ACTS
SUPPLEMENT No. 2 **14th Febuary, 2011.**

ACTS SUPPLEMENT

to The Uganda Gazette No. 10 Volume CIV dated 14th February, 2011.

Printed by UPPC, Entebbe, by Order of the Government.

THE COMPUTER MISUSE ACT, 2011.

ARRANGEMENT OF SECTIONS.

Section.

THE COMPUTER MISUSE ACT, 2011

An Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

DATE OF ASSENT: 1st November, 2010.

Date of Commencement: See Section 1.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY.

1. Commencement.
This Act shall come into force on a date appointed by the Minister by statutory instrument

2. Interpretation.
In this Act, unless the context otherwise requires—

"access" means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective;

"application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system;

"authorised officer" has the meaning assigned to it in section 28;

"child" means a person under the age of eighteen years;

"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 a device or group of such interconnected or related devices;

"computer output" or "output" means a statement, information or representation, whether in written, printed, pictorial, graphical or other form—

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced from a computer;

"computer service" includes computer time, data processing and the storage retrieval of data;

"content" includes components of computer hardware and software;

"currency point" means the value of a currency point specified in the Schedule;

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that—

(a) causes any loss;

(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 electronic representations of information in any form;

"data message" means data generated, sent, received or stored by computer means; and includes—

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"electronic device", "acoustic device", or "other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"electronic record" means data which is recorded or stored on any medium in or by a computer or other similar device, that can be read or perceived by a person or a computer system or other similar device and includes a display, printout or other out put of that data;

"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system;

"information system services" includes a provision of connections, operation facilities, for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"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 of such a function;

"Minister" means the Minister responsible for information and communications technology;

"person" includes any company or association or body of persons corporate or unincorporate;

"program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"traffic data" means any computer data relating to communication by means of a computer system generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

PART II—GENERAL PROVISIONS.

3. Securing access.

A person secures access to any program or data held in a computer if that person—

(a) views, 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 or destroys 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.

4. Using a program.

A person uses a program if the function he or she causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

5. Authorised access.

Access by a person to any program or data held in a computer is authorised if—

(a) the person is entitled to control access to the program or data in question; or

(b) the person has consent to access that program or data from any person who is charged with giving that consent.

6. References.

(1) A reference to a program or data held in a computer includes a reference to any program or data held in any removable storage medium and a computer may be regarded as containing any program or data held in any such medium.

(2) A reference to a program includes a reference to part of a program.

7. Modification of contents.

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 connected to it result into—

(a) a program, data or data message held in the computer concerned being altered or erased; or

(b) a program, data or data message being added to its contents.

8. Unauthorised modification.

Modification is unauthorised if—

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) he or she does not have consent to the modification from a person who is entitled.

PART III—INVESTIGATIONS AND PROCEDURES.

9. Preservation Order.

(1) An investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence; or

(b) where prosecution is instituted, until the final determination of the case or until such time as the court deems fit.

10. Disclosure of preservation Order.

The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data.

11. Production Order.

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling—

(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

PART III—COMPUTER MISUSE OFFENCES.

12. Unauthorised access.

(1) A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a manner that causes the program or data to be modified, damaged, destroyed or rendered ineffective, commits an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performs any of those acts with regard to a password, access code or any other similar kind of data, commits an offence.

(4) A person who utilises any device or computer program specified in subsection (3) in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data, commits an offence.

(5) A person who accesses any information system so as to constitute a denial including a partial denial of service to legitimate users commits an offence.

(6) The intent of a person to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

13. Access with intent to commit or facilitate the commission of a further offence.

(1) A person who commits any acts specified under section 12 with intent to—

(a) commit any other offence; or

(b) facilitate the commission of any other offence,

commits an offence.

(2) The offence to be facilitated under subsection (1)(b) may be one committed by the person referred to in subsection (1) or by any other person.

(3) It is immaterial for the purposes of this section whether the act under this section is committed on the same occasion as the offence under section 12 or on any future occasion.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

14. Unauthorised modification of computer material.

(1) A person who—

(a) does any act which causes an unauthorised modification of the contents of any computer; and

(b) has the requisite intent and the requisite knowledge at the time when he or she does the act,

commits an offence.

(2) For the purposes of subsection (1)(b) the requisite intent is an intent to cause a modification of the contents of any computer and by doing so—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent under subsection (1)(b) need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) the requisite knowledge is knowledge that any modification that the person intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind specified in subsection (2) is intended to be permanent or temporary.

(6) A person who commits an offence under this section is liable on conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

15. Unauthorised use or interception of computer service.

(1) Subject to subsection (2), a person who knowingly—

(a) secures access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service;

(b) 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 whether similar or not; or

(c) 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),

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence is liable to a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven years or both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

16. Unauthorised obstruction of use of computer.

A person who, knowingly and without authority or lawful excuse—

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer,

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

17. Unauthorised disclosure of access code.

(1) A 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 knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

18. Unauthorised disclosure of information.

(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

19. Electronic fraud.

(1) A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) For the purposes of this section "electronic fraud" means deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

20. 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 12, 14, 15 or 16, the person convicted of an offence is, instead of the punishment prescribed in those sections, liable on conviction, to imprisonment for life.

(2) For the purposes of subsection (1), a computer is treated as a "protected computer" if the person committing the offence knows or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for—

(a) the security, defence or international relations of Uganda;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure; or

(d) 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).

21. Abetment and attempts.

(1) A person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence.

(2) Any person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

22. Attempt defined.

(1) When a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.

(2) It is immaterial—

(a) except so far as regards punishment, whether the offender does all that is necessary on his or her part for completing the commission of the offence, or whether the complete fulfillment of his or her intention is prevented by circumstances independent of his or her will, or whether the offender desists of his or her own motion from the further prosecution of his or her intention; or

(b) that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.

23. Child pornography.

(1) A person who—

(a) produces child pornography for the purposes of its distribution through a computer;

(b) offers or makes available child pornography through a computer;

(c) distributes or transmits child pornography through a computer;

(d) procures child pornography through a computer for himself or herself or another person; or

(e) unlawfully possesses child pornography on a computer,

commits an offence.

(2) A person who makes available pornographic materials to a child commits an offence.

(3) For the purposes of this section "child pornography" includes pornographic material that depicts—

(a) a child engaged in sexually suggestive or explicit conduct;

(b) a person appearing to be a child engaged in sexually suggestive or explicit conduct; or

(c) realistic images representing children engaged in sexually suggestive or explicit conduct.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

24. Cyber harassment.

(1) A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

(2) For purposes of this section cyber harassment is the use of a computer for any of the following purposes—

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section.

25. Offensive communication.

Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding one year or both.

26. Cyber stalking.

Any person who willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

27. Compensation.

Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

PART V—MISCELLANEOUS.

28. Searches and seizure.

(1) Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing—

(a) that an offence under this Act has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises,

the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.

(2) An authorised officer may seize any computer system or take any samples or copies of applications or data—

(a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere;

(b) that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or

(c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

(3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant.

(4) The provisions of section 71 of the Magistrates Court's Act apply with the necessary modifications to the issue and execution of a search warrant referred to in subsection (3).

(5) An authorised officer executing a search warrant referred to in subsection (3), may—

(a) at any time search for, have access to and inspect and check the operation of any computer system, application or data if that officer on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant;

(b) require a person having charge of or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant; and

(c) compel a service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to co-operate and assist the competent authorties in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (5), an authorised officer shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities.

(7) A person who obstructs, hinders or threatens an authorised officer in the performance of his or her duties or the exercise of his or her powers under this section commits an offence and is liable on conviction to a fine not exceeding twelve currency points or imprisonment not exceeding six months or both.

(8) A computer system seized or samples or copies of applications or data taken by the authorised officer shall be returned within seventy two hours unless the authorised officer has applied for and obtained an order in an inter party application for extension of the time.

(9) In this section—

"authorised officer" means a police officer who has obtained an authorising warrant under subsection (1); and

"premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hover craft.

29. Admissibility and evidential weight of a data message or an electronic record.

(1) In any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message or an electronic record—

(a) merely on the ground that it is constituted by a data message or an electronic record;

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain; or

(c) merely on the ground that it is not in its original form.

(2) A person seeking to introduce a data message or an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(3) Subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

(4) When assessing the evidential weight of a data message or an electronic record, the court shall have regard to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the authenticity of the data message was maintained;

(c) the manner in which the originator of the data message or electronic record was identified; and

(d) any other relevant factor.

(5) The authenticity of the electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where—

(a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds on which to doubt the authenticity of the electronic records system;

(b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) it is established that the electronic record 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 record or store it under the control of the party seeking to introduce the record.

(6) For the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of any set standard, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

(7) For the avoidance of doubt, this section does not modify the common law or a statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

30. Territorial jurisdiction.

(1) Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is within or outside Uganda.

(2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

(3) For the purposes of this Act, this section applies if, for the offence in question—

(a) the accused was in Uganda at the material time; or

(b) the computer, program or data was in Uganda at the material time.

31. Jurisdiction of courts.

A court presided over by a chief magistrate or magistrate grade I has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the full penalty or punishment in respect of any offence under this Act.

32. Power of Minister to amend Schedule

The Minister may by statutory instrument with the approval of the Cabinet, amend the Schedule to this Act.

SCHEDULE

Section 2.

Currency point

One currency point is equivalent to twenty thousand shillings.

Cross reference

Magistrates Courts Act, Cap.16.