THE STATUTES OF THE REPUBLIC OF SINGAPORE

COMPUTER MISUSE ACT 1993

2020 REVISED EDITION

This revised edition incorporates all amendments up to and including 1 December 2021 and comes into operation on 31 December 2021.

Prepared and Published by

THE LAW REVISION COMMISSION
UNDER THE AUTHORITY OF
THE REVISED EDITION OF THE LAWS ACT 1983

Informal Consolidation – version in force from 8/2/2024

Computer Misuse Act 1993

ARRANGEMENT OF SECTIONS

PART 1

PRELIMINARY

Section

An Act to make provision for securing computer material against unauthorised access or modification, for preventing abuse of the national digital identity service, and for matters related thereto.

[3/2013; 9/2018]

[Act 16 of 2023 wef 08/02/2024]

[30 August 1993]

PART 1

PRELIMINARY

Short title

1. This Act is the Computer Misuse Act 1993.

[3/2013; 9/2018]

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 17, 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 must 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;

"electromagnetic, acoustic, mechanical or other device" means any device, apparatus or program 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;

"national digital identity service" has the meaning given by paragraph 1(1) of the Schedule;

[Act 16 of 2023 wef 08/02/2024]

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

[22/2017]

[Act 16 of 2023 wef 08/02/2024]

"user", in relation to the national digital identity service, has the meaning given by paragraph 1(1) of the Schedule.

[Act 16 of 2023 wef 08/02/2024]

(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 the 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),

and references to access to a program or data (and to an intent to secure such access) are to be read accordingly.

(3) For the purposes of subsection (2)(*c*), a person uses a program if the function the person 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 the person —

(*a*) is not himself or herself entitled to control access of the kind in question to the program or data; and

(*b*) does not have consent to access by him or her 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 is taken as causing it.

(8) Any modification mentioned in subsection (7) is unauthorised if the person whose act causes it —

(*a*) is not himself or herself entitled to determine whether the modification should be made; and

(*b*) 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 2

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 —

(*a*) to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(*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.

(2) This section applies to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

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

(*a*) the access mentioned 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.

Unauthorised modification of computer material

5.—(1) Subject to subsection (2), any person who does any act which the person knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(*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 electromagnetic, 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 —

(*d*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*e*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the 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 —

(*c*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*d*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

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 the person 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.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

Disclosure of password, access code, etc., in relation to national digital identity service

8A.—(1) Any user of the national digital identity service —

(*a*) who discloses any password or access code of the user in relation to the national digital identity service, or provides any other means of securing access in the identity of the user to any program or data held in any computer by way of the national digital identity service; and

(*b*) who does so knowing, or having reasonable grounds to believe, that the purpose of the disclosure or provision is for any person to commit, or to facilitate the commission by any person of, any offence under any written law,

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.

(2) For the purpose of proving an offence under subsection (1), it is not necessary for the prosecution to prove —

(*a*) that the purpose of committing, or facilitating the commission of, an offence was carried out;

(*b*) that the user knew, or had reasonable grounds to believe, that the purpose was to commit, or facilitate the commission of, any specific offence; or

(*c*) that the disclosure or provision was made to any specific person, if the disclosure or provision was made by the user in a manner that was intended to be accessible or retrievable by another person, whether or not that other person is known to the user.

(3) For the purposes of subsection (1)(*b*), a user of the national digital identity service who does an act mentioned in subsection (1)(*a*) is presumed, until the contrary is proved, to have reasonable grounds to believe that the purpose of the disclosure or

provision is for a person to commit, or to facilitate the commission by a person of, an offence under any written law, if —

(*a*) the user does the act for any gain —

(i) whether or not the gain is a wrongful gain;

(ii) whether or not the gain is realised; and

(iii) whether the gain is to the user or to another person;

(*b*) the user does the act knowing that it is likely to cause wrongful loss to any person; or

(*c*) at the time the user does the act, the user fails to take reasonable steps to ascertain the identity and physical location of the person to whom the password, access code or means of securing access is disclosed or provided.

(4) It is not an offence under subsection (1) if the user of the national digital identity service had reasonable grounds to believe that the purpose of the disclosure or provision is to use or access the national digital identity service to carry out a transaction in the identity of the user for a lawful purpose.

[Act 16 of 2023 wef 08/02/2024]

Supplying, etc., credential of another person

8B.—(1) A person shall be guilty of an offence if the person —

(*a*) obtains or retains any credential of another person in relation to the national digital identity service; or

(*b*) supplies, offers to supply, transmits or makes available, by any means, any credential of another person in relation to the national digital identity service.

(2) It is not an offence under subsection (1)(*a*) if the person obtained or retained the credential of the other person for a purpose that is not any of the following purposes:

(*a*) for use in committing, or in facilitating the commission of, any offence under any written law;

(*b*) for the supply or transmission of, or making available, by any means, the credential to be used in committing, or in

facilitating the commission of, any offence under any written law.

(3) It is not an offence under subsection (1)(*b*) if —

(*a*) the person did the act for a purpose other than for the credential of the other person to be used in committing, or in facilitating the commission of, any offence under any written law; and

(*b*) the person did not know or have reason to believe that the credential of the other person will be or is likely to be used to commit, or facilitate the commission of, any offence under any written law.

(4) For the purposes of subsection (1)(*b*), a person does not transmit or make available any credential of another person in relation to the national digital identity service merely because the person provides, or operates facilities for network access, or provides services relating to, or provides connections for, the transmission or routing of data.

(5) A person who is guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(6) In this section —

(*a*) a reference to a credential of another person in relation to the national digital identity service has the meaning given by paragraph 1(2) of the Schedule; and

(*b*) a reference to an offence under any written law includes an offence under subsection (1).

[Act 16 of 2023 wef 08/02/2024]

Supplying, etc., personal information obtained in contravention of certain provisions

9.—(1) A person shall be guilty of an offence if the person, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 —

(*a*) obtains or retains the personal information; or

(*b*) supplies, offers to supply, transmits or makes available, by any means the personal information.

[22/2017]

(2) It is not an offence under subsection (1)(*a*) if the person obtained or retained the personal information for a purpose other than —

(*a*) for use in committing, or in facilitating the commission of, any offence under any written law; or

(*b*) for supply, transmission or making available by any means for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law.

[22/2017]

(3) It is not an offence under subsection (1)(*b*) if —

(*a*) the person did the act for a purpose other than for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law; and

(*b*) the person did not know or have reason to believe that the personal information will be or is likely to be used to commit, or facilitate the commission of, any offence under any written law.

Example 1.— *A* comes across a list of credit card numbers on the Internet belonging to individuals who are customers of *B*, which *A* has reason to believe were obtained by securing access without authority to *B*'s server. *A* downloads the list for the purpose of reporting the unauthorised access to *B*'s server to the police.

A retains the list of credit card numbers and transmits it to *B* for the purpose of informing *B* of the unauthorised access to *B*'s server.

A has downloaded and retained the list of credit card numbers for purposes other than those mentioned in subsection (2)(*a*) and (*b*). Therefore *A* does not commit an offence under subsection (1)(*a*) by reason of subsection (2).

A has transmitted the list to *B* for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If *A* did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then *A* does not commit an offence under subsection (1)(*b*) by reason of subsection (3).

Example 2.— *C*, an employee of *B*, after receiving the list from *A* in *Example* 1, transmits it to *D*, another employee of *B*, for the purpose of facilitating *B*'s investigation of the unauthorised access of *B*'s server.

C has transmitted the list to *D* for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If *C* did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then *C* does not commit an offence under subsection (1)(*b*) by reason of subsection (3).

[22/2017]

(4) For the purposes of subsection (1)(*b*), a person does not transmit or make available personal information merely because the person provides, or operates facilities for network access, or provides services relating to, or provides connections for, the transmission or routing of data.

[22/2017]

(5) A person guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[22/2017]

(6) For the purpose of proving under subsection (1) that a person knows or has reason to believe that any personal information was obtained by an act done in contravention of section 3, 4, 5 or 6, it is

not necessary for the prosecution to prove the particulars of the contravention, such as who carried out the contravention and when it took place.

[22/2017]

(7) In this section —

(*a*) personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password; and

(*b*) a reference to an offence under any written law includes an offence under subsection (1).

[8A

[22/2017]

Obtaining, etc., items for use in certain offences

10.—(1) A person shall be guilty of an offence if the person —

(*a*) obtains or retains any item to which this section applies —

(i) intending to use it to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7; or

(ii) with a view to it being supplied or made available, by any means for use in committing, or in facilitating the commission of, any of those offences; or

(*b*) makes, supplies, offers to supply or makes available, by any means any item to which this section applies, intending it to be used to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7.

[22/2017]

(2) This section applies to the following items:

(*a*) any device, including a computer program, that is designed or adapted primarily, or is capable of being used, for the purpose of committing an offence under section 3, 4, 5, 6 or 7;

(*b*) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

[22/2017]

(3) A person guilty of an offence under subsection (1) shall be liable on conviction —

(*a*) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(*b*) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

[8B

[22/2017]

Enhanced punishment for offences involving protected computers

11.—(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, a person convicted of the offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer is 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.

(3) For the purposes of any prosecution under this section, it is 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.

[9

Abetments and attempts punishable as offences

12.—(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.

[10

PART 3

MISCELLANEOUS AND GENERAL

Territorial scope of offences under this Act

13.—(1) Subject to subsection (3), the provisions of this Act have effect, in relation to any person, whatever the person's nationality or citizenship, outside as well as within Singapore.

[22/2017]

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

(3) For the purposes of this section, this Act applies if —

(*a*) for the offence in question, the accused was in Singapore at the material time;

(*b*) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8), the computer, program or data was in Singapore at the material time;

[Act 16 of 2023 wef 08/02/2024]

(*c*) the offence causes, or creates a significant risk of, serious harm in Singapore; or

[22/2017]

[Act 16 of 2023 wef 08/02/2024]

(*d*) the offence is one under section 8A(1) or 8B(1).

[Act 16 of 2023 wef 08/02/2024]

(4) In subsection (3)(*c*), "serious harm in Singapore" means —

(*a*) illness, injury or death of individuals in Singapore;

(*b*) a disruption of, or a serious diminution of public confidence in, the provision of any essential service in Singapore;

(*c*) a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board; or

(*d*) damage to the national security, defence or foreign relations of Singapore.

Example 1.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the provision of an essential service:

(*a*) publication to the public of the medical records of patients of a hospital in Singapore;

(*b*) providing to the public access to the account numbers of customers of a bank in Singapore.

Example 2.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board:

(*a*) providing to the public access to confidential documents belonging to a ministry of the Government;

(*b*) publication to the public of the access codes for a computer belonging to a statutory board.

[22/2017; 9/2018]

(5) For the purposes of subsection (3)(*c*), it is immaterial whether the offence that causes the serious harm in Singapore —

(*a*) causes the harm directly; or

(*b*) is the only or main cause of the harm.

[22/2017]

(6) In subsection (4)(*b*), "essential service" means any of the following services:

(*a*) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure;

(*b*) emergency services such as police, civil defence or health services.

[9/2018]

(7) In subsection (4)(*c*), "statutory board" means a body corporate or unincorporate established by or under any public Act to perform or discharge a public function.

[11
[22/2017]

Amalgamation of charges

14.—(1) This section applies when a person is alleged to have committed 2 or more acts —

(*a*) each of which is an offence under the same provision in Part 2;

(*b*) that involve the same computer; and

(*c*) that are committed in a period that does not exceed 12 months.

[22/2017]

(2) Despite section 124 of the Criminal Procedure Code 2010, it is sufficient for the charge in respect of those acts to specify, without specifying the exact dates the acts are committed —

(*a*) particulars of that computer; and

(*b*) the dates between which the acts are alleged to have been committed.

[22/2017]

(3) A charge framed in accordance with subsection (2) is treated as a charge of one offence.

[22/2017]

(4) If the particulars mentioned in subsection (2)(*a*) and (*b*) do not give the accused sufficient notice of what the accused is charged with, then the charge must also give details of how the alleged offence was committed as will be sufficient for that purpose.

[11A

[22/2017]

Jurisdiction of Courts

15. A District Court or a Magistrate's Court has jurisdiction to hear and determine all offences under this Act and, despite anything to the contrary in the Criminal Procedure Code 2010, has power to impose the full penalty or punishment in respect of any offence under this Act.

[12

Composition of offences

16.—(1) The Commissioner of Police or any person authorised by the Commissioner may compound any offence under this Act that is prescribed as a compoundable offence by collecting from a person

reasonably suspected of having committed the offence a sum not exceeding $3,000.

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

[12A

Order for payment of compensation

17.—(1) The court before which a person is convicted of any offence under this Act may make an order against the person for the payment by the person of a sum to be fixed by the court by way of compensation to any other person for any damage caused to the other person's 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 is deemed to have been satisfied to the extent of any amount which has been paid to the person under an order for compensation, but the order does not affect 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 is recoverable as a civil debt.

[13

Saving for investigations by police and law enforcement officers

18. Nothing in this Act prohibits 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 or her under any written law.

[14
[15/2010]

Arrest by police without warrant

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

[16

Amendment of Schedule

20. The Minister may, by order in the *Gazette*, amend the Schedule.

[Act 16 of 2023 wef 08/02/2024]

THE SCHEDULE

Sections 2(1), 8B(6)(*a*) and 20

DEFINITIONS RELATING TO NATIONAL DIGITAL IDENTITY SERVICE

1.—(1) In this Act —

"application", in relation to the national digital identity service, means the mobile software application known as "Singpass" published under the name of "Government Technology Agency" that is registered to a user;

"biometric identifier", in relation to the national digital identity service, means an image or video, or an aggregation of images or videos, of a user's face captured electronically through the national digital identity service;

"national digital identity service" means the electronic service known as "Singpass" that is owned by the Government, by which the identity of an individual may be authenticated;

"user", in relation to the national digital identity service, means an individual who has an account registered with the national digital identity service.

(2) In section 8B, a reference to a credential of another person in relation to the national digital identity service is a reference to a password, access code or biometric identifier of that other person in relation to the national digital identity service, or any application registered with the national digital identity service in the identity of that other person.

[Act 16 of 2023 wef 08/02/2024]

LEGISLATIVE HISTORY
COMPUTER MISUSE ACT 1993

(Formerly known as the Computer Misuse and Cybersecurity Act (2007 Ed.))

This Legislative History is a service provided by the Law Revision Commission on a best-efforts basis. It is not part of the Act.

1. Act 19 of 1993 — Computer Misuse Act 1993

Bill	:	17/1993
First Reading	:	18 March 1993
Second and Third Readings	:	28 May 1993
Commencement	:	30 August 1993

2. 1994 Revised Edition — Computer Misuse Act (Chapter 50A)

Operation	:	15 March 1994

3. Act 8 of 1996 — Evidence (Amendment) Act 1996
(Amendments made by section 9 of the above Act)

Bill	:	45/1995
First Reading	:	5 December 1995
Second and Third Readings	:	18 January 1996
Commencement	:	8 March 1996 (section 9)

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

Operation	:	15 March 1994

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

Bill	:	24/1998
First Reading	:	1 June 1998
Second and Third Readings	:	30 June 1998
Commencement	:	1 August 1998

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

Operation	:	15 December 1998

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

Bill	:	22/2003
First Reading	:	16 October 2003

Second and Third Readings	:	10 November 2003
Commencement	:	14 June 2004 (except section 2) 1 September 2004 (section 2)

8. Act 42 of 2005 — Statutes (Miscellaneous Amendments) (No. 2) Act 2005
(Amendments made by section 14 of the above Act)

Bill	:	30/2005
First Reading	:	17 October 2005
Second and Third Readings	:	21 November 2005
Commencement	:	1 January 2006 (section 14)

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

Operation	:	31 July 2007

10. Act 15 of 2010 — Criminal Procedure Code 2010
(Amendments made by section 430 read with item 24 of the Sixth Schedule to the above Act)

Bill	:	11/2010
First Reading	:	26 April 2010
Second Reading	:	18 May 2010
Third Reading	:	19 May 2010
Commencement	:	2 January 2011 (section 430 read with item 24 of the Sixth Schedule)

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

Bill	:	36/2012
First Reading	:	12 November 2012
Second and Third Readings	:	14 January 2013
Commencement	:	13 March 2013

Note: The Computer Misuse Act was renamed as the Computer Misuse and Cybersecurity Act by this Act.

12. Act 22 of 2017 — Computer Misuse and Cybersecurity (Amendment) Act 2017

Bill	:	15/2017
First Reading	:	9 March 2017
Second and Third Readings	:	3 April 2017

Commencement : 1 June 2017

13. Act 9 of 2018 — Cybersecurity Act 2018
(Amendments made by section 49 of the above Act)

Bill : 2/2018

First Reading : 8 January 2018

Second and Third Readings : 5 February 2018

Commencement : 31 August 2018 (section 49)

Note: The Computer Misuse and Cybersecurity Act was renamed as the Computer Misuse Act by this Act.

14. 2020 Revised Edition — Computer Misuse Act 1993

Operation : 31 December 2021

15. Act 16 of 2023 — Computer Misuse (Amendment) Act 2023
(Amendments made by the above Act)

Bill : 13/2023

First Reading : 18 April 2023

Second and Third Readings : 9 May 2023

Commencement : 8 February 2024

Abbreviations

(updated on 29 August 2022)

G.N.	Gazette Notification
G.N. Sp.	Gazette Notification (Special Supplement)
L.A.	Legislative Assembly
L.N.	Legal Notification (Federal/Malaysian)
M.	Malaya/Malaysia (including Federated Malay States, Malayan Union, Federation of Malaya and Federation of Malaysia)
Parl.	Parliament
S	Subsidiary Legislation
S.I.	Statutory Instrument (United Kingdom)
S (N.S.)	Subsidiary Legislation (New Series)
S.S.G.G.	Straits Settlements Government Gazette
S.S.G.G. (E)	Straits Settlements Government Gazette (Extraordinary)

COMPARATIVE TABLE

COMPUTER MISUSE ACT 1993

This Act has undergone renumbering in the 2020 Revised Edition. This Comparative Table is provided to help readers locate the corresponding provisions in the last Revised Edition.

2020 Ed.	2007 Ed.
9	**8A**
10	**8B**
11	**9**
12	**10**
13	**11**
(6)	(5A)
(7)	(6)
14	**11A**
15	**12**
16	**12A**
17	**13**
18	**14**
—	**15** [*Repealed by Act 42 of 2005*]
—	**15A** [*Repealed by Act 9 of 2018*]
19	**16**