



THE STATUTES OF THE REPUBLIC OF SINGAPORE

COMPUTER MISUSE AND CYBERSECURITY ACT

(CHAPTER 50A)

(Original Enactment: Act 19 of 1993)

REVISED EDITION 2007

(31st July 2007)

Prepared and Published by

THE LAW REVISION COMMISSION
UNDER THE AUTHORITY OF
THE REVISED EDITION OF THE LAWS ACT (CHAPTER 275)

Informal Consolidation – version in force from 13/3/2013

Computer Misuse and Cybersecurity Act

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

1. Short title
2. Interpretation

PART II

OFFENCES

3. Unauthorised access to computer material
4. Access with intent to commit or facilitate commission of offence
5. Unauthorised modification of computer material
6. Unauthorised use or interception of computer service
7. Unauthorised obstruction of use of computer
8. Unauthorised disclosure of access code
9. Enhanced punishment for offences involving protected computers
10. Abetments and attempts punishable as offences

PART III

MISCELLANEOUS AND GENERAL

11. Territorial scope of offences under this Act
12. Jurisdiction of Courts
- 12A. Composition of offences
13. Order for payment of compensation
14. Saving for investigations by police and law enforcement officers
15. [*Repealed*]
- 15A. Cybersecurity measures and requirements
16. Arrest by police without warrant

An Act to make provision for securing computer material against unauthorised access or modification, to require or authorise the taking of measures to ensure cybersecurity, and for matters related thereto.

[Act 3 of 2013]

[30th August 1993]

PART I

PRELIMINARY

Short title

1. This Act may be cited as the Computer Misuse and Cybersecurity Act.

[Act 3 of 2013]

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) 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 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 —

- (a) produced by a computer; or
- (b) 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 —

- (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;

“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.

[21/98]

(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 the computer concerned or any other computer —

- (a) any program or data held in the computer concerned is altered or erased;
- (b) any program or data is added to its contents; or
- (c) 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.

[S 92/97]

(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.

PART II

OFFENCES

Unauthorised access to computer material

3.—(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 offence 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.

[21/98]

(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.

[21/98]

(3) For the purposes of this section, it is immaterial that the act in question 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.

Access with intent to commit or facilitate commission of offence

4.—(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.

[21/98]

(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.

[21/98]

(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.

[21/98]

(4) For the purposes of this section, it is immaterial whether —

- (a) the access referred to in subsection (1) is authorised or unauthorised;
- (b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

[21/98]

Unauthorised modification of computer material

5.—(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.

[21/98]

(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.

[21/98]

(3) For the purposes of this section, it is immaterial that the act in question 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.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Unauthorised use or interception of computer service

6.—(1) Subject to subsection (2), any 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; 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),

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.

[21/98]

(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.

[21/98]

(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.

Unauthorised obstruction of use of computer

7.—(1) Any 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,

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.

[21/98]

(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.

[21/98]

Unauthorised disclosure of access code

8.—(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 —

- (a) for any wrongful gain;
- (b) for any unlawful purpose; or
- (c) knowing that it is likely to cause wrongful loss to any person.

[21/98]

(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.

[21/98]

Enhanced punishment for offences involving protected computers

9.—(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.

[21/98]

(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 —

- (a) the security, defence or international relations of Singapore;
- (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, public transportation 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.

[21/98]

(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.

[21/98]

Abetments and attempts punishable as offences

10.—(1) Any 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 shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

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

PART III

MISCELLANEOUS AND GENERAL

Territorial scope of offences under this Act

11.—(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 —

- (a) the accused was in Singapore at the material time; or
- (b) the computer, program or data was in Singapore at the material time.

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.

Composition of offences

12A.—(1) The Commissioner of Police or any person authorised by him may, in his discretion, compound any offence under this Act which is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding \$3,000.

[25/2003]

(2) The Minister may make regulations to prescribe the offences which may be compounded.

[25/2003]

Order for payment of compensation

13.—(1) The court before which a person is convicted of any offence under this Act may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his computer, program or data by the offence for which the sentence is passed.

(2) Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(3) An order of compensation under this section shall be recoverable as a civil debt.

Saving for investigations by police and law enforcement officers

14. Nothing in this Act shall prohibit a police officer, an authorised person within the meaning of section 39 of the Criminal Procedure Code 2010 or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to the powers conferred on him under any written law.

[21/98; 42/2005; 15/2010 wef 02/01/2011]

Power of police officer to access computer and data

15. *[Repealed by Act 42 of 2005]*

Cybersecurity measures and requirements

15A.—(1) Where the Minister is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the national security, essential services or defence of Singapore or foreign relations of Singapore, the Minister may, by a certificate under his hand, authorise or direct any person or organisation specified in the certificate (referred to in this section as the specified person) to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service or any class of computers or computer services.

(2) The measures and requirements referred to in subsection (1) may include, without limitation —

- (a) the exercise by the specified person of the powers referred to in sections 39(1)(a) and (b) and (2)(a) and (b) and 40(2)(a), (b) and (c) of the Criminal Procedure Code (Cap. 68);
- (b) requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat, including —
 - (i) information relating to the design, configuration or operation of any computer, computer program or computer service; and

- (ii) information relating to the security of any computer, computer program or computer service;
 - (c) providing to the Minister or a public officer authorised by him any information (including real-time information) obtained from any computer controlled or operated by the specified person, or obtained by the specified person from another person pursuant to a measure or requirement under paragraph (b), that is necessary to identify, detect or counter any such threat, including —
 - (i) information relating to the design, configuration or operation of any computer, computer program or computer service; and
 - (ii) information relating to the security of any computer, computer program or computer service; and
 - (d) providing to the Minister or a public officer authorised by him a report of a breach or an attempted breach of security of a description specified in the certificate under subsection (1), relating to any computer controlled or operated by the specified person.
- (3) Any measure or requirement referred to in subsection (1), and any direction given by a specified person for the purpose of taking any such measure or complying with any such requirement —
- (a) shall not confer any right to the production of, or of access to, information subject to legal privilege; and
 - (b) subject to paragraph (a), shall have effect notwithstanding any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on the disclosure of information imposed by law, contract or rules of professional conduct.
- (4) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (1) shall be guilty of an offence and 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.

- (5) Any person who, without reasonable excuse —
- (a) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (1); or
 - (b) fails to comply with any direction given by a specified person for the purpose of the specified person taking any such measure or complying with any such requirement,

shall be guilty of an offence and 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.

- (6) No civil or criminal liability shall be incurred by —
- (a) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (1); or
 - (b) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement.

(7) The following persons shall not be treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct:

- (a) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection, or who discloses any information to the Minister or a public officer authorised by the Minister, in compliance with any requirement under that subsection;
- (b) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection.

(8) The following persons, namely:

- (a) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection;
- (b) a person to whom a specified person provides information in compliance with any requirement under subsection (1),

shall not use or disclose the information, except —

- (i) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person;
- (ii) for the purpose of preventing, detecting or countering a threat to a computer, computer service or class of computers or computer services;
- (iii) to disclose to any police officer or other law enforcement authority any information which discloses the commission of an offence under this Act or any other written law; or
- (iv) in compliance with a requirement of a court or the provisions of this Act or any other written law.

(9) Any person who contravenes subsection (8) 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 12 months or to both.

(10) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —

- (a) no information for that offence shall be admitted in evidence in any civil or criminal proceedings; and
- (b) no witness in any civil or criminal proceedings shall be obliged —

- (i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or
- (ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(11) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contains any entry in which any informer is named or described or which may lead to his discovery, the court shall cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

(12) In subsection (1), “essential services” means —

- (a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure; or
- (b) emergency services such as police, civil defence or health services.

[Act 3 of 2013]

Arrest by police without warrant

16. Any police officer may arrest without warrant any person reasonably suspected of committing an offence under this Act.

LEGISLATIVE SOURCE KEY
COMPUTER MISUSE AND CYBERSECURITY ACT
(CHAPTER 50A)

Unless otherwise stated, the abbreviations used in the references to other Acts and statutory provisions are references to the following Acts and statutory provisions. The references are provided for convenience of users and are not part of the Act:

UK CMA 1990	: United Kingdom, Computer Misuse Act 1990 (c. 18)
Canada CLAA 1985	: Canada, Criminal Law Amendment Act 1985 (c. 19)
S Aust. EA 1929	: South Australia, Evidence Act 1929

LEGISLATIVE HISTORY
COMPUTER MISUSE AND CYBERSECURITY ACT
(CHAPTER 50A)

formerly known as the Computer Misuse Act

This Legislative History is provided for the convenience of users of the Computer Misuse Act. It is not part of the Act.

1. Act 19 of 1993 — Computer Misuse Act 1993

Date of First Reading	:	18 March 1993 (Bill No. 17/93 published on 19 March 1993)
Date of Second and Third Readings	:	28 May 1993
Date of commencement	:	30 August 1993

2. 1994 Revised Edition — Computer Misuse Act

Date of operation	:	15 March 1994
-------------------	---	---------------

3. Act 8 of 1996 — Evidence (Amendment) Act 1996

(Consequential amendments made to Act by)

Date of First Reading	:	5 December 1995 (Bill No. 45/95 published on 6 December 1995)
Date of Second and Third Readings	:	18 January 1996
Date of commencement	:	8 March 1996

4. G. N. No. S 92/1997 — Revised Edition of the Laws (Rectification) Order 1997

Date of commencement	:	14 March 1997
----------------------	---	---------------

5. Act 21 of 1998 — Computer Misuse (Amendment) Act 1998

Date of First Reading	:	1 June 1998 (Bill No. 24/98 published on 2 June 1998)
Date of Second and Third Readings	:	30 June 1998
Date of commencement	:	1 August 1998

6. 1998 Revised Edition — Computer Misuse Act (Chapter 50A)

Date of operation	:	15 December 1998
-------------------	---	------------------

7. Act 25 of 2003 — Computer Misuse (Amendment) Act 2003

Date of First Reading	:	16 October 2003 (Bill No. 22/2003 published on 17 October 2003)
Date of Second and Third Readings	:	10 November 2003
Date of commencement	:	14 June 2004 (except section 2) 1 September 2004 (section 2)

8. Act 42 of 2005 — Statutes (Miscellaneous Amendments) (No. 2) Act 2005

Date of First Reading	:	17 October 2005 (Bill No. 30/2005 published on 18 October 2005)
Date of Second and Third Readings	:	21 November 2005
Date of commencement	:	1 January 2006 (section 14 — Amendment of Computer Misuse Act)

9. 2007 Revised Edition — Computer Misuse Act (Chapter 50A)

Date of operation	:	31 July 2007
-------------------	---	--------------

10. Act 15 of 2010 — Criminal Procedure Code 2010

Date of First Reading	:	26 April 2010 (Bill No. 11/2010 published on 26 April 2010)
Date of Second and Third Readings	:	19 May 2010.
Date of commencement	:	2 January 2011

11. Act 3 of 2013 — Computer Misuse (Amendment) Act 2013

Date of First Reading	:	12 November 2012 (Bill No. 36/2012 published on 12 November 2012)
Date of Second and Third Readings	:	14 January 2013
Date of commencement	:	13 March 2013