Digital Policy Office

INFORMATION SECURITY

Baseline IT Security Policy

[S17]

Version 8.1

July 2024

© The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of the Government of the Hong Kong Special Administrative Region of the People's Republic of China.

COPYRIGHT NOTICE

© 2024 by the Government of the Hong Kong Special Administrative Region of the People's Republic of China

Unless otherwise indicated, the copyright in the works contained in this publication is owned by the Government of the Hong Kong Special Administrative Region of the People's Republic of China. 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 of the People's Republic of China. All rights reserved."

If you wish to make copies for purposes other than that permitted above, you should seek permission by contacting the Digital Policy Office.

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
1	The Revision Report is available at the government intranet portal ITG InfoStation		2.0	April 2003
2	Change "Information Technology Services Department" (or "ITSD") to "Office of the Government Chief Information Officer" (or "OGCIO")		2.1	July 2004
3	Change "HKCERT/CC" to "HKCERT" as the revised acronym for Hong Kong Computer Emergency Response Team Coordination Centre	2-2, 2-3	2.2	September 2004
4	Updates were made accordingly to comply with the revised government security requirements.	11-1, 11-2	2.3	November 2004
5	The Revision Report is available at the government intranet portal ITG InfoStation		3.0	May 2006
6	Updated section 8.3.1 and 9.1.6 for observance of Personal Data (Privacy) Ordinance.	8-1, 9-1	3.1	November 2008
7	The Revision Report is available at the government intranet portal ITG InfoStation		4.0	December 2009
8	The Revision Report is available at the government intranet portal ITG InfoStation		5.0	September 2012
9	The Revision Report is available at the government intranet portal ITG InfoStation		6.0	December 2016
10	The Revision Report is available at the government intranet portal ITG InfoStation: (https://itginfo.ccgo.hksarg/content/itsecure/review2021/documents.shtml)		7.0	March 2021

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
11	The Revision Report is available at the government intranet portal ITG InfoStation		8.0	April 2024
12	Change “Office of the Government Chief Information Officer” (or “OGCIO”) to “Digital Policy Office” (or “DPO”) Revise the name of Hong Kong Computer Emergency Response Team Coordination Centre in Chinese version		8.1	July 2024

TABLE OF CONTENTS

1. PURPOSE

With the effective use of Internet services and the general adoption of cloud and mobile computing, the security and survivability of information systems are essential to the economy and society. Our increasing dependence on IT for office works and public services delivery has brought new business focus that the key information systems and data we rely on have to be secure and actively protected for the smooth operations of all government bureaux and departments (B/Ds), underpinning public confidence, security and privacy are fundamental to the effective, efficient and safe conduct of government business.

This document outlines the mandatory minimum security requirements for the protection of all HKSAR government information systems and data assets. B/Ds shall develop, document, implement, maintain and review appropriate security measures to protect their information systems and data assets by:

- Establishing appropriate IT security policy, planning and governance within the B/D in line with this document, including adopting all frameworks and requirements;
- Ensuring appropriate security measures are implemented as detailed in this document;
- Ensuring regular review on continuing suitability, adequacy and effectiveness of the security measures; and
- Improving the suitability, adequacy and effectiveness of the security measures.

The security requirements in this document are designed to be technology neutral. The policy requirements focus on the fundamental objectives and controls to protect information during processing, storage, and transmission.

2. SCOPE

2.1. Applicability

This document adopts and adapts the security areas and controls specified in the Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001: 2022) and the Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002: 2022) published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This document addresses the mandatory security considerations in the following 14 areas:

- Management responsibilities (see section 7);
- IT security policies (see section 8);
- Human resource security (see section 9);
- Asset management (see section 10);
- Access control (see section 11);
- Cryptography (see section 12);
- Physical and environmental security (see section 13);
- Operations security (see section 14);
- Communications security (see section 15);
- System acquisition, development and maintenance (see section 16);
- Outsourcing security (see section 17);
- Security incident management (see section 18);
- IT security aspects of business continuity management (see section 19); and
- Compliance (see section 20).

This document sets the minimum security requirements. B/Ds need to apply enhanced security measures, appropriate to their circumstances and commensurate with the determined risks.

2.2. Target Audience

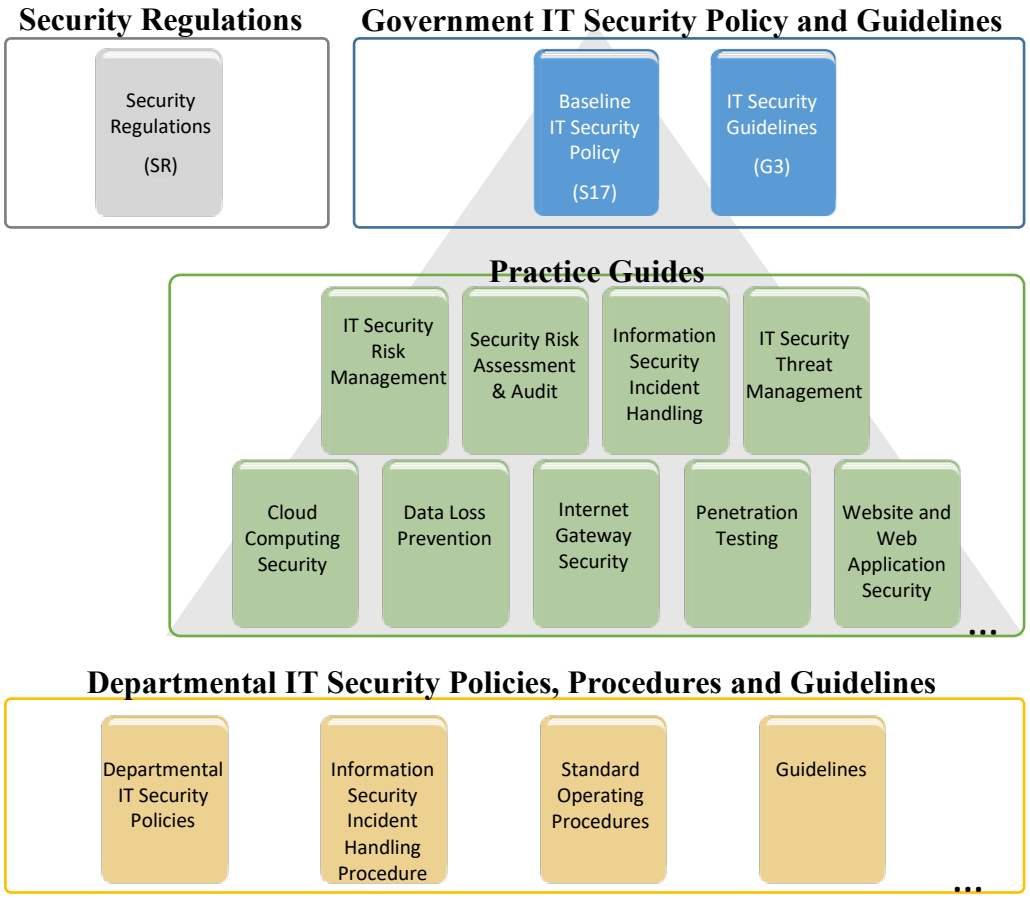
The policy statements are developed for all levels of staff acting in different roles within B/Ds, including management staff, IT administrators, and general IT end users. It is the responsibility of ALL staff to read through the entire document to understand and comply with IT security policies accordingly.

In addition, the document is intended for reference by the vendors, contractors and consultants who provide IT services to the Government.

2.3. Government IT Security Documents

The Government has promulgated a set of security regulations and government IT security policy and guidelines to assist B/Ds in formulating and implementing their IT security policies and control measures to safeguard government information security. B/Ds shall comply with the policy requirements in the Security Regulations (SR), the Baseline IT Security Policy (S17), and the IT Security Guidelines (G3) and follow the implementation guidance in the relevant practice guides. These security documents are indispensable references for information security management.

The following diagram describes the relationship of various IT security documents within the Government:



2.3.1. Security Regulations

Security Regulations, authorised by Security Bureau, provides directives on what documents, material and information need to be classified and to ensure that they are given an adequate level of protection in relation to the conduct of government business.

2.3.2. Government IT Security Policy and Guidelines

The Government IT Security Policy and Guidelines, established by the Digital Policy Office, aim to provide a reference to facilitate the implementation of information security measures to safeguard information assets. References have been made to the Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001: 2022) and the Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002: 2022) published by the ISO and the IEC.

The Government IT Security Policy and Guidelines set out the minimum standards of security requirements and provide guidance on implementing appropriate security measures to protect information assets and information systems.

Baseline IT Security Policy (S17)	A top-level directive statement that sets the minimum standards of a security specification for all B/Ds. It states what aspects are of paramount importance to a B/D. Thus, the Baseline IT Security Policy can be treated as basic rules which shall be observed as mandatory while there can still be other desirable measures to enhance security.
IT Security Guidelines (G3)	Elaborates on the policy requirements and sets the implementation standard on the security requirements specified in the Baseline IT Security Policy. B/Ds shall comply with the IT Security Guidelines for effective implementation of the security requirements.

For topical issues and specific technical requirements, a series of practice guides are developed to support the IT Security Guidelines. Supplementary documents provide guidance notes on specific security areas to assist B/Ds in addressing and mitigating risks brought by emerging technologies and security threats.

All practice guides are available at the ITG InfoStation under the IT Security Theme Page (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml).

2.3.3. Departmental IT Security Policies, Procedures and Guidelines

B/Ds shall formulate their own departmental IT policies, procedures and guidelines based on all the government security requirements and implementation guidance specified in the Security Regulations and the Government IT Security Policy and Guidelines mentioned in Sections 2.3.1 and 2.3.2 above.

3. NORMATIVE REFERENCES

a) The Government of the Hong Kong Special Administrative Region, "Security Regulations"

b) Civil Service Bureau, "Civil Service Regulations"

c) Information security, cybersecurity and privacy protection – Information security management systems – Requirements, ISO/IEC 27001:2022, dated 25 October 2022

d) Information security, cybersecurity and privacy protection – Information security controls, ISO/IEC 27002:2022, dated 15 February 2022

e) Information security technology – Baseline for classified protection of cybersecurity, GB/T 22239-2019, dated 10 May 2019

4. DEFINITIONS AND CONVENTIONS

4.1. Definitions

a)	Tier 1 Information Systems	A related set of hardware and software organised for the collection, processing, storage, communication, or disposition of information, regardless of the source of funding and project type.
b)	Tier 2 Information Systems	Tier 1 information systems which are crucial to the operations of the Government or society and whose failure or disruption will result in a serious impact on government operations or may cause public turmoil and catastrophes.
c)	Essential Services	Services that are critical to the functioning and security of a society and its economy.
d)	Tier 3 Information Systems	Tier 2 information systems which are directly related to the provision of essential service concerned and whose disruption or destruction may cause serious harm to the economy, people's livelihood, public safety, etc.
e)	Confidentiality	Only authorised persons and information systems are allowed to know or gain access to the information stored or processed by information systems in any aspect.
f)	Integrity	Only authorised persons and information systems are allowed to make changes to the information stored or processed by information systems in any aspect.
g)	Availability	Information System is accessible and usable upon demand by authorised persons and information systems.
h)	IT Security Policy	A documented list of management instructions that describes in detail the proper use and management of computer and network resources with the objective of protecting these resources, as well as the information stored or processed by information systems, from any unauthorised disclosure, modifications or destruction.
i)	Classified Information	Refers to the categories of information classified in accordance with the Security Regulations.

j)	Staff	A collective term used to describe all personnel employed or whose service is acquired to work for the Government, including all public officers irrespective of the employment period and terms, non-government secondees engaged through employment agencies, and other term contract services personnel, etc., who may have different accessibility to classified information and are subject to different security vetting requirements. Specific requirements governing human resource security are found in Section 9 of S17.
k)	Data Centre	A centralised data processing facility that houses information systems and related equipment.
l)	Computer Room	A dedicated room for housing computer equipment.
m)	Malware	Programs intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Examples of malware include computer viruses, worms, Trojan horses, and spyware.
n)	Mobile Devices	Portable computing and communication devices with information storage and processing capability. Examples include portable computers, mobile phones, tablets, digital cameras, and audio or video recording devices.
o)	Removable Media	Portable electronic storage media such as magnetic, optical, and flash memory devices, which can be inserted into and removed from a computing device. Examples include external hard drives or solid-state drives, floppy disks, zip drives, optical disks, tapes, memory cards, flash drives, and similar USB storage devices.
p)	Internet of Things (IoT) Devices	Devices that have network connectivity and computing capabilities, which function autonomously to interact with the physical environment by ways of sensing or actuation.

4.2. Conventions

The following is a list of conventions used in this document.

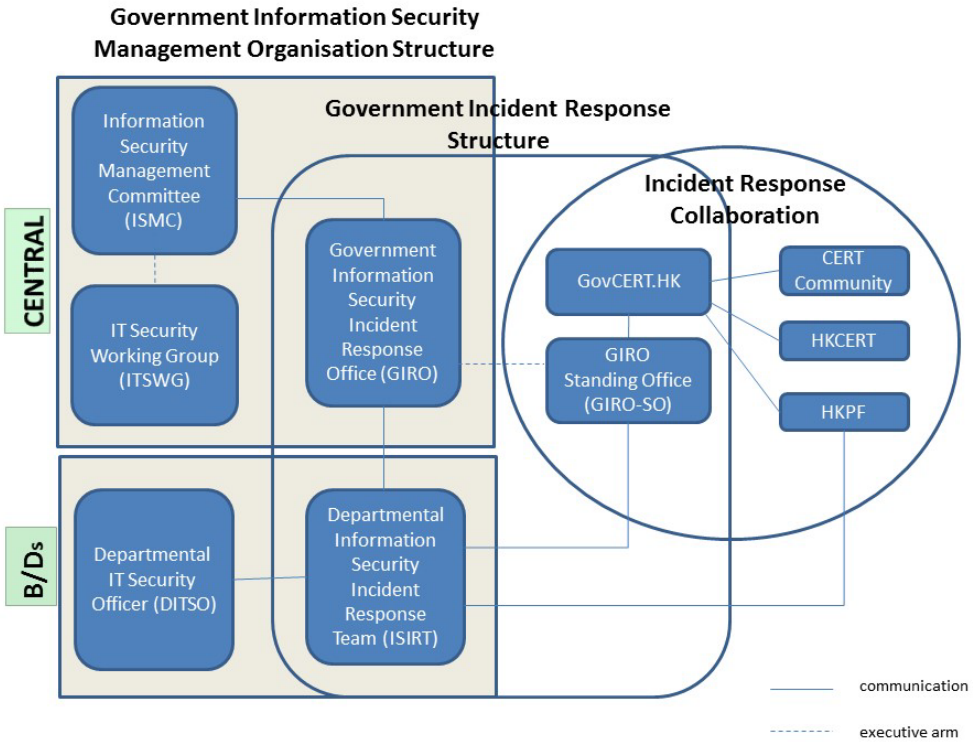
Shall	The use of the word ‘shall’ indicates a mandatory requirement.
Should	The use of the word ‘should’ indicates a best practice, which should be implemented whenever possible.
May	The use of the word ‘may’ indicates a desirable best practice.

5. GOVERNMENT ORGANISATION STRUCTURE ON INFORMATION SECURITY

5.1. Government Information Security Management Framework

To co-ordinate and promote IT security in the Government, an Information Security Management Framework comprising the following five parties has been established:

- Information Security Management Committee (ISMC)
- IT Security Working Group (ITSWG)
- Government Information Security Incident Response Office (GIRO)
- Government Computer Emergency Response Team Hong Kong (GovCERT.HK)
- Bureaux/Departments



Government Information Security Management Framework

The roles and responsibilities of each party are explained in detail in the following sections.

5.1.1. Information Security Management Committee (ISMC)

A central organisation, the Information Security Management Committee (ISMC), was established in April 2000 to oversee 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 B/Ds in the enforcement of IT security related regulations, policies, and guidelines through the IT Security Working Group (ITSWG).

The core members of ISMC comprise representatives from:

- Digital Policy Office (DPO)
- Security Bureau (SB)

Representative(s) from other B/Ds will be co-opted into the committee on a need basis in relation to specific subject matters. DPO will assist in reviewing and clarifying the documents submitted by B/Ds as required in this document.

5.1.2. IT Security Working Group (ITSWG)

The IT Security Working Group (ITSWG) serves as the executive arm of the 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 B/Ds in the enforcement of IT security related regulations, policies and guidelines;
- Monitor the compliance with the Baseline IT Security Policy at B/Ds;
- 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:

- Digital Policy Office (DPO)
- Security Bureau (SB)
- Hong Kong Police Force (HKPF)
- Chief Secretary for Administration's Office (CSO)

Representative(s) from other B/Ds will be co-opted into the working group on a need basis, in relation to specific subject matters.

5.1.3. Government Information Security Incident Response Office (GIRO)

To handle information security incidents occurring in B/Ds, an Information Security Incident Response Team (ISIRT) shall be established in each B/D. The Government Information Security Incident Response Office (GIRO) provides central co-ordination and support to the operation of individual ISIRTs of B/Ds. The GIRO Standing Office serves as the executive arm of GIRO.

The GIRO has the following major functions:

- 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 co-ordinate the handling of multiple-point security attacks (i.e. simultaneous attacks on different government information systems); and
- Enable experience sharing and information exchange related to information security incident handling among ISIRTs of different B/Ds.

The core members of GIRO comprise representatives from:

- Digital Policy Office (DPO)
- Security Bureau (SB)
- Hong Kong Police Force (HKPF)

5.1.4. Government Computer Emergency Response Team Hong Kong (GovCERT.HK)

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) was established in April 2015. In addition to collaborating with GIRO Standing Office in co-ordinating information and cyber security incidents within the Government, it also collaborates with the computer emergency response team community in sharing incident information and threat intelligence, and exchanging best practices to strengthen information and cyber security capabilities in the region. GovCERT.HK has the following major functions:

- Disseminate security alerts on impending and actual threats to B/Ds; and
- Act as a bridge between the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and other computer security incident response teams (CSIRT) in handling cyber security incidents.

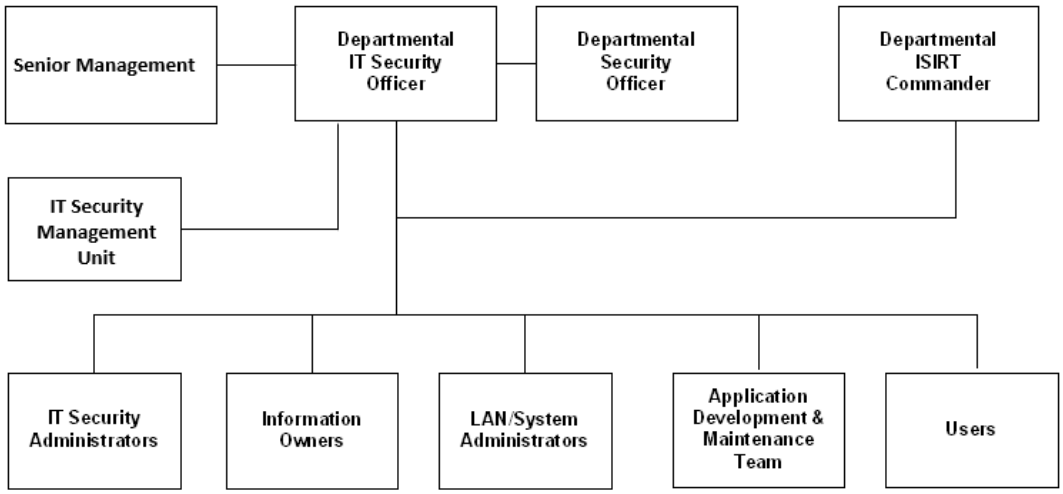
5.1.5. Bureaux/Departments

B/Ds shall be responsible for the security protection of their information assets and information systems. The roles and responsibilities of IT security staff within a B/D are detailed in Section 5.2 - Departmental IT Security Organisation.

5.2. Departmental IT Security Organisation

This section explains the individual roles and responsibilities of a departmental IT security organisation. In order to have sufficient segregation of duties, multiple roles should not be assigned to an individual unless there is a resource limitation.

The following diagram describes a sample departmental IT security management framework:



An Example Organisation Chart for Departmental IT Security Management[1]

5.2.1. Senior Management

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

- Demonstrate leadership in promoting and prioritising IT security within the B/D;
- Direct and enforce the development of security measures;
- Provide the necessary resources required for the measures to be implemented;

[1] The actual IT Security Management structure may vary according to the circumstances of each organisation.

- Ensure participation and accountability at all levels of management, administrative, technical and operational staff, and provide full support to them;
- Foster a culture of security awareness and accountability throughout the B/D; and
- Ensure B/D's IT security strategies align with the business objectives.

5.2.2. Departmental IT Security Officer (DITSO)

Head of B/D shall appoint an officer from the senior management to be the Departmental IT Security Officer (DITSO) and responsible for IT security. Directorate officer responsible for IT management of the B/D is considered appropriate to take up the DITSO role. Depending on the size of the department, departmental grade officers of directorate level who understand the B/D's priorities, the importance of the B/D's information systems and data assets, and the level of security that shall be achieved to safeguard B/Ds, are also considered suitable.

SB and DPO will provide training to DITSOs to facilitate them in carrying out their duties and DITSOs shall attend the designated training. 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 staff in the protection of the information and information systems they use;
- Establish a proper security governance process to evaluate, direct, monitor and communicate the IT security related activities within the B/D;
- Drive regular discussions on IT security issues at the senior management level to acquire adequate support and resources;
- Lead in the establishment, maintenance and implementation of IT security policies, standards, procedures and guidelines;
- Oversee, monitor, review and improve the effectiveness and efficiency of IT security management throughout every stage of IT operations;
- Monitor and ensure compliance with the government IT security requirements;
- Oversee the overall IT security awareness and training programmes within the B/D;
- Co-ordinate with other B/Ds on IT security issues;
- Oversee the overall IT risk management process within the B/D, including ensuring information security risk assessments and audits are performed as necessary and responding to the evolving risk landscape, regulatory changes, technological advancements, and the system criticality;
- Disseminate security alerts on impending and actual threats from the GIRO to responsible parties within the B/D; and
- Initiate investigation and rectification in case of breach of security.

5.2.3. Departmental Security Officer (DSO)

The Head of B/D will designate a Departmental Security Officer (DSO) to perform the departmental security related duties. The DSO will take the role of an executive to:

- Discharge responsibilities for all aspects of security for the B/D; and
- Advise on the set up and review of the security policy.

The DSO may take on the role of the DITSO. Alternatively, in those B/Ds where someone else is appointed, the DITSO shall collaborate with the DSO to oversee the IT security of the B/D.

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

The ISIRT is the central focal point for co-ordinating the handling of information security incidents occurring within the respective B/D. The Head of B/D 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 B/D;
- Make decisions on critical matters such as damage containment, system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery;
- Trigger the departmental disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the B/D;
- 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 reporting information security incidents for central recording and necessary follow-up actions; and
- Facilitate experience and information sharing within the B/D on information security incident handling and related matters.

5.2.5 IT Security Management Unit

B/Ds shall establish an IT security management unit which reports to DITSO and assists DITSO in discharging his/her duties. The size and composition of the unit may vary among B/Ds depending on the business and operational needs of B/Ds. The responsibilities of the IT security management unit include:

- Assist DITSO in developing, establishing, and maintaining the overall IT security strategy and roadmap for the B/D, including formulating IT security policies, baselines, standards, directives, etc;
- Co-ordinate security awareness and training programmes within the B/D;
- Co-ordinate the implementation of IT security initiatives and monitor the status of IT security processes to ensure the effectiveness of IT security management and compliance with government security requirements;
- Facilitate IT security threat and risk management activities and support disaster recovery and business continuity planning functions relating to IT security; and
- Perform any other duties as directed by the DITSO.

5.3. Other Roles

5.3.1. IT Security Administrators

IT Security Administrators shall be responsible for providing security and risk management related support services. His/her responsibilities also include:

- Assist in identifying and mitigating system vulnerabilities;
- Assist in the patch management process;
- Conduct security administrative tasks, such as implementing access controls and managing user privileges;
- Maintain and review audit logs;
- Monitor threat intelligence sources and stay updated on emerging security threats; and
- Operate and maintain security tools and systems, such as intrusion detection and prevention systems.

The IT Security Administrator should not be the same person as the System Administrator. There should be a segregation of duties between the IT Security Administrator and the System Administrator.

Although the IT Security Administrators are responsible for managing the audit logs, they should not tamper with or change any audit log.

B/Ds may appoint an IT Security Auditor, who will be responsible for auditing the work of the IT Security Administrators to ensure that they perform their duties due diligently.

5.3.2. Information Owners

Information Owners shall be the collators and the owners of information stored in information systems. Their primary responsibility is to:

- Determine the data classifications, the authorised data usage, and the corresponding security requirements for protection of the information.

5.3.3. LAN/System Administrators

LAN/System Administrators shall be responsible for the day-to-day administration, operation and configuration of the computer systems and network in B/Ds, whereas Internet System Administrators are responsible for the related tasks for their Internet-facing information systems. Their responsibilities include:

- Implement the security mechanisms and controls in accordance with procedures/guidelines established by the DITSO.

5.3.4. Application Development & Maintenance Team

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

- Liaise with the Information Owner in order to define and implement system security requirements during the development and maintenance of applications; and
- Ensure quality procedures, techniques, and tools are used to produce secure systems.

5.3.5. Users

Users of information systems shall be the staff authorised to access and use the information. Users shall be accountable for all their activities. Responsibilities of a user include:

- Attend security awareness and training programmes directed by the B/D;
- Know, understand, follow and apply all the possible and available security mechanisms to the maximum extent possible;
- Prevent leakage and unauthorised access to information under his/her custody; and
- Safekeep computing and storage devices, and protect them from unauthorised access or malicious attack with his/her best effort.

6. CORE SECURITY PRINCIPLES

This section introduces some generally accepted principles that address information security from a very high-level viewpoint. These principles are fundamental in nature and rarely change. B/Ds shall observe these principles for developing, implementing and understanding security policies. The principles listed below are by no means exhaustive.

- **Information System Security Objectives**
  Information system security objectives or goals are described in terms of three overall objectives: Confidentiality, Integrity and Availability. Security policies and measures shall be developed and implemented according to these objectives.

- **Risk Based Approach**
  A risk based approach shall be adopted to identify, prioritise and address the security risks of information systems in a consistent and effective manner. Proper security measures shall be implemented according to the classified protection of IT security described in Section 7.2 to protect information assets and systems and mitigate security risks to an acceptable level.

- **Security by Design Approach**
  Security by design shall be adopted to incorporate security requirements into the software development lifecycle (SDLC), ensuring that information systems and applications are implemented with appropriate security and data protection measures. Security shall be considered and introduced throughout all phases of the development process in order to minimise rework efforts.

- **Prevent, Detect, Respond and Recover**
  Information security is a combination of preventive, detective, response and recovery measures. Preventive measures avoid or deter the occurrence of an undesirable event. Detective measures identify the occurrence of an undesirable event. Response measures refer to co-ordinated actions to contain damage when an undesirable event (or incident) occurs. Recovery measures restore the confidentiality, integrity and availability of information systems to their expected state.

- **Protection of information while being processed, in transit, and in storage**
  Security measures shall be considered and implemented as appropriate to preserve the confidentiality, integrity, and availability of information while it is being processed, in transit, and in storage. As an example, wireless communication without protection is vulnerable to attacks, and security measures shall be adopted when transmitting classified information.

- **External systems are assumed to be insecure**
  In general, an external system shall be assumed to be insecure. When B/Ds' information assets or information systems connect with external systems, B/Ds shall implement security measures, using either physical or logical means, according to the business requirements and the associated risk levels.

- **Resilience for crucial information systems**
  All crucial information systems shall be resilient to stand against major disruptive events, with measures in place to detect disruption, minimise damage and rapidly respond and recover. Damage containment shall be considered in the resilience plan and implemented as appropriate with an aim to limit the scope, magnitude and impact of an incident for effective recovery.

- **Auditability and Accountability**
  Security shall require auditability and accountability. Auditability refers to the ability to verify the activities in an information system. Evidence used for verification can take the form of audit trails, system logs, alarms, or other notifications. Accountability refers to the ability to audit the actions of all parties and processes which interact with information systems. Roles and responsibilities shall be clearly defined, identified, and authorised at a level commensurate with the sensitivity of information.

  B/Ds shall keep records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures.

- **Continual Improvement**
  To be responsive and adaptive to changing environments and technologies, a continual improvement process shall be implemented for monitoring, reviewing and improving the effectiveness and efficiency of IT security management. Performance of security measures shall be evaluated periodically to determine whether the IT security objectives are met.

7. MANAGEMENT RESPONSIBILITIES

Head of B/Ds shall put in place effective security arrangements to ensure information systems and data assets of the Government are safeguarded, and IT services are delivered securely.

7.1. General Management

7.1.1. B/Ds shall define their departmental IT security organisational framework and the associated roles and responsibilities.

7.1.2. B/Ds shall ensure that security protection is responsive and adaptive to changing environments and technology.

7.1.3. B/Ds shall apply sufficient segregation of duties to avoid the execution of all security functions of an information system by a single individual.

7.1.4. B/Ds shall ensure that the provision for necessary security safeguards and resources are covered in their budgets.

7.1.5. B/Ds shall reserve the right to examine all information stored in or transmitted by government information systems in compliance with the Personal Data (Privacy) Ordinance.

7.2. Security Risk Management

7.2.1 B/Ds shall adopt a risk-based approach to information security to ensure the confidentiality, integrity and availability of information assets and all other security aspects of information systems under their control, including outsourced systems, and monitor compliance with the security policies, guidelines, etc., by their staff and contractors.

7.2.2 B/Ds shall adopt classified protection of IT security by assessing the classifications of all their information systems, including infrastructure facilities and departmental shared IT services, regardless of the source of their funding and implementing tiered security controls according to the system classifications. The assessment details of system classification of all information systems shall be properly documented. The information system classifications shall be endorsed by the Heads of B/Ds or their explicitly delegated officer at directorate level.

8. IT SECURITY POLICIES

B/Ds shall define and enforce their IT security policies to provide management direction and support for protecting information systems and assets in accordance with the business needs and security requirements.

8.1. Management Direction for IT Security

8.1.1. B/Ds shall promulgate and enforce their own IT Security Policy. They shall use the Baseline IT Security Policy document as a basis for their policy development.

8.1.2. B/Ds shall conduct a review of their information security policies, standards, procedures and guidelines periodically.

8.1.3. B/Ds shall clearly define and communicate to users its policy in relation to acceptable use of IT services and facilities.

9. HUMAN RESOURCE SECURITY

B/Ds shall ensure that staff who are engaged in government work are suitable for the roles, understand their responsibilities and are aware of information security risks. B/Ds shall protect the government interests in the process of new, changing or terminating employment.

9.1. New, During or Termination of Employment

9.1.1. B/Ds shall advise all staff of their IT security responsibilities upon being assigned a new post and periodically throughout their term of employment.

9.1.2. Information security is the responsibility of every member of the staff in the Government. Staff shall receive appropriate awareness training and regular updates on the IT Security Policy.

9.1.3. Staff shall be educated and trained periodically in order to enable them to discharge their responsibilities and perform their duties relating to IT security.

9.1.4. Civil servants authorised to access classified information higher than RESTRICTED shall undergo an integrity check as stipulated by the Secretary for the Civil Service. For staff other than civil servants, appropriate background verification checks should be carried out commensurate with the business requirements, the classification of the information that the staff will handle, and the perceived risks.

9.1.5. B/Ds shall include in their IT Security Policy a provision advising civil servants that if they contravene any provision of the Policy, they may be subjected to disciplinary action as stipulated in the Civil Service Regulations and that different levels of disciplinary action may be instigated depending on the severity of the breach.

9.1.6. B/Ds shall include in their IT Security Policy a provision advising all staff other than civil servants which shall be covered in 9.1.5 above, that if they contravene any provision of the Policy, they may be subject to relevant penalty action according to their respective terms of employment, including but not limited to termination of their services to the Government, depending on the severity of the breach.

9.1.7. 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.

9.1.8. No staff shall publish, make private copies of or communicate to unauthorised persons any classified document or information obtained in his official capacity, unless he is required to do so in the interest of the Government. The "need to know" principle shall be applied to all classified information, which should be provided only to persons who require it for the efficient discharge of their work and who have authorised access. If in any doubt as to whether an officer has authorised access to a particular document or classification or information, the Departmental Security Officer should be consulted.

9.1.9. Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the staff and enforced.

10. ASSET MANAGEMENT

B/Ds shall maintain appropriate protection of all hardware, software and information assets and ensure all information systems and assets receive an appropriate level of protection.

10.1. Responsibility for Assets

10.1.1. B/Ds shall ensure that an inventory of information systems, hardware assets, software assets, valid warranties, service agreements and legal/contractual documents are properly owned, kept and maintained.

10.1.2. Information about information systems shall not be disclosed where that information may compromise the security of those systems, except on a need-to-know basis and only if authorised by the DITSO.

10.1.3. 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.

10.1.4. At the time that a member of the staff is transferred or ceases to provide services to the Government, the outgoing officer or staff of external parties shall handover and return computer resources and information to the Government.

10.2. Information Classification

10.2.1. B/Ds shall comply with the government security requirements in relation to the information classification, labelling and handling.

10.2.2. All classified information shall be encrypted in storage irrespective of the storage media.

10.3. Storage Media Handling

10.3.1. B/Ds shall manage the use and transportation of storage media containing classified information.

10.3.2. Storage media with classified information shall be protected against unauthorised access, misuse or physical damage.

10.3.3. All classified information shall be completely cleared or destroyed from storage media before disposal or re-use.

11. ACCESS CONTROL

B/Ds shall prevent unauthorised user access and compromise of information systems and assets and allow only authorised computer resources to connect to the government internal network.

11.1. Business Requirements of Access Control

11.1.1. B/Ds shall enforce the least privilege principle when assigning resources and privileges of information systems to users.

11.1.2. Access to information shall not be allowed unless authorised by the relevant information owners.

11.1.3. Access to information systems containing classified information shall be restricted by means of logical access control.

11.1.4. Access to classified information without appropriate authentication shall not be allowed.

11.2. User Access Management

11.2.1. Procedures for approving, granting and managing user access, including user registration/de-registration, password delivery and password reset, shall be documented.

11.2.2. Data access rights shall be granted to users based on a need-to-know basis.

11.2.3. The use of special privileges shall be restricted and controlled.

11.2.4. User privileges and data access rights shall be clearly defined and reviewed periodically. The review frequency shall be defined and documented. Records for access rights approval and review shall be maintained.

11.2.5. All user privileges and data access rights shall be revoked after a pre-defined period of inactivity or when no longer required. The period of inactivity and the corresponding review frequency shall be defined and documented.

11.2.6. Each user identity (user-ID) shall uniquely identify only one user. Shared or group user-IDs shall not be permitted unless explicitly approved by the DITSO.

11.3. User Responsibilities

11.3.1. Users shall be responsible for all activities performed with their user-IDs.

11.3.2. Passwords shall not be shared or divulged unless necessary (e.g., helpdesk assistance, shared PC and shared files). If passwords must be shared, explicit approval from the DITSO shall 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.

11.3.3. 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 to an acceptable level if encryption is not implementable.

11.4. System and Application Access Control

11.4.1. Authentication shall be performed in a manner commensurate with the sensitivity of the information to be accessed.

11.4.2. Consecutive unsuccessful log-in trials shall be controlled.

11.4.3. B/Ds shall define a strict password policy that details at least minimum password length, initial assignment, restricted words and format, and password life cycle, and include guidelines on suitable systems and user password selection.

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

11.4.5. All vendor-supplied default passwords shall be changed before any information system is put into operation.

11.4.6. All passwords shall be promptly changed if they are suspected of/are being compromised or disclosed to vendors for maintenance and support.

11.5. Mobile Computing and Remote Access

11.5.1. B/Ds shall define appropriate usage policies and procedures specifying the security requirements when using mobile computing and remote access. Appropriate security measures shall be adopted to avoid unauthorised access to or disclosure of the information stored and processed by these facilities. Authorised users should be briefed on the security threats and accept their security responsibilities with explicit acknowledgement.

11.5.2. Security measures shall be in place to prevent unauthorised remote access to government information systems and data.

11.6. IoT Devices

11.6.1. B/Ds shall define and implement proper security measures to ensure the security of IoT devices and data is commensurate with the classification of the information.

11.6.2. The security requirements for mobile devices laid out in this document shall be followed similarly for IoT devices unless it is not technically feasible for implementation. Classified information shall not be stored or processed in privately-owned IoT devices.

12. CRYPTOGRAPHY

B/Ds shall ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

12.1. Cryptographic Controls

12.1.1. B/Ds shall manage cryptographic keys through their whole life cycle, including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

13. PHYSICAL AND ENVIRONMENTAL SECURITY

B/Ds shall prevent unauthorised physical access, damage, theft or compromise of assets, and interruption to the office premises and information systems.

13.1. Secure Areas

13.1.1. 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.

13.1.2. 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 minimise the extent of loss and disruption.

13.1.3. Data centres and computer rooms shall comply with the relevant government requirements on physical security according to the classification of the information system housed.

13.1.4. 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.

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

13.1.6. All visitors to data centres or computer rooms shall be monitored at all times by authorised staff. A visitor access record shall be kept and properly maintained for audit purposes.

13.1.7. All staff shall ensure the security of their offices. Offices that can be directly accessed from public areas and contain information systems or information assets should be locked up when not in use or after office hours.

13.2. Equipment

13.2.1. All information systems shall be placed in a secure environment or attended by staff to prevent unauthorised access. Regular inspection of equipment and communication facilities shall be performed to ensure continuous availability and failure detection.

13.2.2. Staff in possession of mobile devices or removable media for business purposes shall safeguard the equipment in his/her possession and shall not leave the equipment unattended without proper security measures.

13.2.3. IT equipment shall not be taken away from sites without proper control.

13.2.4. If there has been no activity for a pre-defined period of time, to prevent illegal system access attempts, re-authentication shall be activated, or the logon session and connection shall be terminated. Also, the user workstation shall be switched off, if appropriate, before leaving work for the day or before a prolonged period of inactivity.

13.2.5. 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.

14. OPERATIONS SECURITY

B/Ds shall ensure secure operations of information systems, protect the information systems from malware, log IT processes and events, monitor suspicious activities, and prevent exploitation of technical vulnerabilities.

14.1. Operational Procedures and Responsibilities

14.1.1. B/Ds shall manage information systems using the principle of least functionality with all unnecessary services or components removed or restricted.

14.1.2. Changes affecting existing security protection mechanisms shall be carefully considered.

14.1.3. Operational and administrative procedures for information systems shall be properly documented, followed, and reviewed periodically.

14.2. Protection from Malware

14.2.1. Anti-malware protection shall be enabled on all local area network servers, personal computers, mobile devices, and computers connecting to the government internal network via a remote access channel.

14.2.2. B/Ds shall protect their information systems from malware. Malware definitions, as well as their detection and repair engines, shall be updated regularly and whenever necessary.

14.2.3. 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 malware.

14.2.4. Users shall not intentionally write, generate, copy, propagate, execute or involve in introducing malware.

14.2.5. Computers and networks shall only run software that comes from trustworthy sources.

14.2.6. B/Ds should consider the value versus inconvenience of implementing technologies to block non-business websites.

14.2.7. All software and files downloaded from the Internet shall be screened and verified with an anti-malware solution.

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

14.3. Backup

14.3.1. Backups shall be carried out at regular intervals.

14.3.2. B/Ds shall establish and implement backup and recovery policies for their information systems.

14.3.3. Backup activities shall be reviewed regularly. Backup restoration tests shall be conducted regularly. The frequency of backup reviews and restoration tests shall be defined and documented.

14.3.4. Backup media should also be protected against unauthorised access, misuse or corruption.

14.3.5. Backup media containing business essential and/or crucial 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 copy which is disconnected from information systems shall be stored in order to avoid corruption of backup data when an information system is compromised.

14.4. Logging

14.4.1. B/Ds shall define and document policies relating to the logging of activities of information systems under their control (including the retention period) according to the business needs and data classification.

14.4.2. Any log kept shall provide sufficient information to support comprehensive audits of the effectiveness of and compliance with security measures.

14.4.3. 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.

14.4.4. Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity as approved by a directorate officer.

14.4.5. The clocks of information systems shall be synchronised to a trusted time source.

14.5. Control of Operational Environment

14.5.1. Installation of all computer equipment and software shall be done under control and audit.

14.5.2. Changes to information systems shall be controlled by the use of change control procedures. Change records shall be maintained to keep track of the applied changes.

14.6. Technical Vulnerability Management

14.6.1. B/Ds shall implement vulnerability management processes, which include identifying, evaluating, mitigating, and tracking of vulnerabilities of their information systems.

14.6.2. Depending on the risk level, B/Ds shall determine the appropriate patch management strategy, including patch checking and patching frequency for their information systems. B/Ds shall adopt a risk-based approach to determine the patching schedule of each vulnerability by considering its potential impact and the possibility of being exploited. All servers and related devices deployed in Internet-facing information systems shall be subject to stringent patch management.

14.6.3. B/Ds shall protect their information systems from known vulnerabilities by applying the latest security patches recommended by the product vendors according to the patch management strategy or implementing other compensating security measures.

14.6.4. Before security patches are applied, proper risk evaluation and testing should be conducted to minimise the undesirable effects on the information systems.

14.6.5. No unauthorised application software shall be loaded onto a government information system without prior approval from the officer as designated by the B/D.

14.7. IT Security Threat Management

14.7.1. B/Ds shall establish a threat identification, detection and monitoring mechanism and review the mechanism regularly to ensure its effectiveness concerning the nature of information systems and technology advancements.

14.7.2. 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.

15. COMMUNICATIONS SECURITY

B/Ds shall ensure the security of the information transferred within the Government and with any external parties.

15.1. Network Security Management

15.1.1. Internal network addresses, configurations and related system or network information shall be properly maintained and shall not be publicly released without the approval of the concerned B/D.

15.1.2. All internal networks with connections to other government networks or publicly accessible computer networks shall be properly protected.

15.1.3. Proper configuration and administration of information/communication systems is required and shall be reviewed regularly.

15.1.4. B/Ds shall divide their networks into separate network domains to create security boundaries and have better control between them.

15.1.5. Connections made to other networks shall not compromise the security of information processed at another, and vice versa. B/Ds shall define and implement proper security measures to ensure the security level of the departmental information system being connected with another information system under the control of another B/D or external party is not downgraded.

15.1.6. Unauthorised computer resources including those privately-owned shall not be connected to government internal network. If there is an operational necessity, approval from the DITSO shall be sought. B/Ds shall ensure that such usage of computer resources conforms to the same IT security requirements.

15.1.7. B/Ds shall document, monitor, and control wireless communications with connection to government internal network.

15.1.8. Proper authentication and encryption security controls shall be employed to protect data communication over wireless communications with connection to government internal network.

15.1.9. All Internet access shall be either through centrally arranged Internet gateways or B/D's own Internet gateway implemented with secure architecture and proper security measures. In circumstances where this is not feasible or having regard to the mode of use[2], B/Ds may consider allowing Internet access through stand-alone machines, provided that there is an approval and control mechanism at an appropriate level in the B/Ds.

15.1.10. Staff shall not connect workstations and mobile devices to an external network by means of a communication device, such as a dial-up modem, wireless interface, or broadband link, if the workstations or mobile devices are simultaneously connected to a government internal network, unless with the approval from the DITSO.

[2] Such modes of use may include, for example, Internet surfing, electronic message exchange, and the use of official, portable computers while on business trip. The relevant stand-alone machines must still be protected by any applicable security mechanisms.

15.2. Information Transfer

15.2.1. Information classified as higher than CONFIDENTIAL shall be transmitted only under encryption and inside an isolated LAN approved by the Government Security Officer with the technical endorsement of DPO.

15.2.2. CONFIDENTIAL/RESTRICTED information shall be encrypted when transmitted over an un-trusted communication network, and should be encrypted during transmission in any communication network as far as practicable.

15.2.3. 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 DPO.

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

15.2.5. Internal email address lists containing entries for authorised users or government sites shall be properly maintained and protected from unauthorised access and modification.

15.2.6. Agreement on the secure transfer of classified information between B/Ds and external parties shall be established and documented.

15.2.7. Electronic messages from suspicious sources should not be opened or forwarded.

16. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

B/Ds shall ensure that security is an integral part of information systems across the entire life cycle and isolate the development, system testing, acceptance testing, and live operation environments whenever possible.

16.1. Security Requirements of Information Systems

16.1.1. Security planning and implementation of appropriate security measures and controls for systems under development according to the systems' security requirements shall be included.

16.2. Security in Development and Support Processes

16.2.1. B/Ds shall establish and appropriately secure development environments for system development and integration efforts that cover the entire system development life cycle.

16.2.2. Documentation, program source code and listings of applications shall be properly maintained and restricted for access on a need-to-know basis.

16.2.3. Formal testing and review of security measures shall be performed prior to implementation.

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

16.2.5. Change control procedures for requesting and approving program/system changes shall be documented.

16.2.6. B/Ds shall ensure that staff are formally advised of the impact of security changes and usage on information systems.

16.2.7. Application development and system support staff shall not be permitted to access classified information in the production systems unless approval from Information Owner is obtained.

16.3. Test Data

16.3.1. Test data shall be carefully selected, protected and controlled commensurate with its classification. If the use of classified data from production is genuinely required, the process shall be reviewed, documented and approved by Information Owner.

17. OUTSOURCING SECURITY

B/Ds shall ensure the protection of information systems and assets that are accessible by external service providers.

17.1. IT Security in Outsourcing Service

17.1.1 External service providers shall observe and comply with B/Ds' departmental IT security policy and other information security requirements issued by the Government.

17.1.2. B/Ds utilising external services or facilities shall identify and assess the risks to the government data and business operations. Security measures, service levels and management requirements of external services or facilities commensurate with the data classification and business requirements shall be documented and implemented. Security responsibilities of external service providers shall be defined and agreed upon.

17.2. Outsourcing Service Delivery Management

17.2.1. B/Ds shall monitor and review with external service providers to ensure that operations by external service providers are documented and managed properly. Confidentiality and non-disclosure agreements shall be properly managed and reviewed when changes occur that affect the security requirement.

17.2.2. B/Ds shall reserve audit and compliance monitoring rights to ensure external service providers have implemented sufficient controls on government information systems, facilities and data. Alternatively, the external service providers shall provide security audit reports periodically to prove the measures put in place are satisfactory.

17.2.3. B/Ds shall ensure all government data in external services or facilities are cleared or destroyed according to government security requirements at the expiry or termination of the service or upon request of the Government.

17.3. Cloud Computing Security

17.3.1. Information classified as RESTRICTED or above shall not be stored in or processed by public cloud services.

17.3.2 Before signing an agreement with a cloud service provider, B/Ds shall ensure that the shared responsibilities of both parties are clearly defined, documented, and understood.

18. SECURITY INCIDENT MANAGEMENT

B/Ds shall ensure a consistent and effective approach to the management of information security incidents.

18.1. Management of Security Incidents and Improvements

18.1.1. B/Ds shall establish an incident detection and monitoring mechanism to detect, contain and ultimately prevent security incidents.

18.1.2. B/Ds shall ensure that system logs and other supporting information are retained for the proof and tracing of security incidents.

18.1.3. B/Ds shall establish, document, test and maintain a security incident response plan for their information systems.

18.1.4. Staff shall be made aware of the security incident response plan that is in place and shall observe and follow it accordingly.

18.1.5. Any observed or suspected security incidents or security problems in information systems or services shall be reported immediately to the responsible party and handled according to the incident handling procedure.

18.1.6. Staff shall not disclose information about the individuals, B/Ds 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.

19. IT SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

B/Ds shall ensure the availability of information systems and security considerations embedded in disaster recovery plans.

19.1. IT Security Continuity

19.1.1. B/Ds shall plan, implement, and regularly review disaster recovery plans to ensure adequate security measures under such situations.

19.2. Resilience

19.2.1. B/Ds shall ensure adequate resilience to meet the availability requirements of IT services and facilities.

20. COMPLIANCE

B/Ds shall avoid breaches of legal, statutory, regulatory or contractual obligations related to security requirements. Security measures shall be implemented and operated in accordance with the respective security requirements.

20.1. Compliance with Legal and Contractual Requirements

20.1.1. B/Ds shall identify and document all relevant statutory, regulatory and contractual requirements applicable to the operations of each information system.

20.1.2. B/Ds shall keep records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures.

20.1.3. B/Ds shall comply with relevant government requirements in relation to the security of information systems, including, but not limited to, storage, transmission, processing, and destruction of classified information. Information without any security classification should also be protected from unintentional disclosure.

20.1.4. Personal Data (Privacy) Ordinance (Cap. 486) shall be observed when handling personal data. All personal data should be classified as RESTRICTED information or above. Depending on the nature and sensitivity of the personal data concerned and the harm that could result from unauthorised or accidental access, processing, erasure or other use of the personal data, a higher classification and appropriate security measures may be required.

20.2. Security Reviews

20.2.1. 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 before production and prior to major enhancements and changes associated with these systems or applications.

20.2.2. Audit on information systems shall be performed at least once every two years to ensure the compliance of IT security policies and effective implementation of security measures. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

20.2.3. Use of software and programs for performing security risk assessment or security audit shall be restricted and controlled.

21. CONTACT

This document is produced and maintained by the DPO. For comments or suggestions, please send to:

Email: it_security@digitalpolicy.gov.hk

Lotus Notes mail: IT Security Team/DPO/HKSARG@DPO

CMMP email: IT Security Team/DPO

*** ENDS ***