SCHEDULE

Section 2.

Currency point

One currency point is equivalent to twenty thousand shillings.

Cross reference

Magistrates Courts Act, Cap.16.

BILLS
SUPPLEMENT No. 12 14th November, 2008.

BILLS SUPPLEMENT

to the Uganda Gazette No. 56 Volume CI dated 14th November, 2008.

Printed by UPPC, Entebbe by Order of the Government.

THE COMPUTER MISUSE BILL, 2008.

MEMORANDUM.

1. Policy and Principles of Bill

The object of this Bill is 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.

2. The defects in the existing law

It has been realised that Uganda needs to optimally exploit the great resource of ICTs by ensuring that the Ugandan communities, businesses and institutions have access to these new technologies. To achieve this, Uganda needs to create a conducive and enabling environment for all users and beneficiaries of ICT to avoid abuse and misuse. It is also necessary to build trust and ensure security of users of ICT.

3. Remedies proposed

It is against this background that the Computer Misuse Bill has been promoted in order to meet the need of protection of computer use and information that have been identified.

4. Necessity for introduction of the Bill

The Bill is therefore being introduced to provide remedies for the defects in the existing law. The Bill is one of three Bills that it has been found necessary to promote to meet the current situation for now and for the future.

The two other Bills are the Electronic Signatures Bill and Electronic Transactions Bill.

5. Computer misuse refers to unauthorised access to private computers and network systems, deliberate corruption or destruction of other people's data, disrupting the network or systems, introduction of viruses or disrupting the work of others; as well as the creation and forwarding of defamatory material, infringement of copyright, as well as the transmission of unsolicited advertising or other material to outside organisations.

The definition of computer misuse includes the "downloading, displaying, viewing and manipulation of offensive or obscene material". This would include pornography or scenes of violence. In extreme cases this may include the criminal act of downloading or displaying indecent photographs of children.

6. PROVISIONS OF THE BILL

The Bill therefore creates various offences aimed at preventing computer abuse.
The Bill is divided into four Parts.

7. Part I of the Bill—Preliminary

Part I of the Bill incorporating clauses 1 and 2 provides for preliminary matters relating to commencement of the Bill and interpretation of the words and phrases used in the Bill. For instance clause 2 defines "computer" as follows—

> "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, other than—
>
> (a) an automated typewriter or typesetter;
>
> (b) a portable hand held calculator;
>
> (c) a similar device which is non-programmable or which does not contain any data storage facility; or
>
> (d) such other device as the Minister may by statutory instrument prescribe;

Thus the Minister may by statutory instrument prescribe what devices will not fall under the definition of computer.

8. Part II of the Bill—General provisions

Part II of the Bill incorporating clauses 3 to 9 deals with general provisions. Clause 3 deals with application of Part II.

Clause 4 explains the expression "securing access" to any program or data held in a computer by causing a computer to perform any function.

Clause 5 explains the expression "using a program". A person uses a program if the function he or she causes the computer to perform causes the program to be executed or is itself a function of the program.

Clause 6 explains the expression "authorised access". Access by a person to any program or data held in a computer is authorised if the person is entitled to control access to the program or data in question or the person has consent to access that program or data from any person who is charged with giving that consent.

Clause 8 explains what is the modification of contents. A modification of the contents of any computer takes place if by the operations of any function of the computer concerned or any other computer—

(a) a program or data held in the computer concerned is altered or erased or

(b) a program or data is added to its contents

and any act which contributes towards causing such a modification shall be regarded as causing it.

Clause 9 explains the expression "unauthorised modification". Modification isunauthorised 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.

9. Part III of the Bill—Computer misuse offences

Part III of the Bill incorporating clauses 10 to 20 provides for computer misuse offences. For instance clause 10 creates an offence for unauthorised access. A person who intentionally accesses or intercepts any data without authority or permission to do so commits an offence. The penalty for the offence is a fine not exceeding twelve currency points or imprisonment not exceeding six months or both.

Clause 11 of the Bill explains the expression "access with intent to commit or facilitate the commission of a further offence". A person may commit an offence under this section even though the facts are such that the commission of the offence under this section is impossible.

Clause 12 of the Bill creates an offence for unauthorised modification of computer material. A person who does any act which causes an unauthorised modification of the contents of any computer and at the time when he or she does the act, he or she has the requisite intent and the requisite knowledge commits an offence. The penalty for unauthorised modification of computer material is a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

Requisite intent for the purposes of subclause (1) (b) is defined in subclause (2) as read with subclauses (3) and (4).

Clause 17 of the Bill creates the offence of electronic fraud. 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 and another part through the action of the victim of the offence or the action is performed through a computer network or both. The penalty for electronic fraud is a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven years or both.

10. Part IV of the Bill—Miscellaneous

Part IV of the Bill incorporating clauses 21 to 25 deals with miscellaneous provisions of the Bill.

Clause 21 provides for searches and seizure. Where a magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing that an offence has been or is about to be committed in any premises and 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.

Clause 22 makes provision for the admissibility in legal proceedings of data messages or electronic records and indicates weight to be attached to such evidence. It also prescribes safe guards in respect of admissibility of such evidence.

Clause 23 provides for territorial jurisdiction of the Bill. The Bill provides that it shall have effect in relation to any person whatever his or her nationality or citizenship, outside as well as within Uganda.

Clause 24 provides for the jurisdiction of courts. A court presided over by a chief magistrate or magistrate grade I has jurisdiction to hear and determine all offences under this Act and not withstanding anything to the contrary in any written law has power to impose the full penalty or punishment in respect of any offence under the Bill.

Clause 25 provides for the power of the Minister to amend the Schedule. The Minister may, by statutory instrument, with the approval of Cabinet, amend the Schedule to this Bill.

HAM-MUKASA MULIRA,
Minister of Information and Communications Technology (ICT).

THE COMPUTER MISUSE BILL, 2008.

ARRANGEMENT OF CLAUSES.

PART I—PRELIMINARY.

Clause.

Clause.

A BILL for an Act

ENTITLED

THE COMPUTER MISUSE ACT, 2008

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.

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" in relation to an application or data means rendering that application or data, by whatever means, in a form that would enable a person, at the time when it is rendered or subsequently, to take account of that application or data; and includes using the application or data or having it output from the computer system in which it is held in a displayed or printed form or to a storage medium or by means of any other output device, whether attached to the computer system in which the application or data are held or not;

"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 21;

"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, other than—

(a) an automated typewriter or typesetter;

(b) a portable hand held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may by statutory instrument prescribe;

"computer output" or "output" means a statement or representation, whether in written, printed, pictorial, graphical or other form whether similar or not, 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 from a computer;

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

"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 loss aggregating at least fifty currency points in value or such other amount as the Minister may, by statutory instrument 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;

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

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

(b) a stored record;

"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;

"electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means whether similar or not in an information system or for transmission from one information system to another;

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

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

"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;

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

PART II—GENERAL PROVISIONS.

3. Application of Part II.

The provisions of this Part shall have effect for the purposes of this Act.

4. Securing access.

A person secures access to any program or data held in a computer if by causing a computer to perform any function, that person—

(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.

5. 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.

6. 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.

7. 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.

8. 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—

(a) a program or data held in the computer concerned is altered or erased; or

(b) a program or data is added to its contents;

and any act which contributes towards causing such a modification shall be regarded as causing it.

9. 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—COMPUTER MISUSE OFFENCES.

10. Unauthorised access.

(1) A person who intentionally accesses or intercepts any 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 data to be modified destroyed or otherwise 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 with the intent to utilise unlawfully that item to contravene this section, commits an offence.

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

(5) A person who commits an act specified under this section with intent to interfere with access to 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 twelve currency points or imprisonment not exceeding six months or both.

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

(1) A person who commits an offence under section 10 with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of an offence to which this section applies,

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 offence under this section is committed on the same occasion as the offence under section 10 or on any future occasion.

(4) A person may commit an offence under this section even though the facts are such that the commission of the offence under this section is impossible.

(5) A person who commits an offence under this section is liable on conviction to a fine not exceeding seventy-two currency points or imprisonment not exceeding three years or both.

(6) An offence to which this section applies is—

(a) an offence under this Act;

(b) an offence punishable with a fine exceeding seventy two currency points or imprisonment exceeding three years or both.

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

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 or 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 one hundred and twenty currency points or imprisonment not exceeding five years or both.

13. Unauthorised use or interception of computer service.

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

(a) secures access without authority to any computer 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 seventy two currency points or to imprisonment not exceeding three years or both; and in the case of a subsequent conviction, to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five 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.

14. Unauthorised obstruction of use of computer.

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

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

(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 seventy two currency points or imprisonment not exceeding three years or both and; in the case of a subsequent conviction, to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five 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 to imprisonment not exceeding seven years or both.

15. 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 commits an offence if he or she does so—

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

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

16. Unauthorised disclosure of information.

(1) Except for the purposes of this Act or for any prosecution for an offence under any written law 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, the contents of that electronic data, record, book, register, correspondence, information, document or the other material.

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

17. Electronic fraud.

(1) A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven 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 and another part through the action of the victim of the offence or the action is performed through a computer network or both.

18. 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 10, 12, 13 or 14, the person convicted of an offence is, instead of the punishment prescribed in those sections, liable on conviction, to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

(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) if there is, in respect of the computer, program or data, an electronic or other warning conspicuously exhibited stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

19. Abatements and attempts.

(1) A person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act that offence and is liable on conviction to the punishment prescribed for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

20. Child pornography.

(1) A person who—

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

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

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

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

(e) possesses child pornography on a computer system or on a computer-data storage medium,

commits an offence.

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

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

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

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

(3) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

PART IV—MISCELLANEOUS.

21. 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) Subject to subsection (6), 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; and

(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.

(6) An authorised officer may, without a search warrant referred to in subsection (3), seize any computer system or take any samples or copies of applications or data or perform any of the actions referred to in subsection (5)—

(a) if the person having charge of or being otherwise concerned with the operation, custody or care of a computer system, application or data consents to the seizure; or

(b) if that authorised officer on reasonable grounds believes—

(i) that a search warrant will be issued under subsection (3) if he or she applies for such a warrant; and

(ii) that the delay in obtaining the warrant would defeat the object of the search.

(7) 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), whether by virtue of a search warrant or under subsection (6), 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.

(8) 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.

(9) 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.

(10) 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.

22. 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 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.

23. 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 outside as well as within 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.

24. 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.

25. 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.

BILLS
SUPPLEMENT No. 12 14th November, 2008.

BILLS SUPPLEMENT

to the Uganda Gazette No. 56 Volume CI dated 14th November, 2008.

Printed by UPPC, Entebbe by Order of the Government.

THE COMPUTER MISUSE BILL, 2008.

MEMORANDUM.

1. Policy and Principles of Bill

The object of this Bill is 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.

2. The defects in the existing law

It has been realised that Uganda needs to optimally exploit the great resource of ICTs by ensuring that the Ugandan communities, businesses and institutions have access to these new technologies. To achieve this, Uganda needs to create a conducive and enabling environment for all users and beneficiaries of ICT to avoid abuse and misuse. It is also necessary to build trust and ensure security of users of ICT.

3. Remedies proposed

It is against this background that the Computer Misuse Bill has been promoted in order to meet the need of protection of computer use and information that have been identified.

4. Necessity for introduction of the Bill

The Bill is therefore being introduced to provide remedies for the defects in the existing law. The Bill is one of three Bills that it has been found necessary to promote to meet the current situation for now and for the future.