The Office of the
Government Chief Information Officer

BASELINE IT
SECURITY POLICY

[S17]

Version : 3.0

May 2006
The Government of the Hong Kong Special Administrative Region
COPYRIGHT NOTICE

© 2006 by the Government of the Hong Kong Special Administrative Region

Unless otherwise indicated, the copyright in the works contained in this publication is owned by the Government of the Hong Kong Special Administrative Region. You may generally copy and distribute these materials in any format or medium provided the following conditions are met -

(a) the particular item has not been specifically indicated to be excluded and is therefore not to be copied or distributed;
(b) the copying is not done for the purpose of creating copies for sale;
(c) the materials must be reproduced accurately and must not be used in a misleading context; and
(d) the copies shall be accompanied by the words “copied/distributed with the permission of the Government of the Hong Kong Special Administrative Region. All rights reserved.”

If you wish to make copies for purposes other than that permitted above, you should seek permission by contacting the Office of the Government Chief Information Officer.
# TABLE OF CONTENTS

1. **PURPOSE** .................................................................................................................. 1-1

2. **SCOPE** ....................................................................................................................... 2-1
   2.1. **GOVERNMENT INFORMATION SECURITY MANAGEMENT FRAMEWORK** .......................... 2-1
   2.2. **IT SECURITY DOCUMENT OVERVIEW** ........................................................................ 2-4

3. **REFERENCE** .............................................................................................................. 3-1
   3.1. **STANDARDS AND GUIDELINES** .................................................................................. 3-1
   3.2. **OTHER REFERENCES** .................................................................................................. 3-1

4. **DEFINITIONS AND CONVENTIONS** .......................................................................... 4-1
   4.1. **DEFINITIONS** ............................................................................................................. 4-1
   4.2. **CONVENTIONS** .......................................................................................................... 4-2

5. **DEPARTMENTAL IT SECURITY ORGANISATION** ............................................................. 5-1
   5.1. **SENIOR MANAGEMENT** ............................................................................................ 5-1
   5.2. **DEPARTMENTAL IT SECURITY OFFICER (DITSO)** .................................................... 5-1
   5.3. **DEPARTMENTAL SECURITY OFFICER (DSO)** .......................................................... 5-2
   5.4. **DEPARTMENTAL INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT) COMMANDER** 5-2
   5.5. **IT SECURITY ADMINISTRATORS** ................................................................................ 5-3
   5.6. **INFORMATION OWNERS** ......................................................................................... 5-3
   5.7. **LAN/SYSTEM ADMINISTRATORS** ............................................................................. 5-3
   5.8. **APPLICATION DEVELOPMENT & MAINTENANCE TEAM** ........................................ 5-4
   5.9. **USERS OF INFORMATION SYSTEMS** ......................................................................... 5-4

6. **MANAGEMENT RESPONSIBILITIES** ............................................................................. 6-1
   6.1. **GENERAL MANAGEMENT** ..................................................................................... 6-1
   6.2. **OUTSOURCING SECURITY** ........................................................................................ 6-2
   6.3. **CONTINGENCY MANAGEMENT** .................................................................................. 6-2

7. **PHYSICAL SECURITY** ................................................................................................... 7-1
   7.1. **ENVIRONMENT** ....................................................................................................... 7-1
   7.2. **EQUIPMENT SECURITY** ............................................................................................ 7-1
   7.3. **PHYSICAL ACCESS CONTROL** .................................................................................. 7-1

8. **ACCESS CONTROL SECURITY** .................................................................................. 8-1
   8.1. **DATA ACCESS CONTROL** ....................................................................................... 8-1
   8.2. **AUTHENTICATION** ................................................................................................... 8-1
   8.3. **PRIVACY** ................................................................................................................. 8-1
   8.4. **USER IDENTIFICATION** ............................................................................................. 8-1
   8.5. **USER PRIVILEGES MANAGEMENT** ......................................................................... 8-1
   8.6. **PASSWORD MANAGEMENT** .................................................................................... 8-2
   8.7. **NETWORK ACCESS CONTROL** ............................................................................... 8-2
   8.8. **LOGGING** .............................................................................................................. 8-2

9. **DATA SECURITY** .......................................................................................................... 9-1
   9.1. **OVERALL DATA CONFIDENTIALITY** ....................................................................... 9-1
   9.2. **INFORMATION BACKUP** ........................................................................................ 9-1

10. **APPLICATION SECURITY** .......................................................................................... 10-1
    10.1. **APPLICATION DEVELOPMENT & MAINTENANCE** ............................................... 10-1
    10.2. **CONFIGURATION MANAGEMENT & CONTROL** .................................................. 10-1
11. NETWORK & COMMUNICATION SECURITY .................................................................11-1
   11.1. GENERAL NETWORK PROTECTION .................................................................11-1
   11.2. INTERNET SECURITY .........................................................................................11-1
   11.3. EMAIL SECURITY ...............................................................................................11-2
   11.4. PROTECTION AGAINST COMPUTER VIRUS AND MALICIOUS CODE ..........11-2
   11.5. SOFTWARE AND PATCH MANAGEMENT .........................................................11-3
   11.6. WIRELESS SECURITY .......................................................................................11-3

12. SECURITY RISK ASSESSMENT & AUDITING ......................................................12-1
   12.1. SECURITY RISK ASSESSMENT ........................................................................12-1
   12.2. SECURITY AUDITING .......................................................................................12-1

13. SECURITY INCIDENT MANAGEMENT .................................................................13-1
   13.1. SECURITY INCIDENT MONITORING ...............................................................13-1
   13.2. SECURITY INCIDENT RESPONSE .................................................................13-1
1. **PURPOSE**

This document constitutes a Baseline Information Technology (IT) Security Policy that all HKSAR Government's bureaux and departments shall observe and follow.

The policy statements are developed for all levels of staff acting in different roles within bureaux and departments, including management staff, IT administrators, and general IT end users. In order to help readers quickly identify policy statements that are of most concerns to their roles, a tag is attached to the end of each policy statement (section 6 to section 13) for ease of identification. Multiple tags can be attached to a single policy statement if that statement is applicable to multiple roles.

The following tagging convention with three different roles is used:

[M]: Management

[A]: IT Administrator or Application Development Staff

[U]: Computer End-User

Nevertheless, it is the responsibility for ALL staff to read through the entire document to understand and follow IT security policies accordingly.
2. SCOPE

This document addresses security considerations in the following eight areas:

- Management responsibilities;
- Physical security;
- Access control security;
- Data security;
- Application security;
- Network & communication security;
- Security risk assessment & auditing; and
- Security incident management


In coordinating and promoting IT security in the Government, an Information Security Management Framework comprising the following four parties has been established:

- Information Security Management Committee (ISMC)
- IT Security Working Group (ITSWG)
- Government Information Security Incident Response Office (GIRO)
- Bureaux/Departments

The roles of each party are explained in details in the following sections.
2.1.1. Information Security Management Committee (ISMC)

A central organisation, Information Security Management Committee (ISMC), was established in April 2000 to oversee the IT security within the whole government. The committee meets on a regular basis to:

- Review and endorse changes to the Government IT security related regulations, policies and guidelines;
- Define specific roles and responsibilities relating to IT security; and
- Provide guidance and assistance to bureaux and departments in the enforcement of IT security related policies, through the IT Security Working Group (ITSWG).

The core members of ISMC comprise representatives from:

- Office of the Government Chief Information Officer (OGCIO)
- Security Bureau (SB)

Representative(s) from other bureaux/departments will be co-opted into the Committee on a need basis, in relation to specific subject matters.

2.1.2. IT Security Working Group (ITSWG)

The IT Security Working Group (ITSWG) serves as the executive arm of the Information Security Management Committee (ISMC) in the promulgation and compliance monitoring of Government IT security related regulations, policies and guidelines. The ITSWG was established in May 2000 and its responsibilities are to:

- Co-ordinate activities aimed at providing guidance and assistance to bureaux and departments in the enforcement of IT security related regulations, policies and guidelines;
- Monitor the compliance with the Baseline IT Security Policy at bureaux and departments;
- Define and review the IT security related regulations, policies and guidelines; and
- Promote IT security awareness within the Government.

The core members of ITSWG comprise representatives from:

- Office of the Government Chief Information Officer (OGCIO)
- Security Bureau (SB)
- Hong Kong Police Force (HKPF)
- Chief Secretary for Administration’s Office (CSO)
- Information Technology User-Managers Group (ITUG)

Representative(s) from other bureaux/departments will be co-opted into the Working Group on a need basis, in relation to specific subject matters.
2.1.3. Government Information Security Incident Response Office (GIRO)

To handle information security incidents occurring in bureaux/departments, an Information Security Incident Response Team (ISIRT) should be established in each bureau/department. Meanwhile, the Government Information Security Incident Response Office (GIRO) provides central co-ordination and support to the operation of individual ISIRTs of bureaux/departments.

The GIRO has the following major functions:

- Disseminate security alerts on impending and actual threats to DITSOs;
- Maintain a central inventory and oversee the handling of all information security incidents in the Government;
- Prepare periodic statistics reports on Government information security incidents;
- Act as a central office to coordinate the handling of multiple-point security attacks (i.e. simultaneous attacks on different Government information systems);
- Act as a bridge between the HKCERT and the Government regarding Government's information security incidents; and
- Enable experience sharing and information exchange related to information security incident handling among ISIRTs of different bureaux/departments, and the HKCERT.

The core members of GIRO comprise representatives from:

- Office of the Government Chief Information Officer (OGCIO)
- Security Bureau (SB)
- Hong Kong Police Force (HKPF)

2.1.4. Bureaux / Departments

Bureaux/departments are responsible for the security protection of their information systems and computer facilities. The roles and responsibilities of IT security staff within a bureau/department are detailed in Section 5 - DEPARTMENTAL IT SECURITY ORGANISATION.
2.2. IT Security Document Overview

The following diagram describes the relationship of various IT security documents within the Government:
The purpose and overview of the five core IT security documents are described below:

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baseline IT Security Policy</strong></td>
<td>A top-level directive statement that sets the minimum standards of a security specification for all bureaux / departments. It states what aspects are of paramount importance to a bureau / department. Thus, the Baseline IT Security Policy can be treated as basic rules which must be observed as mandatory while there can still be other desirable measures to enhance the security.</td>
</tr>
<tr>
<td><strong>IT Security Guidelines</strong></td>
<td>Introduces general concepts relating to Information Technology Security and elaborates interpretations on the Baseline IT Security Policy. It also provides readers some guidelines and considerations in defining security requirements.</td>
</tr>
<tr>
<td><strong>Internet Gateway Security Guidelines</strong></td>
<td>Acts as a supplementary document to IT Security Guidelines to provide general guidelines on Internet gateway security. These guidelines represent what are regarded as best practices to maintain security risks at an acceptable level under the Internet open platform. It is intended for staff who are involved in the operational and technical functions of Internet gateway services.</td>
</tr>
<tr>
<td><strong>Security Risk Assessment &amp; Audit Guidelines</strong></td>
<td>Acts as a supplementary document to IT Security Guidelines to give an introduction to a generic model for IT security risk assessment and security audit. This document does not focus on how to conduct a security risk assessment or audit. Rather, it provides a reference model to facilitate the alignment on the coverage, methodology, and deliverables of the services to be provided by independent security consultants or auditors.</td>
</tr>
<tr>
<td><strong>Information Security Incident Handling Guidelines</strong></td>
<td>Acts as a supplementary document to IT Security Guidelines to provide a reference for the management, administration and other technical and operational staff to facilitate the development of security incident handling plan, and to be used for preparation for, detection of, and responding to information security incidents.</td>
</tr>
</tbody>
</table>
3. REFERENCE

3.1. Standards and Guidelines

Nil

3.2. Other References

a) Government of Hong Kong Special Administrative Region, “Security Regulations”

b) Civil Service Branch Circular No. 17/94 – Integrity Checking
4. DEFINITIONS AND CONVENTIONS

4.1. Definitions

a) Information System - an electronic information system that processes data electronically through the use of information technology - including but is not limited to: computer systems, servers, workstations, terminals, storage media, communication devices and network resources.

b) Confidentiality - only authorised persons are allowed to know or gain access to the information stored or processed by Information Systems in any aspects.

c) Integrity - only authorised persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.

d) Availability - Information Systems should be available to users at any given or specified period of time.

e) IT Security Policy - a documented list of management instructions that describe in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorised disclosure, modifications or destruction.

f) Classified Information - refers to the categories of information classified in accordance with the Security Regulations.

g) Staff - persons employed by the Government irrespective of the employment period and terms.

h) Data Centre - a centralized data processing facility that houses Information Systems and related equipment. A control section is usually provided that accepts work from and releases output to users.

i) Computer Room - a dedicated room for housing computer equipment.

j) Malicious Codes - programs that cause undesirable effect to the Information Systems. Examples of malicious codes include computer viruses, network worms, trojan horses, logic bombs, and spyware etc.
4.2. Conventions

4.2.1. The following is a list of conventions used in this Manual

Shall the use of the word ‘shall’ indicates a mandatory requirement.

Should the use of the word ‘should’ indicates a requirement for good practice, which should be implemented whenever possible.

May the use of the word ‘may’ indicates a desirable requirement.
5. **DEPARTMENTAL IT SECURITY ORGANISATION**

This section explains the individual role and responsibility of a departmental IT Security organisation. Multiple roles can be assigned to a single staff depending on resource availability.

The following diagram describes a sample Departmental IT Security organisational framework:

![An Example Organisation Chart for Departmental IT Security Management](chart)

5.1. **Senior Management**

The senior management of bureaux/departments shall have an appreciation of IT security, its problems and resolutions. His/her responsibilities include:

- Direct and enforce the development of security measures;
- Provide the necessary resources required for the measures to be implemented; and
- Ensure participation at all levels of management, administrative, technical and operational staff, and provide full support to them.

5.2. **Departmental IT Security Officer (DITSO)**

1 The actual IT Security Management structure may vary according to the circumstances of each organisation.
Bureaux/departments shall appoint a Departmental IT Security Officer (DITSO) to be responsible for IT security. The roles and responsibilities of DITSO shall be clearly defined which include but are not limited to the following:

- Establish and maintain an information protection program to assist all employees in the protection of the information they use;

- Lead in the establishment, maintenance and implementation of information security policies, standards, guidelines and procedures;

- Coordinate with other bureaux and departments on IT security issues;

- Disseminate security alerts on impending and actual threats from the GIRO to responsible parties within the bureau/department;

- Ensure information security risk assessments and audits are performed as necessary; and

- Initiate investigations and rectification in case of breach of security.

5.3. Departmental Security Officer (DSO)

According to the Security Regulations, the Department Head will appoint a Departmental Security Officer to perform the departmental security related duties. A Departmental Security Officer will take the role as an executive to:

- Discharge responsibilities for all aspects of security for the Bureau / Department; and

- Advise on the set up and review of the security policy.

The Departmental Security Officer may take on the role of the Departmental IT Security Officer. Alternatively, in those bureaux/departments where someone else is appointed, the Departmental IT Security Officer shall collaborate with the DSO to oversee the IT security of the bureau/department.

5.4. Departmental Information Security Incident Response Team (ISIRT) Commander

The ISIRT is the central focal point for coordinating the handling of information security incidents occurring within the respective bureau/department. Heads of bureau/department should designate an officer from the senior management to be the ISIRT Commander. The ISIRT Commander should have the authority to appoint core team members for the ISIRT. The responsibilities of an ISIRT Commander include:

- Provide overall supervision and co-ordination of information security incident handling for all Information Systems within the bureau/department;
- Make decisions on critical matters such as system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery etc.;

- Trigger the departmental disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the bureau/department;

- Provide management endorsement on the provision of resources for the incident handling process;

- Provide management endorsement in respect of the line-to-take for publicity on the incident;

- Collaborate with GIRO in the reporting of information security incidents for central recording and necessary follow up actions; and

- Facilitate experience and information sharing within the bureau/department on information security incident handling and related matters.

5.5. IT Security Administrators

IT Security Administrators are responsible for providing security and risk management related support services. They assist in identifying system vulnerabilities and performing security administrative work of the system. His/her responsibilities also include:

- Maintain control and access to the system;

- Check and manage audit logs;

- Maintain user accounts; and

- Promote security awareness within the bureau/department.

The IT Security Administrator may or may not be a technical person, but he/she should not be the same person as the System Administrator. There should be segregation of duties between the IT Security Administrator and the System Administrator.

5.6. Information Owners

Information Owners are the collators and the owners of information stored in databases and data files. Their primary responsibility is to:

- Determine the security requirements and security classifications, usage and protection of the information.

5.7. LAN/System Administrators
LAN/System Administrators are responsible for the day-to-day administration, operation and configuration of the computer systems and network in bureaux/departments, whereas Internet System Administrators are responsible for the related tasks for their Internet-facing Information Systems. Their responsibilities include:

- Implement the security mechanisms in accordance with procedures/guidelines established by the Departmental IT Security Officers.

5.8. Application Development & Maintenance Team

The Application Development & Maintenance Team is responsible for producing the quality systems in the use of quality procedures, techniques and tools. Their responsibilities include:

- Liaise with the Information Owner in order to agree on system security requirements; and
- Define the solutions to implement these security requirements.

5.9. Users of Information Systems

Users of Information Systems are the staff who actually use the information and shall be accountable for all their activities on the Information Systems. Responsibilities of an information system user include:

- Know, understand, follow and apply all the possible and available security mechanisms to the maximum extent possible; and
- Prevent unauthorised access to their computers and workstations at his/her best effort.
6. MANAGEMENT RESPONSIBILITIES

6.1. General Management

6.1.1. Review of information security policies, standards, guidelines and procedures shall be conducted periodically. [M]

6.1.2. Bureaux/departments shall ensure that security protection is responsive and adaptive to changing environment and technology. [M]

6.1.3. Bureaux/departments shall ensure that the provision for necessary security safeguards and resources are covered in their budgets. [M]

6.1.4. Bureaux/departments shall ensure that an inventory of hardware assets, software assets, valid warranties and maintenance service agreements are properly kept and maintained. [M]

6.1.5. Bureaux/departments shall apply sufficient segregation of duties to avoid execution of all security functions of an Information System by a single individual. [M]

6.1.6. Bureaux/departments shall enforce the least privilege principle when assigning resources and privileges of Information Systems to users. [M]

6.1.7. Bureaux /departments shall ensure the confidentiality, integrity and availability of information and all other security aspects of Information Systems under their control including outsourced systems. [M]

6.1.8. Information security is the responsibility of every member of the staff in the Government. As such, bureaux/departments shall educate users about the IT Security Policy and strengthen their security awareness. [M]

6.1.9. Bureaux /departments shall promulgate and enforce their own IT Security Policy. They shall use the Baseline IT Security Policy document as a basis for their own policy document. [M]

6.1.10. Bureaux/departments shall include in their IT Security Policy a provision advising staff that if they contravene any provision of the Policy they may be subjected to disciplinary action under the Public Service (Administration) Order 1997 (see CSB Circular No. 16/85, available on the Central Cyber Government Office site), and that different levels of disciplinary action may be instigated depending on the severity of the breach. [M]

6.1.11. Bureaux/departments shall also include in their IT Security Policy a provision advising all non-Civil Service contract employees that if they contravene any provision of the Policy, their employment contracts may be terminated depending on the severity of the breach. [M]

6.1.12. Staff who use or have unescorted access to Information Systems and resources shall be carefully selected and they shall be made aware of their own responsibilities and duties. They shall be formally notified of their authorisation to access Information Systems. [M]

6.1.13. Staff shall be educated and trained in order to enable them to discharge their responsibilities and perform their duties relating to IT security. [M]
6.1.14. Bureaux/departments shall advise all staff of their IT security responsibilities upon being assigned a new post, and periodically throughout their term of employment. [M]

6.1.15. Staff handling classified systems or systems containing classified information shall undergo an integrity check as stipulated in CSB Circular 17/94. The type of checking (Appointment Checking / Normal Checking / Extended Checking) shall commensurate with the sensitivity level of the information / system that staff will handle. [M]

6.2. Outsourcing Security

6.2.1. Outsourcing or third party service providers shall observe and comply with bureaux/departments' own departmental IT security policy and other information security requirements issued by the Government. [M]

6.2.2. Bureaux/departments shall monitor and review with the outsourcing or third party service providers to ensure that security operations are managed properly. [M]

6.2.3. External consultants, contractors, outsourced staff, and temporary staff who are engaged in Government work shall be subject to the same information security requirements, and have the same information security responsibilities, as Government staff. [M]

6.3. Contingency Management

6.3.1. Plans for emergency response and disaster recovery of mission critical Information Systems shall be fully documented, regularly tested and tied in with the Business Continuity Plan. [M] [A]
7. PHYSICAL SECURITY

7.1. Environment

7.1.1. Careful site selection and accommodation planning of a purpose-built computer installation shall be conducted. Reference to the security specifications for construction of special installation or office as standard should be made. [M] [A]

7.1.2. **Data centres** and **computer rooms** shall have good physical security and strong protection from disaster and security threats, whether natural or caused by other reasons, in order to minimize the extent of loss and disruption. [M] [A]

7.1.3. Backup media containing business essential and/or mission critical information shall be sited at a safe distance from the main site in order to avoid damage arising from a disaster at the main site. [A]

7.1.4. **Data centres** and **computer rooms** shall conform to Level II\(^1\) security if the **Information System** housed involves handling of CONFIDENTIAL information and conform to Level III\(^1\) security for handling of TOP SECRET / SECRET information. [M] [A]

7.2. Equipment Security

7.2.1. All **Information Systems** shall be placed in a secure environment or attended by **staff** to prevent unauthorised access. [A]

7.2.2. **Staff** in possession of laptop, portable computer, personal digital assistant, or mobile computing devices for business purposes shall safeguard the equipment in his/her possession, and shall not leave the equipment unattended without proper security measures. [U]

7.2.3. IT equipment shall not be taken away from sites without proper control. [M] [A]

7.3. Physical Access Control

7.3.1. A list of persons who are authorised to gain access to **data centres**, **computer rooms** or other areas supporting critical activities, where computer equipment and data are located or stored, shall be kept up-to-date and be reviewed periodically. [A]

7.3.2. All access keys, cards, passwords, etc. for entry to any of the computer systems and networks shall be physically secured or subject to well-defined and strictly enforced security procedures. [A]

7.3.3. All visitors to **data centres** or **computer rooms** shall be monitored at all times by an authorised Government staff member. [A]

---

7.3.4. Automatic protection features (e.g. password protected screen saver, keyboard lock) in servers, computer terminals, workstations or microcomputers should be activated if there has been no activity for a predefined period of time to prevent illegal system access attempt. Alternatively, the logon session and connection should be terminated. Also, user workstation should be switched off, if appropriate, before leaving work for the day or before a prolonged period of inactivity. [A] [U]

7.3.5. All staff with separate personal offices that can be directly accessed from public area and contain Information System(s) should lock the doors when these offices are not in use. [U]

7.3.6. The display screen of an Information System on which classified information can be viewed shall be carefully positioned so that unauthorised persons cannot readily view it. [A] [U]
8. ACCESS CONTROL SECURITY

8.1. Data Access Control

8.1.1. Access to information shall not be allowed unless authorised by the relevant information owners. [A] [U]

8.1.2. Data access rights shall be granted to users based on a need-to-know basis. [A] [U]

8.1.3. Data access rights shall be clearly defined and reviewed periodically. [A]

8.1.4. Access to an Information System containing CONFIDENTIAL or above classification information shall be restricted by means of logical access control. [A]

8.2. Authentication

8.2.1. Access to classified information without appropriate authentication shall not be allowed. [A] [U]

8.2.2. Authentication shall be performed in a manner commensurate with the sensitivity of the information to be accessed. [A]

8.2.3. Consecutive unsuccessful log-in trials shall be controlled. [A]

8.3. Privacy

8.3.1. Management reserves the right to examine all information stored in or transmitted by Government Information Systems in accordance with the Personal Data (Privacy) Ordinance. [M] [U]

8.4. User Identification

8.4.1. Each user identity (user-ID) shall uniquely identify only one user. Shared or group user-IDs are not permitted unless explicitly approved by the Departmental IT Security Officer. [A] [U]

8.4.2. Users are responsible for all activities performed with their user-IDs. [U]

8.5. User Privileges Management

8.5.1. All accounts shall be revoked after a pre-defined period of inactivity. [A]

8.5.2. User privileges shall be reviewed periodically. [A]

8.5.3. At the time that a member of the staff is transferred or ceases to provide services to the Government, all related Information Systems privileges shall be promptly terminated.
The outgoing officer shall be responsible for the handover of computer resources to his/her supervisor or the incoming officer for business continuity. [M] [A] [U]

8.5.4. The use of special privileges shall be restricted and controlled. [A]

8.6. Password Management

8.6.1. Bureaux/departments shall define a strict password policy that details at least, minimum password length, initial assignment, restricted words and format, password life cycle, and include guidelines on suitable system and user password selection. [M] [A]

8.6.2. Passwords shall not be shared or divulged unless necessary (e.g., helpdesk assistance, shared PC and shared files). The risk of sharing passwords is that it increases the probability of security being compromised. If passwords must be shared, explicit approval from the Departmental IT Security Officer must be obtained. Besides, the shared passwords should be changed promptly when the need no longer exists and should be changed frequently if sharing is required on a regular basis. [A] [U]

8.6.3. Passwords shall always be well protected when held in storage. Passwords shall be encrypted when transmitted over an un-trusted communication network. Compensating controls shall be applied to reduce the risk exposure of Information Systems to an acceptable level if encryption is not implementable. [A]

8.6.4. Staff are prohibited from capturing or otherwise obtaining passwords, decryption keys, or any other access control mechanism, which could permit unauthorised access. [U]

8.6.5. All vendor-supplied default passwords shall be changed before any Information System is put into operation. [A] [U]

8.6.6. All passwords shall be promptly changed if they are suspected of / are being compromised, or disclosed to vendors for maintenance and support. [A] [U]

8.7. Network Access Control

8.7.1. Prior approval from the Departmental IT Security Officer is required to connect a departmental Information System with another Information System under the control of another bureau/department. The security level of the Information System being connected shall not be downgraded. [A]

8.8. Logging

8.8.1. Bureaux/departments shall define policies relating to the logging of activities of Information Systems under their control according to the business needs and data classification. [M] [A]

8.8.2. Any log kept shall provide sufficient information to support comprehensive audits of the effectiveness of, and compliance of security measures. [A]
8.8.3. Logs shall be retained for a period commensurate with their usefulness as an audit tool. During this period, such logs shall be secured such that they cannot be modified, and can only be read by authorised persons. [A]

8.8.4. Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity supported by the Departmental IT Security Officer. [A] [U]

8.8.5. Regular checking on log records, especially on system/application where classified information is processed/stored, shall be performed, not only on the completeness but also the integrity of the log records. All system and application errors which are suspected to be triggered as a result of security breaches shall be reported and logged. [M] [A] [U]

8.8.6. Clock synchronisation should be configured to keep clocks of Information Systems in sync. [A]
9. DATA SECURITY

9.1. Overall Data Confidentiality

9.1.1. Information about Information Systems that may compromise the security of those systems shall not be disclosed to users, or any other third parties, except on a need-to-know basis and only if authorised by the Departmental IT Security Officer. [A]

9.1.2. Staff shall not disclose information about the individuals, bureaux/departments or specific systems that have suffered from damages caused by computer crimes and computer abuses, or the specific methods used to exploit certain system vulnerabilities, to any people other than those who are handling the incident and responsible for the security of such systems, or authorised investigators involving in the investigation of the crime or abuse. [U]

9.1.3. Staff shall not disclose to any unauthorised persons the nature and location of the Information Systems, and the information system controls that are in use or the way in which they are implemented. [U]

9.1.4. All stored information classified as CONFIDENTIAL or above shall be encrypted. [A] [U]

9.1.5. Bureaux/departments shall comply with the Security Regulations in relation to Information Systems security including, but not limited to, storage, transmission, processing, and destruction of classified information. [M] [A] [U]

9.2. Information Backup

9.2.1. Backup and recovery procedures shall be well documented, properly implemented, and tested periodically. [A]

9.2.2. Backups shall be carried out at regular intervals. [A]

9.2.3. Backup activities shall be reviewed regularly. [A]

9.2.4. Integrity copies of backups shall be stored at a remote distance from the system and be protected. Backup media should also be protected against unauthorized access, misuse or corruption during transportation. [A]
10. APPLICATION SECURITY

10.1. Application Development & Maintenance

10.1.1. Application development staff shall include security planning and implement the appropriate security measures and controls for system under development according to the systems' security requirements. [A]

10.1.2. Documentation and listings of applications shall be properly maintained and restricted on a need-to-know basis. [A]

10.1.3. Formal testing and review on the security controls shall be performed prior to implementation. [A]

10.1.4. The integrity of an application shall be maintained with appropriate security controls such as version control mechanism and separation of environments for development, system testing, acceptance testing, and live operation. [A]

10.1.5. Application development staff shall not be permitted to access production information unless necessary. [A]

10.2. Configuration Management & Control

10.2.1. Change control procedures for requesting and approving program/system changes shall be documented. [A]

10.2.2. Changes affecting existing security protection mechanisms shall be carefully considered. [A]

10.2.3. Installation of all computer equipment and software shall be done under control and audit. [A]

10.2.4. Bureaux/departments shall ensure that staff are formally advised of the impact of security changes and usage on Information Systems. [M] [A]
11. NETWORK & COMMUNICATION SECURITY

11.1. General Network Protection

11.1.1. Internal network addresses, configurations and related system or network information shall not be publicly released without the approval of the concerned bureau/department. [A]

11.1.2. All internal networks with connections to other Government networks or publicly accessible computer networks shall be properly protected. [A]

11.1.3. Security measures shall be in place to prevent unauthorised remote access to the systems and data. [A]

11.1.4. **Staff** are prohibited from connecting workstations to external network by means of communication device, such as dial-up modem, wireless interface, or broadband link, if the workstations are simultaneously connected to a local area network (LAN) or another internal communication network, unless with the approval of the concerned bureau/department. [U]

11.1.5. **Staff** shall not connect any unauthorised Information System device to a Government Information System without prior approval as designated by the bureau/department. [U]

11.1.6. Proper configuration and administration of information / communication systems is required and shall be reviewed regularly. [A]

11.1.7. Connections and links made to other network shall not compromise the security of information processed at another, and vice versa. [A]

11.1.8. Connecting privately owned computer resources to Government internal network requires approval from the Departmental IT Security Officer. Bureaux and departments shall ensure that such usage of personal computer resources conform to the same IT security policy. [U]

11.1.9. CONFIDENTIAL / RESTRICTED information shall be encrypted when transmitted over an un-trusted communication network. [A] [U]

11.1.10. TOP SECRET / SECRET information shall be transmitted only under encryption and inside an isolated LAN approved by the Government Security Officer subject to the technical endorsement of OGCIO. [A] [U]

11.2. Internet Security

11.2.1. All Internet access shall be either through centrally arranged Internet gateways or bureau/department’s own Internet gateway conforming to OGCIO security standards. In circumstances where this is not feasible or having regard to the mode of use\(^1\),

\(^{1}\) Such modes of use may include, for example, Internet surfing, email exchange, and the use of official, portable computers while on business. The relevant standalone machines must still be protected by any applicable security mechanisms.
bureaux/departments may consider allowing Internet access through stand-alone machines, provided that there is an approval and control mechanism at appropriate level in the bureaux/departments. [A]

11.2.2. Bureaux/departments should consider the value versus inconvenience of implementing technologies to blocking non-business web sites. The ability to connect with a specific web site does not in itself imply that users of systems are permitted to visit that site. [M]

11.2.3. Each bureau/department shall clearly define and communicate to users its policy in relation to acceptable Internet usage. [M]

11.2.4. All software and files downloaded from the Internet shall be screened and verified with anti-virus software. [A] [U]

11.2.5. Staff should not execute mobile code or software downloaded from the Internet unless the code is from a known and trusted source. [U]

11.3. Email Security

11.3.1. Each bureau/department shall clearly define and communicate to users its policy in relation to acceptable email usage. [M]

11.3.2. Systems administrators shall establish and maintain a systematic process for the recording, retention, and destruction of electronic mail messages and accompanying logs. [A]

11.3.3. Incoming/outgoing email shall be screened for computer viruses and malicious codes. [A] [U]

11.3.4. Internal email address lists containing entries for authorised users or Government sites shall be properly maintained and protected from unauthorised access and modification. [A]

11.3.5. Email transmission of classified information shall be transmitted only on an Information System approved by the Government Security Officer subject to the technical endorsement of OGCIO. Email transmission of TOP SECRET / SECRET information shall also follow the condition as stipulated in 11.1.10. [U]

11.3.6. Emails from suspicious sources should not be opened or forwarded. [U]

11.4. Protection Against Computer Virus and Malicious Code

11.4.1. Anti-virus software shall always be enabled on all local area network servers and personal computers, and computers connecting to the Government internal network via remote access channel. [A] [U]

11.4.2. Bureaux/departments shall protect their Information Systems from computer viruses and malicious codes. Virus signatures, malicious code definitions as well as their detection and repair engines shall be updated regularly and whenever necessary. [A] [U]
11.4.3. Storage media and files from unknown source or origin shall not be used unless the storage media and files have been checked and cleaned for computer viruses and malicious codes. [U]

11.4.4. Users shall not intentionally write, generate, copy, propagate, execute or involve in introducing computer viruses or malicious codes. [U]

11.4.5. Bureaux/departments shall implement proper measures to protect their wireless or mobile computing devices against computer viruses and malicious codes. [A] [U]

11.5. Software and Patch Management

11.5.1. Computers and networks shall only run software that comes from trustworthy sources. [U]

11.5.2. No unauthorised application software shall be loaded onto a Government Information System without prior approval from officer as designated by the bureau/department. [A] [U]

11.5.3. Bureaux/departments shall protect their Information Systems from known vulnerabilities by applying the latest security patches recommended by the product vendors or implementing other compensating security measures. [A] [U]

11.5.4. Before security patches are applied, proper risk evaluation and testing should be conducted to minimize the undesirable effects to the Information Systems. [A] [U]

11.6. Wireless Security

11.6.1. Bureaux/departments shall document, monitor, and control wireless networks with connection to Government internal network. [A]

11.6.2. Proper authentication and encryption security controls shall be employed to protect data communication over wireless networks with connection to Government internal network. [A] [U]
12. SECURITY RISK ASSESSMENT & AUDITING

12.1. Security Risk Assessment

12.1.1. **Information Systems** security risk assessments for information systems and production applications shall be performed at least once every two years. A security risk assessment shall also be performed prior to major enhancements and changes associated with these systems or applications. [M]

12.1.2. Use of software and programs for security risk assessment analysis shall be restricted and controlled. [A]

12.2. Security Auditing

12.2.1. **Information Systems** shall be periodically evaluated by auditors of an independent and trusted party to determine the minimum set of controls required to reducing risk to an acceptable level. [M]

12.2.2. Auditing of compliance of computer and network security policies shall be performed periodically. [A]

12.2.3. Use of software and programs for security audit analysis shall be restricted and controlled. [A]
13. SECURITY INCIDENT MANAGEMENT

13.1. Security Incident Monitoring

13.1.1. Bureaux/departments shall establish an incident detection and monitoring mechanism to detect, contain and ultimately prevent security incidents. [M]

13.1.2. Bureaux/departments shall ensure that system logs and other supporting information are retained for the proof and tracing of security incidents. [A]

13.2. Security Incident Response

13.2.1. Bureaux/departments shall establish, document and maintain a security incident handling/reporting procedure for their Information Systems. [M]

13.2.2. Staff shall be made aware of the security incident handling/reporting procedure that is in place and shall observe and follow it accordingly. [M]

13.2.3. All network or systems software malfunctions, information security alerts, warnings, suspected vulnerabilities, and the like, and suspected network security problems, shall be reported immediately only to the responsible party according to the incident handling procedure. [A] [U]

13.2.4. Immediate follow-up actions are required on suspected system intrusion according to security incident handling/reporting procedures. [A]

*** End ***