime or terrorist property; or

l) “criminal offence” means an offence punishable under the Pakistan Penal Code, 1860 (Act XLV of 1860) or relating to money laundering, terrorist financing, and offences pertaining to narcotics, arms and ammunitions, and offences under the Customs Act, 1969 (IV of 1969);

m) “freezing” or “seizure” means temporarily prohibiting the transfer, conversion, disposition or movement of property on the basis of an order issued by a court or other authority and includes an order restraining such dealings:

Provided that where the order of freezing and seizure is passed by an authority other than a court of law, the same shall be subject to confirmation by a court of competent jurisdiction within one month of passing the said order;

n) “instrumentalities of crime” means any property,—

i) used in, or employed in connection with, the commission of a criminal offence; or

ii) for which there are reasonable grounds of suspecting that the said property may be used in, or employed in connection with, the commission of a criminal offence; or
iii) whether the property is located or the offence is committed within or outside Pakistan;

o) “money laundering” means an act of money laundering relatable to a “criminal offence” as defined under the Anti-Money Laundering Act, 2010 (VII of 2010);

p) “proceeds of crime” means any property situated within or outside Pakistan derived from or obtained through commission of a criminal offence, committed within or outside Pakistan;

q) “property” means property or assets of any description, movable or immovable, corporeal or incorporeal, tangible or intangible, situated within or outside Pakistan;

r) “rules” means rules made under this Act;

s) “service provider” shall have the same meaning as given to it by section 2(XXVIII) of the Prevention of Electronic crimes Act, 2016 (XL of 2016);

t) “terrorism” shall have the same meaning as given to it by section 6 of the Anti-terrorism Act, 1997 (XXVII of 1997); and

u) “terrorist property” shall have the same meaning as given to it by section 2(Z)(aa) of the Anti-terrorism Act, 1997 (XXVII of 1997).


(1) This Act shall regulate the procedure for rendering and soliciting mutual legal assistance in criminal matters by Pakistan.

2) Subject to the provisions of this Act, the mutual legal assistance may be provided by Pakistan to a country on the principle of reciprocity reduced in writing.

3) Where the Federal Government considers it expedient to provide mutual legal assistance in a criminal matter to a country which has not entered into a reciprocal agreement with Pakistan, it may, by notification in the official Gazette, direct that the provisions of this Act shall, subject to such modifications and conditions as may be specified therein, have effect to that country.

4) This Act shall not be applicable to any offence of a political nature unless directly linked to a criminal matter.

4. Functions of the central authority.

(1) The central authority shall have all such powers as may be necessary to perform its duties and functions under this Act.

2) Without prejudice to the generality of sub-section (1), the central authority shall be authorized to,-

a) make a request, on behalf of Pakistan, to an appropriate authority of a foreign country for mutual legal assistance in relation to a criminal offence in which any investigation has commenced or proceedings instituted within Pakistan or outside Pakistan;

b) receive and deal with the request from any appropriate authority of a foreign country for mutual legal assistance in relation to a criminal offence in which any investigation has commenced or proceedings instituted, within Pakistan or outside Pakistan, or where there are reasonable grounds of suspecting that a criminal offence has been committed within or outside Pakistan;

c) certify or authenticate, or arrange for the certification and authentication of any documents or other material supplied in response to a request for assistance;

d) take practical measures to facilitate the orderly and rapid disposition of request for assistance;

e) make any arrangements deemed necessary in order to transmit the evidentiary material gathered in response to request for assistance to the appropriate authority of the requesting country or to authorize any other authority as prescribed to do so; and

f) carry out such other tasks as provided for in this Act or which may be necessary for effective assistance to be provided or received.

3) The central authority may, having regard to its functions and to exercise its powers efficiently, delegate its functions and powers to one or more subordinate officers not less than the rank of a Joint Secretary.
5. Transmission of information.

(1) The central authority shall not initiate transmitting of any information relating to criminal matters to the appropriate authority in a country concerned with such criminal matters, without prior request by that country: Provided that no request for mutual legal assistance shall be approved by the central authority without issuing notice to the person to whom the request relates.

2) Subject to the provisions of this Act, a request transmitted by a country to any other agency or authority in Pakistan shall be referred by such agency or authority to the central authority and this shall not affect the validity of the request or actions taken thereupon.

6. Form and manner of requests.

The central authority may initiate or receive request for mutual legal assistance, to or from foreign countries, as the case may be, in accordance with the form, manner and conditions as may be prescribed.

7. Mutual legal assistance request by Pakistan.

A request for mutual legal assistance by the central authority to a country subject to the applicable laws of such country may comprise one or more of the following matters, namely:-

a) inquire about the location and identification of witnesses, suspects, perpetrators and offenders;
b) have evidence taken or documents or other articles produced;
c) obtain search warrants or other lawful instruments authorizing a search for evidence relevant to investigations or proceedings in Pakistan, located or as permissible under the domestic law of that country believed to be located in that country and if found, to seize them as permissible under the domestic law of that country;
d) freeze or seize properties that are subject to the proceedings being undertaken in Pakistan in a criminal matter in accordance with the relevant legal process in that country to the extent to which the properties are believed on reasonable grounds to be allocated in that country;
e) transmit to Pakistan any evidence, documents or articles, properties or proceeds realized from the disposal of properties;
f) transfer in custody to Pakistan a person in foreign country who consented to assist Pakistan in the relevant investigation or proceedings;
g) effect service of judicial documents;
h) identify or trace proceeds or instrumentalities of crime or properties for evidentiary purpose;
i) facilitate the voluntary appearance of persons required in relation to any existing proceedings in Pakistan;
j) provide original or certified copies of relevant documents and records, including government, bank, financial, corporate or business records; and
k) provide any other type of assistance that is not contrary to the domestic law of that country.

8. Foreign request for assistance.

(1) Where a country makes a request to the Islamic Republic of Pakistan for mutual legal assistance, the central authority may approve mutual legal assistance for similar purposes as those specified in section 7 to the country in relation to investigations commenced or proceedings instituted in that country.

2) The request under sub-section (1), except as may otherwise be provided for in the domestic law of the country from which information is sought, shall be made out in conformity with the form, as specified by the central authority, which form shall include the following, namely:-

a) the name of the appropriate authority or such other authority concerned with the criminal matter to which the request relates;
b) a description of nature of the criminal matter and a statement setting out a summary of relevant facts and law;
c) the description of the purpose of the request and the nature of assistance being sought;
d) in the case of request to freeze, seize or confiscate assets located in Pakistan, be accompanied with the details of the criminal offence, particulars of any investigation or proceedings commenced in respect of that offence and a copy of any relevant freezing, seizure or confiscation order of the court;
e) details of any procedure that the country wishes to be followed by Pakistan in giving effect to the request, particularly in the case of a request to take evidence, as far as it is not contrary to the laws of Pakistan;

f) a statement setting out any requirements of the country concerning any confidentiality relating to the request and the reasons thereof;

g) details of the period within which the country wishes the request to be complied with;

h) details where applicable, regarding the grounds for believing that the relevant properties to be traced, frozen or seized or confiscated, are located in Pakistan; and

i) any other information that may assist in giving effect to the request.

9. Foreign request for an evidence gathering order or search warrant.

(1) Notwithstanding anything contained in any other law for the time being in force, where the central authority approves the request of a country pursuant to section 8 for the following purposes, namely:-

a) taking of a statement or testimony from a person; or

b) production of documentary or other evidence in Pakistan; or

c) identification of a person, property or record,

the central authority may apply to the court for a search warrant or any evidence gathering order, as the case may be.

2) The court, to which an application is made under subsection (1), may issue a search warrant or, as the case may be, an evidence-gathering order where it is satisfied on the basis of evidence presented before it that there are reasonable grounds to believe that:

a) the acts complained of, if performed in Pakistan, shall constitute an offence under the laws of Pakistan; or

b) the person committing an offence or the witness is in Pakistan.

3) An evidence-gathering order,-

a) shall provide for the manner in which the statement or testimony is to be taken or the evidence is to be obtained or the person or thing to be identified in order to give proper effect to the request unless prohibited under the laws of the Islamic Republic of Pakistan, and, in particular, may require any person named therein to—

i) make a record from data or make a copy of record;

ii) attend court to give evidence or oath; or

iii) produce to the court or to any person, named by the court, anything including any article, record or copy thereof; and

b) may include such terms and conditions as the court considers expedient, including those relating to the interests of the person named therein or of the third party.

4) Where the evidence sought under this Act is a statement or testimony of any person, the court may permit,—

a) any person to whom the foreign investigation, prosecution or proceedings relate or that person’s legal representative to participate in the proceedings; and

b) the legal representative of the country to participate in the proceedings and question the witness.

5) A person named in an evidence-gathering order may refuse to answer a question or to produce a record or thing where such refusal is based on,—

a) a law in force in Pakistan; (b) privilege recognized by a law in force in the country that made the request; or (c) a law in force in the country that made the request provides that the answering of that question or the production of that record or thing by that person in its own jurisdiction is, or shall be deemed to be, a criminal offence.

6) Where a person refuses to answer a question or to produce a record or thing under sub-section (5), the court shall refer the matter to the central authority which shall notify the requesting country accordingly and request it to provide a response on whether the person’s refusal is well founded under the law of that country.

7) Any response received by the central authority from the country in response to a request under sub-section (6) shall be admissible in the evidence gathering proceedings in accordance with law.

8) The court may issue a bailable warrant for the arrest of a person named in an evidence-gathering order where it is satisfied on the basis of evidence presented before it, that the person was personally served with the order and he willfully did not attend or remain in attendance as required or is about to abscond.

9) A person arrested in pursuance of warrant issued under sub-section (8) shall forthwith be brought before the court, to ensure compliance with the order made under sub-section (2), and the court may pass order that the person be detained in custody for a period not exceeding forty-eight hours or released with or without production of sureties.

10) A search warrant,—

a) shall be issued in accordance with the provisions of the Code of Criminal Procedure, 1898 (Act V of 1898);

b) shall specify time and date when the court will hear any representation from any person from whom a record or thing is seized pursuant to the warrant, before any order is made to send it to the country from which it is obtained; and

c) may include such terms and conditions as the court considers desirable including conditions relating to the time or manner of its execution.

11) The person executing a search warrant, issued under subsection (2),—

a) may seize any property which be believed on reasonable grounds has been obtained for, or used in or intend-
ed to be used in connection with the matter specified in the request for mutual legal assistance received by the central authority; and
b) shall, at least three days before the time of the hearing to consider its execution, file in the court a written report concerning the execution of the warrant including a description of the records or things seized.

12) At the hearing to consider the execution of search warrant, the court, after considering any representation made by the central authority or any person from whom record or thing was seized pursuant to the warrant or any person who claims to have an interest in the record or thing may,-
a) order that the record or thing be returned to the person from whom it was seized or to the person lawfully entitled to its possession and that it would be in the public interest to return it; or
b) order that the record or thing be sent to the country, and include in the order such terms and conditions as the court considers necessary -
   i) to give effect to the request from that country;
   ii) with respect to the preservation and return to Pakistan of any record or thing seized so as to respect the interest of a third party.

No record or thing seized and ordered to be sent to a country shall be sent until the central authority is satisfied that the country has agreed to comply with any terms or conditions imposed in respect of the sending abroad of the record or thing.

14) The court may issue an order that the testimony of statement, the identification of a person or thing or any other form of assistance be provided by use of video or audio transmission technology. Any such court shall-
a) order the person to attend at a time and place fixed by the court to give his statement, testify or otherwise provide assistance by video conference and to remain in attendance until excused by the authorities of the requesting country;
b) to answer any questions raised by the authorities of the foreign states, or persons authorized by those authorities, in accordance with the laws that apply to that foreign states; and
c) to produce or show to those authorities at the time and place fixed by the court, prosecutor or other authority any item, including any document or copy thereof and may include any other appropriate conditions.

15) The costs of establishing a video or telephone link, costs related to the servicing of a video or telephone link in name of state shall be borne by the requesting state, unless otherwise agreed.

10. Limitation on use of evidence.

Any evidentiary material provided to a country by Pakistan as a result of a request for gathering of evidence under this Act,-
a) shall not be used for any other purpose than the investigation, prosecution or judicial proceedings in respect of which the request for assistance was made; and
b) shall be inadmissible as evidence in any proceedings other than the proceedings in respect of which it was obtained.

11. Foreign requests for assistance from persons serving imprisonment.

(1) Where the central authority approves a request of a country to have a person serving a term of imprisonment in Pakistan, transferred to the requesting country for fixed period to give evidence or assist in an investigation or proceedings in that country relating to an offence committed or suspected on reasonable ground to have been committed against the laws of the requesting country, in respect of conduct which if occurred in Pakistan constitutes a criminal offence, the central authority shall apply to the court for a transfer order.

2) The court, to which an application is made under subsection (1), may make a transfer order where, after having considered among other things any document filed or information given in support of the application, it is satisfied that the person serving imprisonment has made an informed consent to such transfer.

3) A transfer order, made under sub-section (2),-
a) shall set out the name of the person serving imprisonment and his place of confinement with a specific provision for the safety, security and well being of the person being transferred;
b) shall require the person who has custody of the person to deliver him into the custody of the person who is designated in the order or who is a member of the class of persons so designated;
c) shall require the person receiving the person into custody to take him to the requesting country and on return of the person to Pakistan, to return him to the place of confinement where he was detained when the order was made through immigration officer, or to such other place of confinement as the central authority subsequently may notify;
d) shall specify the reasons for the transfer;
e) shall fix the period of time at, or before the expiration of, which the person must be returned to Pakistan;
f) shall have written undertaking from the requesting country that the person will not be detained, prosecuted, extradited to a third country or punished for any offence against the law of the foreign country that is alleged to have committed, or that was committed, before the person's departure from Pakistan;
g) shall have written undertaking from the requesting country that the person shall be provided consular access to Pakistani diplomatic personnel in that country and shall not to be required to give evidence in any proceeding in the foreign country other than in respect of conduct which if occurred in the Islamic Republic of Pakistan constitutes a criminal offence, to which the request relates;
h) may include such terms or conditions relating to the protection of the interest of the person as the court considers appropriate; and
i) an undertaking from the requesting country must be procured to ensure that the requesting country to whom the person is transferred shall not require Pakistan to initiate extradition proceedings for the return of the person so transferred.

4) The time spent in transit to and in custody of the requesting country by a person pursuant to transfer order under subsection (2) shall be deemed to have been spent in service of the sentence.

12. Detention of a person in Pakistan in response to request by Pakistan.

(1) The central authority may, by written notice, authorize temporary detention in Pakistan of a person in detention in a country who is transferred from that country to Pakistan pursuant to a request under clause (f) of section 7, for such period as may be agreed with that country for the purposes of request and return the person in custody to that country.

2) A person in respect of whom a notice is issued under subsection (1) shall, so long as the notice is in force,
a) be permitted to enter Pakistan and remain in Pakistan for the purpose of the request and to leave Pakistan when no longer required for that purpose; and
b) while in custody in Pakistan for the purpose of request, be deemed to be in lawful custody.

3) The central authority may at any time vary notice under sub-section (1), where the country makes a request for release of the person from custody, either immediately or on the specified date, and direct that the person be released from custody accordingly.

4) The provisions of this section shall apply, mutatis mutandis, in the case of any detained person in transit through Pakistan from one foreign country to another pursuant to a request for assistance of the kind referred to in this section.

5) Any person in Pakistan under this section who is in Pakistan in response to a request by the central authority under this Act to give evidence in any proceedings or to give assistance in relation to an investigation, prosecution or the related proceedings, may not
a) be detained, prosecuted or punished for any other criminal offence that occurred prior to his arrival in Pakistan; and
b) be subjected to judicial process in any other matter before the person's departure from the country pursuant to the request.

13. Foreign request to the Islamic Republic of Pakistan for freezing or seizure orders.

(1) Where the central authority approves a request of a country pursuant to section 10 to restrain dealings in any properties, some or all of which are located in Pakistan, the central authority may apply to the court for a freezing or seizure order.

2) The court to which an application is made under subsection (1) may after providing the person with the opportunity of being heard issue a freezing or seizure order, where the court is satisfied that there are reasonable grounds to believe that
a) an offence has been committed by a person under the laws of the requesting country which, if committed in Pakistan, also constitutes a criminal offence in Pakistan;
b) an investigation or proceedings have commenced in the country relating to that offence;
c) properties derived by the person, by himself or any other person on his behalf, from the commission of the offence are located in Pakistan; and
d) an order has been made in the country having the effect of confiscating such properties.

3) Where a competent court of requesting country has passed a freezing or seizure order, or has passed any amendment in respect thereof, the central authority shall apply to have the same registered with the court and the freezing or seizure order, or the amendment thereof, as the case may be, shall not be effective in Pakistan until it is so registered. Where a foreign freezing or seizure order is registered in accordance with this section, a copy of any amendments made in the order of the country, whether before or after registration, may be registered in the same manner as the order was registered, but shall not have effect for the purpose of this Act until
they are so registered.
4) The court shall, on application by the central authority, cancel the registration of a foreign freezing or seizure order, if it appears that the order has ceased to have effect in that country.
5) Subject to sub-section (6), where the foreign freezing or seizure order is a facsimile of a duly authenticated foreign order, or amendment made in such order, the facsimile shall be regarded for the purpose of this Act as the duly authenticated foreign order.
6) Registration effected by means of a facsimile shall cease to have effect at the end of a period of fourteen days commencing on the date of registration, unless a duly authenticated original order has been registered by that time.

14. Foreign confiscation order.

(1) Where the central authority approves a request of a country for enforcement of a confiscation order in relation to any property which is believed on reasonable ground to be located in Pakistan, the central authority may apply to the court for enforcement of the confiscation order against such property.
2) The court shall issue adequate notice to all persons appearing to have an interest in the property against which the confiscation order may be executed.
3) Any person with an interest in the property against which the application for execution of the confiscation order has been filed may, within thirty days of receiving notice under sub-section (2), make an application objecting to the confiscation.
4) The court to which an application is made under subsection (1) may order to enforce the foreign confiscation order, where it is satisfied that there are reasonable grounds to believe that-
   a) an offence has been committed by a person under the laws of the requesting country which, if committed in Pakistan, also constitutes a criminal offence in Pakistan;
   b) the foreign confiscation order has been made in the country in relation to the offence referred to in clause (a);
   c) the confiscation order is in force in the requesting country and is not subject to appeal;
   d) the properties specified in the confiscation order are located in Pakistan; and
   e) the person, whose property is the subject of the confiscation order, had appeared or participated in the proceedings or intentionally refused to do so despite having notice of the proceedings which culminated into such confiscation order being passed.
5) The central authority may enter into arrangements with the requesting country for transfer to the central authority the whole or part of any property, proceeds or instrumentalities of crime confiscated in Pakistan in response to a request for the enforcement of a confiscation order pursuant to this Act.

15. Request to recover foreign fines.

(1) Where the central authority approves a request from a country to enforce payment of a fine imposed by a court of that country, it shall make an application to the court to enforce payment of the fine in the manner as if the fine has been imposed by a court in Pakistan.

explanation.— For the purpose of this section, the expression “fine” shall include any pecuniary penalty determined by a foreign court to represent the value of any property, benefit, advantage, obtained or derived directly or indirectly as a result of the commission of an offence.
2) The court may pass the order for enforcement of fine, if it is satisfied that-
   a) the foreign order is in force in that country and is not subject to appeal; and
   b) where the person, who is the subject of the foreign order, had appeared or participated in the proceedings or intentionally refused to do so despite having notice of the proceeding, which culminated into such confiscation order being passed.
3) No proceedings under sub-section (1) shall be instituted after the expiry of three years from the date when the fine was imposed.

16. Application of specific procedures sought by the requesting country.

A request for assistance shall be executed in accordance with any procedure specified in the request, unless such execution is contrary to the provisions of any law or the Constitution of the Islamic Republic of Pakistan.
17. Refusal of request for assistance.

(1) A request for mutual legal assistance to Pakistan under this Act may be refused by the central authority if—
   a) granting the request is prejudicial to the sovereignty, security, public interest or national interests of Pakistan;
   b) there are reasonable grounds to believe that the request has been made for the purpose of punishing a
      person by reason of his race, sex, sexual orientation, religion, nationality, ethnic origin, language, colour, age,
      mental or physical disability or political reason;
   c) the provision of assistance is prejudicial to an investigation or ongoing proceedings in Pakistan, the execution
      of the request for assistance may be postponed until the finalization of the investigation or proceedings;
   d) the provision of the assistance imposes an excessive burden on the resources of the Federal, Provincial or lo-
      cal authorities of Pakistan;
   e) the authorities of Pakistan are prohibited by the domestic law or order of a court from carrying out any ac-
      tion requested with regard to any similar offence, had it been subject to domestic investigation, prosecution or
      judicial proceedings;
   f) it would be contrary to the laws of Pakistan; or
   g) the request is in violation of international conventions of human rights.

2) Notwithstanding anything contained in sub-section (1) or the provisions of any other law for the time being in
   force in Pakistan, assistance under this Act shall not be refused—
   a) on the ground of bank secrecy; or
   b) on the sole ground that the offence for which assistance is sought is also considered to involve fiscal matters.

18. Non-disclosure of confidential requests for assistance.

(1) Unless otherwise authorized by law, a person who, because of his official capacity or office has knowledge of
    the,—
    a) contents of such request made under this Act;
    b) fact that such a request has been or is about to be made; or
    c) fact that such a request has been reused, shall not disclose those contents or those facts except to the extent
       that the disclosure is necessary to execute the foreign request.

2) Any person who contravenes the provision of sub-section (1), shall be deemed to have committed an offence
   and shall on conviction be punished with imprisonment of six months or with fine not exceeding five hundred
   thousand rupees or with both.

3) The court may order the person providing a statement or testimony, or the custodian of evidence or informa-
   tion being provided under this Act, to keep confidential the fact of having such statement or testimony or having
   produced such evidence or information. The failure in this respect is liable to a sentence which on conviction
   may entail imprisonment of six months or with fine not exceeding five hundred thousand rupees or with both.

19. Expedited preservation and disclosure of information system.

(1) Upon request by a country setting forth,—
   a) the need for specified electronic data to be preserved;
   b) the urgency of preserving it;
   c) sufficient information to locate the electronic data; and
   d) a statement that a request for production of the data will follow,
   he central authority may issue an order to any person in the Islamic Republic of Pakistan to preserve and safe-
   guard such data.

2) The order under sub-section (1) shall lapse if the request for production is not received within forty-five days
   of the request for preservation.

20. Production, search and seizure of information system.

(1) Upon request of a country, the central authority may make an application to the court to issue an order for
   the production of,—
a) specified electronic data in the possession or control of a person which is stored in a computer system and is reasonably believed to be connected with a criminal matter pending in the requesting country; and
b) electronic data in the possession or control of service provider, where such data or information is reasonably believed to be connected to criminal matter pending in the requesting country.
2) The court may issue a search warrant or order authorizing a person designated by it to search or otherwise access any computer system or part thereof in which computer data may be stored.
3) The search warrant or order issued pursuant to subsection (1) may authorize the designated person, where necessary, to:
   a) seize or otherwise secure an information system or part thereof;
   b) make and retain a copy of the electronic data;
   c) maintain the integrity of the relevant electronic data; and
   d) render inaccessible or remove the electronic data in the accessed information system.
4) The person in possession of the electronic data or information system sought to be searched, seized or produced, may file an application within fourteen days of notice of an order under subsection (3) objecting to such seizure, copying, retaining or otherwise handing of such electronic data: Provided that until the expiry of the said fourteen days from the date of the notice of the order, the electronic data shall be kept secured and no copies or extracts from the data shall be allowed.


The execution of a request for mutual legal assistance in Pakistan shall be conducted without charge to the requesting country, except for:

a) costs incurred by the attendance of experts in the territory of Pakistan; or
b) costs incurred by the transfer of a person in custody; or

2) The costs of establishing a video or audio or telephone link, costs related to the servicing of a video or telephone link in Pakistan, the remuneration of interpreters provided by it and allowances to witnesses and their travelling shall be borne by that country.
For the purposes of this Act, the following terms are defined, as follows:

a) “Addressee” refers to a person who is intended by the originator to receive the electronic data message or electronic document, but does not include a person acting as an intermediary with respect to that electronic data message or electronic document.

b) “Computer” refers to any device or apparatus singly or interconnected which, by electronic, electro-mechanical, optical and/or magnetic impulse, or other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.

c) “Electronic data message” refers to information generated, sent, received or stored by electronic, optical or similar means.

d) “Information and Communication System” refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document.

e) “Electronic signature” refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.

f) “Electronic document” refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

g) “Electronic key” refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.

h) “Intermediary” refers to a person who in behalf of another person and with respect to a particular electronic data message or electronic document sends, receives and/or stores or provides other services in respect of that electronic data message or electronic document.

i) “Originator” refers to a person by whom, or on whose behalf, the electronic document purports to have been created, generated and/or sent. The term does not include a person acting as an intermediary with respect to that electronic document.

j) “Service provider” refers to a provider of —

i) Online services or network access, or the operator of facilities therefor, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user’s choosing; or

ii) The necessary technical means by which electronic documents of an originator may be stored and made accessible to a designated or undesignated third party.

Such service providers shall have no authority to modify or alter the content of the electronic document received or to make any entry therein on behalf of the originator, addressee or any third party unless specifically authorized to do so, and who shall retain the electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.
CHAPTER II
Legal Recognition of Electronic Data Messages and Electronic Documents

SECTION 6(6). Legal Recognition of Electronic Data Message.

Information shall not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message purporting to give rise to such legal effect, or that it is merely incorporated by reference in that electronic data message.

SECTION 7(7). Legal Recognition of Electronic Documents.

Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing, and —

a) Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that —

i) The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and

ii) The electronic document is reliable in the light of the purpose for which it was generated and in the light of all relevant circumstances.

b) Paragraph (a) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the document not being presented or retained in its original form.

c) Where the law requires that a document be presented or retained in its original form, that requirement is met by an electronic document if —

i) There exist a reliable assurance as to the integrity of the document from the time when it was first generated in its final form; and

ii) That document is capable of being displayed to the person to whom it is to be presented: Provided, That no provision of this Act shall apply to vary any and all requirements of existing laws on formalities required in the execution of documents for their validity.

For evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.

This Act does not modify any statutory rule relating to the admissibility of electronic data messages or electronic documents, except the rules relating to authentication and best evidence.

SECTION 8(8). Legal Recognition of Electronic Signatures.

An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if the signature is an electronic signature and proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which —

a.) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;

b.) Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all circumstances, including any relevant agreement;

c.) It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and

d.) The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.
SECTION 9(9). Presumption Relating to Electronic Signatures

In any proceedings involving an electronic signature, it shall be presumed that,
 a.) The electronic signature is the signature of the person to whom it correlates; and
 b.) The electronic signature was affixed by that person with the intention of signing or approving the electronic
document unless the person relying on the electronically signed electronic document knows or has notice of
defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the
circumstances.

SECTION 10(10). Original Documents.

(1) Where the law requires information to be presented or retained in its original form, that requirement is met
by an electronic data message or electronic document if:
a) the integrity of the information from the time when it was first generated in its final form, as an electronic
data message or electronic document is shown by evidence "aliumde" or otherwise; and
b) where it is required that information be presented, that the information is capable of being displayed to the
person to whom it is to be presented.
2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law sim-
ply provides consequences for the information not being presented or retained in its original form.
3) For the purposes of subparagraph (a) of paragraph (1):
a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered,
   apart from the addition of any endorsement and any change which arises in the normal course of communica-
tion, storage and display; and
b) the standard of reliability required shall be assessed in the light of the purpose for which the information was
   generated and in the light of all the relevant circumstances.

SECTION 11(11). Authentication of Electronic Data Messages and Electronic Documents.

Until the Supreme Court by appropriate rules shall have so provided, electronic documents, electronic data
messages and electronic signatures, shall be authenticated by demonstrating, substantiating and validating a
claimed identity of a user, device, or another entity in an information or communication system, among other
ways, as follows:
a) The electronic signature shall be authenticated by proof that a letter, character, number or other symbol in
electronic form representing the persons named in and attached to or logically associated with an electronic
data message, electronic document, or that the appropriate methodology or security procedures, when appli-
cable, were employed or adopted by a person and executed or adopted by such person, with the intention of
authenticating or approving an electronic data message or electronic document;
b) The electronic data message or electronic document shall be authenticated by proof that an appropriate
security procedure, when applicable was adopted and employed for the purpose of verifying the originator of an
electronic data message or electronic document, or detecting error or alteration in the communication, content
or storage of an electronic document or electronic data message from a specific point, which, using algorithm
or codes, identifying words or numbers, encryptions, answers back or acknowledgment procedures, or similar
security devices.
The Supreme Court may adopt such other authentication procedures, including the use of electronic notariza-
tion systems as necessary and advisable, as well as the certificate of authentication on printed or hard copies of
the electronic documents or electronic data messages by electronic notaries, service providers and other duly
recognized or appointed certification authorities.
The person seeking to introduce an electronic data message or electronic document in any legal proceeding has
the burden of proving its authenticity by evidence capable of supporting a finding that the electronic data mes-
sage or electronic document is what the person claims it to be.
In the absence of evidence to the contrary, the integrity of the information and communication system in which
an electronic data message or electronic document is recorded or stored may be established in any legal pro-
ceeding —
a) By evidence that at all material times the information and communication system or other similar device was
operating in a manner that did not affect the integrity of the electronic data message or electronic document,
and there are no other reasonable grounds to doubt the integrity of the information and communication system;
b) By showing that the electronic data message or electronic document was recorded or stored by a party to the proceedings who is adverse in interest to the party using it; or
c) By showing that the electronic data message or electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using the record.

**SECTION 12(12). Admissibility and Evidential Weight of Electronic Data Messages or Electronic Documents**

In any legal proceedings, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence —
a. On the sole ground that it is in electronic form; or
b. On the ground that it is not in the standard written form, and the electronic data message or electronic document meeting, and complying with the requirements under Sections 6 or 7 hereof shall be the best evidence of the agreement and transaction contained therein.
In assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, stored or communicated, the reliability of the manner in which its originator was identified, and other relevant factor shall be given due regard.

**SECTION 13(13). Retention of Electronic Data Message or Electronic Document.**

Notwithstanding any provision of law, rule or regulation to the contrary —
a) The requirement in any provision of law that certain documents be retained in their original form is satisfied by retaining them in the form of an electronic data message or electronic document which —
   i. Remains accessible so as to be usable for subsequent reference;
   ii. Is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to accurately represent the electronic data message or electronic document generated, sent or received;
   iii. Enables the identification of its originator and addressee, as well as the determination of the date and the time it was sent or received.
b) The requirement referred to in paragraph (a) is satisfied by using the services of a third party, provided that the conditions set forth in subparagraphs (i), (ii) and (iii) of paragraph (a) are met.

**CHAPTER III Communication of Electronic Data Messages or Electronic Documents**

**SECTION 16(16). Formation and Validity of Electronic Contracts**

(1) Except as otherwise agreed by the parties, an offer, the acceptance of an offer and such other elements required under existing laws for the formation of contracts may be expressed in, demonstrated and proved by means of electronic data messages or electronic documents and no contract shall be denied validity or enforceability on the sole ground that it is in the form of an electronic data message or electronic document, or that any or all of the elements required under existing laws for the formation of the contracts is expressed, demonstrated and proved by means of electronic data messages or electronic documents.
2) Electronic transactions made through networking among banks, or linkages thereof with other entities or networks, and vice versa, shall be deemed consummated upon the actual dispensing of cash or the debit of one account and the corresponding credit to another, whether such transaction is initiated by the depositor or by an authorized collecting party: Provided, That the obligation of one bank, entity, or person similarly situated to another arising therefrom shall be considered absolute and shall not be subjected to the process of preference of credits.
SECTION 17(17). Recognition by Parties of Electronic Data Message or Electronic Document.

As between the originator and the addressee of an electronic data message or electronic document, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic data message or electronic document.

SECTION 18(18). Attribution of Electronic Data Message.

(1) An electronic data message or electronic document is that of the originator if it was sent by the originator himself.

2) As between the originator and the addressee, an electronic data message or electronic document is deemed to be that of the originator if it was sent:
   a) by a person who had the authority to act on behalf of the originator with respect to that electronic data message or electronic document; or
   b) by an information system programmed by, or on behalf of the originator to operate automatically.

3) As between the originator and the addressee, an addressee is entitled to regard an electronic data message or electronic document as being that of the originator, and to act on that assumption, if:
   a) in order to ascertain whether the electronic data message or electronic document was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
   b) the electronic data message or electronic document as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify electronic data messages or electronic documents as his own.

4) Paragraph (3) does not apply:
   a) as of the time when the addressee has both received notice from the originator that the electronic data message or electronic document is not that of the originator, and has reasonable time to act accordingly; or
   b) in a case within paragraph (3) sub-paragraph (b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic data message or electronic document was not that of the originator.

5) Where an electronic data message or electronic document is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the electronic data message or electronic document as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the electronic data message or electronic document as received.

6) The addressee is entitled to regard each electronic data message or electronic document received as a separate electronic data message or electronic document and to act on that assumption, except to the extent that it duplicates another electronic data message or electronic document and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic data message or electronic document was a duplicate.

SECTION 19(19). Error on Electronic Data Message or Electronic Document

The addressee is entitled to regard the electronic data message or electronic document received as that which the originator intended to send, and to act on that assumption, unless the addressee knew or should have known, had the addressee exercised reasonable care or used the appropriate procedure —

a) That the transmission resulted in any error therein or in the electronic data message or electronic document when the electronic data message or electronic document enters the designated information system, or

b) That electronic data message or electronic document is sent to an information system which is not so designated by the addressee for the purpose.
SECTION 20. Agreement on Acknowledgment of Receipt of Electronic Data Messages or Electronic Documents.

The following rules shall apply where, on or before sending an electronic data message or electronic document, the originator and the addressee have agreed, or in that electronic document or electronic data message, the originator has requested, that receipt of the electronic document or electronic data message be acknowledged:
(a) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by or through any communication by the addressee, automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the electronic data message or electronic document has been received.
(b) Where the originator has stated that the effect or significance of the electronic data message or electronic document is conditional on receipt of the acknowledgment thereof, the electronic data message or electronic document is treated as though it has never been sent, until the acknowledgment is received.
(c) Where the originator has not stated that the effect or significance of the electronic data message or electronic document is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and if the acknowledgment is not received within the time specified in subparagraph (c), the originator may, upon notice to the addressee, treat the electronic data message or electronic document as though it had never been sent, or exercise any other rights it may have.

SECTION 21(20). Time of Dispatch of Electronic Data Messages or Electronic Documents.

Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic data message or electronic document occurs when it enters an information system outside the control of the originator or of the person who sent the electronic data message or electronic document on behalf of the originator.

SECTION 22(21). Time of Receipt of Electronic Data Messages or Electronic Documents.

Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic data message or electronic document is as follows:
a.) If the addressee has designated an information system for the purpose of receiving electronic data messages or electronic documents, receipt occurs at the time when the electronic data message or electronic document enters the designated information system: Provided, however, That if the originator and the addressee are both participants in the designated information system, receipt occurs at the time when the electronic data message or electronic document is retrieved by the addressee.
b.) If the electronic data message or electronic document is sent to an information system of the addressee that is not the designated information system, receipt occurs at the time when the electronic data message or electronic document is retrieved by the addressee;
c.) If the addressee has not designated an information system, receipt occurs when the electronic data message or electronic document enters an information system of the addressee.
These rules apply notwithstanding that the place where the information system is located may be different from the place where the electronic data message or electronic document is deemed to be received.

SECTION 23(22). Place of Dispatch and Receipt of Electronic Data Message or Electronic Documents.

Unless otherwise agreed between the originator and the addressee, an electronic data message or electronic document is deemed to be dispatched at the place where the originator has its place of business and received at the place where the addressee has its place of business. This rule shall apply even if the originator or addressee had used a laptop other portable device to transmit or receive his electronic data message or electronic docu-
ment. This rule shall also apply to determine the tax situs of such transaction.
For the purpose hereof —
a. If the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business.
b. If the originator or the addressee does not have a place of business, reference is to be made to its habitual residence; or
c. The “usual place of residence” in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.


Subject to applicable laws and/or rules and guidelines promulgated by the Department of Trade and Industry with other appropriate government agencies, parties to any electronic transaction shall be free to determine the type and level of electronic data message or electronic document security needed, and to select and use or implement appropriate technological methods that suit their needs.

PART IV
Electronic Transactions in Government

SECTION 27(26). Government Use of Electronic Data Messages, Electronic Documents and Electronic Signatures

Notwithstanding any law to the contrary, within two (2) years from the date of the effectivity of this Act, all departments, bureaus, offices and agencies of the government, as well as all government-owned and -controlled corporations, that pursuant to law require or accept the filing of documents, require that documents be created, or retained and/or submitted, issue permits, licenses or certificates of registration or approval, or provide for the method and manner of payment or settlement of fees and other obligations to the government, shall —
a) accept the creation, filing or retention of such documents in the form or electronic data messages or electronic documents;
b) issue permits, licenses, or approval in the form of electronic data messages or electronic documents;
c) require and/or accept payments, and issue receipts acknowledging such payments, through systems using electronic data messages or electronic documents; or
d) transact the government business and/or perform governmental functions using electronic data messages or electronic documents, and for the purpose, are authorized to adopt and promulgate, after appropriate public hearing and with due publication in newspapers of general circulation, the appropriate rules, regulations, or guidelines, to among others, specify —
1) the manner and format in which such electronic data messages or electronic documents shall be filed, created, retained or issued;
2) where and when such electronic data messages or electronic documents have to be signed, the use of an electronic signature, the type of electronic signature required;
3) the format of an electronic data message or electronic document and the manner the electronic signature shall be affixed to the electronic data message or electronic document;
4) the control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records or payments;
5) other attributes required of electronic data messages or electronic documents or payments; and
6) the full or limited use of the documents and papers for compliance with the government requirements:
Provided, That this Act shall by itself mandate any department of the government, organ of state or statutory corporation to accept or issue any document in the form of electronic data messages or electronic documents upon the adoption, promulgation and publication of the appropriate rules, regulations, or guidelines.
SECTION 28(27). RPWEB to Promote the Use of Electronic Documents or Electronic Data Messages in Government and to the General Public.

Within two (2) years from the effectivity of this Act, there shall be installed an electronic online network in accordance with Administrative Order 332 and House of Representatives Resolution 890, otherwise known as RPWEB, to implement Part IV of this Act to facilitate the open, speedy and efficient electronic online transmission, conveyance and use of electronic data messages or electronic documents amongst all government departments, agencies, bureaus, offices down to the division level and to the regional and provincial offices as practicable as possible, government-owned and controlled corporations, local government units, other public instrumentalities, universities, colleges and other schools, and universal access to the general public.

The RPWEB network shall serve as initial platform of the government information infrastructure (GII) to facilitate the electronic online transmission and conveyance of government services to evolve and improve by better technologies or kinds of electronic online wide area networks utilizing, but not limited to, fiber optic, satellite, wireless and other broadband telecommunication mediums or modes.

o facilitate the rapid development of the GII, the Department of Transportation and Communications, National Telecommunications Commission and the National Computer Center are hereby directed to aggressively promote and implement a policy environment and regulatory or non-regulatory framework that shall lead to the substantial reduction of costs of including, but not limited to, lease lines, land, satellite and dial-up telephone access, cheap broadband and wireless accessibility by government departments, agencies, bureaus, offices, government-owned and controlled corporations, local government units, other public instrumentalities and the general public, to include the establishment of a government website portal and a domestic internet exchange system to facilitate strategic access to government and amongst agencies thereof and the general public and for the speedier flow of locally generated internet traffic within the Philippines.

The physical infrastructure of cable and wireless system for cable TV and broadcast excluding programming and content and the management thereof shall be considered as within the activity of telecommunications for the purpose of electronic commerce and to maximize the convergence of ICT in the installation of the GII.

SECTION 29(28). Authority of the Department of Trade and Industry and Participating Entities.

The Department of Trade and Industry (DTI) shall direct and supervise the promotion and development of electronic commerce in the country with relevant government agencies, without prejudice to the provisions of Republic Act 7653 (Charter of Bangko Sentral ng Pilipinas) and Republic Act No. 337, (General Banking Act) as amended.

Among others, the DTI is empowered to promulgate rules and regulations, as well as provide quality standards or issue certifications, as the case may be, and perform such other functions as may be necessary for the implementation of this Act in the area of electronic commerce to include, but not limited to, the installation of an online public information and quality and price monitoring system for goods and services aimed in protecting the interests of the consuming public availing of the advantages of this Act.

PART V
Final Provisions

SECTION 30(29). Extent of Liability of a Service Provider.

Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of the electronic data message or electronic document for which the person or party acting as a service provider as defined in Section 5, merely provides access if such liability is founded on —

. ) The obligations and liabilities of the parties under the electronic data message or electronic document;

. ) The making, publication, dissemination or distribution of such material or any statement made in such material, including possible infringement of any right subsisting in or in relation to such material: Provided, That

. The service provider does not have actual knowledge, or is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes
any rights subsisting in or in relation to such material;
i. The service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and
ii. The service provider does not directly commit any infringement or other unlawful act and does not induce or cause another person or party to commit any infringement or other unlawful act and/or does not benefit financially from the infringing activity or unlawful act of another person or party: Provided, further, That nothing in this Section shall affect —

) Any obligation founded on contract;
) The obligation of a service provider as such under a licensing or other regulatory regime established under written law; or
) Any obligation imposed under any written law;
) The civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any material, or to preserve evidence of a violation of law.

**SECTION 31(30). Lawful Access.**

Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key.

**SECTION 32(31). Obligation of Confidentiality.**

Except for the purposes authorized under this Act, any person who obtained access to any electronic key, electronic data message or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.

**SECTION 33. Penalties.**

The following Acts shall be penalized by fine and/or imprisonment, as follows:
)

(32) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents shall be punished by a minimum fine of One hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;
)

(33) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of One hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;
)

(34) Violations of the Consumer Act or Republic Act No. 7394 and other relevant or pertinent laws through transactions covered by or using electronic data messages or electronic documents, shall be penalized with the same penalties as provided in those laws;
)

(35) Other violations of the provisions of this Act, shall be penalized with a maximum penalty of One million pesos (P1,000,000.00) or six (6) years imprisonment.
SECTION 34(36). Implementing Rules and Regulations.

The DTI, Department of Budget and Management and the Bangko Sentral ng Pilipinas are hereby empowered to enforce the provisions of this Act and issue implementing rules and regulations necessary, in coordination with the Department of Transportation and Communications, National Telecommunications Commission, National Computer Center, National Information Technology Council, Commission on Audit, other concerned agencies and the private sector, to implement this Act within sixty (60) days after its approval. Failure to issue rules and regulations shall not in any manner affect the executory nature of the provisions of this Act.

SECTION 39(40). Reciprocity.

All benefits, privileges, advantages or statutory rules established under this Act, including those involving practice of profession, shall be enjoyed only by parties whose country of origin grants the same benefits and privileges or advantages to Filipino citizens.

2001 RULES ON ELECTRONIC EVIDENCE

A.M. No. 01-7-01-SC

Acting on the Memorandum dated 18 June 2001 of the Committee on the Revision of the Rules of Court to Draft the Rules on E-Commerce Law [R.A. No. 8792] submitting the Rules on Electronic Evidence for this Court’s consideration and approval, the Court Resolved to APPROVED the same. The Rules on Electronic Evidence shall apply to cases pending after their effectivity. These Rules shall take effect on the first day of August 2001 following their publication before the 20th of July in two newspapers of general circulation in the Philippines 7th July 2001.

RULES ON ELECTRONIC EVIDENCE

Rule 1

COVERAGE

Section 1. Scope. – Unless otherwise provided herein, these Rules shall apply whenever an electronic document or electronic data message, as defined in Rule 2 hereof, is offered or used in evidence.

Section 2. Cases covered. – These Rules shall apply to all civil actions and proceedings, as well as quasi-judicial and administrative cases.

Section 3. Application of other rules on evidence. – In all matters not specifically covered by these Rules, the Rules of Court and pertinent provisions of statutes containing rules on evidence shall apply.

Rule 2

DEFINITION OF TERMS AND CONSTRUCTION

Section 1. Definition of terms. – For purposes of these Rules, the following terms are defined, as follows:

a) “Asymmetric or public cryptosystem” means a system capable of generating a secure key pair, consisting of a private key for creating a digital signature, and a public key for verifying the digital signature.
b) “Business records” include records of any business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit, or for legitimate or illegitimate purposes.

c) “Certificate” means an electronic document issued to support a digital signature which purports to confirm the identity or other significant characteristics of the person who holds a particular key pair.

d) “Computer” refers to any single or interconnected device or apparatus, which, by electronic, electro-mechanical or magnetic impulse, or by other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.

e) “Digital signature” refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer’s public key can accurately determine:

[...]

f) “Digitally signed” refers to an electronic document or electronic data message bearing a digital signature verified by the public key listed in a certificate.

g) “Electronic data message” refers to information generated, sent, received or stored by electronic, optical or similar means.

h) “Electronic document” refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. It includes digitally signed documents and any print-out or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document. For purposes of these Rules, the term “electronic document” may be used interchangeably with “electronic data message”.

i) “Electronic key” refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable only with a matching electronic key.

j) “Electronic signature” refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedure employed or adopted by a person and executed or adopted by such person with the intention of authenticating, signing or approving an electronic data message or electronic document. For purposes of these Rules, an electronic signature includes digital signatures.

k) “Ephemeral electronic communication” refers to telephone conversations, text messages, chatroom sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.

l) “Information and communication system” refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar devices by or in which data are recorded or stored and any procedure related to the recording or storage of electronic data messages or electronic documents.

m) “Key pair” in an asymmetric cryptosystem refers to the private key and its mathematically related public key such that the latter can verify the digital signature that the former creates.

n) “Private key” refers to the key of a key pair used to create a digital signature.

o) “Public key” refers to the key of a key pair used to verify a digital signature.

Section 2. Construction. – These Rules shall be liberally construed to assist the parties in obtaining a just, expeditious, and inexpensive determination of cases.

The interpretation of these Rules shall also take into consideration the international origin of Republic Act No. 8792, otherwise known as the Electronic Commerce Act.

Rule 3

ELECTRONIC DOCUMENTS

Section 1. Electronic documents as functional equivalent of paper-based documents. – Whenever a rule of evidence refers to the term writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these Rules.

Section 2. Admissibility. – An electronic document is admissible in evidence if it complies with the rules on admissibility prescribed by the Rules of Court and related laws and is authenticated in the manner prescribed by these Rules.

Section 3. Privileged communication. – The confidential character of a privileged communication is not lost solely on the ground that it is in the form of an electronic document.
Rule 4
BEST EVIDENCE RULE

Section 1. Original of an electronic document. – An electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is a printout or output readable by sight or other means, shown to reflect the data accurately.

Section 2. Copies as equivalent of the originals. – When a document is in two or more copies executed at or about the same time with identical contents, or is a counterpart produced by the same impression as the original, or from the same matrix, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original, such copies or duplicates shall be regarded as the equivalent of the original.

Notwithstanding the foregoing, copies or duplicates shall not be admissible to the same extent as the original if:
   a) a genuine question is raised as to the authenticity of the original; or
   b) in the circumstances it would be unjust or inequitable to admit the copy in lieu of the original.

Rule 5
AUTHENTICATION OF ELECTRONIC DOCUMENTS

Section 1. Burden of proving authenticity. – The person seeking to introduce an electronic document in any legal proceeding has the burden of proving its authenticity in the manner provided in this Rule.

Section 2. Manner of authentication. – Before any private electronic document offered as authentic is received in evidence, its authenticity must be proved by any of the following means:
   a) by evidence that it had been digitally signed by the person purported to have signed the same;
   b) by evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or
   c) by other evidence showing its integrity and reliability to the satisfaction of the judge.

Section 3. Proof of electronically notarized document. – A document electronically notarized in accordance with the rules promulgated by the Supreme Court shall be considered as a public document and proved as a notarial document under the Rules of Court.

Rule 6
ELECTRONIC SIGNATURES

Section 1. Electronic signature. – An electronic signature or a digital signature authenticated in the manner prescribed hereunder is admissible in evidence as the functional equivalent of the signature of a person on a written document.

Section 2. Authentication of electronic signatures. – An electronic signature may be authenticated in any of the following manner:
   a) By evidence that a method or process was utilized to establish a digital signature and verify the same;
   b) By any other means provided by law; or
   c) By any other means satisfactory to the judge as establishing the genuineness of the electronic signature.

Section 3. Disputable presumptions relating to electronic signatures. – Upon the authentication of an electronic signature, it shall be presumed that:
   a) The electronic signature is that of the person to whom it correlates;
   b) The electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person's consent to the transaction embodied therein; and
   c) The methods or processes utilized to affix or verify the electronic signature operated without error or fault.

Section 4. Disputable presumptions relating to digital signatures. – Upon the authentication of a digital signature, it shall be presumed, in addition to those mentioned in the immediately preceding section, that:
   a) The information contained in a certificate is correct;
   b) The digital signature was created during the operational period of a certificate;
   c) No cause exists to render a certificate invalid or revocable;
   d) The message associated with a digital signature has not been altered from the time it was signed; and,
   e) A certificate had been issued by the certification authority indicated therein.
Rule 7
EVIDENTIARY WEIGHT OF ELECTRONIC DOCUMENTS

Section 1. Factors for assessing evidentiary weight. – In assessing the evidentiary weight of an electronic document, the following factors may be considered:
a) The reliability of the manner or method in which it was generated, stored or communicated, including but not limited to input and output procedures, controls, tests and checks for accuracy and reliability of the electronic data message or document, in the light of all the circumstances as well as any relevant agreement;
b) The reliability of the manner in which its originator was identified;
c) The integrity of the information and communication system in which it is recorded or stored, including but not limited to the hardware and computer programs or software used as well as programming errors;
d) The familiarity of the witness or the person who made the entry with the communication and information system;
e) The nature and quality of the information which went into the communication and information system upon which the electronic data message or electronic document was based; or
f) Other factors which the court may consider as affecting the accuracy or integrity of the electronic document or electronic data message.

Section 2. Integrity of an information and communication system. – In any dispute involving the integrity of the information and communication system in which an electronic document or electronic data message is recorded or stored, the court may consider, among others, the following factors:
a) Whether the information and communication system or other similar device was operated in a manner that did not affect the integrity of the electronic document, and there are no other reasonable grounds to doubt the integrity of the information and communication system;
b) Whether the electronic document was recorded or stored by a party to the proceedings with interest adverse to that of the party using it; or

Rule 8
BUSINESS RECORDS AS EXCEPTION TO THE HEARSAY RULE

Section 1. Inapplicability of the hearsay rule. – A memorandum, report, record or data compilation of acts, events, conditions, opinions, or diagnoses, made by electronic, optical or other similar means at or near the time of or from transmission or supply of information by a person with knowledge thereof, and kept in the regular course or conduct of a business activity, and such was the regular practice to make the memorandum, report, record, or data compilation by electronic, optical or similar means, all of which are shown by the testimony of the custodian or other qualified witnesses, is excepted from the rule on hearsay evidence.

Section 2. Overcoming the presumption. – The presumption provided for in Section 1 of this Rule may be overcome by evidence of the untrustworthiness of the source of information or the method or circumstances of the preparation, transmission or storage thereof.

Rule 9
METHOD OF PROOF

Section 1. Affidavit evidence. – All matters relating to the admissibility and evidentiary weight of an electronic document may be established by an affidavit stating facts of direct personal knowledge of the affiant or based on authentic records. The affidavit must affirmatively show the competence of the affiant to testify on the matters contained therein.

Section 2. Cross-examination of deponent. – The affiant shall be made to affirm the contents of the affidavit in open court and may be cross-examined as a matter of right by the adverse party.
Rule 10
**EXAMINATION OF WITNESSES**

Section 1. *Electronic testimony.* – After summarily hearing the parties pursuant to Rule 9 of these Rules, the court may authorize the presentation of testimonial evidence by electronic means. Before so authorizing, the court shall determine the necessity for such presentation and prescribe terms and conditions as may be necessary under the circumstances, including the protection of the rights of the parties and witnesses concerned.

Section 2. *Transcript of electronic testimony.* – When examination of a witness is done electronically, the entire proceedings, including the questions and answers, shall be transcribed by a stenographer, steno typist or other recorder authorized for the purpose, who shall certify as correct the transcript done by him. The transcript should reflect the fact that the proceedings, either in whole or in part, had been electronically recorded.

Section 3. *Storage of electronic evidence.* – The electronic evidence and recording thereof as well as the stenographic notes shall form part of the record of the case. Such transcript and recording shall be deemed prima facie evidence of such proceedings.

Rule 11
**AUDIO, PHOTOGRAPHIC, VIDEO, AND EPHEMERAL EVIDENCE**

Section 1. *Audio, video and similar evidence.* – Audio, photographic and video evidence of events, acts or transactions shall be admissible provided it shall be shown, presented or displayed to the court and shall be identified, explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy thereof.

Section 2. *Ephemeral electronic communications.* – Ephemeral electronic communications shall be proven by the testimony of a person who was a party to the same or has personal knowledge thereof. In the absence or unavailability of such witnesses, other competent evidence may be admitted.

A recording of the telephone conversation or ephemeral electronic communication shall be covered by the immediately preceding section.

If the foregoing communications are recorded or embodied in an electronic document, then the provisions of Rule 5 shall apply.

Rule 12
**EFFECTIVITY**

Section 1. *Applicability to pending cases.* – These Rules shall apply to cases pending after their effectivity.

Section 2. *Effectivity.* – These Rules shall take effect on the first day of August 2001 following their publication before the 20th of July 2001 in two newspapers of general circulation in the Philippines.

---

**2012 REPUBLIC ACT NO. 10175**

*(Cybercrime Prevention Act)*

**CHAPTER 1**

**PRELIMINARY PROVISION**

**Section 3. Definition of Terms**-

For purpose of this Act, the following terms are hereby defined as follow:

- Access refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system, or communication network.
- Alteration refers to modification or change, in form or substance, of an existing computer data or program.
Communication refers to the transmission of information ICT media, including voice, video and other forms of data.

Computer refers to an electronic, magnetic, optical, electrochemical, or other data processing or communication device, or grouping of such devices, capable of performing local, arithmetic, routing, or storage functions and which includes any storage facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including device with data processing capabilities like mobile phone, smart phones, computer networks, and other devices connected to the internet.

Computer data refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages whether stored in local computer system or online.

Computer program refers to a set of instructions executed by the computer achieve intended results.

Computer system refers to any device or group of interconnected or related device, one or more of which, pursuant to a program, performs automated processing of data. It covers any type of device with data processing capabilities included but not limited to, computer and mobile phones. The device consisting of hardware and software may include input, output and storage components which may stand alone or be connected in a network or other similar devices. It also includes computer data storage device or media.

Without right refers to either (i) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications or relevant principles under the law.

Cyber refers to computer network, the electronic medium in which online communication takes place.

Critical infrastructure refers to the computer system, and/or networks whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or distraction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety or any combination of those matters.

Cybersecurity refers to the collection of tools, polices, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Database refers to representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or have been prepared, processed or stored in a formalized manner and which are intended for use in a computer system.

Interception refers to listening to, recording, monitoring or surveillance of the content communications, including procuring of the content data, either directly, through access and use of computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

Service provider refers to:

Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Subscriber's information refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers information of its services other than traffic or content data and by which identity can be established:

The type of communication service used, the technical provisions taken thereto and the period of service;

The subscriber's identity, postal or geographical address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and

Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Traffic data or non-content data refers to any computer data other then the content of the communication including but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

CHAPTER II
PUNISHABLE ACTS

Section 4. Cybercrime Offenses

The following acts constitute the offense of cybercrime punishable under this Act:

Offences against the confidentiality, integrity and availability of computer data system:

Illegal Access- The access to the whole or any part of computer system without right.
Illegal Interception - The interception made by technical means without right of any non-public transmission of computer data to, from or within a computer system carrying such compute data.

Data Interference - The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

System Interference - The intentional alteration or reckless hindering or interference with the functioning of a computer system, causing damage, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

Misuse of Device:
- The use, production, sale procurement, importation, distribution, or otherwise making available, without right, of:
  - A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act;
  - A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act.

Data Interference:
- The possession of an item referred to in paragraph 5(a)(i) or (ii) above with intent to use said devices for the purpose of committing any of the offenses under this section.

Cyber-squatting - The acquisition of domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:
- Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration;
- Identical or in any way similar with the name of a person other than the registrant, in case of personal name; and
- Acquired without right or with intellectual property interests in it.

Computer-related Offenses:

Computer-related Forgery:
- The input, alteration or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purpose as if it were authentic, regardless whether or not the data is directly readable and intelligible; or
  - The act of knowing using computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design.

Computer-related Fraud - The unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent provided that if no damage has yet been cause, the penalty imposable shall be one (1) degree lower.

Computer-related Identity Theft - The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right provided that if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

Content-related Offences:

Cybersex - The wilful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of computer system, for favor or consideration.

Child Pornography - The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system or any other similar means which may be devised in the future.

Unsolicited Commercial Communications - The transmission of commercial electronic communication with the use of computer system which seek to advertise, sell, or offer for sale products and services are prohibited unless:
- There is prior affirmative consent from the recipient; or
  - The primary intent of the communication is for service and/or administrative announcement from the sender to its existing users, subscribers or customers; or
  - The following conditions are present:
    - The commercial electronic communication contains a simple, valid, and reliable way for the recipient to reject receipt of further commercial electronic messages (opt-out) from the same source;
    - The commercial electronic communication does not purposely disguise the source of the electronic message; and
    - The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

Libel - The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.
Section 5. Other Offences.

The following shall also constitute an offence:
. Aiding or abetting in the commission of cybercrime of any person who wilfully abets or aids in the commission of any offences enumerated in this Act shall be held liable.
Attempt the commission of cybercrime. Any person who wilfully attempts to commit any of the offences enumerated in this Act shall be held liable.

Section 6.

All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, though and with the use of information and communications technologies shall be covered by the relevant provisions of this Act, provided that the penalty to be imposed shall be one (1) degree higher than that provided for by Revised Penal Code, as amended, and special laws, as the case may be.

Section 7. Liability under Other Laws.

A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws.

CHAPTER IV
ENFORCEMENT AND IMPLEMENTATION

Section 10. Law Enforcement Authorities

The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

Section 11. Duties of Law Enforcement Authorities.

To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports and such other documents as may be required to the Departments of Justice (DOJ) for review and monitoring.


Law enforcement authorities, which due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of computer system.
Traffic data refer only to the communication’s origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.
All other data to be collected or sized or disclosed will require a court warrant.
Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.
The court warrant required under this section shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed. Or is about to be committed; (2) that there are reasonable ground to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and (3) that there are no other means readily available for obtaining such evidence.

**Section 13. Preservation of Computer Data.**

The integrity of traffic data and subscriber information relating to communication services provided for a minimum period of six months from the date of the transaction. Content data shall be similarly preserved for six months from the date of receipt of the order from law enforcement authorities requiring its preservation. Law enforcement authorities may order a one-time extension for another six months provided that once computer data preserved, transmitted or stored by service provider is used as evidence in a case, the mere furnishing to such service of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case. The service provider order to preserve computer data shall keep confidential the order and its compliance.

**Section 14. Disclosure of Computer Data**

Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber’s information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid compliant officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

**Section 15. Search, Seizure and Examination of Computer Data**

Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

- To secure a computer system or computer data storage medium;
- To make and retain a copy of those computer data secured;
- To maintain the integrity of the relevant stored computer data;
- To conduct forensic analysis or examination of computer data storage medium; and
- To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination. Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

**Section 16. Custody of Computer Data**

All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authorities who may access the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposit with the court. The package so deposited shall not be opened, or the recordings replayed or used in evidence,
or their contents revealed, except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

**Section 17 Destruction of Computer Data**

Upon expiration of the periods as provided in Section 13 and 15, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of preservation and examination.

**Section 18. Exclusionary Rule**

Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

**Section 19. Restricting or blocking access to Computer Data**

When a computer data is prima facie found to be in violation of the provisions of this Act, the DOJ shall issue an order to restrict or block access to such computer data.

**CHAPTER V  
JURISDICTION**

**Section 21. Jurisdiction**

The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offence was committed, was the Philippines. They shall be designed special cybercrime courts manned by special trained judges to handle cybercrime cases.

**CHAPTER VI  
INTERNATIONAL COOPERATION**

**Section 22. General Principles Relating to International Cooperation**

All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer system and data, or for the collection of evidence in electronic form of a criminal offence shall be given full force and effect.
CHAPTER VII
COMPETENT AUTHORITIES

Section 23. Department of Justice (DOJ)

There is hereby created an Offence of Cybercrime within the DOJ designed as the central authority in all matters related to international mutual assistance and extradition.

Section 24. Cybercrime Investigation and Coordinating Center.

There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, for police coordination among concerned agencies and for the formulation and enforcement of the national cybersecurity plan.

Section 25. Composition.

The CICC shall be headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO_DOST) as Chairperson with the Director of the NBI as Vice Chairperson; the Chief of the PNP; Head of the DOJ Office of Cybercrime; and one (1) representative from the private sector and academe, as members. The CICC shall be manned by a secretariat of selected existing personnel and representatives from the different participating agencies.

Section 26. Power and Function.

The CICC shall have the following powers and functions:

- To formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offences through a computer emergency team (CERT);
- To coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for this Act;
- To monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;
- To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;
- To coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other related projects;
- To recommend the enactment of appropriate laws, issuances, measures and policies;
- To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions; and
- To perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as may be necessary for the proper implementation of this Act.
For purposes of this Act, knowledge or intent may be established by direct evidence or inferred from the attendant circumstances.

SEC 3. Definition of Terms – As used in this Act:

(...) (h) Property or funds refer to financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

SEC. 22. Implementing Rules and Regulations.

Within thirty (30) days from the effectivity of this Act, the AMLC, in coordination with relevant government agencies, shall promulgate rules and regulations to implement effectively the provisions of this Act. The rules and regulations to be promulgated may include, but not limited to, designation, delisting, notification of matters of interest of persons affected by the Act, exceptions for basic, necessary and extraordinary expenses, matters of evidence, definition of probable cause, inter-agency coordination, publication of relevant information, administrative offenses and penalties, procedures and forms, and other mechanisms for implementation of the Act.

2019 PROPOSED AMENDMENTS TO THE 1989 REVISED RULES ON EVIDENCE

RULE 128 - GENERAL PROVISIONS

Section 1. Evidence defined. – Evidence is the means, sanctioned by these Rules, of ascertaining in a judicial proceeding the truth respecting a matter of fact. (1)

Section 2. Scope. – The rules of evidence shall be the same in all courts and in all trials and hearings, except as otherwise provided by law or these Rules. (2)

Section 3. Admissibility of evidence. – Evidence is admissible when it is relevant to the issue and not excluded by the Constitution, the law or these Rules. (3a)

Section 4. Relevancy; collateral matters. – Evidence must have such a relation to the fact in issue as to induce belief in its existence or non-existence. Evidence on collateral matters shall not be allowed, except when it tends in any reasonable degree to establish the probability or improbability of the fact in issue. (4)

RULE 130 - RULES OF ADMISSIBILITY

A. OBJECT (REAL) EVIDENCE

Section 1. Object as evidence. – Objects as evidence are those addressed to the senses of the court. When an object is relevant to the fact in issue, it may be exhibited to, examined or viewed by the court. (1)
B. DOCUMENTARY EVIDENCE

Section 2. Documentary evidence. – Documents as evidence consist of writings, recordings, photographs or any material containing letters, words, sounds, numbers, figures, symbols, or their equivalent, or other modes of written expression offered as proof of their contents. Photographs include still pictures, drawings, stored images, x-ray films, motion pictures or videos. (2a)

1. Original Document Rule

Section 3. Original document must be produced; exceptions. – When the subject of inquiry is the contents of a document, writing, recording, photograph or other record, no evidence is admissible other than the original document itself, except in the following cases:

a) When the original is lost or destroyed, or cannot be produced in court, without bad faith on the part of the offeror;
b) When the original is in the custody or under the control of the party against whom the evidence is offered, and the latter fails to produce it after reasonable notice, or the original cannot be obtained by local judicial processes or procedures;
c) When the original consists of numerous accounts or other documents which cannot be examined in court without great loss of time and the fact sought to be established from them is only the general result of the whole;
d) When the original is a public record in the custody of a public officer or is recorded in a public office; and
e) When the original is not closely-related to a controlling issue (3a)

Section 4. Original of document.

a) An “original” of a document is the document itself or any counterpart intended to have the same effect by a person executing or issuing it. An “original” of a photograph includes the negative or any print therefrom. If data is stored in a computer or similar device, any printout or other output readable by sight or other means, shown to reflect the data accurately, is an “original.”
b) A “duplicate” is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original.
c) A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original, or (2) in the circumstances, it is unjust or inequitable to admit the duplicate in lieu of the original. (4a)

Section 45. Records of regularly conducted business activity.

– A memorandum, report, record or data compilation of acts, events, conditions, opinions, or diagnoses, made by writing, typing, electronic, optical or other similar means at or near the time of or from transmission or supply of information by a person with knowledge thereof, and kept in the regular course or conduct of a business activity, and such was the regular practice to make the memorandum, report, record, or data compilation by electronic, optical or similar means, all of which are shown by the testimony of the custodian or other qualified witnesses, is excepted from the rule on hearsay evidence. (43a)
Interpretation

3.—(1) In Parts 1, 2 and 3, unless the context otherwise requires —
copy of a document" includes —
a) in the case of a document falling within paragraph (d) but not paragraph (e) of the definition of “document”, a transcript of the sounds or other data embodied in it;
b) in the case of a document falling within paragraph (e) but not paragraph (d) of that definition, a reproduction or still reproduction of the image or images embodied in it, whether enlarged or not;
c) in the case of a document falling within paragraphs (d) and (e) of that definition, such a transcript together with such a still reproduction; and

d) in the case of a document not falling within paragraph (e) of that definition of which a visual image is embodied in a document falling within that paragraph, a reproduction of that image, whether enlarged or not,

and any reference to a copy of the material part of a document must be construed accordingly;
document” includes, in addition to a document in writing —
a) any map, plan, graph or drawing;
b) any photograph;
c) any label, marking or other writing which identifies or describes anything of which it forms a part, or to which it is attached by any means whatsoever;
d) any disc, tape, soundtrack or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom;
e) any film (including microfilm), negative, tape, disc or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and
f) any paper or other material on which there are marks, impressions, figures, letters, symbols or perforations having a meaning for persons qualified to interpret them;
electronic record” means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or transmitted from one information system to another;
evidence” includes —
a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence; and
b) all documents produced for the inspection of the court: such documents are called documentary evidence;

fact” includes —
a) any thing, state of things, or relation of things, capable of being received by the senses; and
b) any mental condition of which any person is conscious;
illustrations
a) That there are certain objects arranged in a certain order in a certain place is a fact.
b) That a man heard or saw something is a fact.
c) That a man said certain words is a fact.
d) That a man holds a certain opinion, has a certain intention, acts in good faith or fraudulently, or uses a particular word in a particular sense, or is or was at a specified time conscious of a particular sensation, is a fact.
e) That a man has a certain reputation is a fact.

Presumptions

4.—(1) Whenever it is provided by this Act that the court may presume a fact, it may either regard such fact as proved unless and until it is disproved, or may call for proof of it.
2) Whenever it is directed by this Act that the court is to presume a fact, the court is to regard such fact as proved unless and until it is disproved.
3) When one fact is declared by this Act to be conclusive proof of another, the court is, on proof of the one fact, to regard the other as proved, and is not to allow evidence to be given for the purpose of disproving it.

Evidence may be given of facts in issue and relevant facts

5. Evidence may be given in any suit or proceeding of the existence or non-existence of every fact in issue and of such other facts as are hereinafter declared to be relevant, and of no others.
**Explanation.**—This section does not enable any person to give evidence of a fact which the person is disentitled to prove by any provision of the law for the time being in force relating to civil procedure.

**Illustrations**

(a) A is tried for the murder of B by beating B with a club with the intention of causing B's death. At A's trial the following facts are in issue:

i) A's beating B with the club;
ii) A's causing B's death by such beating;
iii) A's intention to cause B's death.

(b) A, a party to a suit, does not comply with a notice given by B, the other party, to produce for B's inspection a document referred to in A's pleadings. This section does not enable A to put such document in evidence on A's behalf in such suit, otherwise than in accordance with the conditions prescribed by the Rules of Court or the Family Justice Rules, as the case may be.

### 9. Facts necessary to explain or introduce relevant facts

(g) A seeks to adduce evidence against B in the form of an electronic record. The method and manner in which the electronic record was (properly or improperly) generated, communicated, received or stored (by A or B), the reliability of the devices and the circumstances in which the devices were (properly or improperly) used or operated to generate, communicate, receive or store the electronic record, may be relevant facts (if the contents are relevant) as authenticating the electronic record and therefore as explaining or introducing the electronic record, or identifying it as the relevant electronic record to support finding that the record is, or is not, what its proponent A claims.

### Rules for filing and receiving evidence and documents in court by using information technology

36A.—(1) The Rules Committee constituted under the Supreme Court of Judicature Act (Cap. 322), and the Family Justice Rules Committee constituted under the Family Justice Act 2014, may make rules to provide for the filing, receiving and recording of evidence and documents in court by the use of information technology in such form, manner or method as may be prescribed. (2) Without prejudice to the generality of subsection (1), such rules may —

a) modify such provisions of this Act as may be necessary for the purpose of facilitating the use of electronic filing of documents in court;

b) provide for the burden of proof and rebuttable presumptions in relation to the identity and authority of the person sending or filing the evidence or documents by the use of information technology; and provide for the authentication of evidence and documents filed or received by the use of information technology.

### Primary evidence

64. Primary evidence means the document itself produced for the inspection of the court (…). Illustration: A person is shown to have been in possession of a number of placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original.

Explanation 3.—Notwithstanding Explanation 2, if a copy of a document in the form of an electronic record is shown to reflect that document accurately, then the copy is primary evidence.

Illustrations:

a) An electronic record, which has been manifestly or consistently acted on, relied upon, or used as the information recorded or stored on the computer system (the document), is primary evidence of that document.

b) If the electronic record has not been manifestly or consistently acted on, relied upon, or used as a record of the information in the document, the electronic record may be a copy of the document and treated as secondary evidence of that document.
Secondary evidence

65. Secondary evidence means and includes —
a) certified copies given under the provisions hereinafter contained;
b) except for copies referred to in Explanation 3 to section 64, copies made from the original by electronic, electrochemical, chemical, magnetic, mechanical, optical, telematic or other technical processes, which in themselves ensure the accuracy of the copy, and copies compared with such copies;
c) copies made from or compared with the original;
d) counterparts of documents as against the parties who did not execute them;
e) oral accounts of the contents of a document given by some person who has himself seen it.

Proof of signature and handwriting of person alleged to have signed or written document produced

69.—(1) If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.
2) This section shall not apply to any electronic record or electronic signature to which the Electronic Transactions Act 1998 applies.

Presumptions in relation to electronic records

116A.—(1) Unless evidence sufficient to raise doubt about the presumption is adduced, where a device or process is one that, or is of a kind that, if properly used, ordinarily produces or accurately communicates an electronic record, the court shall presume that in producing or communicating that electronic record on the occasion in question, the device or process produced or accurately communicated the electronic record.

Illustration
seeks to adduce evidence in the form of an electronic record or document produced by an electronic device or process. A proves that the electronic device or process in question is one that, or is of a kind that, if properly used, ordinarily produces that electronic record or document. This is a relevant fact for the court to presume that in producing the electronic record or document on the occasion in question, the electronic device or process produced the electronic record or document which A seeks to adduce.

2) Unless evidence to the contrary is adduced, the court shall presume that any electronic record generated, recorded or stored is authentic if it is established that the electronic record was generated, recorded or stored in the usual and ordinary course of business by a person who was not a party to the proceedings on the occasion in question and who did not generate, record or store it under the control of the party seeking to introduce the electronic record.

Illustration
seeks to adduce evidence against B in the form of an electronic record. The fact that the electronic record was generated, recorded or stored in the usual and ordinary course of business by C, a neutral third party, is a relevant fact for the court to presume that the electronic record is authentic.

3) Unless evidence to the contrary is adduced, where an electronic record was generated, recorded or stored by a party who is adverse in interest to the party seeking to adduce the evidence, the court shall presume that the electronic record is authentic in relation to the authentication issues arising from the generation, recording or storage of that electronic record.

Illustration
seeks to adduce evidence against B in the form of an electronic record. The fact that the electronic record was generated, recorded or stored by B, who opposes the relevance of the evidence, is a relevant fact for the court to presume that the electronic record is authentic.

4) For the purposes of subsection (2), in criminal proceedings a party to the proceedings shall include —
a) the police officer or other officer of a law enforcement agency who was involved in the investigation of offences allegedly committed by the accused person; or
b) an accomplice of the accused person even though he is not charged with an offence in the same proceedings.

5) The Minister may make regulations providing for a process by which a document may be recorded or stored through the use of an imaging system, including providing for the appointment of one or more persons or organisations to certify these systems and their use, and for any matters incidental thereto, and an “approved process” in subsection (6) means a process that has been approved in accordance with the provisions of such
6) Where an electronic record was recorded or stored from a document produced pursuant to an approved process, the court shall presume, unless evidence to the contrary is adduced, that the electronic record accurately reproduces that document.

7) The matters referred to in this section may be established by an affidavit given to the best of the deponent’s knowledge and belief.

2006 MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT

Object of Act 3.

The object of this Act is to facilitate the provision and obtaining, by Singapore, of international assistance in criminal matters, including —

a) the provision and obtaining of evidence and things;
b) the making of arrangements for persons to give evidence or assist in criminal investigations;
c) the recovery, forfeiture or confiscation of property in respect of offences;
d) the restraining of dealings in property, or the freezing of assets, that may be recovered, forfeited or confiscated in respect of offences;
e) the execution of requests for search and seizure;
f) the location and identification of witnesses and suspects; and
he service of documents. Act not to limit cooperation with international organisations, etc.

(1) This Act does not prevent the provision or obtaining of international assistance in criminal matters to or from the International Criminal Police (Interpol) or any other international organisation.

2) This Act does not prevent the provision or obtaining of international assistance in criminal matters to or from any foreign country other than assistance of a kind that may be provided or obtained under this Act.

Requests for taking of evidence, etc.

8. —(1) The Attorney-General may request the appropriate authority of a foreign country to arrange for —

a) evidence to be taken in the foreign country; and
b) the evidence to be sent to the Attorney-General, if the Attorney-General is satisfied that there are reasonable grounds for believing that such evidence would be relevant to any criminal proceedings in Singapore.

2) The Attorney-General may request the appropriate authority of a foreign country —

a) to assist in obtaining, by search and seizure if necessary, any thing in the foreign country or a photograph or copy thereof; and
b) to arrange for the thing or the photograph or copy thereof to be sent to the Attorney-General, if the Attorney-General is satisfied that there are reasonable grounds for believing that such thing would be relevant to a criminal matter in Singapore.

3) Any evidence, thing or photograph or copy of a thing received by the Attorney-General pursuant to a request under subsection (1) or (2) may, subject to the provisions of the Criminal Procedure Code (Cap. 68) and the Evidence Act (Cap. 97), be admitted as evidence at any criminal proceedings to which the request relates.

4) In estimating the weight, if any, to be attached to a statement contained in any thing received by the Attorney-General pursuant to a request made under subsection (1) which has been admitted as evidence in any criminal proceedings to which the request relates, the court shall have regard to —

a) whether it was possible to challenge the statement by questioning the person who made it; and
b) whether the law of the foreign country concerned allowed the parties to the criminal proceedings to be legally represented when the evidence was being taken.

Taking of evidence for criminal proceedings

21. —(1) Where a request is made by the appropriate authority of a foreign country that evidence be taken in Singapore for the purposes of any criminal proceedings pending in a court in the foreign country, the Attorney-
General may by notice in writing, subject to such conditions as the Attorney-General may specify in the notice, authorise a Magistrate to take the evidence and transmit the evidence to the appropriate authority. (2) Upon receipt of the notice made under subsection (1), the Magistrate shall —

a) take the evidence of each witness appearing before him to give evidence in relation to the criminal matter as if the witness were giving evidence on a charge against a person for an offence against the law of Singapore;

b) cause the evidence to be reduced in writing and certify at the end of that writing that the evidence was taken by him; and

c) cause the writing, so certified, to be sent to the Attorney-General.

3) The proceedings may be conducted in the presence or absence of the person to whom the criminal proceedings in the foreign country relates or of his legal representative (if any).

4) The certificate referred to in subsection (2) shall state whether the person to whom the criminal proceedings in the foreign country relates or his legal representative (if any) was present at the proceedings.

5) The laws for the time being in force with respect to the compelling of persons to attend before a Magistrate, and to give evidence, answer questions and produce documents, upon the hearing of a charge against a person for an offence against the law of Singapore shall apply, so far as they are capable of application, with respect to the compelling of persons to attend before a Magistrate, and to give evidence, answer questions and produce documents, for the purposes of this section.

6) For the purposes of this section, the person to whom the criminal proceedings in the foreign country relates is competent, but not compellable, to give evidence.

7) No person who is required under this section to give evidence for the purposes of any criminal proceedings in a foreign country shall be required to answer any question that the person could not be compelled to answer in those proceedings in that country. (8) A duly certified foreign law immunity certificate is admissible in proceedings under this section as prima facie evidence of the matters stated in the certificate.

9) Evidence taken under this section shall not be admissible in evidence, or otherwise used, for the purposes of any judicial proceedings, disciplinary proceedings, or other proceedings, in Singapore except a prosecution of the person who gave that evidence for the offence of perjury, or contempt of court, in respect of that evidence.

authentication of documents 42. —(1) Subject to sections 13, 31 and 32 and the rules of law relating to the admissibility of evidence, any document that is obtained, provided, or produced pursuant to a request made under this Act and that is duly authenticated is admissible in evidence in any criminal proceedings. (2) A document is duly authenticated for the purposes of subsection (1) if —

a) it purports to be signed or certified by a judge, magistrate, or official in or of a foreign country; and

b) either — (i) it is verified by the oath of a witness, or of an official of the government of that country; or (ii) it purports to be sealed with an official or public seal of that country or of a Minister of State, or of a department or official of the government, of that country.

3) Nothing in this section prevents the proof of any matter, or the admission in evidence of any document, in accordance with any other provision of this Act or any other law of Singapore.

COMPUTER MISUSE AND CYBERSECURITY ACT

PART I PRELIMINARY

2. Interpretation

(1) In this Act, unless the context otherwise requires —

computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —

. an automated typewriter or typesetter;

. a portable hand-held calculator;

. a similar device which is non-programmable or which does not contain any data storage facility;

. or such other device as the Minister may, by notification in the Gazette, prescribe;

computer output" or "output" means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact —

. produced by a computer;

. or accurately translated from a statement or representation so produced;

computer service" includes computer time, data processing and the storage or retrieval of data; “damage” means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of
data, a program or system, or information, that —
. causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;
. modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;
. causes or threatens physical injury or death to any person; or
. threatens public health or public safety;
"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;
"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;
"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;
"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;
"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.
2) For the purposes of this Act, a person secures access to any program or data held in a computer if by causing a computer to perform any function he —
. alters or erases the program or data;
. copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
. uses it; or
. causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.
3) For the purposes of subsection (2)(c), a person uses a program if the function he causes the computer to perform —
. causes the program to be executed; or
. is itself a function of the program.
4) For the purposes of subsection (2)(d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.
5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if —
. he is not himself entitled to control access of the kind in question to the program or data; and
. he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.
6) A reference in this Act to any program or data held in a computer includes a reference to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.
7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer —
. any program or data held in the computer concerned is altered or erased;
. any program or data is added to its contents; or
. any act occurs which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as causing it.
8) Any modification referred to in subsection (7) is unauthorised if —
. the person whose act causes it is not himself entitled to determine whether the modification should be made; and
. he does not have consent to the modification from any person who is so entitled.
9) A reference in this Act to a program includes a reference to part of a program.

PART II OFFENCES

3. Unauthorised access to computer material.

(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an of-
fence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

3) For the purposes of this section, it is immaterial that the act in question is not directed at —
   . any particular program or data;
   . a program or data of any kind; or
   . a program or data held in any particular computer

4. Access with intent to commit or facilitate commission of offence

(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

4) For the purposes of this section, it is immaterial whether —
   . the access referred to in subsection (1) is authorised or unauthorised;
   . the offence to which this section applies is committed at the same time when the access is secured or at any other time

5. Unauthorised modification of computer material

(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

3) For the purposes of this section, it is immaterial that the unauthorized access or interception is not directed at —
   . any particular program or data;
   . a program or data of any kind; or a program
   . or data held in any particular computer.

2) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

6. Unauthorised use or interception of computer service.

(1) Subject to subsection (2), any person who knowingly —
   . secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;
   . intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or
   . uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine

3) For the purposes of this section, it is immaterial that the unauthorized access or interception is not directed at —
. any particular program or data;
. program or data of any kind; or
. program or data held in any particular computer.

7. Unauthorised obstruction of use of computer

(1) Any person who, knowingly and without authority or lawful excuse —
. interferes with, or interrupts or obstructs the lawful use of, a computer; or
. impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,
shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

8. Unauthorised disclosure of access code.

(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —
. for any wrongful gain;
. for any unlawful purpose; or
. knowing that it is likely to cause wrongful loss to any person.
2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

9. Enhanced punishment for offences involving protected computers

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.
2) For the purposes of subsection (1), a computer shall be treated as a “protected computer” if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —
. the security, defence or international relations of Singapore;
. the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
. the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
. the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.
3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.
PART III MISCELLANEOUS AND GENERAL

11. Territorial scope of offences under this Act.

(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

3) For the purposes of this section, this Act shall apply if, for the offence in question — the accused was in Singapore at the material time; or the computer, program or data was in Singapore at the material time. [UK CMA 1990, ss. 4 and 5] Jurisdiction of Courts

12. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act.

(REVISED EDITION 2007)

Amendment of section 2

2. Section 2(1) of the Computer Misuse and Cybersecurity Act (called in this Act the principal Act) is amended by deleting the words “or apparatus” in the definition of “electro-magnetic, acoustic, mechanical or other device” and substituting the words “, apparatus or program”.

New sections 8A and 8B

3. The principal Act is amended by inserting, immediately after section 8, the following sections:

Supplying, etc., personal information obtained in contravention of certain provisions

8A

(1) A person shall be guilty of an offence if the person, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 —

a) obtains or retains the personal information; or

b) supplies, offers to supply, transmits or makes available, by any means the personal information.

2) It is not an offence under subsection (1)(a) if the person obtained or retained the personal information for a purpose other than —

a) for use in committing, or in facilitating the commission of, any offence under any written law; or

b) for supply, transmission or making available by any means for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law.

3) It is not an offence under subsection (1)(b) if —

a) the person did the act for a purpose other than for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law; and

b) the person did not know or have reason to believe that the personal information will be or is likely to be used to commit, or facilitate the commission of, any offence under any written law.

Example 1.— A comes across a list of credit card numbers on the Internet belonging to individuals who are customers of B, which A has reason to believe were obtained by securing access without authority to B’s server. A downloads the list for the purpose of reporting the unauthorised access to B’s server to the police. A retains the list of credit card numbers and transmits it to B for the purpose of informing B of the unauthorised access to B’s server.

A has downloaded and retained the list of credit card numbers for purposes other than those mentioned in subsection (2)(a) and (b). Therefore A does not commit an offence under subsection (1)(a) by reason of subsection (2).
A has transmitted the list to B for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If A did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then A does not commit an offence under subsection (1)(b) by reason of subsection (3).

Example 2.— C, an employee of B, after receiving the list from A in Example 1, transmits it to D, another employee of B, for the purpose of facilitating B's investigation of the unauthorised access of B's server. C has transmitted the list to D for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If C did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then C does not commit an offence under subsection (1)(b) by reason of subsection (3).

4) For the purposes of subsection (1)(b), a person does not transmit or make available personal information merely because the person provides, or operates facilities for network access, or provides services relating to, or provides connections for, the transmission or routing of data.

5) A person guilty of an offence under subsection (1) shall be liable on conviction —
   a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and
   b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

6) For the purpose of proving under subsection (1) that a person knows or has reason to believe that any personal information was obtained by an act done in contravention of section 3, 4, 5 or 6, it is not necessary for the prosecution to prove the particulars of the contravention, such as who carried out the contravention and when it took place.

7) In this section —
   a) personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password; and
   b) a reference to an offence under any written law includes an offence under subsection (1).

8B

(1) A person shall be guilty of an offence if the person —
   a) obtains or retains any item to which this section applies —
      i) intending to use it to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7; or
      ii) with a view to it being supplied or made available, by any means for use in committing, or in facilitating the commission of, any of those offences; or
   b) makes, supplies, offers to supply or makes available, by any means any item to which this section applies, intending it to be used to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7.

2) This section applies to the following items:
   a) any device, including a computer program, that is designed or adapted primarily, or is capable of being used, for the purpose of committing an offence under section 3, 4, 5, 6 or 7;
   b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

3) A person guilty of an offence under subsection (1) shall be liable on conviction —
   a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and
   b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both."

Amendment of section 11

4. Section 11 of the principal Act is amended —
   a) by deleting the words “subsection (2)” in subsection (1) and substituting the words “subsection (3)”; and
   b) by deleting subsection (3) and substituting the following subsections:
      (3) For the purposes of this section, this Act applies if —
         a) for the offence in question, the accused was in Singapore at the material time;
         b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8), the computer, program or data was in Singapore at the material time; or
         c) the offence causes, or creates a significant risk of, serious harm in Singapore.
   4) In subsection (3)(c), “serious harm in Singapore” means —
      a) illness, injury or death of individuals in Singapore;
b) a disruption of, or a serious diminution of public confidence in, the provision of any essential service within the meaning of section 15A(12) in Singapore;

c) a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board; or

d) damage to the national security, defence or foreign relations of Singapore.

Example 1.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the provision of an essential service:

(a) publication to the public of the medical records of patients of a hospital in Singapore;

(b) providing to the public access to the account numbers of customers of a bank in Singapore.

Example 2.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board:

(a) providing to the public access to confidential documents belonging to a ministry of the Government;

(b) publication to the public of the access codes for a computer belonging to a statutory board.

5) For the purposes of subsection (3)(c), it is immaterial whether the offence that causes the serious harm in Singapore —

a) causes such harm directly; or

b) is the only or main cause of the harm.

6) In subsection (4)(c), “statutory board” means a body corporate or unincorporate established by or under any public Act to perform or discharge a public function.”.

New section 11A

1A.—(1) This section applies when a person is alleged to have committed 2 or more acts —

a) each of which is an offence under the same provision in Part II;

b) that involve the same computer; and

c) that are committed in a period that does not exceed 12 months.

2) Despite section 124 of the Criminal Procedure Code (Cap. 68), it is sufficient for the charge in respect of those acts to specify —

a) particulars of that computer; and

b) the dates between which the acts are alleged to have been committed, without specifying the exact dates the acts are committed.

3) A charge framed in accordance with subsection (2) is treated as a charge of one offence.

4) If the particulars mentioned in subsection (2)(a) and (b) do not give the accused sufficient notice of what the accused is charged with, then the charge must also give details of how the alleged offence was committed as will be sufficient for that purpose.”.

2019 EVIDENCE ACT

Interpretation 3.

(1) In Parts I, II and III, unless the context otherwise requires

copy of a document” includes —

a) in the case of a document falling within paragraph (d) but not paragraph (e) of the definition of “document”, a transcript of the sounds or other data embodied in it;

b) in the case of a document falling within paragraph (e) but not paragraph (d) of that definition, a reproduction or still reproduction of the image or images embodied in it, whether enlarged or not;

c) in the case of a document falling within paragraphs (d) and (e) of that definition, such a transcript together with such a still reproduction; and

d) in the case of a document not falling within paragraph (e) of that definition of which a visual image is embodied in a document falling within that paragraph, a reproduction of that image, whether enlarged or not, and any reference to a copy of the material part of a document must be construed accordingly;

document” includes, in addition to a document in writing —

a) any map, plan, graph or drawing;

b) any photograph;

c) any label, marking or other writing which identifies or describes anything of which it forms a part, or to which it is attached by any means whatsoever;
d) any disc, tape, sound-track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom;
e) any film (including microfilm), negative, tape, disc or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced therefrom; and
f) any paper or other material on which there are marks, impressions, figures, letters, symbols or perforations having a meaning for persons qualified to interpret them;
electronic record means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or transmitted from one information system to another;
evidence includes
a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence;
b) all documents produced for the inspection of the court: such documents are called documentary evidence;
fact includes
a) any thing, state of things, or relation of things, capable of being received by the senses;
b) any mental condition of which any person is conscious;
illustrations
a) That there are certain objects arranged in a certain order in a certain place is a fact.
b) That a man heard or saw something is a fact.
c) That a man said certain words is a fact.
d) That a man holds a certain opinion, has a certain intention, acts in good faith or fraudulently, or uses a particular word in a particular sense, or is or was at a specified time conscious of a particular sensation, is a fact.
e) That a man has a certain reputation is a fact. “fact in issue” includes any fact from which either by itself or in connection with other facts the existence, non-existence, nature or extent of any right, liability or disability asserted or denied in any suit or proceeding necessarily follows; Illustrations A is accused of the murder of B. At his trial the following facts may be in issue: that A caused B's death; that A intended to cause B's death; that A had received grave and sudden provocation from B

Relevancy of facts

Evidence may be given of facts in issue and relevant facts.

Evidence may be given in any suit or proceeding of the existence or non-existence of every fact in issue and of such other facts as are hereinafter declared to be relevant, and of no others. Explanation.—This section shall not enable any person to give evidence of a fact which he is disentitled to prove by any provision of the law for the time being in force relating to civil procedure. Illustrations
a) A is tried for the murder of B by beating him with a club with the intention of causing his death. At A’s trial the following facts are in issue: A’s beating B with the club; A’s causing B’s death by such beating; A’s intention to cause B’s death.
b) A, a party to a suit, does not comply with a notice given by B, the other party, to produce for B’s inspection a document referred to in A’s pleadings. This section does not enable A to put such document in evidence on his behalf in such suit, otherwise than in accordance with the conditions prescribed by the Rules of Court or the Family Justice Rules (as the case may be).

Relevancy of facts forming part of same transaction.

Facts which, though not in issue, are so connected with a fact in issue as to form part of the same transaction are relevant, whether they occurred at the same time and place or at different times and places. Illustrations
a) A is accused of the murder of B by beating him. Whatever was said or done by A or B or the bystanders at the beating or so shortly before or after it as to form part of the transaction is a relevant fact.
b) A is accused of waging war against the Government by taking part in an armed insurrection in which property is destroyed, troops are attacked and gaols are broken open. The occurrence of these facts is relevant as forming part of the general transaction, though A may not have been present at all of them.
c) A sues B for a libel contained in a letter forming part of a correspondence. Letters between the parties relating to the subject out of which the libel arose and forming part of the correspondence in which it is contained are
relevant facts though they do not contain the libel itself.
d) The question is whether certain goods ordered from B were delivered to A. The goods were delivered to several intermediate persons successively. Each delivery is a relevant fact.

Facts which are the occasion, cause or effect of facts in issue 7.

Facts which are the occasion, cause or effect, immediate or otherwise, of relevant facts or facts in issue, or which constitute the state of things under which they happened or which afforded an opportunity for their occurrence or transaction, are relevant.

Illustrations

a) The question is whether A robbed B. The facts that shortly before the robbery B went to a fair with money in his possession, and that he showed or mentioned the fact that he had it to third persons, are relevant.
b) The question is whether A murdered B. Marks on the ground produced by a struggle at or near the place where the murder was committed are relevant facts.
c) The question is whether A poisoned B. The state of B's health before the symptoms ascribed to poison and habits of B known to A which afforded an opportunity for the administration of poison, are relevant facts.

Motive, preparation and previous or subsequent conduct 8.

(1) Any fact is relevant which shows or constitutes a motive or preparation for any fact in issue or relevant fact.
2) The conduct of any party or of any agent to any party to any suit or proceeding in reference to such suit or proceeding or in reference to any fact in issue therein or relevant thereto, and the conduct of any person an offence against whom is the subject of any proceeding, is relevant if such conduct influences or is influenced by any fact in issue or relevant fact, and whether it was previous or subsequent thereto.

explanation 1.—The word “conduct” in this section does not include statements unless those statements accompany and explain acts other than statements; but this explanation is not to affect the relevancy of statements under any other section of this Act.

Facts necessary to explain or introduce relevant facts 9.

Facts necessary to explain or introduce a fact in issue or relevant fact, or which support or rebut an inference suggested by a fact in issue or relevant fact, or which establish the identity of any thing or person whose identity is relevant, or fix the time or place at which any fact in issue or relevant fact happened or which show the relation of parties by whom any such fact was transacted, are relevant in so far as they are necessary for that purpose.

When facts not otherwise relevant become relevant 11.

Facts not otherwise relevant are relevant
a) if they are inconsistent with any fact in issue or relevant fact;
b) if by themselves or in connection with other facts they make the existence or non-existence of any fact in issue or relevant fact highly probable or improbable.

In suits for damages facts tending to enable court to determine amount are relevant 12.

In suits in which damages are claimed, any fact which will enable the court to determine the amount of damages which ought to be awarded is relevant.
Facts relevant when right or custom is in question 13.

Where the question is as to the existence of any right or custom, the following facts are relevant: (a) any transaction by which the right or custom in question was created, claimed, modified, recognised, asserted or denied or which was inconsistent with its existence; and (b) particular instances in which the right or custom was claimed, recognised or exercised or in which its exercise was disputed, asserted or departed from.

Existence of course of business when relevant 16.

When there is a question whether a particular act was done, the existence of any course of business, according to which it naturally would have been done, is a relevant fact.

Admissibility of evidence as to credibility of maker, etc., of statement admitted under certain provisions 32C.

(1) Where in any proceedings a statement made by a person who is not called as a witness in those proceedings is given in evidence by virtue of section 32(1) —
   a) any evidence which, if that person had been so called, would be admissible for the purpose of undermining or supporting that person's credibility as a witness, is admissible for that purpose in those proceedings; and (b) as regards any matter which, if that person had been so called, could have been put to him in cross-examination for the purpose of undermining his credibility as a witness, being a matter of which, if he had denied it, evidence could not have been adduced by the cross-examining party, evidence of that matter may with the leave of the court be given for that purpose.

2) Where in any proceedings a statement made by a person who is not called as a witness in those proceedings is given in evidence by virtue of section 32(1), evidence tending to prove that, whether before or after he made that statement, he made another statement (orally, written or otherwise) inconsistent with the first-mentioned statement is admissible for the purpose of showing that he has contradicted himself.

3) For the purposes of section 32(1)(b), subsections (1) and (2) apply in relation to both the maker of the statement and the person who originally supplied the information from which the statement was made.

4) Section 32(2) applies for the purposes of this section as it applies for the purposes of section 32(1).

Relevancy of certain evidence for proving in subsequent proceeding the truth of facts therein stated 33.

Evidence given by a witness in a judicial proceeding, or before any person authorised by law to take it, is relevant for the purpose of proving in a subsequent judicial proceeding, or in a later stage of the same judicial proceeding, the truth of the facts which it states, when the witness is dead or cannot be found or is incapable of giving evidence, or is kept out of the way by the adverse party, or if his presence cannot be obtained without an amount of delay or expense which under the circumstances of the case the court considers unreasonable subject to the following provisions:
   a) the proceeding was between the same parties or their representatives in interest;
   b) the adverse party in the first proceeding had the right and opportunity to cross-examine; and
   c) the questions in issue were substantially the same in the first as in the second proceeding.

Opinions of experts 47.

(1) Subject to subsection (4), when the court is likely to derive assistance from an opinion upon a point of scientific, technical or other specialised knowledge, the opinions of experts upon that point are relevant facts.

2) An expert is a person with such scientific, technical or other specialised knowledge based on training, study or experience.

3) The opinion of an expert shall not be irrelevant merely because the opinion or part thereof relates to a matter
of common knowledge.
4) An opinion which is otherwise relevant under subsection (1) shall not be relevant if the court is of the view
that it would not be in the interests of justice to treat it as relevant.
Facts bearing upon opinions of experts 48. Facts not otherwise relevant are relevant if they support or are in-
consistent with the opinions of experts when such opinions are relevant.

PART II PROOF

Documentary evidence

Proof of contents of documents 63

The contents of documents may be proved by primary or by secondary evidence.

Primary evidence 64.

Primary evidence means the document itself produced for the inspection of the court.
Explanation 1.—Where a document is executed in several parts, each part is primary evidence of the document.
Where a document is executed in counterpart, each counterpart being executed by one or some of the parties
only, each counterpart is primary evidence as against the parties executing it.
Explanation 2.—Where a number of documents are all made by one uniform process, as in the case of printing,
lithography or photography, each is primary evidence of the contents of the rest; but where they are all copies
of a common original they are not primary evidence of the contents of the original. Illustration A person is
shown to have been in possession of a number of placards, all printed at one time from one original. Any one
of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the
contents of the original.
Explanation 3.—Notwithstanding Explanation 2, if a copy of a document in the form of an electronic record is
shown to reflect that document accurately, then the copy is primary evidence.
Illustrations
a) An electronic record, which has been manifestly or consistently acted on, relied upon, or used as the informa-
tion recorded or stored on the computer system (the document), is primary evidence of that document.
b) If the electronic record has not been manifestly or consistently acted on, relied upon, or used as a record of
the information in the document, the electronic record may be a copy of the document and treated as secondary
evidence of that document.

Secondary evidence 65.

Secondary evidence means and includes —
a) certified copies given under the provisions hereinafter contained;
b) except for copies referred to in Explanation 3 to section 64, copies made from the original by electronic,
electrochemical, chemical, magnetic, mechanical, optical, telematic or other technical processes, which in themselves ensure the accuracy of the copy, and copies compared with such copies;
c) copies made from or compared with the original;
d) counterparts of documents as against the parties who did not execute them;
e) oral accounts of the contents of a document given by some person who has himself seen it.
Illustrations
a) A photograph of an original is secondary evidence of its contents, though the 2 have not been compared, if it
is proved that the thing photographed was the original.
b) A copy compared with a copy of a letter made by a copying machine is secondary evidence of the contents of
the letter if it is shown that the copy made by the copying machine was made from the original.
c) [Deleted by Act 4 of 2012 w.e.f. 01/08/2012]
d) A copy transcribed from a copy but afterwards compared with the original is secondary evidence, but the
copy not so compared is not secondary evidence of the original, although the copy from which it was tran-
scribed was compared with the original.
e) Neither an oral account of a copy compared with the original nor an oral account of a photograph or ma-
nachine-copy of the original is secondary evidence of the original.

**Proof of documents by primary evidence 66.**

Documents must be proved by primary evidence except in the cases mentioned in section 67. Cases in which secondary evidence relating to documents may be given 67.—

1) Secondary evidence may be given of the existence, condition or contents of a document admissible in evi-
dence in the following cases:
   a) when the original is shown or appears to be in the possession or power of —
      i) the person against whom the document is sought to be proved;
      ii) any person out of reach of or not subject to the process of the court; or
      iii) any person legally bound to produce it, and when, after the notice mentioned in section 68, such person does not produce it;
   b) when the existence, condition or contents of the original have been proved to be admitted in writing by the
      person against whom it is proved or by his representative in interest;
   c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot for
      any other reason not arising from his own default or neglect produce it in reasonable time;
   d) when the original is of such a nature as not to be easily movable;
   e) when the original is a public document within the meaning of section 76;
   f) when the original is a document of which a certified copy is permitted by this Act or by any other law in force
      for the time being in Singapore to be given in evidence;
   g) when the originals consist of numerous accounts or other documents which cannot conveniently be exam-
      ined in court, and the fact to be proved is the general result of the whole collection.

2) In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible. (3) In case (b),
   the written admission is admissible.

4) In case (e) or (f), a certified copy of the document but no other kind of secondary evidence is admissible.

5) In case (g), evidence may be given as to the general result of the documents by any person who has examined
   them and who is skilled in the examination of such documents.

**Proof of documents in certain cases 67A.**

Where in any proceedings a statement in a document is admissible in evidence by virtue of section 32(1), it may
be proved by the production of that document or (whether or not that document is still in existence) by the
production of a copy of that document, or of the material part of it, authenticated in a manner approved by the
court.

**Rules as to notice to produce 68.**

(1) Secondary evidence of the contents of the documents referred to in section 67(1)(a) shall not be given unless
the party proposing to give such secondary evidence has previously given to the party in whose possession or
power the document is, or to his solicitor, such notice to produce it as is prescribed by law; and if no notice is
prescribed by law, then such notice as the court considers reasonable under the circumstances of the case.

2) The notice mentioned in subsection (1) shall not be required in order to render secondary evidence admis-
sible in any of the following cases or in any other case in which the court thinks fit to dispense with it:
   a) when the document to be proved is itself a notice;
   b) when from the nature of the case the adverse party must know that he will be required to produce it;
   c) when it appears or is proved that the adverse party has obtained possession of the original by fraud or force;
   d) when the adverse party or his agent has the original in court;
   e) when the adverse party or his agent has admitted the loss of the document;
   f) when the person in possession of the document is out of reach of or not subject to the process of the court.
Manner of giving voluminous or complex evidence 68A

(1) Evidence may be given in the form of charts, summaries or other explanatory material, in electronic or other medium, if it appears to the court that —
   a) the materials would be likely to aid the court’s comprehension of other evidence which is relevant and admissible according to the provisions of this Act or any other written law; and (b) the evidence that is to be given by any party is so voluminous or complex that the court considers it convenient to assess the evidence by reference to such materials.

2) Any fact or opinion asserted in any material referred to in subsection (1) shall be proved by relevant and admissible evidence, and if such fact or opinion is one that is admissible only on the proof of some other fact or opinion, such last-mentioned fact or opinion must be proved before evidence is given of the fact or opinion first mentioned, unless the party undertakes to give proof of such fact or opinion and the court is satisfied with such undertaking. [8/96]

3) In any proceedings where any material referred to in subsection (1) is adduced in evidence, the court may —
   a) direct the party to provide such material in electronic or other medium;
   b) require the provision of such material or copy thereof, including the identity and address of the person who prepared the material, to the other parties; and
   c) specify a period within which such material or copy thereof must be provided to all parties to the proceedings.

Proof of signature and handwriting of person alleged to have signed or written document produced 69.

(1) If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person’s handwriting must be proved to be in his handwriting

2) This section shall not apply to any electronic record or electronic signature to which the Electronic Transactions Act 1998 applies

Proof of execution of document required by law to be attested 70.

If a document is required by law to be attested, it shall not be used as evidence until one attesting witness at least has been called for the purpose of proving its execution, if there is an attesting witness alive and subject to the process of the court and capable of giving evidence.

Proof where no attesting witness found 71.

If no such attesting witness can be found, or if the document purports to have been executed in the United Kingdom of Great Britain and Northern Ireland, it must be proved that the attestation of one attesting witness at least is in his handwriting, and that the signature of the person executing the document is in the handwriting of that person.

Admission of execution by party to attested document 72.

The admission of a party to an attested document of its execution by himself shall be sufficient proof of its execution as against him, though it is a document required by law to be attested. Proof when attesting witness denies the execution 73. If the attesting witness denies or does not recollect the execution of the document, its execution may be proved by other evidence.
Proof of document not required by law to be attested 74.

An attested document not required by law to be attested may be proved as if it was unattested.

Comparison of signature, writing or seal with others admitted or proved 75.

(1) In order to ascertain whether a signature, writing or seal is that of the person by whom it purports to have been written or made, any signature, writing or seal, admitted or proved to the satisfaction of the court to have been written or made by that person, may be compared by a witness or by the court with the one which is to be proved, although that signature, writing or seal has not been produced or proved for any other purpose.

2) The court may direct any person present in court to write any words or figures for the purpose of enabling the court to compare the words or figures so written with any words or figures alleged to have been written by such person.

3) This section shall apply also, with any necessary modifications, to finger impressions.

Presumptions as to documents

Presumption as to genuineness of certified copies 81.

(1) The court shall presume to be genuine every document purporting to be a certificate, certified copy or other document which is by law declared to be admissible as evidence of any particular fact, and which purports to be duly certified by any public officer in Singapore or any officer in Malaysia who is duly authorised thereto, if such document is substantially in the form and purports to be executed in the manner directed by law in that behalf.

(2) The court shall also presume that any officer by whom any such document purports to be signed or certified held, when he signed it, the official character which he claims in such document.

Presumption as to documents produced as record of evidence 82.

Whenever any document is produced before any court purporting to be a record or memorandum of the evidence or of any part of the evidence given by a witness in a judicial proceeding or before any officer authorised by law to take such evidence, or to be a statement or confession by any prisoner or accused person, taken in accordance with law and purporting to be signed by any Judge or Magistrate or by any such authorised officer, the court shall presume — (a) that the document is genuine; (b) that any statements as to the circumstances under which it was taken, purporting to be made by the person signing it, are true; and (c) that such evidence, statement or confession was duly taken.

Presumption as to certified copies of foreign judicial records 88.

The court may presume that any document purporting to be a certified copy of any judicial record of any country not forming part of the Commonwealth is genuine and accurate if the document purports to be certified in any manner which is certified by any representative of the President or of Her Britannic Majesty in or for such country to be the manner commonly in use in that country for the certification of copies of judicial records.

Presumption as to telegraphic messages 90.

The court may presume that a message forwarded from a telegraph office to the person to whom such message purports to be addressed corresponds with a message delivered for transmission at the office from which
the message purports to be sent; but the court shall not make any presumption as to the person by whom such message was delivered for transmission.
Admission defined.

17. (1) An admission is a statement, oral or documentary, which suggests any inference as to any fact in issue or relevant fact, and which is made by any of the persons and under the circumstances herein-after mentioned.

Confession defined.

(2) A confession is an admission made at any time by a person accused of an offence stating or suggesting the inference that he committed that offence.

Admissions not conclusive proof but may estop.

31. Admissions are not conclusive proof of the matters admitted, but they may operate as stop sunder the provisions hereinafter contained.

Admissions of execution by party to a tested document.

70. The admission of a party to an attested document of its execution by himself shall be sufficient proof of its execution as against him, though it be a document required by law to be attested.

Presumptions as to documents

Presumption as to genuineness of certified copies

79. (1) The court shall presume every document purporting to be a certificate, certified copy, or other document, which is by law declared to be admissible as evidence of any particular fact, and which purports to be duly certified by any officer in Sri Lanka, to be genuine: Provided that such document is substantially in the form and purports to be executed in the manner directed by law in that behalf. (2) The court shall also presume that any officer, by whom any such document purports to be signed or certified, held, when he signed it, the official character which he claims in such paper.

Presumption as production of record of evidence

80. Whenever any document is produced before any court purporting to be a record or memorandum of the evidence or any part of the evidence given by a witness in a judicial proceeding or before any officer authorized by law to take such evidence, or to be a statement or confession by any prisoner or accused person taken in accordance with law and purporting to be signed by any Judge or Magistrate or by any such officer as aforesaid,
the court shall presume—
i) that the document is genuine;
ii) that any statements, as to the circumstances under which it was taken, purporting to be made by the persons
signing it, are true; and
iii) that such evidence, statement, or confession was duly taken.

**MUTUAL ASSISTANCE IN CRIMINAL MATTERS ACT,**
**NO. 25 OF 2002**

**Object of the Act**

111. The object of this Act is to facilitate the provision and obtaining, by Sri Lanka of assistance in criminal matters, including —
a) the location and identification of witnesses or suspects;
b) the service of documents;
c) the examination of witnesses;
d) the obtaining of evidence, documents or other articles;
e) the execution of requests for search and seizure;
f) the effecting of a temporary transfer of a person in custody to appear as a witness; (g) the facilitation of the
personal appearance of witnesses;
g) the provision of documents and other records
h) the location, of the proceeds of any criminal activity;
i) the enforcement of orders for the payment of fines or for the forfeiture of freezing of property.

**PART IV - ASSISTANCE IN RELATION TO TAKING OF EVIDENCE AND PRODUCTION OF DOCUMENTS OR OTHER ARTICLES**

10. (1) Where the appropriate authority of a specified country makes a request to the Central Authority that —
a) evidence be taken in Sri Lanka; or
b) documents or other articles in Sri Lanka be produced, for the purposes of a proceeding in relation to a criminal matter in the specified country, the Central Authority may in his discretion refer such request to a Magistrate, authorized by a general or special order made by the President of the Court of Appeal to take such evidence or to receive such documents or articles, and shall, upon receipt of such evidence, documents or articles from such Magistrate, transmit the same to the appropriate authority of the specified country.
2) Every request made under subsection (1) by the appropriate authority of a specified country shall, so far as circumstances of the case permit, specify—
a) the names and addresses or the official designations of the witnesses to be examined; (b) the questions to be put to the witnesses or the subject matter about which they are to be examined;
b) whether it is desired that the witnesses be examined orally or in writing;
c) any provision of the law of the specified country as to privileges or exemptions from giving evidence which appear relevant to the request ; and
d) any special requirements of the law of the specified country as to the manner of taking evidence relevant to its admissibility in that country;
e) whether it is desired that the original of a document be produced or whether a certified copy of the document would be sufficient.
3) Where the taking of evidence or the production of documents or other articles under subsection (1) has been authorized—
a) the Magistrate specified in the authorization may take the evidence on oath of each witness appearing before such Magistrate to give evidence in relation to such matter, and such Magistrate shall— (i) cause the evidence to be taken in writing and certify that the evidence was taken by such Magistrate; and (ii) cause the evidence so certified to be sent to the Central Authority;
b) a Magistrate may, require the production before him, of the documents or other articles and, where the documents or other articles are so produced, the Magistrate shall send the documents, or where it is impracticable to send such documents to the Central Authority or where the request relates only to copies of such documents, copies of such documents certified to be true copies by the Magistrate, or the other articles, as the case may be,
to the Central Authority.
4) The evidence of any witness may be taken in the presence or absence of the person to whom the proceeding in the specified country relates or his legal representative, if any.
5) The Magistrate conducting a proceeding under subsection (3) shall permit—
   a) the person to whom the proceeding in the specified country relates;
   b) the appropriate authority of the specified country, to have legal representation at the proceeding before the Magistrate.
6) The certificate of the Magistrate under subsection (3) shall state whether legal representation was permitted at the proceedings conducted under that subsection and whether any of the following persons were present at the time the evidence was taken or the documents or other articles were produced:—
   a) the person to whom the proceeding in the specified country relates or his legal representative, if any;
   b) any other person giving evidence or producing documents or other articles or his legal representative, if any.
7) The provisions of the Code of Criminal Procedure Act, No. 15 of 1979 relating to the compelling of attendance of witnesses and the production of documents by witnesses shall apply in relation to a Magistrate's Court which is authorized to take such evidence. (8) The Central Authority shall cause the certificate of the Magistrate sent to him under subsection (3) to be transmitted to the appropriate authority of the specified country.
9) A person who is required to give evidence, or produce documents or other articles, for the purposes of a proceeding in relation to a criminal matter in a specified country shall not be compelled to answer a question, or produce a document or article, that the person is not compelled to answer or produce, as the case may be, in such proceeding in the specified country.
10) A duly authenticated foreign law immunity certificate shall be admissible in proceedings under this section as prima facie evidence of the matters stated in such certificate but shall not, without the consent of the appropriate authority, be used for any purpose other than for the purposes of the Criminal matter specified in the request.

1. (1) The Central Authority may, at the request of a court exercising criminal jurisdiction in Sri Lanka, request the appropriate authority of a specified country to arrange for—
   a) evidence to be taken in the specified country ; or
   b) documents or other articles to be produced in the specified country, for the purposes of a proceeding in relation to a criminal matter in that court.
2) Where the Central Authority receives, from the appropriate authority in a specified country, in response to a request made by him under subsection (1)—
   a) any evidence taken in such specified country;
   b) any document or other article produced in such specified country, such evidence, document or article shall be admissible in any proceeding to which such request relates but shall not, without the consent of such appropriate authority, be used for the purpose other than for the purposes of the criminal matter specified in such request.

MUTUAL LEGAL ASSISTANCE IN CRIMINAL MATTERS
(AMENDMENT ACT), NO. 24 OF 2018

Replacement of section 3 of the principal enactment.

3. Section 3 of the principal enactment is hereby repealed and the following section substituted therefor:—
   “Object of the Act.

3. (1) The object of this Act is to facilitate the provision and obtaining by Sri Lanka of assistance in criminal and related matters, including: (a) the locations and identification of witnesses or suspects; (b) the service of documents; (c) the examination and interviewing of witnesses or suspected persons; (d) the provision and obtaining of evidence, documents, other articles or information; (e) the execution of requests for search and seizure; (f) the effecting of temporary transfer of a person in custody to appear as a witness; (g) the facilitation of the personal appearance of witnesses; (h) the criminal infringement of intellectual property including copyright infringement; (i) the information relating to the location of a computer system or any other property connected with any criminal activity; (j) the enforcement of any orders for the payment of fines; (k) the forfeiture or freezing of property pursuant to the relevant laws on such matters; (l) the tracing of crimes committed via internet, information communications technology, cloud computing,
blockchain technology and other computer networks including the trading in of any digital currencies; (m) the bribery of any foreign public official or official of a public international organization and their respective proxies and beneficiaries; (n) the expedited preservation of stored computer data and expedited disclosure of preserved traffic data and data retention; (o) the location of proceeds of a criminal activity; (p) the use of documentary evidence obtained in a specified country through specific authorization to be made admissible in a judicial proceeding; and (q) the admissibility and applicability of evidence led from a specified country through video conferencing technology. (2) Nothing in this Act shall preclude the granting or obtaining of any other form or nature of assistance for investigation in connection with judicial proceedings, connected with criminal matters to or from a specified country or specified organization. Such assistance may include controlled operations, joint investigations, the use of other special investigative techniques including the use of diverse search engines and the transfer of criminal proceedings to another court.

5A. Prompt response to requests.

(1) The Central Authority, on receiving a request may as soon as possible either approve, approve partially, approve subject to such conditions as may be necessary, postpone or refuse such request.
2) Upon receipt of a request the Central Authority shall promptly– (a) direct a competent authority to process the information in respect of the request; (b) inform the appropriate authority of a specified country or specified organization– (i) of the outcome of the execution of the request, with reasons; (ii) of any reasons that render impossible the execution of the request or are likely to delay it significantly.

5B. Transmission of information spontaneously in exigent situations.

(1) The Central Authority may direct a competent authority to spontaneously transmit information requested relating to a criminal matter to an appropriate authority of a specified country or specified organization in exigent situations, on the assurance of reciprocity and on such conditions as may be necessary for the purposes of confidentiality. (2) For the purpose of this section an “exigent situation” shall be determined by the Central Authority, having considered the gravity of the offence or the insidious nature of the criminal matter, setting out reasons in writing.

6A. “Confidentiality.

(1) Every officer referred to under section 4 shall consider all matters strictly confidential. (2) Unless otherwise authorized by law, a person who, because of his official capacity or office, and being aware of the confidential nature of the request, has knowledge of— (a) the contents of such request made under this Act; (b) the fact that such request has been, or is about to be made; or (c) the fact that such request has been granted or refused, shall not disclose such content or facts except to the extent that the disclosure is necessary to execute the foreign request.
3) In order to comply with a request, if confidentiality cannot be upheld as specified in subsection (2), the Central Authority shall be promptly informed and the Central Authority shall in turn inform the appropriate authority of a specified country or specified organization, which shall then determine whether the request should nevertheless be executed. (4) Any person who fails to comply with this section, commits an offence and shall be liable on conviction by the High Court of the Province to a fine exceeding one hundred thousand rupees taking into consideration the nature and gravity of the non-compliance. Provided, however, such fine shall not exceed a sum of five million rupees in any given case. (5) For the purposes of this Act, a request for information relating to a criminal matter may be granted after ensuring the authenticity of the requesting person.

10. Amendment of section 10 of the principal enactment.

Section 10 of the principal enactment is hereby amended in subsection (1) thereof by the repeal of all the words from “for the purpose of proceeding” to the end of that paragraph and the substitution therefor of the following:— “for the purposes of a proceeding in relation to a criminal matter in the specified country or specified organization, the Central Authority shall promptly refer such request to a competent authority or as required,
to the Chief Magistrate of the Colombo Magistrate’s Court to take such evidence or to receive such documents or articles, and shall, upon receipt of such evidence, documents or articles from such Magistrate or competent authority, as the case may be, transmit the same to the appropriate authority of the specified country or specified organization.”.

11. Section 11 of the principal enactment is hereby repealed and the following section substituted therefor:–

(1) The Central Authority may, on the request of a court or a competent authority, request the appropriate authority of a specified country or specified organization to arrange for– (a) evidence including computer evidence to be taken; (b) investigative material to be produced; (c) bank statement to be produced; or (d) any other documents or other articles to be produced, for the purposes of investigating a criminal matter and a proceeding of a criminal matter. (2) Where the Central Authority receives from the appropriate authority of a specified country or specified organization,– (a) any evidence taken, and where such evidence is in relation to computer evidence, being certified as a true copy by any judicial authority or the appropriate authority, such evidence; (b) investigative material, bank statement produced, any other document or other article produced in such specified country or specified organization, duly authenticated under section 21, shall be admissible in any proceeding to which such request relates. (3) Any information received under this section shall not be used for any purpose other than the criminal matter specified in such request, without the written consent of such appropriate authority.”

PART VIIA
EXPEDITED PRESERVATION OF STORED DATA IN RELATION TO COMPUTER CRIMES

20A. Relevant Secretary to a Ministry to make order to preserve data.

Where the Central Authority is of the opinion that expedited preservation is required of stored computer data or traffic data, the Central Authority shall inform the Secretary to the Ministry of the Minister assigned the relevant subject to make an order for the expedited preservation of stored computer data or traffic data, as the case may be, or to both such data, for the period specified under section 20B.

20B. Period of preservation of data

All data for which an order is made under section 20A shall be preserved for a minimum period of six years.

20C. Mode of preservation.

(1) Records of data preserved under this Part shall be maintained in a manner and form that will enable an institution to immediately comply with the request for information in the form in which it is requested. (2) A copy of the record may– (a) be kept in a machine readable form to conveniently obtain a print thereof; (b) be kept in an electronic form, to enable a readable copy to be readily obtained and an electronic signature of the person who keeps the records is inserted for purposes of verification; (c) where necessary, entail freezing of the stored computer data; or (d) be updated, if necessary.

20D. Release of preserved data.

(1) Preserved data shall be released for the purpose of criminal investigation or judicial proceedings on a request duly made by the appropriate authority for such period as specified in the request.
2) Every order made under section 20A shall lapse on the expiry of the time period specified under section 20B or on the expiry of the period specified in the request. (3) Where in the course of granting a request to preserve traffic data concerning a specific communication, the Central Authority is informed that a service provider in another country was involved in the transmission of the communication, the Central Authority shall instruct the relevant competent authority to disclose, such amount of traffic data as is sufficient to identify that service provider and the path through which the communication was transmitted, prior to receipt of the request for production.

### 20E. Production of stored computer data

Subject to any written law on admissibility of computer data and notwithstanding the provisions of Part VI of this Act, upon the request of an appropriate authority of a specified country or specified organization, for computer data or information to investigate the criminal matter, the Magistrate may issue an order to enable the production of—

(a) specified computer data in the possession or control of a person stored in a computer system or a computer data storage medium; and

(b) the necessary subscriber information in the possession or control of a service provider.

### 20F. Search and seizure of computer data.

(1) Upon the request by an appropriate authority of a specified country or specified organization, a warrant may be issued under section 15, mutatis mutandis, to search or otherwise access any computer system or part thereof as well as any computer storage medium in which computer data may be stored. (2) The search warrant issued by the Magistrate within whose jurisdiction such computer or computer system is believed to be located, may authorize the police officer or any other designated person, where necessary, to—

(a) seize or otherwise secure a computer system or part thereof, or a computer data storage medium; (b) make and retain a copy of that computer data; (c) maintain the integrity of the relevant stored computer data; and (d) render inaccessible or remove that computer data in the accessed computer system.”.

### 20. Replacement of section 24 of the principal enactment.

Section 24 of the principal enactment is hereby repealed and the following section substituted therefor:-

4. In this Act, unless the context otherwise requires—“appropriate authority” in relation to—

(a) a specified country means the person, howsoever described, designated to receive and transmit requests for assistance in criminal matters, by or under any law of that country; 

(b) a specified organization means the person howsoever described, designated to receive and transmit requests for assistance in criminal matters; 

blockchain technology means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, with necessary permission or without permission, or driven by crypto economics or not. The data on the ledger shall be protected with cryptography, be immutable and auditable and shall provide true information; 

competent authority means a law enforcement authority or any other authority established by law; “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function; 

computer system shall have the same meaning as in the Computer Crime Act, No. 24 of 2007; “controlled operation” includes an operation that—

(a) involves the participation of law enforcement officers; 

(b) is conducted for the purpose of—(i) obtaining evidence that may lead to the prosecution of a person for a serious offence; (ii) arresting any person involved in criminal activity or corrupt conduct; (iii) frustrating criminal activity or corrupt conduct; (iv) carrying out an activity that is reasonably necessary to facilitate the achievement of any purpose referred to in sub-paragraph (i), (ii) or (iii); 

(c) may involve the supervision of a law enforcement officer or any other authorized person, where such conduct constitutes an offence in Sri Lanka; 

country or “foreign State” includes a colony, territory, protectorate or other dependency of such country or foreign State, or a ship or an aircraft registered in such country or foreign State, and shall be deemed to include the Hong Kong Special Administration Region of the Peoples Republic of China; “criminal matter” means—
a) violation of any law relating to a criminal offence; and
b) an investigation, prosecution or judicial proceedings related to a criminal offence and includes- (i) the forfeiture or confiscation of any property or proceeds of crime upon conviction or non conviction basis; (ii) the imposition or recovery of a pecuniary penalty; (iii) the tracing, freezing and restraint of property that may be forfeited or confiscated;
digital currency— (a) includes a digital representation of value that— (i) is used as a medium of exchange, unit of account or store of value; and (ii) may not be denominated in legal tender; and (b) does not include— (i) a transaction in which a merchant grants, as part of an affinity or rewards program, value that cannot be taken from or exchanged with the merchant for legal tender, bank credit or digital currency; or (ii) a digital representation of value issued by or on behalf of a publisher and used solely within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform;
document includes—
a) any of, or any part of any of, the following things:— (i) any paper or other material on which there is writing; (ii) a map, plan, drawing, photograph or similar thing; (iii) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; (iv) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device; (v) any article on which information has been stored or recorded, either mechanically or electronically; (vi) any other record of information; or
b) any copy, reproduction or duplicate of such a thing; or
c) any part of such a copy, reproduction or duplicate;
duly authenticated" in relation to a document, means a document authenticated as provided for in section 21;
“foreign law immunity certificate” means a certificate given or declaration made, by the appropriate authority of a specified country or under the law of a specified country, certifying or declaring that under the law of that specified country, persons referred to generally or specifically, could or could not, either generally or in specified proceedings or either generally or under specified circumstances, be required to answer a specified question, or to produce a specified document; “foreign public official” means— (a) an employee or official of a foreign government body; or (b) an individual who performs work for a foreign government body under a contract; or (c) an individual who holds or performs the duties of an appointment, office or a position under a law of a foreign State or of a part of a foreign State; or
d) an individual who holds or performs the duties of his appointment, office or position created by custom or convention of a foreign State or of a part of a foreign State; or
e) an individual who is otherwise in the service of a foreign government body including service as a member of a military force or police force; or (f) a member of the executive, judiciary or magistracy of a foreign State or of part of a foreign State; or (g) a member or officer of the legislature of a foreign State or of a part of a foreign State; or (h) an individual who— (i) is an authorized intermediary of a foreign public official covered by any of the above paragraphs; or (ii) holds himself or herself out to be the authorized intermediary of a foreign public official covered by any of the above paragraphs;
freezing" means to prohibit the transfer, conversion, disposition or movement of property, any assets or computer data on the basis of, and for the duration of the action initiated by the appropriate authority or a court;
Minister” means the Minister appointed under Article 43 or Article 44 of the Constitution, to whom the subject of Justice is assigned;
official of a public international organization" means— (a) an employee of a public international organization; or (b) an individual who performs work for a public international organization under a contract; or (c) an individual who holds or performs the duties of an office or position in a public international organization; or (d) an individual who is otherwise in the service of a public international organization; or (e) an individual who— (i) is an authorized intermediary of an official of a public international organization covered by any of the above paragraphs; or
ii) holds himself or herself out to be the authorized intermediary of an official of a public international organization covered by any of the above paragraphs;
proceeds of crime" includes any property, benefit or advantage that is wholly or partly obtained, derived or realized directly or indirectly as a result of the commission of a criminal act or omission; “property” means any currency, and includes any asset of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible whether situated in Sri Lanka or elsewhere, and legal documents or instruments in any form whatsoever including electronic or digital form, evidencing title to, or interest in, such assets, including but not limited to bank credits, travelers’ cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit and includes any legal or equitable interest in any such property;
public international organization” means—
a) an organization— (i) of which two or more countries, or the governments of two or more countries, are members; or (ii) that is constituted by persons representing two or more countries, or representing the governments of two or more countries; or (b) an organization established by, or a group of organizations constituted by— (i) organizations of which two or more countries, or the governments of two or more countries, are members; or (ii) organizations that are constituted by the representatives of two or more countries, or the governments of two or more countries; or (c) an organization that is— (i) an organ of, or office within, an organization described in paragraph (a) or (b); or
ii) a commission, council or other body established by an organization so described or such an organ; or (iii) a 
committee, or subcommittee of a committee, of an organization described in paragraph (a) or (b), or of such an 
organ, council or body;

serious offence” means an offence punishable with death or with imprisonment for a term not less than one 
year; and

traffic data” shall have the same meaning as in the Computer Crime Act, No.24 of 2007.”

2007 COMPUTER CRIME ACT

PART I COMPUTER CRIME

Securing unauthorised access to a computer an offence.

3. Any person who intentionally does any act, in order to secure for himself or for any other person, access to—
(a) any computer ; or (b) any information held in any computer, knowing or having reason to believe that he has 
no lawful authority to secure such access, shall be guilty of an offence and shall on conviction be liable to a fine 
not exceeding one hundred thousand rupees, or to imprisonment of either description for a term which may 
extend to five years, or both such fine and imprisonment.

Doing any act to secure unauthorised access in order to commit an offence

4. Any person who intentionally does any act, in order to secure for himself or for any other person, access to—
(a) any computer ; or (b) any information held in any computer, knowing or having reason to believe that he has 
no lawful authority to secure such access and with the intention of committing an offence under this Act or any 
other law for the time being in force, shall be guilty of an offence and shall on conviction be liable to a fine not 
exceeding two hundred thousand rupees or to imprisonment of either description for a term which may extend 
to five years or to both such fine and imprisonment. Explanation 1— for the purposes of paragraph (a) the mere 
turning on of a computer is sufficient. Explanation 2— for the purposes of paragraph (b)- (a) there should be an 
intention to secure any programme or data held in any computer ;
b) the access intended to be secured, should be unauthorised; (c) it is not necessary to have access directed at 
any particular programme, data or computer.

Causing a computer to perform a function without lawful authority an offence.

5. Any person who, intentionally and without lawful authority causes a computer to perform any function 
knowing or having reason to believe that such function will result in unauthorised modification or damage or 
potential damage to any computer or computer system or computer programme shall be guilty of an offence 
and shall on conviction be liable to a fine not exceeding three hundred thousand rupees or to imprisonment of 
either description for as term which may extend to five years or to both such fine and imprisonment. Illustra-
tions For any unauthorised modification or damage or potential damage to any computer or computer system 
or computer programme to take place, any one of the following may occur:— (a) impairing the operation of any 
computer, computer system or the reliability of any data or information held in any computer; or (b) destroying, 
deleting or corrupting, or adding, moving or altering any information held in any computer; (c) makes use of a 
computer service involving computer time and data processing for the storage or retrieval of data; (d) introduc-
es a computer program which will have the effect of malfunctioning of a computer or falsifies the data or any 
information held in any computer or computer system.

explanation- for the purposes of paragraphs (a) to (d) above, it is immaterial whether the consequences referred 
to therein were of a temporary or permanent nature.
Offences committed against national security &c.

6. (1) Any person who intentionally causes a computer to perform any function, knowing or having reason to believe that such function will result in danger or imminent danger to—
   a) national security;
   b) the national economy; or
   public order, shall be guilty of an offence and shall on conviction be punishable with imprisonment of either description for a term not exceeding five years.
   2) In a prosecution for an offence under paragraphs (a) or (c) of subsection (1), a Certificate under the hand of the Secretary to the Ministry of the Minister in charge of the subject of Defence or, in a prosecution for an offence under paragraph (b) of subsection (1), a Certificate under the hand of the Secretary to the Ministry of the Minister in charge of the subject of Finance, stating respectively, that the situation envisaged in subsection (1) did in fact exist in relation to national security or public order, or the national economy, as the case may be, shall be admissible in evidence and shall be prima facie evidence of the facts stated therein.

Dealing with data &c., unlawfully obtained an offence.

7. Any person who, knowing or having reason to believe that any other person has without lawful authority obtained information from a computer or a storage medium of a computer,— (a) buys, receives, retains, sells, or in any manner deals with ; or
   b) offers to buy or sell, or in any manner deals with ; or (c) downloads, uploads, copies or acquires the substance or meaning of, any such information shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years, or to both such fine and imprisonment. Explanation.—For the purposes of sections 9 and 10— (a) It is immaterial that the offender had authority to access the computer or had authority to perform the function ; (b) The offender need not have intended to cause or have had the knowledge that he is likely to cause, loss or damage to any particular person or institution.

Illegal interception of data an offence.

8. Any person, who, knowingly or without lawful authority intercepts— (a) any subscriber information or traffic data or any communication, to, from or within a computer ; or (b) any electromagnetic emissions from a computer that carries any information, shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years, or to both such fine and imprisonment.

Using of illegal devices an offence.

9. Any person who, without lawful authority produces, sells, procure for use, imports, exports, distributes or otherwise makes available— (a) any device, including a computer or computer program ; (b) a computer password, access code or similar information by which the whole or any part of a computer is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence under this Act shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years, or to both such fine and imprisonment.
Unauthorised disclosure of information enabling access to a service, an offence.

10. Any person who, being entrusted with information which enables him to access any service provided by means of a computer, discloses such information without any express authority to do so or in breach of any contract expressed or implied, shall be guilty of an offence and shall on conviction be liable to a fine not less than one hundred thousand rupees and not exceeding three hundred thousand rupees or to imprisonment of either description for a term not less than six months and not exceeding three years or to both such fine and imprisonment.

Attempts to commit offence.

11. Any person who attempts to commit an offence under sections 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 of this Act or to cause such an offence to be committed, shall be guilty of an offence and shall on conviction be liable to a fine not exceeding one half of the maximum fine provided for each of such offences, or to imprisonment of either description for a term not exceeding one half of the maximum term provided for each of such offences, or to both such fine and imprisonment.

Abetment of an offence.

12. (1) Any person who abets the commission of an offence under this Act shall be guilty of the offence of abetment and shall on conviction— (a) if the offence abetted is committed in consequence of the abetment, be liable to the same punishment as is provided for the offence; and (b) if the offence is not committed in consequence of the abetment, be liable — (i) where the maximum fine or term of imprisonment is provided for, to a fine not exceeding one fourth of the maximum fine provided for the offence or to imprisonment of either description for a term not exceeding one fourth of the maximum term provided for the offence, or to both such fine and imprisonment; and (ii) where the maximum fine or imprisonment is not provided for or the maximum term of imprisonment is life, to a fine not exceeding two hundred and fifty thousand rupees or to imprisonment of either description for a term not exceeding five years, or to both such fine and imprisonment. (2) The term ‘abet’ shall have the same meaning as in sections 100 and 101 of the Penal Code (Chapter 19) and the provisions of sections 101A, 103, 104, 105, 106 and 107 of the Penal Code (Chapter 19) shall mutatis mutandis apply in relation to the abetment of any offence under this Act.

Conspiring to commit an offence.

13. (1) Any person who conspires to commit an offence under this Act shall be guilty of an offence and shall, on conviction be punished with the punishment prescribed for abetting the commission of that offence. 2) The term “conspire” shall have the same meaning as in subsection (2) of section 113A of the Penal Code (Chapter 19) and the provisions of that section shall mutatis mutandis apply in relation to conspiracy to commit any offence under this Act.

PART II INVESTIGATIONS

Powers of search and seizure with warrant.

18. (1) An expert or a police officer may, for the purposes of an investigation under this Act under the authority of a warrant issued in that behalf by a Magistrate on application made for such purpose,— (i) obtain any information including subscriber information and traffic data in the possession of any service provider; (ii) intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication. (2) Notwithstanding the provisions of subsection (1), an expert or a police officer may without a warrant exercise all or any of the powers referred to in that subsection, if— (a) the investigation needs to be
conducted urgently; and (b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible; and (c) there is a need to maintain confidentiality regarding the investigation.

3) The provisions of sections 36, 37 and 38 of the Code of Criminal Procedure Act, No. 15 of 1979 shall not apply in relation to the arrest of a person for an offence under this Act. (4) The Minister may by regulation prescribe the manner in which and the procedures required to be followed in respect of, the retention and interception of data and information including traffic data, for the purposes of any investigation under this Act.

**Preservation of information.**

19. (1) Where an expert or a police officer is satisfied that any information stored in a computer is reasonably required for the purposes of an investigation under this Act and that there is a risk that such information may be lost, destroyed, modified or rendered inaccessible, he may by written notice require the person in control of such computer or computer system to ensure that the information be preserved for such period not exceeding seven (07) days as may be specified in such notice. (2) On an application made to a Magistrate having jurisdiction, the period for which the information is to be preserved may be extended for such further period, which in the aggregate shall not exceed up to ninety days.

**Normal use of computer not to be hampered.**

20. Every police officer and every expert who conducts any search, inspection or does any other thing in the course of an investigation, shall make every endeavour to ensure that the ordinary course of legitimate business for which any computer may be used is not hampered by such search, inspection or investigation and shall not seize any computer, computer system or part thereof, if such seizure will prejudice the conduct of the ordinary course of business for which the computer is used, unless— (a) it is not possible to conduct the inspection on the premises where such computer, computer system or part thereof is located; or (b) seizure of such computer, computer system or part thereof is essential to prevent the commission of the offence or the continuance of the offence or to obtain custody of any information which would otherwise be lost, destroyed, modified or rendered inaccessible.

**Power of police officer to arrest, search and seize.**

21. (1) Any police officer may, in the course of an investigation under this Act, exercise powers of arrest, search, or seizure of any information accessible within any premises, in the manner provided for by law: Provided that a police officer making an arrest without a warrant of person suspected of committing an offence under this Act, shall without unnecessary delay and within twentyfour hours of such arrest, exclusive of the time taken for the journey from the place of arrest to the presence of the Magistrate, produce such person before the Magistrate of the Court nearest to the place that the suspect is arrested. (2) No police officer shall access any computer for the purpose of an investigation under this Act unless the Inspector General of Police has certified in writing that such police officer possesses adequate knowledge and skill in the field of information communication technology and is thereby possessed of the required expertise to perform such a function.

**Police officer to record and afford access to seized data.**

22. (1) Where any item or data has been seized or rendered inaccessible in the course of an investigation, the police officer conducting the search shall issue a complete list of such items and data including the date and time of such seizure or of rendering it inaccessible to the owner or person in charge of the computer or computer system. (2) Subject to the provisions of subsection (3), a police officer may upon application made by the owner or person in control of the computer or computer system, permit a person nominated by such owner or person to issue such person a copy of such data. (3) A police officer shall not grant permission or give such copies under subsection (2) if it appears that such permission would be prejudicial to any criminal investigation or proceeding.
Confidentiality of information obtained in the course of an investigation.

24. (1) Every person engaged in an investigation under this Act shall maintain strict confidentiality with regard to all information as may come to his knowledge in the course of such investigations and he shall not disclose to any person or utilize for any purpose whatsoever any information so obtained other than in the discharge of his duties under this Act. (2) Every service provider from whom any information has been requested or obtained and any person to whom a written notice has been issued for the preservation of any information shall maintain strict confidentiality in relation to such information and the fact that such information has been requested, obtained or required to be preserved, and shall not make any disclosure in regard to such matters other than with lawful authority. (3) A service provider shall not be held liable under the civil or criminal law for the disclosure of any data or other information for the purposes of an investigation under this Act. (4) Any person who contravenes the provisions of subsections (1) and (2) shall commit an offence and shall on conviction be liable to a fine not exceeding three hundred thousand rupees or to imprisonment of either description for a term not exceeding two years or to both such fine and imprisonment.

PART III MISCELLANEOUS

Proof of document issued by an expert or a Police Officer.

26. (1) Every document duly signed and issued by an expert or a police officer, as the case may be, and duly authenticated by an expert in the prescribed manner, shall be admissible in evidence and shall be prima facie evidence of the facts stated therein. (2) for the purposes, of this section the expression “document” shall include a certificate, declaration, information, data, report or any other similar document.

Minister to notify requesting State, of measures taken against persons for whose extradition request is made

33. Where a request is made to the Government of Sri Lanka, by or on behalf of another Government for the extradition of any person accused or convicted of an offence under this Act, the Minister shall on behalf of the Government of Sri Lanka, forthwith notify the Government of the requesting State of the measures which the Government of Sri Lanka has taken, or proposes to take, for the prosecution or extradition of that person for that offence

Rights of certain persons arrested for offences under this Act.

34. Where a person who is not a citizen of Sri Lanka is arrested for an offence under this Act, such person shall be entitled— (a) to communicate without delay, with the nearest appropriate representative of the State of which he is a national or which is otherwise entitled to protect his rights or if he is a stateless person, with the nearest appropriate representative of the State in the territory of which he was habitually resident ; and b) to be visited by a representative of that State ; and (c) be informed of his rights under paragraphs (a) and (b).

Assistance to Convention States &c

35. (1) The provisions of the Mutual Assistance in Criminal Matters Act, No. 25 of 2002 shall, wherever it is necessary for the investigation and prosecution of an offence under this Act, be applicable in respect of the providing of assistance as between the Government of Sri Lanka and other States who are either Commonwealth countries specified by the Minister by Order under section 2 of the aforesaid Act or Non-Commonwealth countries with which the Government of Sri Lanka entered into an agreement in terms of the aforesaid Act. (2) In the case of a country which is neither a Commonwealth country specified by the Minister by Order under section 2 of the aforesaid Act nor a Non-Commonwealth country with which the Government of Sri Lanka entered into an agree-
ment in terms of the aforesaid Act, then it shall be the duty of the Government to afford all such assistance to, and may through the Minister request all such assistance from, a convention country, as may be necessary for the investigation and prosecution of an offence under this Act (including assistance relating to the taking of evidence and statements, the serving of process and the conduct of searches). (3) The grant of assistance in terms of this section may be made subject to such terms and conditions as the Minister thinks fit.

OFFENCES UNDER THIS ACT, NOT TO BE POLITICAL OFFENCES & C., FOR THE PURPOSES OF THE EXTRADITION LAW

36. Notwithstanding anything in the Extradition Law, No. 8 of 1977, an offence specified in the Schedule to that Law and in this Act, shall for the purposes of that law be deemed not to be an offence of a political character or an offence connected with a political offence or an offence inspired by political motives, for the purposes only of the extradition of any person accused or convicted of any such offence, as between the Government of Sri Lanka and any requesting State, or of affording assistance to a requesting State under section 35.

Interpretation.

38. In this Act, unless the context otherwise requires,—
computer” means an electronic or similar device having information processing capabilities;
storage medium” means any [electronic or similar device] from which information is capable of being reproduced, with or without the aid of any other article or device;
computer programme” means a set of instructions expressed in words, codes, schemes or any other form, which is capable when incorporated in a medium that the computer can read, of causing a computer to perform or achieve a particular task ;
computer system” means a computer or group of interconnected computers, including the internet;
document” includes an electronic record;
electronic record” means, information, record or data generated, stored, received or sent in an electronic form or microfilm, or by any other similar means;
function” in relation to a computer, includes logic, control or carrying out of an arithmetical process, deletion, storage and retrieval and communication to or within a computer;
information” includes data, text, images, sound, codes, computer programmes, databases or microfilm;
service provider” means—
a) a public or private entity which provides the ability for its customers to communicate by means of a computer system; and
b) any other entity that processes or stores computer data or information on behalf of that entity or its customers;
subscriber information” means any information, contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services;
traffic data” means data—
a) that relates to the attributes of a communication by means of a computer system;
b) data generated by a computer system that is part of a service provider; and
c) which shows communications origin, destination, route, time, data, size, duration or details of subscriber information.
CHAPTER I
GENERAL PROVISIONS

Objectives of the Act.

2. The objectives of the Act shall be— (a) to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty; (b) to encourage the use of reliable forms of electronic commerce; (c) to facilitate electronic filing of documents with Government and to promote efficient delivery of Government services by means of reliable forms of electronic communications; and (d) to promote public confidence in the authenticity, integrity and reliability of data messages, electronic documents, electronic records or other communications.

CHAPTER II
RECOGNITION DATA MESSAGES AND OTHER COMMUNICATIONS IN ELECTRONIC FORM

Legal recognition of electronic records.

3. No data message, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity or enforceability on the ground that it is in electronic form.

Requirement for writing.

4. Notwithstanding the fact that the provisions of written laws for the time being in force in Sri Lanka attach legal validity to certain instruments, only if such instruments have been reduced to writing, such requirement shall be deemed to be satisfied by a data message, electronic document, electronic record or other communication in electronic form if the information contained therein is accessible so as to be usable for subsequent reference.

Requirements for original form.

5. (1) Where the law requires information to be presented or retained in its original form, that requirement shall be deemed to be satisfied by a data message, electronic document, electronic record or other communication in electronic form if there exists a reliable assurance as to the integrity of the information from the time when it was made available in electronic form and the information contained in the data message, electronic document, electronic record or other communication is available and can be used for subsequent reference. (2) For the purposes of subsection (1)— (a) the criterion for assessing the integrity of information, is whether such information has remained complete and unaltered, apart from the addition of any endorsement or any change which arises in the normal course of communication, storage or display; and (b) the standard for reliability of the assurance shall be assessed having regard to the purpose for which the information was generated and all other relevant circumstances.
Requirements for retention

6. The requirement under any law that information be retained, shall be deemed to be satisfied by the retention in electronic form of information contained in a data message, electronic document, electronic record or other communication notwithstanding the fact that such information was not originally generated in electronic form, if— (a) the information in the data message, electronic document, electronic record or communication is accessible so as to be usable for subsequent reference; and (b) the data message, electronic document, electronic record or communication is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and (c) such information, enables the identification of the origin and destination of the data message, electronic document, electronic record or other communication and the date and time when such information was generated, sent or received, is retained: Provided that the provisions of this section shall not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

Legal recognition of electronic signatures

7. Where any Act or enactment provides that any information or communication shall be authenticated by affixing the signature, or that any document should be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to be satisfied, if such information or matter is authenticated by means of an electronic signature. Explanation.— for the purpose of this section, “sign” with its grammatical variations and cognate expressions, shall, with reference to a person mean, the affixing of his hand-written signature or any mark on any document and the expression, “signature” shall be construed accordingly.

Use of electronic records and electronic signatures in Government institutions and statutory bodies.

8. (1) Where any written law for the time being in force requires— (a) the filing of any form, application, or any other document with any Government department, office, body or agency owned or controlled by the Government or a statutory body in a particular manner; (b) the issue of grant of any license, permit or approval; or (c) the receipt of payment of money, procurement or other transaction to be effected in a particular manner, then, notwithstanding anything to the contrary contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, creation, retention, issue, grant, receipt, payment, procurement or transaction, as the case may be, is effected in the form of electronic records as may be specified by the relevant Ministry, Government department, Institution, statutory body or public corporation or other similar body. (2) The relevant authority requiring the use of electronic records specified in subsection (1), may recommend the making of regulations for the purpose of authorizing or facilitating the use of electronic communications or electronic records, to the Minister in charge of the subject, by specifying- (a) the manner and format in which such electronic records shall be filed, created, retained or issued; (b) where such electronic documents or electronic records have to be signed, the type of electronic signature required; (c) the manner and format in which such signature shall be affixed to the electronic documents or electronic records and the identity of, or the criteria which, a Certification Authority or Certification Service Provider used by such person filing the document should possess; (d) the control process and procedures required in order to secure confidentiality, authenticity and integrity of electronic documents, records, procurements, transactions or payments; (e) the manner or method of payment of any fee or charges for the filing, creation, retention or issue of any electronic record under paragraph (a); (f) the manner of doing anything which under any such provisions is required to be done as evidence in writing or otherwise using a document, notice or instrument; (g) the manner of doing anything which under any such provision, is required to be or which may be, done by post or other specified means of delivery; (h) the doing of anything which under any such provision is required to be, or which may be, authorized by a person's signature or seal; (i) the making of any statement or declaration which under any such provision is required to be made under oath; (j) the making of any payment that is required to be, or which may be, made under any such provision; (k) any other matter relating to electronic records or payments that are presently specified for the corresponding paper documents.
Publication in electronic forms of Gazette &c., deemed to be publication.

9. Where any Act or enactment provides that any Proclamation, rule, regulation, order, by-law, notification, or other matter shall be published in the Gazette, then such requirement shall be deemed to have been satisfied if such rule, regulation, order, by-law, notification or other matter is published in an electronic form of the Gazette.

No right to insist on records being in electronic form.

10. Nothing contained in the preceding sections shall confer a right upon any person to insist that any Ministry, Government Department, Institution, Statutory Body or Public Corporation or other similar body should accept or issue, any document in the form of electronic records or effect any monetary transaction in electronic form.

CHAPTER III
ELECTRONIC CONTRACTS

Electronic Contracts

11. In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed in electronic form. A contract shall not be denied legal validity or enforceability on the sole ground that it is in electronic form.

Attribution of electronic records.

12. (1) Unless otherwise agreed as between an originator and the addressee, a data message, electronic document, electronic record or other communication shall be deemed to be that of the originator, if it was sent— (a) by the originator himself; (b) by a person who had the authority to act for and on behalf of the originator in respect of that data message, electronic document, electronic record or other communication; or (c) by an automated information system programmed by, or on behalf of the originator.

2) Unless otherwise agreed as between the originator and the addressee, the addressee is to regard a data message, electronic document, electronic record or other communication as being that of the originator, and is entitled to act on that assumption, if:— (a) the addressee has no reason to doubt the authenticity of the data message, electronic document, electronic record or other communication; or (b) there do not exist any circumstances where the addressee knows, or ought to have known by exercising reasonable care, that the data message, electronic document, electronic record or other communication was authentic.

Acknowledgement of receipt.

13. (1) Where the originator has not agreed with the addressee that acknowledgement of receipt be given in a particular form or by a particular method, such an acknowledgement may be given by— (a) any data message, electronic document, electronic record or other communication by the addressee, automated or otherwise; or (b) any conduct of the addressee, sufficient to indicate to the originator that the data message, electronic document, electronic record or other communication has been received. (2) Where the originator has stipulated that data message, electronic document, electronic record or other communication shall be binding only on receipt of an acknowledgement of receipt of such data message, electronic document, electronic record or other communication by him, then, unless acknowledgement has been so received, the data message, electronic document, electronic record or other communication shall be deemed to have never been sent by the originator.

3) Where the originator has not stipulated that the data message, electronic document, electronic record or other communication shall be binding only on receipt of such acknowledgement of receipt, and the acknowledgement of receipt had not been received by the originator within the time specified or agreed, or if no time has been specified or agreed to, within a reasonable time, then the originator may give notice to the addressee stat-
ing that no acknowledgement of receipt has been received by him, and specifying a reasonable time by which the acknowledgement of receipt must be received by him and if no acknowledgement of receipt is received within the aforesaid time limit he may after giving notice to the addressee, treat the data message, electronic document, electronic record or other communication as though it has never been sent.

### Time and place of dispatch and receipt of electronic records.

14. (1) Unless otherwise agreed to between the originator and the addressee, the dispatch of a data message, electronic document, electronic record or other communication occurs when it enters an information system outside the control of the originator, or if the data message, electronic document, electronic record or other communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the data message, electronic document, electronic record or other communication is received. (2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message, electronic document, electronic record or other communication shall be determined as follows, namely: — (a) if the addressee has designated an information system for the purpose of receiving data messages, electronic document, electronic record or other communications: (i) receipt occurs at the time when the data message, electronic document, electronic record or other communication enters the designated information system; or (ii) if the data message, electronic document, electronic record or other communication is sent to an information system of the addressee that is not the designated information system, receipt occurs at the time when the data message, electronic document, electronic record or other communication is retrieved by the addressee. (3) Unless otherwise agreed between the originator and the addressee, the data message, electronic document, electronic record or other communication is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business. (4) The provisions of subsection (2) shall apply notwithstanding that the place where the information system is located may be different from the place where the data message, electronic document, electronic record or other communication is deemed to have been received under subsection (3). (5) For the purposes of this section— (a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business. (b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business; c) “usual place of residence” in relation to a body corporate, means the place where it is registered; (d) if the originator and the addressee are in different time zones, time refers to Universal Standard Time.

### Variation by agreement

15. The Minister may by regulation prescribe the matters which may be agreed to between the parties to such contract, involving the generating, sending, receiving, storing or otherwise processing of data messages, electronic documents, electronic records or other communication, in relation to the provisions of Chapter III.

### Liability of Certification Service Providers.

16. (1) A Certification Service Provider shall not be subject to any civil or criminal liability for any transaction under this Act in respect of third party information in the form of data messages, electronic documents, electronic records or other communications to which he merely provides access, if such liability is founded on — (a) the making, publication, dissemination, or distribution of such information or any statement made in such information; or (b) the infringement of any rights subsisting in or in relation to such information. (2) Nothing in this section shall effect— (a) any obligation founded on contract; (b) the obligations of a Certification Service Provider providing such services under a licensing or other regulatory regime established under any written law; or (c) any obligation imposed under any written law or by a court to remove, block or deny access to any information.
Avoidance of doubt

17. For the avoidance of doubt it is hereby declared that— (a) if an offer and acceptance of an offer has been in whole or in part expressed by means of an electronic record, an electronic signature attached to, or logically associated with, such electronic record shall not be denied legal effect solely on the ground that it is with an electronic signature; (b) if an electronic communication is used in the formation of a contract, the contract shall not be denied validity or enforceability solely on the ground that an electronic record had been used for such purpose; (c) the accepted principles of common law relating to contracts that the offeror may prescribe the method of communicating acceptance, shall not be affected by anything contained in this Chapter; (d) a contract formed by the interaction of an automated message system and a natural person or by the interaction of automated message systems, shall not be denied validity or enforceability solely on the ground that there was no review or intervention by a natural person of the final contract or of each of the actions carried out by the automated message system.

CHAPTER IV
CERTIFICATION AUTHORITY AND CERTIFICATION OF SERVICE PROVIDERS

Designation of a Certification Authority.

18. (1) There shall be a Certification Authority designated by the Minister for the purposes of this Act in consultation with the Minister in charge of the subject of Information and Communication Technology.
2) In designating a Certification Authority the Minister may by Order published in the Gazette, designate any Government Department, Public Corporation, Statutory Body, Institution, or authority or any branch or unit thereof which shall be charged with the implementation of the provisions of this Chapter; the Minister shall in making the Order take into consideration the capacity of the Government Department, Public Corporation, Statutory Body, Institution or authority to be designated in relation to its overall ability to discharge the obligations under this Act in ensuring the proper functioning of certification services by accredited Certification Service Providers.

Powers of Certification Authority.

19. The Certification Authority shall have the power to– (a) identify the criteria which will form the basis for accreditation of Certification Service Providers and the qualifications required by them; (b) hear appeals and specify the procedure to be followed in the granting of accreditation for the purposes of this Act; (c) specify the procedure for the hearing of appeals in the event of a refusal to grant or renew accreditation under section 20, as the case may be; (d) issue licences or any other form of authorisation to Certification Service Providers to provide prescribed services; (e) require Certification Service Providers to maintain such records and registers as may be prescribed; (f) from time to time call for information as may be necessary from Certification Service Providers and issue directions to such Certification Service Providers.

Accreditation of Certification Service Providers.

20. (1) No person shall function as an accredited Certification Service Provider unless he holds a valid certificate of accreditation issued under the Sri Lanka Accreditation Board for Conformity Assessment Act, No. 32 of 2005. (2) Nothing in this Act shall be construed as impeding or in any way restricting the rights of any certification service provider to engage in the business of providing certification services without being accredited. (3) A certificate of accreditation to a Certification Service Provider may be granted in accordance with provisions of the Sri Lanka Accreditation Board for Conformity Assessment Act, No. 32 of 2005, in keeping with the criteria for accreditation specified by the Certification Authority under paragraph (a) of section 19.
CHAPTER V RULES GOVERNING EVIDENCE

Applicability of the Rules of Evidence.

21. (1) Notwithstanding anything to the contrary in the Evidence Ordinance or any other written law, the following provisions of this section shall be applicable for the purposes of this Act. (2) Any information contained in a data message, or any electronic document, electronic record or other communication— (a) touching any fact in issue or relevant fact; and (b) compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity, shall be admissible in any proceedings: Provided that, direct oral evidence of such fact in issue or relevant fact if available, shall be admissible; and there is no reason to believe that the information contained in a data message, or any electronic document, electronic record or other communication is unreliable or inaccurate: Provided further that, for the purposes of paragraphs (a) and (b), if any information is contained in a data message, electronic document, electronic record or other communication made by a person— (i) who is dead or who by reason of his bodily or mental condition is unfit to attend as a witness; or (ii) who is outside Sri Lanka and where reasonable steps have been taken to find such person and he cannot be found; or (iii) who does not wish to give oral evidence through fear; or (iv) who is prevented from so giving evidence, evidence relating to such information shall, if available, be admissible. (3) The Courts shall, unless the contrary is proved, presume the truth of information contained in a data message, or in any electronic document or electronic record or other communication and in the case of any data message, electronic document, electronic record or other communication made by a person, that the data message, electronic document or electronic record or other communication was made by the person who is purported to have made it and similarly, shall presume the genuineness of any electronic signature or distinctive identification mark therein.


CHAPTER VI MISCELLANEOUS

Regulations.

24. (1) The Minister may, in consultation with the Minister in Charge of the subject of Information and Communication Technology, make regulations in respect of any matter required or authorized by this Act to be made, or for the purpose of carrying out or giving effect to the objectives of this Act, as specified in subsection (2). (2) In particular and without prejudice to the generality of the powers conferred by subsection (1), the Minister may make regulations for and in respect of all or any of the following matters:— (a) specifying the electronic infrastructure and guidelines that are— (i) sufficiently secure to meet the needs of Ministries, Government Departments, bodies or agencies owned and controlled by the Government, and Statutory bodies; (ii) interoperable to the maximum extent possible; (b) the conditions of service of the members of the Certification Authority in relation to the implementation of the provisions of this Act; (c) the powers, duties and functions of a person, body of persons, statutory body or institution being appointed as a Certification Authority in terms of section 18 and the other terms and conditions applicable to them; (d) criteria for accreditation of certification service providers under section 20, its cryptography services, electronic signature or advance electronic signature and security procedures or any other legal consequences connected therewith; (e) the procedure for appeals against refusal to grant or renew an accreditation certificate; (f) the qualifications required of persons seeking to provide certifications services; (g) the procedure for the recognition of Certification Service Providers, the issue of licences to such Certification Service Providers and the categories of services required to be provided by them; (h) the records to be maintained by the Certification Service Providers and the manner in which information has to be furnished to the Certification Authority by such Certification Service Provider; and (i) the matters referred to in section 15. (3) Every regulation made by the Minister shall be published in the Gazette and shall as soon as convenient after its publication in the Gazette be brought before Parliament for approval. (4) Every regulation, which is not so approved, shall be deemed to be rescinded as from the date of such disapproval, but without
prejudice to anything previously done thereunder. (5) The date on which such regulations shall be deemed to be so rescinded shall be published in the Gazette.

**Sinhala text to prevail in case of inconsistency.**

25. In the event of any inconsistency between the Sinhala and Tamil texts of this Act, the Sinhala text shall prevail.

**Interpretation**

26. For the purposes of this act, unless the context otherwise requires —

addressee” means the person intended by the originator to receive the communication but does not include an intermediary;

“Certification Authority” means the Certification Authority appointed in terms of Chapter IV of the Act;

“certification services” means any service which is provided to the senders or recipients of information in electronic form, or to those storing such information, and is designed to facilitate the use of cryptographic techniques for the purpose of ascertaining that the confidentiality, authenticity and integrity of such information is secured;

Certification Service Provider” means a person providing certification services within the meaning of this Act;

communication” means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer that a person is required to make or chooses to make in connection with an electronic transaction within the meaning of this Act;

“computer” means an electronic or similar device having information processing capabilities; “data message” means information generated, sent, received or stored by electronic, magnetic, optical or other similar means;

“electronic” means information generated, sent received or stored by electronic, magnetic, optical, or similar capacities regardless of the medium;

electronic document” includes documents, records, information, communications or transactions in electronic form;

electronic record” means a written document, or other record created, stored, generated, received, or communicated by electronic means;

electronic signature” means any letters, numbers, symbols, images, characters or any combination thereof in electronic form, applied to, incorporated in or logically associated with an electronic document, with the intention of authenticating and, or approving the same, in order to establish authenticity or integrity, or both;

information” includes text, message, data, voice, sound, database, video, signals, software, computer programs, including object codes and source codes;

information system” means an electronic system for creating, generating, sending, receiving, storing, reproducing, displaying, recording or processing information;

intermediary” means a person acting as a service provider on behalf of another person in relation to the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it;

network service provider” means a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services;

originator” means a person by who or on whose behalf the communication purports to have been sent or generated prior to receipt or storage, if any, but it does not include a person acting as an intermediary with respect to that communication;

provides access” in relation to third-party information, means the provision of the necessary technical means by which third-party information may be accessed and includes the automatic and temporary storage of the third-party information for the purpose of providing assess;

“security procedure” means a procedure which in relation to a certificate issued by a certification service provider, is specified in its certification practice statement for establishing the authenticity or integrity, or both, of any electronic document, which may require the use of algorithms or codes, identifying words and numbers, encryption, answer back or acknowledgment procedures, software, hardware or similar security devices;

“third party” in relation to a network service provider means a person over whom the provider has no effective control;
21. (1) Notwithstanding anything to the contrary in the Evidence Ordinance or any other written law, the following provisions of this section shall be applicable for the purposes of this Act.

2) Any information contained in a data message, or any electronic document, electronic record or other communication—

a) touching any fact in issue or relevant fact; and

b) compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity, shall be admissible in any proceedings: Provided that, direct oral evidence of such fact in issue or relevant fact if available, shall be admissible; and there is no reason to believe that the information contained in a data message, or any electronic document, electronic record or other communication is unreliable or inaccurate: Provided further that, for the purposes of paragraphs (a) and (b), if any information is contained in a data message, electronic document, electronic record or other communication made by a person—

i) who is dead or who by reason of his bodily or mental condition is unfit to attend as a witness; or

ii) who is outside Sri Lanka and where reasonable steps have been taken to find such person and he cannot be found; or

iii) who does not wish to give oral evidence through fear; or

iv) who is prevented from so giving evidence, evidence relating to such information shall, if available, be admissible

3) The Courts shall, unless the contrary is proved, presume the truth of information contained in a data message, or in any electronic document or electronic record or other communication and in the case of any data message, electronic document, electronic record or other communication made by a person, that the data message, electronic document or electronic record or other communication was made by the person who is purported to have made it and similarly, shall presume the genuineness of any electronic signature or distinctive identification mark therein.

This Act shall be called the “Electronic Transactions Act B.E. 2544 (A.D. 2001)”

This Act shall apply to all civil and commercial transactions performed by using a data message, except the transactions prescribed by a Royal Decree to be excluded from this Act wholly or partly. The provisions of paragraph one do not prejudice any law or rule enacted for consumer protection. This Act shall apply to the transactions in connection with the carrying out of the affairs of the State as prescribed in Chapter 4.

In this Act:

“transaction” means any act relating to a civil and commercial activity or carrying out of the affairs of the State as prescribed in Chapter 4.

“electronics” means an application of an electron means, an electrical means, an electromagnetic means or any other means of a similar nature including an application of an optical means, a magnetic means or a device in connection with an application of any of the aforesaid means;

“electronic transaction” means a transaction in which an electronic means is used in whole or in part;

“information” means an incident or fact regardless of whether expressed in the form of a letter, number, sound, image or any other form capable of connotation by itself or through any means;

“data message” means information generated, sent, received, stored or processed by electronic means, such, as electronic data interchange (EDI), electronic mail, telegram, telex or facsimile;

“electronic signature” means letter, character, number, sound or any other symbol created in electronic form and affixed to a data message in order to establish the association between a person and a data message for the purpose of identifying the signatory who involves in such data message and showing that the signatory approves the information contained in such data message;

“information system” means a system of (data message) processing by using an electronic device for generating, sending, receiving, storing or processing a data message;

“electronic data interchange” means the despatch or receipt of information by an electronic from computer to computer using an agreed standard;

“originator” means a person by whom the data message purports to have been sent or generated prior to storage before being sent pursuant to the method designated by such person, whether such data message is sent by such person, or generated in the name of or on behalf of such person, but does not include an intermediary with respect to that data message;

“addressee” means a person who is intended by the originator to receive the data message and who receives such data message, but does not include an intermediary with respect to that data message;

“intermediary” means a person who, on behalf of another person, sends, receives or stores a particular data message, including the providing of other services with respect to that data message;

“certificate” means a data message or other record confirming the link between a signatory and signature creation data;

“signatory” means a person that holds signature creation data and creates the electronic signature either on his own behalf or on behalf of other persons;

“relying party” means a person that may act on the basis of a certificate or an electronic signature;

“State agency” means a Ministry, Bureau, Department, other Government agency by a different name and having the status of a Department, a provincial administration, a local administration and a State enterprise established by an Act or a Royal Decree and shall also include a juristic person, a group of persons or a person having the power and duties to perform the State affairs in any matter whatsoever;

“Commission” means the Electronic Transaction Commission;
“Minister” means the Minister in charge of this Act.

CHAPTER I - ELECTRONIC TRANSACTIONS

Section 7

Information shall not be denied legal effect and enforceability solely on the ground that it is in the form of a data message.

Section 8

Subject to the provision of Section 9, in the case where the law requires any transaction to be made in writing, to be evidenced in writing or supported by a document which must be produced, if the information is generated in the form of a data message which is accessible and usable for subsequent reference without its meaning being altered, it shall be deemed that such information is made in writing, is evidenced in writing or is supported by a document.

Section 9

In the case where a person is to enter a signature in a writing, it shall be deemed that such data message bears a signature if:
1) the method used is capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being his own; and
2) such method is a reliable one and appropriate for the purpose for which the data message is generated or sent, having regard to the surrounding circumstances or an agreement between the parties.

Section 10

In the case where the law requires that any information be presented or retained in its original form as an original document, if such information is presented or retained in the form of data message pursuant to the following requirements, it shall be deemed that such information is presented or retained as an original document under the law:
1) a reliable method is used with the data message to assure the integrity of the information from the time when it is generated in its final form; and
2) the information is capable of being subsequently displayed.

The integrity of the information under (1) shall be determined by having regard to its completeness and unalteration, apart from the addition of any endorsement or record or any change which may arise in the normal course of communication, storage or display of the information, which does not affect the integrity of that information. In determining the method used for assuring the integrity of the information under (1), all relevant circumstances must be taken into consideration, including the purpose for which such information is generated.

Section 11

The admissibility of a data message as an evidence in the legal proceedings shall not be denied solely on the grounds that it is a data message. In assessing the evidential weight of a data message whether it is reliable or not, regard shall be had to the reliability of the manner in which or the method by which the data message was generated, stored or communicated, the manner in which or the method by which the completeness and integrity of the information was maintained, the manner in which or the method by which the originator was identified or indicated, including all relevant circumstances.
Section 12

Subject to the provision of Section 10, in the case where the law requires that certain documents or information be retained, if such retention is made in the form of a data message pursuant to the following requirements, it shall be deemed that such document or information is retained pursuant to the requirements of the law:
1) that data message is accessible so as to be usable for subsequent reference without its meaning being altered;
2) that data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
3) the information, if any, which specifies the source, origin and destination of a data message including the date and time sent or received, is retained.
The provisions of paragraph one shall not apply to the information the sole purpose of which is to enable the data message to be sent or received. The State agency responsible for retaining any document or information may prescribe additional details with respect to the requirement in retaining such document or information insofar as they are not contrary to the provisions of this Section.

CHAPTER II - ELECTRONIC SIGNATURES

Section 26

An electronic signature is considered to be a reliable electronic signature if it meets the following requirements:
1) the signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
2) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;
3) any alteration to the electronic signature, made after the time of signing, is detectable; and (4) where a purpose of the legal requirement for a signature is to provide assurance as to the completeness and integrity of the information and any alteration made to that information after the time of signing is detectable. The provision of paragraph one does not limit that there is no other way to prove the reliability of an electronic signature or the adducing of the evidence of the non-reliability of an electronic signature.

Section 27

Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
1) exercise reasonable care to avoid unauthorized use of its signature creation data;
2) without undue delay, notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
a) the signatory knows or should have known that the signature creation data have been lost, damaged, compromised, unduly disclosed or known in the manner inconsistent with their purpose;
b) the signatory knows from the circumstances occurred that there is a substantial risk that the signature creation data may have been lost, damaged, compromised, unduly disclosed or known in the manner consistent with their purpose;
3) where a certificate is issued to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory which are relevant to the certificate throughout its life-cycle, or as specified in the certificate.

Section 28

Where a certification service is provided to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall perform as follows:
1) act in accordance with representations made by it with respect to its policies and practices; (2) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life-cycle, or as specified in the certificate;
3) provide reasonably accessible means which enable a relying party to ascertain in all material representations from the certificate in the following matters:
   a) the identity of the certification service provider;
   b) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;
   c) that signature creation data were valid at or before the time when the certificate was issued;
4) provide reasonably accessible means which enable a relying party to ascertain from the certificate or otherwise as follows:
   d) the method used to identity the signatory;
   e) any limitation on the purpose or value for which the signature creation data or the certificate may be used;
   f) that the signature creation data are valid and have not been lost, damaged, compromised, unduly disclosed or known in a manner inconsistent with their purpose;
   g) any limitation on the scope or extent of liability stipulated by the certification service provider;
   h) the availability of the means for the signatory to give notice upon the occurrence of the events pursuant to Section 27 (2); and
   i) a timely revocation service is offered;
5) where services under subparagraph (4) (e) are offered, provide a means for a signatory to give notice pursuant to Section 27 (2) and, where services under (4) (f) are offered, ensure the availability of a timely revocation service;
6) utilize trustworthy systems, procedures and human resources in performing its services.

Section 31

A certificate or an electronic signature shall be deemed to be legally effective without having to consider:
1) the geographic location where the certificate is issued or the electronic signature created or used; or
2) the geographic location of the place of business of the issuer of the certificate or signatory. A certificate issued in a foreign country shall have the same legal effect as a certificate issued in the country if the level of reliability used in issuing such certificate is not lower than as prescribed in this Act. An electronic signature created or used in a foreign country shall have the same legal effect in the country as an electronic signature created or used in the country if the level of reliability used in creating or using such electronic signature is not lower than as prescribed in this Act. In determining whether which certificate or electronic signature offers reliability pursuant to paragraph two or paragraph three, regard shall be had to recognized international standards and any other relevant factors.

2007 Act on Commission of Offences Relating to Computer, B.E. 2550

(Amended by Commission of Computer-Related Offences Act (No.2), B.E.2560(2017)

Section 3

In this Act: “Computer System" means computer device or set of computer devices that are connected and cooperated with another whereby command, program or else, and work process for automatic data processing thereof has been set up;
Computer Data" means data, text, command, program or else stored in computer system and being able to be processed by computer system, including electronic data under the law on electronic transactions;
Computer Traffic Data" means data in relation to the communication of computer system that indicates the origin, source, terminal, route, time, date, size, duration, type of service or else relating to the communication of such computer system;
Service Provider" means;
1) the one who provides others an internet access service or any other services that enable their communication via Computer System irrespective of whether such service is provided on his or her behalf or on behalf of or for the benefit of other persons;
2) the one who provides Computer Data storage service for the benefit of other persons; “Client” means the one who makes use of service provided by a service provider without regard to service charge;
“Competent Official” means a person appointed by the Minister for the execution of this Act; “Minister” means the Minister having charge and control of the execution of this Act.

Chapter 2 - Competent Officials

Section 18

Subject to section 19, for the purpose of investigations and inquiries in the case where there is a reasonable cause to believe that the commission of an offence under this Act has occurred or in the case where a request is made under paragraph two, the competent official shall have any of the following powers to the extent necessary for using the matters concerned as evidence involving the commission of the offence and in the finding of the offender:

1) addressing a written enquiry to, or issuing a summons on, a person connected with the commission of the offence for the purpose of giving statements, furnishing written explanations or furnishing documents, data or any other evidence in an intelligible form;

2) summoning computer traffic data from providers of services relating to communications via computer systems or from other persons concerned;

3) ordering a service provider to hand over to the competent official data concerning users, which are required to be retained under section 26 or which are in possession or in custody of the service provider, or to retain the such data;

4) making a copy of computer data or computer traffic data from a computer system in respect of which there is a reasonable cause to believe that an offence is committed therein, in the case where such computer system is not yet in possession of the competent official;

5) ordering the person having in possession or custody computer data or equipment used for retaining computer data to hand over such computer data or equipment to the competent official; (6) inspecting or accessing a computer system, a computer data, a computer traffic data or equipment used for retaining computer data of any person, which is evidence or may be used as evidence in connection with the commission of an offence or which facilitates inquiries leading to the finding of offenders, and also ordering such person to furnish relevant computer data or computer traffic data to the extent necessary;

7) decrypting computer data of any person or ordering persons concerned in the encryption of computer data to undertake decryption thereof or co-operate with the competent official in such decryption;

8) seizing or attaching a computer system to the extent necessary only for the purpose of acquiring the knowledge of details of offences and offenders.

For the purpose of investigations and inquiries by inquiry officials under the Criminal Procedure Code in criminal offences under other laws involving the use of a computer system, a computer data or equipment for the retention of computer data as an element or part of the commission of the offence or involving a computer data connected with the commission of a criminal offence under other laws, the inquiry official may request the competent official under paragraph one to take action under paragraph one, or if such facts are apparent to the competent official on account of the performance of duties under this Act, the competent official shall expeditiously gather facts and evidence and make a notification to officials concerned for further proceedings.

The person receiving a request from the competent official under paragraph one (1), (2) and (3) shall take action in response to the request without delay, provided that it shall not be later than seven days as from the date of receipt of the request, or within the period of time specified by the competent official, which must not be less than seven days and must not be more than fifteen days except in the case where permission is obtained from the competent official when there exists a reasonable cause. In this regard, the Minister may, by publication in the Government Gazette, prescribe the period of time within which action must be taken by service providers, as appropriate for respective types of service providers.

Section 19

In exercising the powers of the competent official under section 18 (4), (5), (6), (7) and (8), the competent official shall file a motion to the Court of competent jurisdiction for giving an order permitting the competent official to take action for which the motion is filed. In this regard, the motion must indicate, to the extent possible, a reasonable cause to believe that any person commits or is about to commit any particular act which is an offence, a reason for the exercise of the power, the nature of the commission of the offence and details as to the equipment used in the commission of the offence as well as the offender. The Court shall expeditiously consider such motion.
Then the Court gives an order granting permission, the competent official shall, before taking action in pursuit of the Court's order, furnish a copy of the record of the reasonable cause leading to the exercise of the power under section 18 (4), (5), (6), (7) and (8) to the owner or possessor of the computer system concerned for the evidentiary purpose. But, if the owner or possessor of the computer is not at that place, the competent official shall furnish such copy of the record to such owner or possessor at the earliest possible opportunity. The competent official leading the performance of the action under section 18 (4), (5), (6), (7) and (8) shall furnish a copy of the record of details thereof and reasons therefor to the Court of competent jurisdiction within forty-eight hours as from the commencement of the action, for the evidentiary purpose. The making a copy of computer data under section 18 (4) shall be permissible only where there is a reasonable cause to believe that the commission of an offence has occurred and shall not cause impediment to the operation of business of the owner or possessor of such computer data to the extent in excess of necessity.

In conducting a seizure or attachment under section 18 (8), in addition to the requirement that a copy of the written instrument indicating the seizure or attachment be furnished to the owner or possessor of the computer system in question for the evidentiary purpose, the competent official shall not seize or attach the same for a period exceeding thirty days. In the case where it is necessary to have a seizure or attachment for a longer period, a motion may be filed with the Court of competent jurisdiction for an extension of the period of seizure or attachment, provided that the Court may grant extension of time on one or more occasions, with the aggregate period not exceeding sixty days. When the necessity for the seizure or attachment ceases to exist or such period of time expires, the competent official must return the computer system seized or withdraw the attachment forthwith.

The written instrument indicating the seizure or attachment under paragraph five shall be as prescribed in the Ministerial Regulation.”

Section 20

In the case where the commission of an offence under this Act is the dissemination of Computer Data that may affect the security of the Kingdom as prescribed in Book II, Title I or Title III of the Penal Code or is contrary to public order or good morals, the Competent Official may, with approval of the Minister, apply a motion together with evidence to the court that having jurisdiction for the order to block the dissemination of that Computer Data. In the case where the court has the order to block the dissemination of the Computer Data under paragraph one, the Competent Official may conduct blocking himself or herself, or order the Service Provider to do so.

Section 21

If it appears to the Competent Official that any Computer Data consisting of undesirable program, the Competent Official may apply a motion to the court that having jurisdiction to forbid the sale or distribution of that Computer Data, to order the owner or possessor of that Computer Data to stop using, destroy or modify that Computer Data, or to impose condition of use, having in possession or distributing that undesirable program. The undesirable program under paragraph one means any program that affects Computer Data, Computer System or other programs by causing damage, destruction, alteration or addition, interruption or deviation from determined command or causing other things as prescribed by the Ministerial Regulation, except the program which is designed to protect or modify the aforesaid program as notified by the Minister in the Royal Gazette.

Section 22

The Competent Official shall not disclose or deliver Computer Data, Computer Traffic Data or client data obtained under section 18 to any person. The provisions of paragraph one shall not apply to the commission of any act for the benefit of carrying out of legal actions against the offender under this Act or against the Competent Official who abuses of power or the commission of any act in accordance with the order or permission of the court. Any Competent Official who violates the provisions of paragraph one shall be liable to imprisonment for a term of not exceeding three years or to a fine of not exceeding sixty thousand baht or to both.
Section 23

Any Competent Official who acts negligently causing any other person to know Computer Data, Computer Traffic Data or client data obtained under section 18 shall be liable to imprisonment for a term of not exceeding one year or to a fine of not exceeding twenty thousand baht or to both.

Section 24

Any person who knows computer data, computer traffic data or users' data acquired by the competent official or the inquiry official under section 18 and discloses such data to any person shall be liable to imprisonment for a term not exceeding two years or to a fine not exceeding forty thousand Baht or to both.

Section 25

Data, computer data or computer traffic data acquired by the competent official under this Act or acquired by the inquiry official under section 18 paragraph two shall be admissible into evidence in accordance with the provisions of the Criminal Procedure Code or other laws on evidence taking, provided that they have not occurred in consequence of any inducement, promise, threat or deceit or any other unlawful means.

Section 26

A service provider must retain computer traffic data for a period of not less than ninety days as from the date on which such data enter a computer system, provided that, in the case of necessity, the competent official may order any service provider to retain computer traffic data for a period exceeding ninety days but not exceeding two years as a matter of an individually exceptional case and on an ad hoc basis.

Section 29

In performance of duties under this Act, the Competent Official shall be a senior administrative official or a superior police official under the Criminal Procedure Code and shall have the power to obtain a complaint or incrimination and shall have the power to conduct investigation and inquiry the offences under this Act. In conducting an arrest, detain, search, file of inquiry and legal proceedings against the offender under this Act, all powers of the senior administrative officer or superior police officer or inquiry official under the Criminal Procedure Code shall be exercised by the Competent Official in cooperation with responsible inquiry official to carry out the authority. The Prime Minister as the supervisor of the Royal Thai Police and the Minister shall jointly issue the regulation in relation to guidelines and procedure for the execution under paragraph two.

Remark:- The rationale for the issue of this Act as of today is that a computer system is essential to business operations and the human way of life, as such, if any person commits an act that disables the working of a computer system according to the pre-determined instructions or that causes a working error – a deviation from that required by the pre-determined instructions or that resorts to any means to illegally know of, correct or destroy a third party's data contained in a computer system or that uses a computer system to disseminate false or pornographic computer data, then that act will damage and affect the country's economy, society and security including people's peace and good morals. Therefore, it is deemed appropriate to stipulate measures aimed at preventing and suppressing such acts. Hence the enactment of this Act.
Section 2.

In this Code:

10) "Investigation" means a search for facts and evidence, which an administrative or police official has made in accordance with his power and duty, in order to preserve public order and to ascertain the particulars of an offence;

11) "Inquiry" means the collection of evidence and other proceeding conducted by an inquiry official according to the provisions of this Code in connection with an alleged offence, for the purpose of ascertaining the facts or establishing the guilt and securing the punishment of the offender;

Chapter II Criminal Warrants

Part III Warrant of Search

Section 69.

The grounds, upon which a warrant of search may be issued, are as follows:

1) To discover and seize any article which may be used as evidence in the course of an inquiry, preliminary examination or trial;

2) To discover and seize any article the possession of which is an offence, or which has been unlawfully obtained or which is reasonable suspected to have been used or intended to be used for committing an offence;

3) To discover and rescue any person who is wrongfully restrained or confined;

4) To discover any person against whom a warrant of arrest has been issued;

5) To discover and seize any article according to the judgment or order of a Court, in case of such discovery or seizure cannot be otherwise effected. Section 70.- The search-warrant for the purpose of finding and arresting the person shall be prohibited to issue unless there will also be the arrest-warrant of such person, and the official to execute the search-warrant must have both the search-warrant and the arrest-warrant.

Title V Arrest, Detention, Imprisonment, Search and Provisional Release

Chapter II Search

Section 91.

The provisions of Section 81/1 shall be brought to be applied to search mutatis mutandis.

Section 92.-

It is prohibited to search in private place without the search warrant or Court's order, unless the government official or police official is inspector, and in the following case:

1) In case of scream to help from inside of the private place or any other voice or circumstance shows that there is danger occurred in such private place;
2) In case of offence appearing in the presence is being made in the private place;
3) In case of the person, who has committed in-the-presence, is being followed closely behind to arrest and take refuge or serious grounds for suspecting that to have entered in hiding within such private place;
4) In case of evidence as may be reasonable that chose to have in one's procession constitutes an offence or acquires with commission of an offence or having used or having had for using in commission of an offence or able to be the evidence proving connection of an offence to be hide or in such place. With reasonable grounds to be believed that on account of the delay more than the search warrant will be brought, such chose will be transferred or have been destroyed;
5) In case of such private place where the arrested person is host, and such arrest with the arrest warrant or the arrest under section 78; Exercise of power according (4), the government official or police official as inspector, shall deliver the copy of note inspecting and the list of chose acquired by inspection, including the list to be made to show the grounds for being. able to search as book to occupier of the premises to be searched, if there is not occupier there, the book, as aforesaid, shall be delivered to person as aforesaid forth with being able to do, and the grounds and inspection-result shall be reported as book to commander in more rank than.»

Section 94.-

Any administrative or police official making a search in a private place shall require the owner, occupant or keeper of the place to be searched to allow him free ingress into it and to afford him every reasonable facility to execute the warrant. In such case, he shall produce the warrant or, in case where he can make a search without a warrant, make known his name and official position.

If the persons mentioned in the foregoing paragraph refuse the entry, the official shall have the power to use force to affect the entry. In case of necessity he may open or pull down gates, doors, windows, fences or the like.

Section 98.-

A search in a private place shall be confined to the person or article intended to be found. But there are the following exceptions:
1) In case of a search is made for unspecified articles, the official making the search has the power to seize any article likely to be used as evidence in favour of or against the alleged offender or accused; (2) The official making a search has the power to arrest or seize any other person or article in the place searched, provided such other person or article is liable to arrest or seizure under another warrant or in case of flagrant offence.

Section 99.-

In such search, the official must try to avoid to cause the damage and disorder as far as possible.

Section 100.-

If it is reasonable suspected that any person found in any place where a search is made or is about to be made will cause such obstruction as to render the search futile, the official making the search has the power to place him under custody, or to have him watched over whilst the search is bearing made, in so far as it is necessary to prevent him from causing such obstruction. If there be reasonable grounds for suspecting that such person has concealed on his body any of the articles intended to be found, the official making the search has the power to have that person searched as provided in Section 85.

Section 101.-

Things seized in the search shall be wrapped up or contained in the parcel and sealed or marked essentially.
Section 105.

If a letter, postcard, telegram, printed matter or any other document sent by or to the alleged offender or accused through a post and telegraph office and not yet delivered is wanted by the authority for the purpose of an inquiry, preliminary examination, trial or other proceedings under this Code, the order to the postal and telegraphic authority to deliver such document shall be applied for from the Court. If any such document is, in the opinion of the Director-General of the Police Department or the Commissioner of Changvad, wanted for any such purpose, he may require the postal and telegraphic authority to detain such document pending an order from the Court. The provisions of this Section shall not be applied to the correspondence of an alleged offender or accused with his counsel.

DIVISION V EVIDENCE
CHAPTER I GENERAL PROVISIONS

Section 226.

Any material, documentary or oral evidence, likely to prove the guilt or the innocence of the accused, is admissible, provided it is not obtained through any inducement, promise, threat, deception or other unlawful means; such evidence shall be produced in accordance with the provisions of this Code or other laws governing production of evidence.

Section 226/1.-

In case where it is appearing in Court that any evidence arised duly but derived by acting in bad faith or derived by means of the data arisen or derived wrongfully, such evidence shall not be admitted by the Court, unless the admission of such evidence will have more useful effect on giving justice than bad effect arisen from an impact on the standard of criminal justice work system or basic right and liberty of people. In consideration of admitting an evidence according to the first paragraph the Court shall consider all circumstance of case without thinking of the following factors; (1) Proval Value, importance and convincing of evidence. (2) Circumstances and gravity of offence in case. (3) Nature and injury being arisen from the acting in bad faith. (4) A person, doing wrongful act being a cause of deriving the evidence, is punished or not and how it is.

Section 226/2.

The evidence being concerned with other offences or injured behavior of the accused person shall not be admitted by Court, in order to verify that the accused person is an offender in instituted case, unless any one of the following evidences. (1) The evidence being directly concerned with elements of offence in the instituted case. (2) The evidence showing manner, way or a particular form of commit an offence of the accused person. (3) The evidence rebutting the accused person's allegation of his doing or good behavior. Under the provisions in the first paragraph, adducing such evidence is not prohibited in order that the Court can use it for consideration of punishment determination or addition.

Section 226/3.

An oral statement given in the Court by any individual witness or noted in a document or other material referred as an evidence in the Court, if it is submitted to be verified shall be deemed as a hearsay evidence. The hearsay evidence shall not be admitted by Court, unless; (1) Condition, nature, source of derivation and minor fact of such hearsay witness are believable that the fact is provable or (2) It is necessary because a person who has seen, heard or known the statement concerned with case in which a statement shall be directly made in person is a witness, can not appear as a witness and there is a reasonable cause in the interest of justice to admit
such a hearsay evidence. In case where the Court thinks it is not fit to admit any hearsay evidence and the party concerned applies for objection before the Court's proceeding with case, the Court shall write a report specifying the name, kind and the nature of witness, telling the reason of unacceptance and objection of the concerning party. For the reason being risen by an objecting party, the Court shall, under his consideration, write in the report or determine such a party to file a written statement with Court in order to collect it in a file.

**Section 226/4.**

In the case of sexual offence, the accused person shall not adduce evidence or make cross-examination with a question being concerned with the injured person's sexual behavior to other person out of the accused person, unless it is permitted by Court according to the application. The application according to the first paragraph shall be permitted in case where the Court thinks it will cause the justice in trying and adjudicating the case.

**Section 226/5.**

In the trial stage, if there is a necessary or reasonable ground, the Court may admit the note of testimony in the stage of preliminary examination or the note of testimony of the witness who has given testimony in other case as other evidence in the case.

**Section 227.-**

The Court shall exercise its discretion in considering and weighing all the evidence taken. No judgment of conviction shall be delivered unless and until the Court is fully satisfied that an offence has actually been perpetrated and that the accused has committed that offence. Where any reasonable doubt exists as to whether or not the accused has committed the offence, the benefit of doubt shall be given to him.

**Section 227/1.-**

In consideration of carrying weight of a hearsay evidence, an implicated evidence, the evidence without a chance for the accused person to give a cross-examination or the evidence with any other defection which may have an impact on believableness of the evidence, the Court must do it carefully and should not believe only such an evidence for punishing the accused person, unless there is a strong reason, a special circumstance of case or other supporting evidence.

The appurtenant evidence, according to the first paragraph, means other admissible evidence of which source is free from the evidence requiring such appurtenant evidence and it must have a provable value supporting other appurtenant evidence to become more believable.

**Section 228.-**

During the course of a trial, the Court may, of its own motion or upon the application of a party, take additional evidence; such may be taken by the Court itself or by commission.

**Section 229.-**

Evidence is taken by the Court, either within the court's precincts or outside as the Court thinks fit according to the nature of the evidence.
Section 229/1.-

Subject to Section 173/1, in preliminary examination or trial, a prosecutor has to file a list specifying evidences showing the type and nature, of object, places in brief or documents as it can, including the name, address of a person or expert whom the prosecutor desires to adduce or apply to the Court for examination or appointment not less than fifteen days before the day of preliminary examination or taking of evidence, together with a copy of the list specifying evidences as said in enough number for giving to the accused person. The accused person shall file the list specifying evidences and its copy before the day of the accused person's taking of evidence.

For examination the case of application for restitution of an exhibit forfeited under the Court's order or the case of applying for the Court's forfeiture of property, the concerned person shall file a list specifying evidence with the Court not less than seven days before the day of examination, together with enough number of a copy of such list for other concerned persons to take it. In case where the period of time fixed for filing a list specifying evidence according to the first paragraph of the second paragraph, as the case may be, has been expired, if a party or a concerned person who has filed the list specifying evidence has a reasonable ground showing that he could not know an evidence must be adduced or does not know there have been some evidences or has any other reasonable ground, or if a party or a concerned person of any party who has not filed such list specifying evidences to satisfy the Court that there is a reasonable ground for being unable to file list specifying evidences in such fixed period of time, Such a party or a person may apply for permission to present the said evidence to the Court, along with the list specifying evidences and its copy at any time before finalizing the taking of evidence of that party. In case where such a party or a person has filed the list specifying evidences, or before finalizing trial in case where such a party or person does not file a list specifying evidences and the Court thinks that it is necessary to take of the said evidence for giving a decision of an important issue fairly, the Court shall have power to give permission to take and admit such an evidence.

The Court is prohibited to permit taking of and admitting any evidence mentioned by a party or a concerned person that he has not expressed intention to allude to the evidence according to the first paragraph, the second paragraph or the third paragraph or according to section 173/1, the second paragraph or the third paragraph, but in case where the Court thinks that it is necessary to safeguard a witness or take such evidence in order to give a decision fairly or in order to give a chance to the accused person for defending a case in plenary manner, the Court has power to permit taking and admitting such evidence.

Section 230.-

In case where the concerning party make a request or the Court thinks fit, the Court may take evidence out of Court, or there is a cause of necessity, the evidence cannot be appeared for taking at in that Court and the taking of evidence in other way cannot be made, the Court has power to commit an issue to other Court for taking the evidence instead of it, the Court receiving an issue shall have the same authority as the former Court, including authority to commit it to other Court. Under the provisions of Section 172 and Section 172 bis, the file or copy of prosecution, copy of statement and documents or an exhibit, as it is necessary, to the Court receiving an issue for taking evidence if the accused person is being under detention in the period of trial, the controller shall hand the accused person over to the Court receiving an issue, but if the accused person, as in case according to section 172 bis, is not in full satisfaction of hearing trial he may file a question of witness or a statement to have an evidence examined, the Court shall take an evidence as it be. When the taking of evidence as assigned has been finished, a memorandum and documents or an exhibit shall be return to the former Court.

Section 230/1.-

In case of necessity, the witness cannot be brought to give testimony in Court, where a party makes a request or the Court thinks fit, the Court may permit such a witness to give testimony to other Court or the government office to other place out of the Court, with holding telecasting picture and sound in the manner of meeting in screen, all of this must be under the control of Court having an area of power over that local area according to the rule and method prescribed in the regulations of the president of the Dika Court, with agreement of general meeting of Dika Court and it shall be enforced after publishing in government gazette. Giving testimony according to the first paragraph shall be deemed as if a witness gives testimony in the trial room of Court. Section 230/2.- In case where taking evidence according to Section 230/1 cannot be made, if a party make a request or the Court thinks fit, the Court may permit to offer a statement note emphasizing on the fact or the opinion of a statement maker whose residence is in foreign country to the Court instead of bringing an oral evidence to give testimony to the Court. All of this, the testimony giver's right to appear in Court for giving more testimony shall
riot be cut out.
The particulars of statement note according to the first paragraph are as follows; (1) Name of Court and number of case. (2) Date and place of making statement note. (3) Name and surname of a party. (4) Name, surname, age, address and occupation of a testimony giver and his relationship to a party. (5) The details of the fact or the opinion of a testimony giver. (6) Signature of a testimony giver and a party offering the statement note for a testimony giver’s signature, Section 47, the third paragraph of Civil Procedure Code shall be enforced mutatis mutandis. To amend the testimony note filed with Court shall be prohibited, except amendment of insignificant error or fault.

Section 231.- Where any party or person is to give or produce any kind of the following evidence: (1) Any document or fact which is still an official secret; (2) Any confidential document or fact which has been acquired by or made known to him by virtue of his profession or duty; (3) Any process, design or other work protected from publicity by law; the said party or person is entitled to refuse to give or produce such evidence unless he has obtained the permission from the authority or the person concerned with such secret. Where any party or person refuses to give or produce the evidence as aforesaid, the Court has the power to summon the authority or person concerned with such secret to appear and give explanation in order that the Court may decide whether or not there is any ground to support such refusal. Where the Court is of opinion that the refusal is groundless, it shall order such party or person to give or produce such evidence.

CHAPTER III DOCUMENTARY EVIDENCE

Section 238.-

Only original documents are admissible as evidence; however, if the originals are not available, certified copies thereof or oral evidence of their contents are acceptable. If official documents are cited as evidence, even where the originals are still available, copies thereof certified by the authorities may be sent, unless otherwise directed in the summons.

Section 239.-

Where any document is cited as evidence by a party but is not in his possession, if he informs the Court of the nature of the document and the place where it can be found, the Court shall summon the person in possession of the document to deliver it to the Court.

Section 240.-

In case where the Court does not fix the day of evidence examination according to Section 173/1, if a party desires to allude the document under his ownership as an evidence, such document shall be filed with Court before the day of preliminary examination or the day of taking an evidence not less than fifteen days in order that other party can have a chance to examine and copy such document before taking that documentary evidence, unless the document which a party desires to rely upon is the note of witness' testimony or the document in which the witness' name and address are appeared or the Court deems expedient to give other order due to condition and necessity of that document. In the case out of the enforcement of serving document according to the first paragraph, if there is a document appearing as an evidence in the stage of Court, it shall be read or sent to a party for examination. If any party wants a copy, the Court has power to order the party alluding such document to send a copy to other party, as it thinks fit. If any party does not serve the document according to the second paragraph or does not serve a documentary evidence or a material evidence according to Section 173/2, the first paragraph, the court has power to unaccept such evidence, unless the Court is of opinion that it is a case in the interest of justice or such action is not intentionally made and does not another party lose a chance of his proceeding with the case.
CHAPTER IV MATERIAL EVIDENCE

Section 241.-

Anything, which is used as material evidence, must be brought to the Court. In case of it is not possible to bring it, the Court shall proceed to examine it and make a memorandum of the examination at the place where the thing is, at such time and by such means as the Court thinks fit according to the nature of the evidence.

Section 242.-

In the course of an inquiry, preliminary examination or trial, anything used as material evidence shall be shown to the party or witness concerned. If there is an unwrapping or breaking of the seal, the rewrapping or re-sealing shall be made in the presence of the party or witness concerned.

2008 CRIMINAL CODE

TITLE I

PROVISIONS APPLICABLE TO GENERAL OFFENCES

CHAPTER 1

DEFINITIONS

Section 1. In This Code:

(7) “Document” means any paper or other material for expressing the meaning by letters, figures, plan or another design, whether it be by way of printing, photographing or any other means, which is evidence of such meaning.
8) “Official document” means a document drawn up or authenticated by an official in the course of his duty, and includes also a. copy of such document authenticated by an official in the course of his duty;
9) “Document of right” means a document evidencing the creation, modification, transfer, reservation or extinction of a right;
10) “Signature” includes a finger-print and mark put to a document by a person in lieu of his signature;
14) “Electronics Card” means that:
A) Any of documents or materials in any description whatever that issuer having issued to the person entitled to use, irrespective of whether the specified name or not, by data or cipher noted by applying and using the ways of electron, electricity, long wave or any way in the same nature including to apply and use the ways of fight or magnet to be sense appeared by any of letters, figures, ciphers or symbols either able to be seen or not to be seen by the naked eyes;
B) Data, cipher, account number, any of set-numbers of electron or figures which issuer having issued to the person entitled to use by any of documents or materials not to be issued, but there is he way to use in the same manner as (A) ; or
C) Anything else to be used in corroboration of the electronic data for showing the relationship between person and electronic data by the object for specifying the owned person.
TITLE I/I
THE OFFENCE IN RESPECT OF TERRORIZATION

Section 135/1.

Whoever, performing the Criminal Offence, as follows:
1) Commit an act of violence or exercise any act to cause a danger to life or a body harm or any person’s freedom harm seriously;
2) Commit any act to cause seriously injury to transportation-system, communication-system or structure base of public interest;
3) Commit any act to cause injury to any State’s property or any person’s property or an envelopment to cause likely cause an important economic injury;
If such act is made by the aim to treated or enforce Thai Government, Foreign Government or International Organization make or not to make any act to cause seriously injury or for making a disorder by causing the people to be terrified, such person committing an offence of terrorization must be punished with death, imprisonment for life or imprisonment from three years to twenty years and fine from six ten thousands Baht to one million Baht;
Doings by demonstration, convocation, protestation, argument or movement for demanding Government aid or to be received Justice is not offence of terrorization.

Section 135/2.

Whoever:
1) Treated to make a terrorization under circumstances advisable to be believed that such person ill do as treatment really; or
2) Collect forces or arms, procure or gather property, give or receive a training terrorization, prepare any other act or conspire each other to terrorize or commit any offence in a part of plan to terrorize or abet people into a part of terrorization or ones know the terrorists and commit any act to be covered; such person shall be imprisoned as from two years to ten years and fined as from four ten thousands Baht to two hundred thousands Baht.

Section 135/4.

Whoever to be the member of a body of persons who there is resolution of or notification subject to Security Council of the United Nations Organization designating as a body of persons to have committed an act as terrorization, and Thai Government has notified to acknowledge notification or resolution as aforesaid, such person shall be imprisoned not more than seven years and fined not more than hundred thousands and four ten thousands Baht.
Nature 1/1 with Section 135/1 to Section 135/4 prescribed by the Act Amending the Criminal Code, E. 2546, Section 4 (G.G. 120 A. 76, dated in G.G. 11 August 2546).
THE ACT ON MUTUAL ASSISTANCE IN CRIMINAL MATTERS B.E. 2535

PART 2
Inquiry and Producing Evidence

Section 15

Upon receipt the request for assistance from a foreign state to take statement of persons or gathering evidence located in Thailand at the stage of inquiry, the Competent Authorities shall direct an inquiry official to execute such request. The Inquiry Official shall have authority to take statement of persons or gathering evidence as requested under paragraph one and, if necessary, to search and size any document or article in accordance with rules, means, and conditions set forth in the Criminal Procedure Code. When the taking statement of person or gathering evidence has been finished, the Inquiry Official shall report and deliver all evidence derived therefrom to the Competent Authorities.

Section 16

If the mutual assistance treaty between Thailand and Requesting State requires a document to be authenticated, the Competent Authorities shall have the power to instruct the person in charge of keeping the said document to attest it in accordance with the forms and means specified in the treaty or as defined by the Central Authority.

Section 17

Upon receipt the request for assistance from a foreign state to take the testimony of witness in Thai Court, the Central Authority shall direct the public prosecutor to execute such request. The Public Prosecutor shall have the power to apply to the Court having jurisdiction over the domicile or residence of the person who will be the witness or who has in possession or keep the documents or other evidence, and request for the testimony or adducting of the evidence, and the Court shall have the power to try the case conforming to the provisions enshrined in the Criminal Procedure Code. After the completion of testimony, the Public Prosecutor shall apply to the court requesting for the record of testimony as well as other evidence and deliver all to the Central Authority for further operation.

PART 4
Serving Documents

Section 21

Upon receipt the request for assistance from a foreign state to serve legal document, the Competent Authorities shall execute such request and report to the central Authority. If the legal document to be served under the request is such that requiring the appearance of a person before an authority or the court in the Requesting State, the Competent Authorities shall serve the said document for a reasonable time prior to scheduled appearance. The result of service of documents shall be reported in accordance with the forms and means defined by the Central Authority unless otherwise specified in the treaty then the provision of the treaty shall prevail.
Section 22

The provisions regarding penalty in case of non-compliance with the lawful instruction of the authority or of the Court shall not be applied to the person served with a document calling for his appearance before an authority or the court in the Requesting State, if he is not a national of such state.

PART 5
Search and Seizure

Section 23

Upon receipt the request for assistance from a foreign state to search or seize and deliver any article, the Competent Authorities shall have the power to search or issue a warrant of search and size in accordance with the law if there shall be a reasonable ground to do so.

Section 24

As regards the search and seizure under Section 23, the provisions relating to search under the Criminal Procedure Code shall be applied, mutatis mutandis.

Section 25

The Competent Authorities conducting search or seizure of article in compliance with the request of assistance shall certify the continuity of custody, identity of the article, as well as integrity of its condition, and shall deliver the said article together with the certificate thereof to the Central Authority.

Section 36

The agency seeking assistance from foreign state shall present its request to the Central Authority.

Section 37

The request to seek assistance from a state including all documents to be sent thereto shall be in line with the forms, rules, means, and conditions defined by the Central Authority.

Section 38

The Central Authority shall consider whether it is appropriate according to regulation, details, facts and supporting documents, to request assistance from a foreign state, and then notify the requesting agency his determination thereof.
A determination of Central Authority in regard to the request seeking for assistance shall be final unless otherwise instructed by the Prime Minister.
Section 39

The requesting shall comply with the commitment of Thailand towards the Requested State regarding the confidentiality of the requested information or evidence unless such information or evidence is necessary for the public trial which is the consequence of the investigation, inquiry, prosecution or other criminal proceeding referred to in the request.

Section 40

No person entering to testify or give statement in Thailand in accordance with this Act shall be subject to service of process or be detained or subject to any other restriction of personal liberty by reason of any acts which proceeded his departure from the Requested State.

The safeguard in paragraph one shall cease when the person, having had the opportunity to leave Thailand within fifteen consecutives days after notification that his presence was no longer required by the appropriate authorities, shall have nonetheless stayed in or voluntarily returned after having left Thailand.

Section 41

All evidence and documents derived under this Act shall deemed as admissible for hearing
CHAPTER I General Provisions

Section 2 General Principles

1. The present Decree-Law and the legal regime arising therefrom shall ensure the satisfaction of the basic requirements for providing telecommunications services to the populations and public and private entities from the various activity sectors, through the creation of conditions conducive to the development and diversification of services of this nature.

2. The objective defined in subsection 2.1 shall conform to the following basic principles:

   a) Ensure the existence and availability of a universal service, consisting of a minimum range of telecommunications services provided
      within the national territory, on a permanent basis, with adequate quality conditions and at prices that can be afforded by all users;
   
   b) Ensure the financial and economic feasibility of the universal service through the granting of exclusivity in the provision of certain telecommunications services and the establishment of a compensation fund;
   
   c) Ensure that providers of competitive services are granted equal access to the market,
      i) while observing the rules for protecting competition;
   
   d) Ensure that users, under similar circumstances, are given equal treatment in the access to and use of telecommunications services.

Section 3 - Classification

1- Telecommunications means the transmission, reception or emission of a signal, representing symbols, writing, images, sounds or information of any nature by way of wires, optical systems, by electronic means or by other electromagnetic systems.

2- Depending on the nature of a user, telecommunications are classified as public or private. Public telecommunications are deemed to be those which aim to meet the generic collective need to transmit and receive messages and information.

CHAPTER II On public telecommunications

Section 12 - Public telecommunications service

1. Every public telecommunication service is provided under an exclusivity regime by the universal service operator, being governed by a concession contract to be entered into with the State.

2. Public telecommunication services are considered to be, notably:

   a) the mobile telecommunications service;
   
   b) the commuted data transmission service;
   
   c) the circuit hire service.
3. Excepted from subsection 12.1 are the provision of Internet services and the provision of value added services, with strict regard for the provisions of section 23, such services being deemed to be those which, having the fixed telephone service or the commuted data transmission service as their only support, do not require telecommunications infrastructure of their own and can be distinguished from the very services that serve as their support.

4. The telecommunications service provider referred to in the subsection above may be any natural or corporate person authorised by the regulatory entity to that effect, under the terms established by the applicable regulations.

Section 14 Interconnection

1. Interconnection shall be ensured through the basic telecommunications network and public telecommunications infrastructure.

2. Interconnection agreements between the universal service operator and operators or providers of telecommunications services shall not be subject to any rules and shall be entered into in accordance with the principles of transparency and non-discrimination.

3. Interconnection quality shall be equal to that provided by the universal service operator to itself, to companies where it holds stakes or to any entity to which interconnection is ensured.

4. Interconnection shall not be subject to unjustified interruptions or unavailability of services.

5. Any dispute relating to interconnection shall be submitted to the regulatory entity for arbitration, without prejudice to recourse to ordinary jurisdiction.

CHAPTER III - Common provisions - Section 15

Obligations of operators and providers of telecommunications services

Operators and providers of public telecommunications services shall furnish adequate and updated information on the terms and conditions for providing services that are part of the contracts to be entered into with clients, under the terms established by the regulations to be approved as a follow-up to the present Decree-Law.

2005 CRIMINAL PROCEDURE CODE

(Código de Processo Penal)

Pending submission in English version.

DECREE-LAW NO. 4/2005 OF SPECIAL REGIMES WITHIN THE CRIMINAL PROCEDURE

(…) In the fight against very serious forms of crime, such as terrorism and violent or highly organized crime, the need was felt to ensure the existence of instruments that are capable of responding to facts considered by society as deserving special prevention, combat, and punishment measures (…) Thus, for certain cases of terrorism and violent or highly organized crime, the present decree-law provides for special norms of criminal procedure to allow the conduct of home searches, checks, seizures and detentions outside of flagrante delicto without prior judicial authorization.
The objective of the present statute is to define special regimes in the area of criminal procedure to allow, without prior judicial authorization, the conduct of home searches, checks, seizures and detentions outside of flagrante delicto, as well as provide a special regime for the control of communications, in cases of terrorism and violent or highly organized crime.

For the purpose of the present statute, it can only be considered terrorism and violent or highly organized crime the conducts that:

b) Integrate crimes of terrorism, terrorist organization, or criminal association;
c) Are intentionally directed against the life, physical integrity, or liberty of persons and are punished with a maximum penalty equal to, or higher than, eight years;
d) Integrate crimes of serious drug trafficking, active and passive corruption, abuse of power, peculation, money laundering, unjust enrichment, and trafficking of persons or trafficking of arms, as long as the crime is committed in an organized way; or
e) Integrate crimes against the Rule of Law, coercion against constitutional organs, service or collaboration with enemy armed forces, acts of sabotage against national defence, and violation of State secrets or of diplomatic loyalty, as long as the crime is committed in an organized way.

In cases of terrorism or violent or highly organized crime, the order or authorization referred to in article 177.1 of the Code of Criminal Procedure may be requested to the judge of the places where the conversation or communication may eventually take place, or to the judge from the headquarters of the competent entity for the criminal investigation.

1. The Public Prosecutor Service may also order home searches in case of terrorism or violent or highly organized crime whenever there is well grounded circumstantial evidence of the imminent commitment of a crime that puts at risk the life or the physical integrity of any person.
2. In the cases referred to in the preceding paragraph, the home search operation shall be immediately communicated to the competent judge who shall examine it with a view to its validation, on pain of the home search being considered null and void.
Article 5 Checks

1. The Public Prosecution Service and the police authorities may also order checks in cases of terrorism or violent or highly organized crime whenever there is well grounded circumstantial evidence of the imminent commitment of a crime that puts at risk the life or the physical integrity of any person.
2. Police organs may also conduct checks without prior authorization or order in the circumstances referred to in the preceding paragraph.
3. In the cases referred to in the preceding paragraphs, the check operation shall be immediately communicated to the competent judge who shall examine with a view to its validation, on pain of the check operation being considered null and void.

Article 6 Seizures

1. The Public Prosecution Service and the police authorities may also order seizures in cases of terrorism or violent or highly organized crime whenever there is grounded circumstantial evidence of the imminent commitment of a crime that puts at risk the life or the physical integrity of any person.
2. The organs of police may also conduct seizures without prior authorization or order in the circumstances referred to in the preceding paragraph.
3. In the cases referred to in the preceding paragraphs, the seizure shall be immediately communicated to the competent judge who shall examine it with a view to its validation, on pain of the seizure being considered null and void.

Article 7 control of conversation or communications

In cases of terrorism or violent or highly organized crime, the order or authorization referred to in article 177.1 of the Code of Criminal Procedure may be requested to the judge of the places where the conversation or communication may eventually take place, or to the judge from the headquarters of the competent entity for the criminal investigation.
1999 PENAL CODE

Article 84.- Terrorism

1. Those who intend to oppose the people's administration and infringe upon the life of officials, public employees or citizens shall be sentenced to between twelve and twenty years of imprisonment, life imprisonment or capital punishment.
2. In the case of committing crimes by infringing upon physical freedom and/or health, the offenders shall be sentenced to between five and fifteen years of imprisonment.
3. In the case of committing crimes by threatening to infringe upon life or committing other acts of moral intimidation, the offenders shall be sentenced to between two and seven years of imprisonment.
4. Those who terrorise foreigners in order to cause difficulties to the international relations of the Socialist Republic of Vietnam shall also be penalized according to this Article.

2007 LAW ON LEGAL ASSISTANCE

Chapter III- LEGAL ASSISTANCE IN CRIMINAL MATTERS

Article 17. Scope of criminal legal assistance


Article 18. Criminal legal mandate dossiers

1. A criminal legal mandate dossier comprises the following documents: a) A competent proceedings-conducting body's written request for criminal legal assistance; b) The written criminal legal mandate prescribed in Article 19 of this Law. c) A criminal legal mandate dossier is made in three sets in accordance with this Law and the law of the requested country. Language used in the dossiers complies with Article 5 of this Law.


1. A criminal legal mandate document must contain the following details: a) Date, month, year and place of making the document; b) Name and address of the legal mandator; c) Name and address or head office of the legal mandatory; d) Full names and places of permanent residence or working of individuals, full names, addresses or head offices of agencies or organizations directly involved in the criminal legal mandate; dd) The jobs subject to criminal legal mandates, clearly indicating the mandate purpose; summarized contents of
the case, related circumstances, applicable legal provisions and penalties; schedule of investigation, prosecution and trial; the mandate performance duration.

2. In addition to the contents defined in Clause 1 of this Article, depending on each specific case and at the request of competent bodies of Vietnam or foreign countries, a criminal legal mandate document may cover the following contents:

a) Signs of identity, nationality and places of residence of subjects in the criminal case or persons having information relating to that case;

b) Matters to be questioned, questions to be asked, documents, dossiers or material evidences shown and, if possible, a description of characters and appearance of persons requested to produce documents, dossiers and material evidences with regard to evidence collection mandates;

c) Contents of jobs, questions and requests for summoned witnesses and experts;

d) Description of assets and places where assets need to be searched for; grounds for determining that the assets acquired from commission of crimes are located in the requesting country and may fall under the jurisdiction of the requesting country; the execution of court judgments or rulings on mandate for search, seizure of, or look for, confiscation of assets acquired from commission of crimes;

d) Measures applicable to the criminal legal mandate, which may lead to detection or recovery of assets acquired from commission of crimes;

e) Requests or procedures of the requesting country to ensure the effective performance of legal mandate, mode or form of supplying information, evidence, documents and articles;

f) The purpose, expected time and itinerary of the trip in case competent persons of the requesting country need to arrive in the territory of the requested country for the purpose related to the legal mandate;

g) The criminal judgment or ruling of a court and documents, evidence or other information necessary for the performance of legal mandates.

In case the information stated in the criminal legal mandate document defined in Clauses 1 and 2 of this Article is not sufficient for the performance of legal mandate, competent bodies of the requested country may also send documents to the requesting country, requesting the supply of additional information and fixing a specific deadline for reply on the additional results.

**Article 20. Requesting foreign countries to provide criminal legal assistance**

1. Vietnams competent proceedings-conducting bodies, in the course of handling criminal cases, may request competent foreign bodies to provide legal assistance in the following circumstances:

a) Service of paper, dossiers and documents on persons who are residing in the requested countries;

b) Summon of witness and experts who are living in the requested countries;

c) Collection or supply of evidence in the requested countries for settlement of criminal cases in Vietnam;

d) Examination of penal liability of persons who are staying in the countries of which they bear the nationality;

e) Other circumstances prescribed by Vietnamese law.

2. Requests for criminal legal assistance from foreign countries must be made in the form of criminal legal mandate under the provisions of this Law.

**Article 26. Supply of information**

Upon request of competent bodies of Vietnam or foreign countries, the Supreme Peoples Procuracy shall request competent bodies of foreign countries or competent proceedings-conducting bodies of Vietnam to supply information relating to criminal legal assistance requests or copies of the criminal judgments or rulings of courts which have taken legal effect on citizens of the requesting countries.

**Article 27. Use of information and evidence in criminal legal assistance**

1. Information or evidence supplied by competent proceedings-conducting bodies of Vietnam may be used only for the purposes stated in the criminal legal mandates, must not be disclosed or transferred, unless prior written consent of competent bodies of Vietnam is obtained.

2. Competent proceedings-conducting bodies of Vietnam shall apply appropriate measures to keep secret criminal legal mandates, mandate contents, enclosed documents and criminal proceedings to be conducted under legal mandates. In case of non-performance of criminal legal mandates of foreign countries under the law on
Article 28. Request for penal liability examination; hand-over of files and material evidence of cases to foreign countries

1. For cases involving foreigners who committed crimes in the Vietnamese territory but have fled abroad and Vietnam has made an extradition request which was, however, rejected by foreign competent bodies, the agencies which are handling the cases shall transfer the case files to the Supreme Peoples Procuracy for requesting the countries where the offenders are present to continue with the penal liability examination. When deciding to transfer the case files, the Supreme Peoples Procuracy may also transfer material evidence of the cases.

2. The Supreme Peoples Procuracy shall prescribe specific conditions for receipt and transfer of case files and material evidence.

2003 CRIMINAL PROCEDURE CODE

Part Eight- INTERNATIONAL COOPERATION
Chapter XXXVI - GENERAL PROVISIONS ON INTERNATIONAL COOPERATION IN CRIMINAL PROCEEDINGS

Article 340.- Principles for international cooperation in criminal proceedings

International cooperation in criminal proceedings between the bodies with procedure-conducting competence of the Socialist Republic of Vietnam and foreign authorities with corresponding competence shall be effected on the principles of respect for each other’s national independence, sovereignty and territorial integrity, non-intervention in each other’s internal affairs, equality and mutual benefit, compliance with the Constitution of the Socialist Republic of Vietnam and fundamental principles of international laws.

International cooperation in criminal proceedings shall be carried out in conformity with the international agreements which the Socialist Republic of Vietnam has signed or acceded to and the laws of the Socialist Republic of Vietnam.

Where the Socialist Republic of Vietnam has not yet signed or acceded to relevant international agreements, the international cooperation in criminal proceedings shall be effected on the principle of reciprocity but in contravention of the laws of the Socialist Republic of Vietnam, international laws and international practices.

Article 341.- Provision of judicial assistance

When rendering judicial assistance, the bodies as well as persons with procedure-conducting competence of the Socialist Republic of Vietnam shall apply the provisions of relevant international agreements which the Socialist Republic of Vietnam has signed or acceded to and the provisions of this Code.
The bodies with procedure-conducting competence of the Socialist Republic of Vietnam may refuse to implement judicial assistance requests in criminal proceedings in one of the following cases:
1. Judicial assistance requests fail to comply with the international agreements which the Socialist Republic of Vietnam has signed or acceded to and the laws of the Socialist Republic of Vietnam;
2. The implementation of judicial assistance requests is detrimental to the national sovereignty, security or other important interests of the Socialist Republic of Vietnam.

### 2016 LAW ON NETWORK INFORMATION SECURITY

*(Law N. 86/2015/QH13)*

#### CHAPTER I GENERAL PROVISIONS

#### Article 1. Scope

This law provides regulations on network information security activities, rights and duties of agencies, organizations and individuals in securing network information security; civil cryptography; technical standards and norms of network information security; business in information security; human development for network information security; state management of network information security;

#### Article 2. Subject of application

This law shall apply to any Vietnamese agencies organization, individual; foreign organization and individual in Vietnam who directly involves in or is related to network information security activities in Vietnam.

#### Article 3 Definitions

In this Law, the following terms shall be construed as follows:
1. Network information security means the protection of network information and information systems against any illegal access, use, disclosure, interruption, amendment or sabotage in order to ensure the integrity, confidentiality and availability of information.
2. Network is the environment where information is supplied, transmitted, collected, processed, stored and exchanged via telecommunication networks and computer networks.
3. Information system means any assembly of hardware, software and database which is purposely set up for establishment, supply, communication, collection, handling, storage and exchange of network information.
4. National important information system means an information system that any of its sabotage will result in damage particularly serious to national defense and security.
5. Information system owner means an organization or individual who has the power to directly manage its/his/her own information system.
6. Violation of network information security means an act of illegal access to, use, disclosure, interruption, amendment or sabotage of information or information system.
7. Information security incident means a failure of information or an information system with consequent impacts on its confidentiality, integrity or availability.
8. Information security risk means a subjective or objective factor that potentially affects the status of network information security.
9. Information security risk assessment means detection, analysis and estimation of a damage or threat to information or information system.
10. Information security risk management means providing a set of measures to reduce network information...
security risks.

11. Malicious software (Malware) means a software that is able to cause any abnormal operation to an information system in part or in whole, or to illegally reproduce, change, or delete information stored in the information system.

12. Malware filter system means a combination of hardware and software connected to a network in order to detect, block, filter and reckon malware up.

13. Electronic address means an address in use for sending and receiving cyber information that can be an email address, telephone number, Internet address and other similar forms.

14. Information conflict means two or more local and foreign organizations taking measures of information technology or technique to damage an information system, a program or an information source.

15. Personal information means information associated with the identity of a specific person.

16. Personal information owner means the person identified by the personal information.

17. Handling personal information means performance of one or more operations to collect, edit, use, store, supply, share, and disperse personal information in the network for commercial purposes.

18. Civil cryptography means cryptographic techniques and encrypted products in use for confidentiality or authentication of the information which is beyond the domain of state secret. 19. Network information security product means any hardware or software product which is functioned to protect information and information system.

20. Network information security service means the service to protect information and information system.

**Article 6 International cooperation on network information security**

1. International cooperation on network information security should abide by the principles as follows:
   a) Respecting the independence, sovereignty and territorial integrity of countries without intervention in internal affairs of the others, for equality and mutual benefits;
   b) Complying with Vietnam laws and international treaties to which the Socialist Republic of Vietnam is a state member.

2. Contents of international cooperation on network information security:
   a) International cooperation on research and application of science, technique and engineering of network information security;
   b) International cooperation in prevention and fighting against illegal acts in relation with network information security, and against the abuse of information network for terrorist acts; c) Other international cooperation on network information security.

**Article 7 Prohibited acts**

1. Illegal prevention of network information transmission; intervention, access, damaging, deletion, change, reproduction and misleading of network information.

2. Illegal affecting, blocking the normal operation of an information system or legal access possibility of users to an information system.

3. Attack, illegal invalidation to disable the measures in place to protect network information security for an information system; attack, illegal appropriation of rights to control, and sabotage of an information system.

4. Sending spams, malware, establishing a fake or swindling information system.

5. Illegal collection, use, dissemination of or trading in personal information of others; exploitation of a weakness point of an information system to collect and exploit personal information.

6. Illegal access to the confidential code and legally encoded information of agencies, organization, or individuals; disclosure of information of civil code products; use of and trading in civil code products of unclear origin.
CHAPTER II ASSURANCE OF NETWORK INFORMATION SECURITY

Section 1 NETWORK INFORMATION PROTECTION

Article 9. Classification of information

1. The organization with information in its possession shall classify it by confidentiality in order to take appropriate protection measures.
2. Information in the domain of state secret shall be classified and protected as set forth in regulations on protection of state secrets. The organization using classified or unclassified information for activities in its field shall be responsible for establishing regulations and procedures to handle information, to determine the contents and methods to record permitted accesses to classified information.

Article 10 Administration of information sending

1. Sending network information shall ensure the requirements as follows:
   a) not faking the sending source;
   b) complying with regulations herein and relevant laws.
2. Organizations, individuals must not send commercial information to a recipient’s electronic address without his/her prior consent, request, or when the recipient refuses it, except for the cases where the recipient is obliged to receive the information under current laws.
3. Telecommunications companies, enterprises providing telecommunications application services, and enterprises rendering information technology services that send information shall:
   a) Comply with legal regulations on information storage, and protection of personal information and private information of organizations, individuals;
   b) Take measures to stop and respond upon receipt of any notice from organizations, individuals of sending information in violation of legal regulations;
   c) Make it available for recipients to have rights to refuse further receive information;
   d) Provide technical and professional conditions necessary for competent state bodies to, upon request, perform duties of state administration of network information security.

Article 11 Prevention, detection, blocking and treatment of malware

1. Agencies, organizations, and individuals shall be responsible for prevention and blocking of malware as instructed or required by competent state bodies.
2. Owners of national important information systems shall deploy professional and technical systems to prevent, detect, block and handle malware in due time.
3. Organizations shall provide services of email, information transmission and storage shall have malware filtration systems in place during sending, receiving, and storing of information in their own systems and shall report to competent agencies as stipulated by laws.
4. Internet service providers shall take measures to manage, prevent, detect, and block the dispersal of malware and treatment thereof upon request of competent state bodies.
5. The Ministry of Information and Communications shall be in charge and cooperate with the Ministry of Defense, the Ministry of Public Security, relevant ministries, sectors for organizing to prevent, detect, block and handle malware that is causative of impacts in national defense and security.

Article 12 Assurance of telecommunication resources

1. Organizations, individuals using telecommunication resources shall:
   a) Take managerial and technical measures to avoid information insecurity that is originated from their own frequencies, stocks of numbers, domain names and Internet addresses;
   b) Provide, upon request, information relating to security of telecommunications resources and cooperate with competent agencies.
2. Internet service providers shall manage, cooperate and avoid information insecurity that is originated from their own Internet resources and clients, provide sufficient information upon request of competent state bodies; cooperate for connection and routing in order to secure safe and stable operations of the Vietnam domain name server system.

3. The Ministry of Information and Communications shall be responsible for network information security for the Vietnam domain name servers.

**Article 13 Response to network information security incidents**

1. A response to network information security incidents means an activity to handle with and remedy any incidents causative of network information insecurity.

2. Any response to a network information security incident shall comply with the principles as follows:
   a) Timely, speedy, accurate and effective;
   b) Compliant with legal regulations on coordination of responses to network information security incidents;
   c) Cooperative between local and foreign agencies, organizations and businesses.

3. Ministries and equivalents, agencies under the Government, People’s Committees of provinces and cities subordinate to the Central Government, telecommunications companies, and owners of national important information systems shall establish or appoint specialized divisions in charge of responses to network information security incidents.

4. The Ministry of Information and Communications shall coordinate nationwide responses to network information security incidents and detail the coordination of responses to network information security incidents.

**Article 14 Emergency response to secure national network information security**

1. Emergency response to secure national network information security means urgent response in case of catastrophic circumstance or upon request of competent agencies in order to secure national network information security.

2. Emergency response to secure national network information security shall comply with the principles as follows:
   a) Organization and implementation as decentralized;
   b) Action in a rapid, strict and close coordinative manner;
   c) Application of scientific and engineering measures to ensure effectiveness and feasibility.

3. The system of emergency responses to secure national network information security includes:
   a) Emergency response plan to secure national network information security;
   b) Emergency response plan for urgent responses to secure network information security of state bodies, political and social-political organizations;
   c) Emergency response plan for urgent responses to secure network information security of localities;
   d) Emergency response plan for urgent responses to secure network information security of telecommunications companies.

4. The responsibility of concerned parties for coordination to secure national network information security is as follows:
   a) The Prime Minister makes decisions on the plans for emergency response to secure national network information security;
   b) The Ministry of Information and Communications shall direct and coordinate to secure national network information security;
   c) Ministries, sectors and local authorities shall coordinate and direct emergency responses to secure network information security at ministries, sectors and localities;
   d) Telecommunications companies shall implement and coordinate with the Ministry of Information and Communications and relevant ministries, sectors and localities to secure national network information security.

**Article 15 Responsibilities of organizations, individuals in network information security**

1. Agencies, organizations, individuals involving in network information security activities shall cooperate with competent state bodies and other organizations, individuals in securing network information security.

2. Agencies, organizations, individuals using network services shall timely inform the service provider or response-specialized division on detection of any act of sabotage or network information security incident.
Article 16 Principles of personal information protection in network

1. Individuals using network services shall protect their own personal information and compliance with laws on supply of personal information.
2. Organizations, individuals handling personal information shall ensure network information security for the personal information they handle.
3. Organizations, individuals handling personal information shall build up and publicize their policies applicable to handling and protection of personal information of their own organizations, individuals.
4. Personal information protection shall adhere to regulations of this Law and specific regulations of relevant fields.
5. Handling of personal information for the purpose of national defense, security, social order and security or for non-commercial purposes shall observe other regulations of relevant laws.

Article 17 Collection and use of personal information

1. Organizations, individuals handling personal information shall:
a) Collect personal information only after obtaining the consent of information owner on the scope and purpose of the information collection and use;
b) Use collected personal information for any purpose different from the initial one only after obtaining the personal information owner's agreement.
c) Must not share, disperse the collected, accessed or controlled personal information to any third party, unless it is agreed by the personal information owner or requested by competent state bodies.
2. State bodies shall be responsible for the confidentiality and storage of personal information that they collect.
3. The personal information owner shall have rights to require any organization, individual handling personal information to provide his/her personal information that is collected and stored by the organization, individual.

Article 18 Updating, change and deletion of personal information

1. The personal information owner shall have rights to require organizations, individuals handling personal information to update, change, and delete his/her personal information that the handling organizations, individuals collect, store or to cease, if he/she previously agrees on, the supply of his/her personal information to a third party.
2. Upon receipt of a valid requirement of updating, change or deletion of personal information from the owner or a valid requirement of ceasing the supply of his/her personal information to a third party, organizations, individuals handling personal information shall:
a) Fulfill the requirement and notice the personal information owner thereof or provide the personal information owner with rights to access, update, change or delete his/her own personal information;
b) Take suitable measures to protect personal information; notice the personal information owner thereof in cases that it is not yet possible to fulfill the requirement due to technical or other factors.
3. Organizations, individuals handling personal information shall delete the stored personal information when the purpose of use is accomplished or the storage period expires and shall notice the personal information owner thereof, unless otherwise stipulated by laws.

Article 19 Protection of personal information security in network

1. Organizations, individuals handling personal information shall take appropriate managerial and technical measures to protect personal information that they collect and store; comply with technical standards and norms of network information security.
2. In cases of technical incidents or risks thereof, organizations, individuals handling personal information are required taking remedial, blocking measures as soon as possible.
Article 20. Obligations of state administration agencies in network personal information protection

1. Establishing online information channels to receive feedbacks and recommendations by organizations, individuals in relation with personal information security.
2. Periodically inspecting, examining organizations and companies handling personal information; inspecting without prior notice when needed.

Section 3 INFORMATION SYSTEM PROTECTION

Article 21 Classification in security of information systems

1. Security classification of an information system means determination of its network information security level in the increment order from 1 to 5 to take managerial and technical measures to protect it accordingly.
2. Information system shall be categorized into security levels as follows:
   a) Level 1 is the level that when an information system is sabotage, it will damage legitimate rights and benefits of organizations, individuals, not public benefits, social order and safety, national defense or security;
   b) Level 2 is the level that when an information system is sabotage, it will severely damage legitimate rights and benefits of organizations, individuals, damage public benefits, not social order and safety, national defense or security;
   c) Level 3 is the level that when an information system is sabotage, it will severely damage production, public benefits, social order or damage safety, national defense or security;
   d) Level 4 is the level that when an information system is sabotage, it will extremely damage public benefits, social order or damage safety, or severely damage national defense or security;
   e) Level 5 is the level that when an information system is sabotage, it will extremely damage national defense or security;
3. The Government shall stipulate details of criteria, power, sequence and procedures to determine the security levels of information systems responsibilities for securing network information security at every level.

Article 22. Duties on information system protection

1. To determine security levels of information systems
2. To assess and manage security risks to information systems.
3. To urge, supervise and examine the protection of information systems.
4. To take measures to protect information systems.
5. To comply with the reporting regime.
6. To conduct public information for raising awareness about network information security.

Article 23 Measures to protect information systems

1. Issuing regulations on network information security in designing, construction, management, operation, use, and cancellation of information systems.
2. Applying technical measures in accordance with technical standards and norms of network information security to prevent, avoid of and remedy network information security incidents.
3. Inspecting and monitoring of the compliance with regulations and evaluation of effectiveness of managerial and technical measures in use.
4. Monitoring of information system security.
Article 24 Monitoring security of information system

1. Monitoring security of information system is action to select subjects, tools for monitoring, collecting and analyzing information status of the monitored subjects to identify the factors that might constitute impacts on the information system; to report and warn of any act of violation of network information security or any act that might cause any network information security incident to the information system; to analyze the crucial key factors that affect the network information security status; to recommend changes in technical measures.

2. Subjects to safety status monitoring include: firewall, access control, main information route, important server, device or terminal.

4. Telecommunications companies, information technology service providers and network information security service providers shall cooperate with information system owners in monitoring of information system safety upon request of competent state bodies.

Article 25 Responsibilities of information system owners

1. Information system owners shall protect information systems pursuant to regulations in Articles 22, 23 and 24 of this law. 2. Information systems owners using state budget shall perform according the responsibilities set forth in item 1 hereof and shall:
   a) Have plans for network information protection that are appraised by competent state bodies when the information system is established, expanded or upgraded.
   b) Appoint individual(s) or division(s) in charge of network information security.

Article 26 National important information systems

1. The establishment, expansion and upgrading of national important information system shall be subject to network information security auditing prior to operation and exploitation.

2. The Ministry of Information and Communications shall preside over and cooperate with the Ministry of Defense, the Ministry of Public Security and relevant ministries and sectors to prepare a list of national important information systems and submit for the Prime Minister to issue.

Article 27 Responsibilities for securing network information security for national important information systems

1. Owners of national important information systems shall:
   a) Implement regulations set forth in Article 25.2 of this Law;
   b) Periodically assess network information security risks. This shall be done by a specialized organization that is appointed by competent authorities;
   c) Deploy standby solutions for information systems;
   d) Make protective plans and maneuver plans for protecting national important information systems.

2. The Ministry of Information and Communications shall:
   a) Preside over and cooperate with owners of national important information systems, the Ministry of Public Security and relevant ministries and sectors to instruct, supervise, inspect and examine activities of network information security protection for national important information systems, except for the systems set forth in items 3 and 4 of this Article;
   b) Require telecommunications companies, information technology companies to participate in technical consultancy, support and response to network information security incidents for information systems of national importance.

3. The Ministry of Public Security shall preside over, instruct, supervise, inspect and examine activities of network information security protection for national important information systems under its administration; cooperate with the Ministry of Information and Communications, relevant owners of national important information systems, ministries, sectors and People's Committees at various levels in safeguarding national important information systems upon request of competent agencies.

4. The Ministry of Defense shall preside over, instruct, supervise, inspect, and examine network information security protection activities for national important information systems under its administration.
5. The Government Information Security Commission shall preside and apply encoding solutions to national important information systems that belong to state bodies, political and social-political organizations; cooperate with owners of national important information systems in network information security monitoring under current laws.

### Section 4 PREVENTION OF NETWORK INFORMATION CONFLICTS

#### Article 28 Responsibilities of organizations and individuals in prevention of network information conflicts

1. Organizations and individuals shall, within their duties and power:
   a) Prevent sabotage information from their own information systems; cooperate to identify sources, drive back and remedy consequences of cyber attacks via information systems of local and foreign organizations and individuals.
   b) Block any act of domestic or foreign organizations and individuals that is aimed at sabotage of the network integrity.
   c) Eliminate the implementation of illegal acts by local and foreign organizations and individuals on the network that severely affects national defense and security, social order and security.
2. The Government shall provide details for prevention of network information conflicts.

#### Article 29 Prevention of network use for the purpose of terrorism

1. Measures to stop network use for the purpose of terrorism include:
   a) Neutralization of the Internet source in use for the terrorist act;
   b) Blocking the establishment and expansion of information exchange in relation to signals, factors, methods and usages of the Internet for the purpose of terrorism, targets and operations of cyber terrorism organizations;
   c) Exchange of experiences and practices in controlling of Internet sources, chase and control of contents of websites having terrorist purposes;
2. The Government shall provide details of responsibilities for implementation and measures to stop network use for the purpose of terrorism.

### 2018 LAW ON CYBER SECURITY

#### Chapter I GENERAL PROVISIONS

#### Article 2. Definitions In this Law, the following terms are construed as follows:

1. Cybersecurity means the assurance that activities in cyberspace will not cause harm to national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals.
2. Cybersecurity protection means the prevention, detection, avoidance of and dealing with acts which infringe cybersecurity.
3. Cyberspace means the connected network of information technology [IT] infrastructure comprising telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases, where [being the environment in which] people perform social acts without being limited by space and time.
5. National cyberspace infrastructure means the system of technical and material facilities in order to [which] create, transmit, collect, process, archive and exchange information in national cyberspace comprising: (a) Transmission systems comprising the national transmission system, internationally connected transmission systems, satellite systems and transmission systems of enterprises providing services on telecom networks and on the Internet and other added value services in cyberspace; (b) Core service systems comprising the national...
information flow and navigation system, the national domain name resolution system (DNS), the national authentication system [public key infrastructure system] (PKI/CA), service supply systems for Internet connection and access of service providers on telecom networks, the Internet and [providers of] other added value services in cyberspace; (c) IT services and applications comprising online services; and IT applications with network connection serving management and operation by agencies, organizations and important financial and economic groups; and the national database. Online services comprise e-government, e-commerce, websites, online forums, social networking and blogs; (d) IT infrastructure of smart cities2, the internet of things, complex virtual reality systems, cloud computing, large data systems, fast data systems and artificial intelligence systems.

6. International network gateway means the place where transmission and reception of network signals takes place between Vietnam and other countries and territories.

7. Cybercrime means activities of using cyberspace, IT or e-facilities to commit a crime as regulated [defined] in the Criminal Code.

8. Cyberattack means an act of using cyberspace, IT or e-facilities to destroy [hack] and/or interrupt the operation of telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases or e-facilities of agencies, organizations and individuals.

9. Cyberterrorism means using cyberspace, IT or e-facilities to commit an act of terrorism or terrorist financing.

10. Cyberespionage means a deliberate act of bypassing a warning, access code, other code or firewall or using the administration right of another person or other means to unlawfully appropriate or collect information or information resources on a telecom network, the Internet, a computer network, an information system, an information processing and control system, a database or e-facility of an agency, organization or individual.

11. Digital account means information used to authenticate, verify and/or delegate power to use applications and services in cyberspace.

12. Cybersecurity threat means a situation occurring in cyberspace which presents indications of a threat to infringe national security, and/or to cause serious harm to social order and safety and/or to the lawful rights and interests of agencies, organizations and individuals.

13. Cybersecurity incident [or breakdown] means any unusual occurrence in cyberspace which infringes upon national security, social order and safety and/or the lawful rights and interests of organizations and individuals.

14. Dangerous cybersecurity situation means an occurrence in cyberspace when there is an act which seriously infringes national security [or] causes particularly serious harm to social order and safety and/or to the lawful rights and interests of agencies, organizations and individuals.

Article 4. Principles of cybersecurity protection

1. Compliance with the Constitution and law; ensuring the interests of the State and the lawful rights and interests of agencies, organizations and individuals.

2. Leadership by the Vietnamese Communist Party and uniform administration by the State; mobilization of the combined strength of the political system and the entire nation; and development of the key role of the Cybersecurity Task Force.

3. Close association between tasks for protecting cybersecurity and information systems critical for national security with the tasks for socio-economic development, ensuring human rights and civil rights, and facilitating [all] agencies, organizations and individuals to conduct activities in cyberspace.

4. Proactive prevention, detection, ending, fighting and defeating all acts using cyberspace to infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals; and readiness to prevent any cybersecurity threat.

5. Implementing cybersecurity protective activities for the national cyberspace infrastructure; applying measures to protect information systems critical for national security.

6. Information systems critical for national security shall be evaluated and certified as satisfying cybersecurity conditions prior to their commissioning for operation and use, and shall be regularly inspected [audited] and supervised for cybersecurity during the process of their use, with prompt response to and remedying of any cybersecurity incident.

7. Any act in breach of the law on cybersecurity must be promptly and strictly dealt with.

Article 7. International cooperation on cybersecurity

1. International cooperation on cybersecurity is conducted on the basis of respect for independence, sovereignty and territorial integrity, of non-interference in each other's internal affairs, equality and mutual benefit.

2. The contents of international cooperation on cybersecurity comprise:
   a) Research and analysis of the orientation of cybersecurity;
   b) Formulation of regimes and policies which promote cooperation regarding cybersecurity activities between
Vietnamese organizations and individuals on the one hand with foreign and international organizations on the other hand;
c) Sharing of information and experience; and assistance with training, equipment and technology which pro-
tects cybersecurity; (d) Preventing and combating cybercrime, and acts infringing cybersecurity; and preventing cybersecurity threats;
dd) Consultancy, training and development of cybersecurity [protective] human resources;
e) Arranging international seminars, conferences and forums on cybersecurity;
g) Acceding to and implementing international treaties and agreements on cybersecurity;
h) Implementing programs and projects on international cooperation on cybersecurity.
i) Undertaking other activities of international cooperation on cybersecurity.
3. The Ministry of Public Security is responsible before the Government to preside over coordination in conduct-
ing international cooperation on cybersecurity, except for those activities of international cooperation under the authority of the Ministry of National Defence. The Ministry of National Defence is responsible before the Gov-
ernment to conduct international cooperation on cybersecurity within the managerial scope of such ministry. The Ministry of Foreign Affairs is responsible to coordinate with the Ministry of Public Security and the Ministry of National Defence in conducting international cooperation on cybersecurity. The Government shall make a decision in a case where international cooperation on cybersecurity falls within the responsibility of a number of ministries and branches [line ministries].
4. Any other Ministry, line ministry or locality [wishing to] undertake activities of international cooperation on cybersecurity must first obtain a written opinion from the Ministry of Public Security prior to undertaking same, except in the case of activities conducted by the Ministry of National Defence.

CHAPTER 3
PREVENTION OF AND DEALING WITH AN INFRINGEMENT OF CYBERSECURITY

Article 18. Prevention of and combatting use of cyberspace, information technology and electronic media in order to breach the law on national security, social order and safety.

1. Conduct being the use of cyberspace, IT and electronic media in order to breach the law on national security, social order and safety comprises: (a) Posting and/or disseminating information in cyberspace with the contents prescribed in clauses 1 to 5 of article 16 and the conduct prescribed in article 17.1 of this Law; (b) Appropriating assets/property; organizing gambling including gambling via the Internet; stealing international telecom charges on the Internet; and breaching copyright and intellectual property rights in cyberspace; (c) Falsifying websites of agencies, organizations or individuals; forging, circulating, stealing, buying or selling, collecting or exchanging unauthorized credit card information or bank accounts of other people; unlawfully issuing, providing or using payment means; (d) Disseminating, advertising or purchasing and selling goods or services on the list of those prohibited by law; (dd) Guiding other people to conduct acts in breach of law; (e) Other acts of using cyberspace, IT or e-facilities to breach the law on national security, social order and safety
2. Cybersecurity Task Forces are responsible to prevent and combat conduct being the use of cyberspace, IT, or e-facilities to breach the law on national security, social order and safety.

Article 19. Prevention of and combating cyberattacks

1. Acts constituting a cyberattack and cyberattack-related acts comprise: (a) Distributing informatics programs which cause harm to a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility; (b) Hindering, disordering, paralyzing, interrupting or stop-
ping the operation of, and/or illegally preventing the transmission of data by a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility; (c) Infiltrating, harming or appropriating data stored or transmitted on a telecom network, the Internet, a computer network, information systems, information processing and control systems, database or e-facility; (d) Infiltrat-
ing, creating or exploiting security vulnerabilities or weaknesses and system services in order to appropriate information and/or to earn illicit profit; (dd) Producing, purchasing and selling, exchanging or donating tools, devices [equipment] and software with the function of attacking a telecom network, the Internet, a computer network, information system, information processing and control system, database or e-facility in order to use such objects [tools, devices and software] for illegal purposes; (e) Performing other acts which affect the normal
operation of any telecom network, the Internet, computer network, information system, information processing and control system, database or e-facility.

2. Information system administrators are responsible to apply technical measures to prevent and avoid the acts prescribed in sub-clauses (a), (b), (c), (d) and (e) of clause 1 above with respect to information systems within their managerial scope.

3. When a cyberattack occurs and infringes or threatens to infringe national sovereignty, interests and security and/or causes serious harm to social order and safety, the Cybersecurity Task Force shall preside over coordination with information system administrators and relevant organizations and individuals to apply measures to determine the origin of the cyberattack and collect evidence; and shall require enterprises providing services on telecom networks, the Internet and other added value services on cyberspace [cyberspace service providers] to block and filter information in order to prevent and eliminate acts of cyberattack, and shall promptly provide complete relevant information and data.

4. The responsibility to prevent and combat cyberattack is regulated as follows: (a) The Ministry of Public Security shall preside over coordination with relevant Ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article which infringe or threaten to infringe national sovereignty, interests and security or cause serious harm to social order and safety throughout the entire country, except in the cases prescribed in subclauses (b) and (c) below; (b) The Ministry of National Defence shall preside over coordination with relevant Ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article with respect to military information systems; (c) The Government Cipher Committee shall preside over coordination with ministries and line ministries to prevent, detect and deal with the acts prescribed in clause 1 of this article with respect to cipher information systems under such Committee.

Article 20. Prevention of and combating cyberterrorism

1. Competent State agencies are responsible to apply measures stipulated in this Law, article 29 of the law on network information security and the law on prevention of and combating against terrorism, to deal with cyberterrorism.

2. Information system administrators shall regularly review and inspect information systems within their managerial scope in order to eliminate cyberterrorism threats.

3. Any agency, organization or individual which detects any indication or any act of cyberterrorism must promptly notify a CTF thereof. An agency receiving such notice is responsible to receive complete/full news of such cyberterrorism and promptly notify same to the CTF.

4. The Ministry of Public Security shall preside over coordination with relevant Ministries and line ministries to prevent and combat cyberterrorism, to apply measures to neutralize cyberterrorism sources, to deal with cyberterrorism, and to minimize consequences occurring to information systems, except in the cases prescribed in clauses 5 and 6 of this article.

5. The Ministry of National Defence shall preside over coordination with relevant Ministries and line ministries to prevent and combat cyberterrorism, and to apply measures to deal with cyberterrorism occurring to military information systems.

6. The Government Cipher Committee shall preside over coordination with relevant Ministries and line ministries to prevent and combat cyberterrorism, and to apply measures to deal with cyberterrorism occurring to cipher information systems under such Committee.

Article 25. Protection of cybersecurity of national cyberspace infrastructure and international network gateways

1. The protection of cybersecurity of the national cyberspace infrastructure and international network gateways must closely combine requirements on cybersecurity protection with requirements on socio-economic construction and development; international network gateways are encouraged to be located within the territory of Vietnam; and organizations and individuals are encouraged to participate in investment in building national cyberspace infrastructure.

2. Agencies, organizations and individuals managing and operating national cyberspace infrastructure and international network gateways have the following responsibilities: (a) To protect cybersecurity within the scope of their managerial authority; to be subject to management, investigation and inspection by, and to comply with requirements on cybersecurity protection of competent State agencies; (b) To facilitate and implement necessary technical measures and professional activities when requested in order for competent State agencies to perform cybersecurity protective tasks.
Article 26. Guarantees relating to information security in cyberspace

1. Websites, portals [and] specialized pages on social networks of agencies, organizations and individuals must not provide, upload or transmit any information with the contents prescribed in clauses 1 to 5 of article 16 of this Law and other information containing contents infringing national security.

2. Any domestic or foreign enterprise which provides services on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service provider] has the following responsibilities: (a) To authenticate information when a user registers a digital account; to maintain confidentiality of information and accounts of users; to provide user information to the Cybersecurity Task Force under the Ministry of Public Security when so requested in writing in order to serve investigation of and dealing with breaches of the law on cybersecurity; (b) To prevent the sharing of information and to delete information with the contents prescribed in clauses 1 to 5 inclusive of article 16 of this Law on services or information systems directly managed by any agency or organization no later than twenty four (24) hours after the time of a request from the CTF under the Ministry of Public Security or from a competent agency under the Ministry of Information and Communications, and to save/maintain system logs in order to serve investigation of and dealing with breaches of the law on cybersecurity within a [specified] period [to be] stipulated by the Government; (c) Not to provide or to cease provision of services on telecom networks and on the Internet and other value added services to organizations and individuals who upload in cyberspace information with the contents prescribed in clauses 1 to 5 of article 16 of this Law, when requested by the CTF under the Ministry of Public Security or by a competent agency under the Ministry of Information and Communications.

3. Domestic and foreign service providers on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service providers] carrying out information, data about service users’ relationships and data generated by service users in Vietnam must store such data in Vietnam for a [specified] period [to be] stipulated by the Government. Foreign enterprises referred to in this clause must have branches or representative offices in Vietnam.

4. The Government shall provide detailed regulations on clause 3 of this article.

DECREE NO.55/2001/ND-CP ON THE MANAGEMENT, PROVISION, AND USE OF INTERNET SERVICES

CHAPTER I
General Provisions

Article 1

1. The management, provision and use of internet services in Vietnam shall be governed by this Decree. All domestic organizations and individuals; foreign organizations and individuals engaged in the internet sector in Vietnam must comply with this Decree.

2. Where an international treaty relating to the internet to which the Socialist Republic of Vietnam is a signatory or participant contains provisions which are inconsistent with this Decree, the international treaty shall prevail.

Article 2

1. The internet is an information system which is connected in the form of Internet Protocol (IP) and uses a system of global uniform addresses aimed at providing different services and applications to users.

2. In Vietnam, the internet is an important part of the national information infrastructure, shall be protected by law and shall not be interfered with by any person. All State bodies, organizations and individuals shall be responsible for ensuring safety and security of systems of equipment and information on the internet.
Article 6

1. Information which is retained, transmitted and received from the internet must comply with the relevant provisions of the Law on Media, the Law on Publication, the Ordinance on Protection of State Secrets and the laws relating to intellectual property and management of information on the internet.
2. Organizations and individuals providing and using internet services shall be responsible for information retained or transmitted by them on the internet.

Article 8

Confidentiality of private information of organizations and individuals on the internet shall be ensured in accordance with the provisions of the Constitution and the law. The authorized State body shall control information on the internet in accordance with the provisions of the law.

Article 9

No person shall be permitted to obstruct the lawful right to use internet services. Entities and enterprises providing internet services shall be entitled to refuse to provide services in the case where an organization or individual using such services breaches the laws relating to the internet.

Article 10

The coding and decoding of information on the internet must comply with the laws relating to encryption.

Article 11

The following acts shall be prohibited:
1. Disabling or destroying systems of equipment and obstructing the provision and use of internet services.
2. Stealing and illegally using passwords, encryption codes and private information of organizations and individuals on the internet.
3. Abusing the internet to oppose the State of the Socialist Republic of Vietnam; disrupting security and order; infringing upon ethics and fine customs, and committing other breaches of the law.

CHAPTER II Establishment of Systems of Equipment, Provision and Use of Internet Services

Article 13

Enterprises providing internet services shall include the following:
1. Internet access service providers (ISPs), being enterprises in all economic sectors which are issued by the General Department of Posts and Telecommunications with a licence to provide internet access services. Internet access service providers must comply with this Decree and the regulations on management of internet access services issued by the General Department of Posts and Communications.
2. Internet connection service providers (IXPs), being State owned enterprises or shareholding companies in which the State holds a controlling share or special share which are issued by the General Department of Posts and Telecommunications with a licence to provide internet connection services. Internet connection service pro-
providers must comply with this Decree and the regulations on management of internet connection services issued by the General Department of Posts and Communications.

Article 23

Internet resources shall include the system of names and numbers used for the internet which are uniformly identified globally. In Vietnam, internet resources shall from part of national information resources which should be managed, planned and used effectively.

Article 24

The State shall implement an appropriate policy on management in order to facilitate internet access or connection service providers in gradually reducing prices or tariff of internet access or connection services to a rate equal to or lower than the average rate of other countries in the region aimed at rapidly universalizing the internet in Vietnam and improving the competitiveness of Vietnamese enterprises during international economic integration.

Article 25

Organizations and individuals producing or importing systems of equipment, providing internet services and using internet resources shall be responsible for paying taxes, charges and fees in accordance with the provisions of the law. Preferential tax treatment shall be subject to applicable regulations of the State.

Article 26

In order to ensure the interests of service users, internet service providers shall be responsible for:
1. Registering and publishing quality standards of services in accordance with the State regulations on management of quality of services.
2. Ensuring the provision of services to users in accordance with the registered and published standards.
3. Reporting and being subject to inspections and examinations by State administrative bodies in charge of quality of services as stipulated.

Article 27

Internet connection shall be carried out on the basis of the following principles:
1. The establishment and use of telecommunications lines for connection between the systems of equipment of different entities or enterprises providing internet services and the public telecommunications network must comply with the regulations relating to telecommunications.
2. Internet connection service providers (IXPs) may connect with each other and with the international internet.
3. Internet access service providers (ISPs) may connect with each other and with internet connection service providers.
4. Separate internet access providers (Separate ISPs) may connect with internet connection service providers and internet access service providers, but may not directly connect with each other.
5. Internet application service providers (OSPs) or internet information service providers may connect with internet connection service providers and internet access service providers.
6. Internet agents may connect with the enterprises providing internet services with which they sign an agency contract.
CHAPTER IV Complaints, Inspections, Examinations and Dealing With Breaches

Article 43

Principles of penalty, terms of penalty, procedures for penalty for administrative offences, aggravating factors, extenuating factors, limitation periods for penalty and the time-limits when administrative offences relating to the internet are deemed not to be subject to penalty shall be in accordance with the provisions of the Ordinance on Dealing with Administrative Offences.

Article 44

Any organizations or individuals causing damage to other organizations or individuals in relation to the provision and use of internet services shall make compensation therefor as required by law.

Article 45

Any acts of abusing the internet to oppose the Socialist Republic of Vietnam, causing a breach of safety and security; and other serious offences of a criminal nature shall be subject to prosecution for criminal liability in accordance with law.