CAYMAN ISLANDS


# COMPUTER MISUSE LAW

**(2015 Revision)**

**Supplement No. 3 published with Extraordinary Gazette No. 53 of 17th July, 2015.**

## PUBLISHING DETAILS

Law 8 of 2000 consolidated with 19 of 2012.

Revised under the authority of the Law Revision Law (1999 Revision).

Originally enacted-

Law 8 of 2000-20th July, 2000
Law 19 of 2012-31st August, 2012.

Consolidated and revised this 2nd day of July, 2015.

**CAYMAN ISLANDS**


# COMPUTER MISUSE LAW

**(2015 Revision)**

## Arrangement of Sections

Section Page

**CAYMAN ISLANDS**

# COMPUTER MISUSE LAW

**(2015 Revision)**

ENACTED by the Legislature of the Cayman Islands.

## Short title

**1**. This Law may be cited as the *Computer Misuse Law (2015 Revision)*.

## Interpretation

**2**. (1) References in this Law to information held in a computer include references to information held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing information held in such medium.

(2) In this Law —

"**computer service**" includes computer time, data processing and the storage or retreval of information;

"**electronic, acoustic, mechanical or other device**" means any device or apparatus that is used or 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;

"**information**" includes data, text, images, sounds, codes, computer programmes, software and databases;

"**modification**" has the meaning assigned by section 8;

"**related inchoaite offence**", in relation to an offence under this Act, means an offence under section 302, 304, 305 or 306 of the *Penal Code* (*2013 Revision*);

"**securing access**" has the meaning assigned by section 8; and

"**unauthorised**", in relation to access to or modification of any information held in a computer, has the meaning assigned by section 8.

### Unauthorised access to computer material

**3**. (1) A commits an offence under this section if —

(a) he causes a computer to perform a function with intent to secure access to information held in a computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at —

(a) any particular information;

(b) information of any particular kind; or

(c) information held in any particular computer.

(3) A person who commits an offence under this section is liable on summary conviction to a fine of $5,000 or to imprisonment for a term of two years, or to both.

(4) Where a person is convicted of committing an offence under subsection (1) and he has caused, during the commission of the offence, damage to a computer or any other damage arising directly from the damage to the computer and the damage exceeds $10,000, he shall be liable on summary conviction to a fine of $20,000 or to imprisonment for a term of five years, or to both.

### Unauthorised access with intent to commit or facilitate the commission of further offences

**4**. (1) A person who causes a computer to perform a function for the purpose of securing access without authority to information held in a computer with intent to commit an offence to which this section applies or to facilitate the commission of such an offence (whether by himself or by any other person) commits an offence and is liable on summary conviction to a fine of $30,000 or to imprisonment for a term of seven years, or to both.

(2) This section applies to offences —

(a) involving —

(i) property;

(ii) fraud; or

(iii) dishonesty; or

(b) which cause bodily harm,

and which are punishable on conviction with imprisonment for a term of two years or more.

(3) For the purposes of this section, it is immaterial whether the offence to which this section applies is committed at the same time as the unauthorised access is secured or on any future occasion.

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

### Unauthorised modification of computer material

**5**. (1) A person commits an offence if —

(a) he does an act which causes an unauthorised modification of the contents of a computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) —

(a) "**requisite intent**" is the intent to cause a modification to the contents of a computer and by so doing —

(i) to impair the operation of a computer;

(ii) to enhance the operation of a computer in order to secure unauthorised access to information in any other computer;

(iii) to prevent or hinder access to information held in a computer; or

(iv) to impair the operation of such programme or the reliability of any such programme,

but the intent need not be directed at a particular computer, particular information or information of any particular kind, or any particular modification or a modification of any particular kind; and

(b) "**requisite knowledge**" is knowledge that any modification which is intended to be caused is unauthorised.

(3) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it is, or is intended to be, permanent or temporary.

(4) A modification of the contents of a computer shall not be regarded as damaging a computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(5) A person who commits an offence under this section is liable on summary conviction to a fine of $6,000 or to imprisonment for a term of two years, or to both.

(6) Where a person is convicted of committing an offence under subsection (1) and he has caused, during the commission of the offence, damage to a computer or any other damage arising directly from the damage to the computer and the damage exceeds $10,000, he shall be liable on summary conviction to a fine of $20,000 or to imprisonment for a term of five years, or to both.

### Unauthorised use or interception of computer service

**6**. (1) A person who knowingly —

(a) secures access without authority to a 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 or output 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),

commits an offence and is liable on summary conviction to a fine of $6,000 or to imprisonment for a term of two years, or to both.

(2) Where a person is convicted of committing an offence under subsection (1) and he has caused, during the commission of the offence, any damage to a computer or any other damage arising directly from the damage caused to the computer and the damage exceeds $10,000, he shall be liable on summary conviction to a fine of $20,000 or to imprisonment for a term of five 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 information;

(b) information of any kind; or

(c) information held in any particular computer.

### Causing computer to cease to function

**7**. (1) A person commits an offence if —

(a) he causes a computer to cease to function permanently or temporarily; and

(b) at the time he engages in conduct that causes a computer to cease to function permanently or temporarily he has —

(i) knowledge that the conduct is unauthorised;

(ii) the requisite knowledge; and

(iii) the requisite intent.

(2) For the purpose of subsection (1)(b) —

(a) "**requisite knowledge**" is knowledge that the conduct would or would be likely to cause a computer to cease to function permanently or temporarily; and

(b) "**requisite intent**" is intent to cause a computer to cease to function and by so doing —

(i) prevent or hinder access to the computer; or

(ii) impair the operation of the computer,

but the intent need not be directed at a particular computer.

(3) A person who commits an offence under this section is liable on summary conviction to a fine of $6,000 or to imprisonment for a term of two years, or to both.

(4) Where a person is convicted of committing an offence under subsection (1) and he has caused, during the commission of the offence, damage to a computer or any other damage arising directly from the damage caused to the computer and the damage exceeds $10,000, he shall be liable on summary conviction to a fine of $20,000 or to imprisonment for a term of five years, or to both.

### Meaning of "securing access", "modification" and "unauthorised"

**8**. (1) A person secures access to information held in a computer if by causing a computer to perform a function he —

(a) alters or erases the information;

(b) copies or moves the information —

(i) to a different location in the storage medium in which it is held; or

(ii) to any other storage medium;

(c) uses the information; or

(d) has the information output from the computer in which it is held (whether by having it displayed or in any other manner),

and references in this Law to securing access or an intent so to do shall be construed accordingly.

(2) For the purposes of subsection (1)(c), a person uses information if the function he causes the computer to perform causes the information to be executed or is itself a function of the information.

(3) For the purposes of subsection (1)(d) —

(a) information is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or other information is output (and, in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of information, it is capable of being processed by a computer) is immaterial.

(4) Access of any kind by a person to information held in a computer is unauthorised if —

(a) he is not himself entitled to control access of the kind in question to the information; and

(b) he does not have consent to such access from the person who is so entitled.

(5) A modification of the contents of a computer takes place if, by the operation of any function of the computer concerned or any other computer —

(a) information held in the computer is altered, moved or erased;

(b) information is added to its contents,

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

(6) Such a modification 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 the person who is so entitled.

### Territorial scope of offences under this Law

**9**. The provisions of this Law shall have effect in relation to any person outside as well as within the Islands; and where an offence under this Law is committed by a person in any place outside of the Islands, he may be dealt with as if the offence had been committed within the Islands if the offence relates to a computer or information situate in the Islands.

### Territorial scope of inchoate offences

**10**. (1) On a charge of conspiracy to commit an offence under this Law the following questions are immaterial to the accused's guilt —

(a) the question where a person became a party to the conspiracy; and

(b) the question whether any act, omission or other event occurred in the Islands.

(2) On a charge of attempting to commit an offence under this Law the following questions are immaterial to the accused's guilt —

(a) the question where the attempt was made; and

(b) the question whether it had an effect in the Islands.

(3) On a charge of incitement to commit an offence under this Law the question where the incitement took place is immaterial to the accused's guilt.

### Proceedings for an offence under this Law

**11**. (1) Proceedings for an offence under this Law may be brought within a period of three years from the date on which evidence sufficient in the opinion of the Director of Public Prosecutions to warrant the proceedings came to his knowledge; but no such proceedings shall be brought more than five years after the commission of the offence.

(2) A certificate purporting to be under the hand of the Director of Public Prosecutions and specifying the date upon which such facts first came to his notice shall be evidence that such facts came to his notice on that date.

### Conviction of section 3 offence as alternative to section 4,5, 6 or 7

**12**. If on the trial of a person charged with an offence under section 4, 5, 6 or 7 or any related inchoate offence, the court finds him not guilty of the offence charged they may find him guilty of an offence under section 3 or any related inchoate offence if on the facts shown he could have been found guilty of that offence.

### Police powers

**13**. (1) A police officer may arrest without warrant a person who has committed or is committing, or whom the police officer with reasonable cause suspects to have committed, or to be committing or is about to commit, an offence under this Law.

(2) Any power of seizure conferred on a police officer who has entered premises by virtue of a warrant issued under the *Criminal Procedure Code (2014 Revision)* in relation to an offence under this Act, or any related inchoate offence, shall be construed as including a power to require any information relating to the warrant which is held in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is intelligible (whether or not with the use of a computer).

### Forfeiture

**14**. (1) Where a person is convicted of an offence under this Law, or any related inchoate offence, and the court is satisfied that any property which was in his possession or under his control at the time he was apprehended for the offence or when a summons in respect of it was issued —

(a) has been used for the purpose of committing, or facilitating the commission of, the offence in question or any other such offence; or

(b) was intended by him to be used for that purpose,

the court may order that property to be forfeited to the Crown, and may do so whether or not it deals with the offender in respect of the offence in any other way.

(2) A court shall not order the forfeiture of anything to the Crown if a person claiming to be the owner or otherwise interested in it applies to be heard by the court unless an opportunity has been given to that person to show cause why the order should not be made.

(3) An application under this section cannot be made by the person convicted of the offence that led to the forfeiture.

### Evidence from computer records

**15**. (1) In proceedings for an offence under this Law or a related inchoate offence, any relevant computer 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 or suspect 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 so admissible, the court may draw any reasonable inference from the circumstances in which the output was made or otherwise came into being.

### Supplementary provisions on evidence

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

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

(b) giving such particulars of any device involved in the production of that computer 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 admissible in those proceedings as *prima facie* evidence of anything stated in the certificate.

### Order for payment of compensation

**17**. (1) The court before which a person is convicted of an offence under this Law 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 or information 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.

**Publication in revised and consolidated form authorised by the Cabinet this 14th day of July, 2015.**

**Meredith Hew**
*Acting Clerk of Cabinet*