

**Act 2**

*Computer Misuse Act*

**2011**

THE COMPUTER MISUSE ACT, 2011.

ARRANGEMENT OF SECTIONS.

PART I—PRELIMINARY.

*Section.*

1. Commencement.
2. Interpretation.

PART II—GENERAL PROVISIONS.

3. Securing access.
4. Using a program.
5. Authorised access.
6. References.
7. Modification of contents.
8. Unauthorised modification.

PART III—INVESTIGATIONS AND PROCEDURES.

9. Preservation Order.
10. Disclosure of preservation Order.
11. Production Order.

PART IV—COMPUTER MISUSE OFFENCES.

12. Unauthorised access.
13. Access with intent to commit or facilitate commission of further offence.
14. Unauthorised modification of computer material.
15. Unauthorised use or interception of computer service.
16. Unauthorised obstruction of use of computer.
17. Unauthorised disclosure of access code.

Section.

18. Unauthorised disclosure of information.
19. Electronic fraud
20. Enhanced punishment for offences involving protected computers.
21. Abetments and attempts.
22. Attempt defined.
23. Child pornography.
24. Cyber harassment.
25. Offensive communication.
26. Cyber stalking.
27. Compensation.

PART V—MISCELLANEOUS.

28. Search and seizure.
29. Administratively and evidential weight of a data message or an electronic record.
30. Territorial jurisdiction.
31. Jurisdiction of courts.
32. Power of Minister to amend Schedule to this Act.

SCHEDULE.

Currency point.

**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.