LAWS OF BRUNEI

CHAPTER 194
COMPUTER MISUSE ACT

S 65/00

REVISED EDITION 2007

LAWS OF BRUNEI

REVISED EDITION 2007

CHAPTER 194

COMPUTER MISUSE ACT

ARRANGEMENT OF SECTIONS

Section

PART I

PRELIMINARY

1. Citation.

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

GENERAL

11. Territorial scope of offences under this Act.

12. Court of Magistrate to have full jurisdiction.

13. Order for payment of compensation.

14. Saving for investigations by police and law enforcement officers.

15. Evidence from computer records.

16. Supplementary provisions on evidence.

17. Proof of document or copy thereof.

18. Power of police officer to access computer and data.

19. Arrest by police without warrant.

COMPUTER MISUSE ACT

An Act to make provision for securing computer material against unauthorised access or modification and for matters related thereto

Commencement: 21st June 2000
[S 65/00]

PART I

PRELIMINARY

Citation.

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

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

(b) such other device as the Minister may, by notification in the *Gazette*, prescribe;

"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;

"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;

"function" includes logic, control, arithmetic, deletion, storage and retrieval, read and write, 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;

"Minister" means the Minister of Finance;

"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;

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

(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 that computer or any other computer —

(a) any program or data held in that computer is altered or erased;

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

(c) any act which impairs the normal operation of any computer,

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

(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 is guilty of an offence and liable on conviction to a fine not exceeding $5,000, imprisonment for a term not exceeding 2 years or both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both.

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

(3) For the purposes of this section, it is immaterial that the act in question was 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 a computer with intent to commit an offence to which this section applies is 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 is liable on conviction to a fine not exceeding $50,000, imprisonment for a term not exceeding 10 years or both.

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

(a) the access referred to in subsection (1) was authorised or unauthorised;

(b) the offence to which this section applies was committed at the same time when the access was secured or at any other time.

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 is guilty of an offence and is liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000, imprisonment for a term not exceeding 5 years or both.

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

(3) For the purposes of this section, it is immaterial that the act in question was 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 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 paragraphs *(a)* or *(b)*,

is guilty of an offence and is liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both, and in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or imprisonment for a term not exceeding 5 years or both.

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

(3) For the purposes of this section, it is immaterial that an unauthorised access or interception was 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,

is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000, imprisonment for a term not exceeding 5 years or both.

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

Unauthorised disclosure of access code.

8. (1) Any person who knowingly and without authority discloses any password, access code or other means of gaining access to any program or data held in any computer is 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.

(2) Any person guilty of an offence under subsection (1) is liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000, imprisonment for a term not exceeding 5 years or both.

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 sections 3, 5, 6 or 7, the person convicted of such offence is in lieu of the punishments respectively prescribed in those sections, liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 20 years or both.

(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, program or data was used directly in connection with or necessary for —

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

(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 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 had the requisite knowledge referred to in subsection (2) if there was, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that program or data will attract an enhanced penalty under this section.

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 is shall be guilty of that offence and 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

GENERAL

Territorial scope of offences under this Act.

11. (1) Subject to subsection (2), this Act shall have effect in relation to any person, whatever his nationality, whether within or outside Brunei Darussalam; and where an offence under this Act has been committed by any person outside Brunei Darussalam, he may be dealt with as if the offence had been committed within Brunei Darussalam.

(2) For the purposes of subsection (1), this Act shall apply if, for the offence in question —

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

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

Court of Magistrate to have full jurisdiction.

12. Notwithstanding the provisions of any written law to the contrary, a Court of a Magistrate shall have jurisdiction to try any offence under this Act and to award the full punishment for any offence.

Order for payment of compensation.

13. (1) The court before which a person has been 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 has been 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, any person authorised in writing by the Commissioner of Police under section 18(1) or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to his powers conferred under any written law.

Evidence from computer records.

15. (1) Notwithstanding sections 35A and 35B of the Evidence Act (Chapter 108), in any proceedings under this Act any relevant output shall be admissible as evidence of any fact stated therein if it is shown —

(a) that there is no reasonable ground for believing that the output is inaccurate because of improper use of the computer and that no reason exists to doubt the truth or reliability of the output; or

(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the output or the accuracy of its contents.

(2) For the purpose of deciding whether or not such output is admissible, the court may draw any reasonable inference from the circumstances in which the output was made or otherwise came into being.

(3) The Minister may, with the approval of His Majesty the Sultan and Yang Di-Pertuan, make rules requiring that, in any proceedings where it is desired to give a statement in evidence by virtue of this section, such information concerning the statement shall be provided in such form and at such time as may be so required.

Supplementary provisions on evidence.

16. (1) In any proceedings where it is desired to admit output in evidence in accordance with section 15, a certificate —

(a) identifying the output and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that output as may be appropriate for the purpose of showing that the output was produced by a computer;

(c) dealing with any of the matters mentioned in section 15(1); and

(d) purporting to be signed by a person occupying a responsible position in relation to the operation of the computer at all relevant times,

shall be admitted in those proceedings as evidence of anything stated in the certificate.

(2) If the person referred to in subsection (1)*(d)* who occupies a responsible position in relation to the operation of the computer did not have control or access over any relevant records and facts in relation to the production by the computer of the output, a supplementary certificate signed by another person who had such control or access and made in accordance with subsections (1)*(a)* to *(c)* shall be evidence of anything stated in the certificate.

(3) For the purposes of subsections (1) and (2), it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(4) Notwithstanding subsections (1) and (2), a court may require oral evidence to be given of anything of which evidence could be given by a certificate under that subsection.

(5) Any person who in a certificate tendered in a court under subsections (1) or (2) makes a statement which he knows to be false or does not believe to be true is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 2 years or both.

(6) In estimating the weight, if any, of any admissible output, regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the output and, in particular —

(a) to the question whether the information which the output reproduces or is derived from was supplied to the relevant computer, or recorded for the purpose of being supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and

(b) to the question whether any person concerned with the supply of information to that computer, or with the operation of that

computer or any equipment by means of which the admissible output was produced by it, had any incentive to conceal or misrepresent the facts.

(7) For the purposes of subsection (6), information shall be taken to be supplied to a computer whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment.

Proof of document or copy thereof.

17. Notwithstanding the provisions of the Evidence Act (Chapter 108), where in any proceedings any output is admissible in evidence in accordance with section 15, it may be proved —

(a) by the production of that output; or

(b) (whether or not that output is still in evidence) by the production of a copy of that output, or the material part of it,

authenticated in such manner as the court may approve.

Power of police officer to access computer and data.

18. (1) A police officer or any person authorised in writing by the Commissioner of Police shall —

(a) be entitled at any time to —

(i) have access to and inspect and check the operation of any computer to which this section applies;

(ii) use or cause to be used any such computer to search any data contained in or available to such computer; or

(iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section;

(b) be entitled to require —

(i) the person by who or on whose behalf the police officer or investigation officer has reasonable cause to suspect any computer to which this section applies is or has been used; or

(ii) any person having charge of, or otherwise concerned with the operation of, such computer,

to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph *(a)*; or

(c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence.

(2) This section applies to a computer which a police officer or any person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.

(3) The powers referred to in subsections (1)*(a)* (ii) and (iii) and in subsection (1)*(c)* shall not be exercised except with the consent of the Public Prosecutor.

(4) Any person who obstructs the lawful exercise of the powers under subsection (1)*(a)* or who fails to comply with a request under subsections (1)*(b)* or *(c)* is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 3 years or both.

(5) For the purposes of this section —

“decryption information” means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;

“encrypted data” means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;

"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

Arrest by police without warrant.

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

Available from
Attorney General's Chambers
The Law Building, Jalan Tutong
Bandar Seri Begawan BA1910
Brunei Darussalam

$5.00
COMPUTER MISUSE ACT
CAP. 194, 2007 Ed.

Printed by
The Government Printing Department
Brunei Darussalam