



REPUBLIC OF SINGAPORE  
**GOVERNMENT GAZETTE**  
**ACTS SUPPLEMENT**

*Published by Authority*

---

---

**NO. 30]**

**FRIDAY, DECEMBER 12**

**[2003**

---

---

**First published in the *Government Gazette*, Electronic Edition, on 10th December 2003 at 5:00 pm.**

The following Act was passed by Parliament on 10th November 2003 and assented to by the President on 28th November 2003:—

**REPUBLIC OF SINGAPORE**

---

**No. 25 of 2003.**

I assent.

(LS)

S R NATHAN,  
*President.*  
28th November 2003.

An Act to amend the Computer Misuse Act (Chapter 50A of the 1998 Revised Edition).

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

**Short title and commencement**

1. This Act may be cited as the Computer Misuse (Amendment) Act 2003 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

**New section 12A**

2. The Computer Misuse Act is amended by inserting, immediately after section 12, the following section:

**“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.

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

**New section 15A**

3. The Computer Misuse Act is amended by inserting, immediately after section 15, the following section:

**“Preventing or countering threats to national security, etc.**

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

(2) The measures referred to in subsection (1) may include, without limitation, the exercise by the authorised person or organisation of the powers referred to in section 15.

(3) 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.
- (4) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contain 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.
- (5) In subsection (1), “essential services” means —
- (a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation or public key infrastructure; and
  - (b) emergency services such as police, civil defence or medical services.”.
-