OGC® DOCUMENT: S17

OGC®
Making location count.

BASELINE IT SECURITY POLICY

STANDARD
Implementation

APPROVED

Version: 6.0
Submission Date: XXX
Approval Date: XXX
Publication Date: 2016-12

OGC®
Making location count.

License Agreement

Copyright notice

Note

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The Open Geospatial Consortium shall not be held responsible for identifying any or all such patent rights.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the standard set forth in this document, and to provide supporting documentation.

CONTENTS

I SECURITY CONSIDERATIONS

No security considerations have been made for this document.

1

SCOPE

1 SCOPE

1.1. Applicability

This document adopts and adapts the security areas and controls specified in the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standards on information security management systems (ISO/IEC 27001:2013) and code of practice for information security controls (ISO/IEC 27002:2013). This document addresses mandatory security considerations in the following 14 areas:

- Management responsibilities (see Clause 10);
- IT security policies (see Clause 11);
- Human resource security (see Clause 12);
- Asset management (see Clause 13);
- Access control (see Clause 14);
- Cryptography (see Clause 15);
- Physical and environmental security (see Clause 16);
- Operations security (see Clause 17);
- Communications security (see Clause 18);
- System acquisition, development and maintenance (see Clause 19);
- Outsourcing security (see Clause 20);
- Security incident management (see Clause 21);
- IT security aspects of business continuity management (see Clause 22); and
- Compliance (see Clause 23)

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

1.2. Target Audience

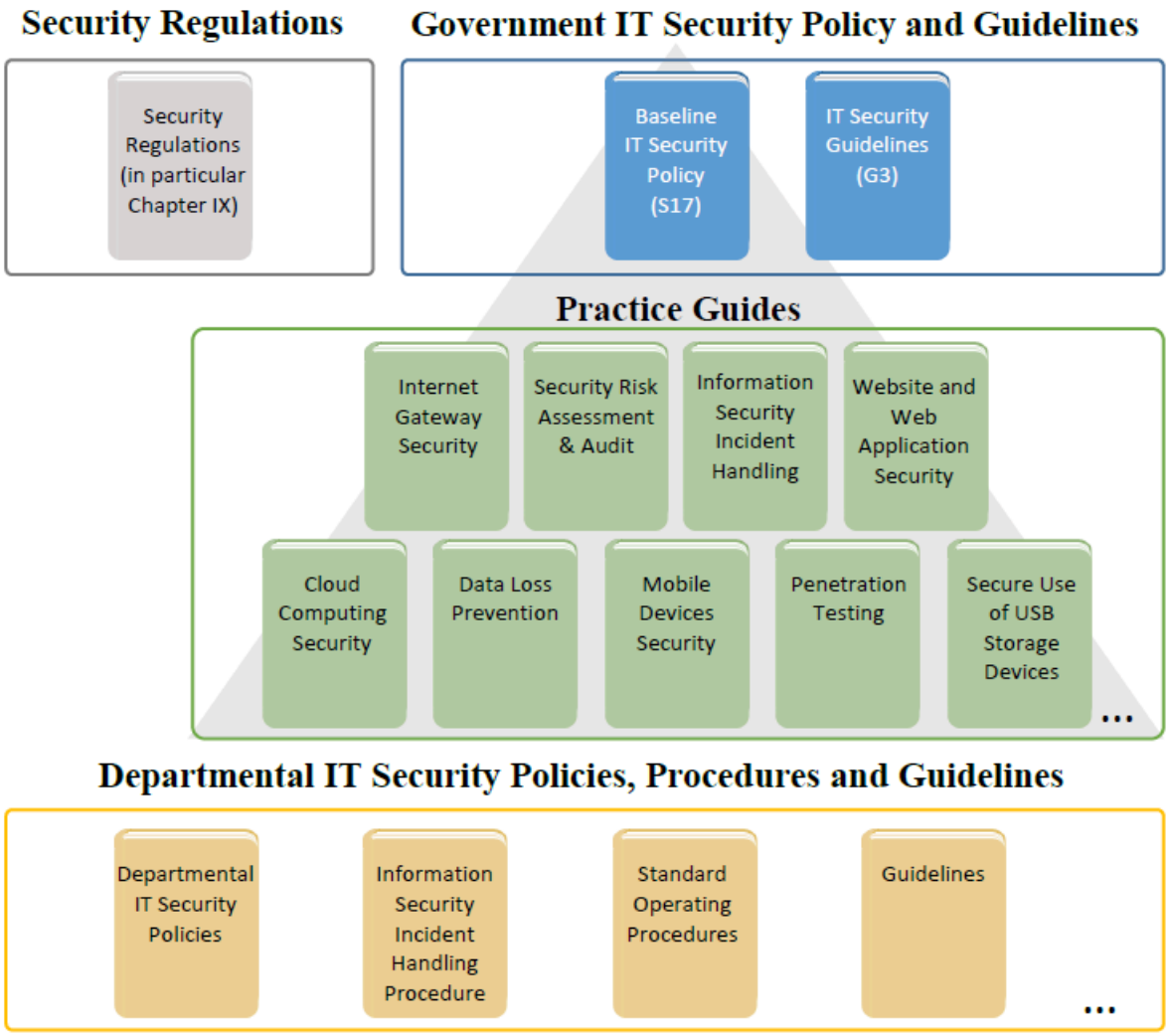
The policy statements are developed for all levels of staff acting in different roles within B/Ds, including management staff, IT administrators, and general IT end users. It is the responsibility for ALL staff to read through the entire document to understand and follow IT security policies accordingly.

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

1.3. 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's information security. B/Ds shall comply with the policy requirements in both the Security Regulations (SR) and the Baseline IT Security Policy (S17), and follow the implementation guidance in the IT Security Guidelines (G3).

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



1.3.1. 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. Chapter IX provides specific requirements to regulate the security of government records in electronic form.

1.3.2. Government IT Security Policy and Guidelines

Government IT Security Policy and Guidelines, established by the Office of the Government Chief Information Officer, aim at providing a reference to facilitate the implementation of information security measures to safeguard information assets. They are made heavy reference to the recognised International standards on information security management systems (ISO/IEC 27001:2013) and code of practice for information security controls (ISO/IEC 27002:2013).

They set out the minimum standards of security requirements and provide guidance on implementing appropriate security measures to protect the 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 the 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 follow 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 provides guidance notes on specific security areas to assist B/Ds to address and mitigate 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).

1.3.3. 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 Clause 1.3.1 and Clause 1.3.2 above.

2

NORMATIVE REFERENCES

2 NORMATIVE REFERENCES

There are no normative references in this document.

1. Government of Hong Kong Special Administrative Region, “Security Regulations”
2. Civil Service Bureau, “Civil Service Regulations”
3. Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001: 2013, dated 1 October 2013
4. Information technology – Security techniques – Code of practice for information security controls, ISO/IEC 27002: 2013, dated 1 October 2013

3

COPYRIGHT NOTICE

3 COPYRIGHT NOTICE

4

AMENDMENT HISTORY

4 AMENDMENT HISTORY

Table 1

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 Security Regulations.	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 (http://itginfo.ccgo.hksarg/content/itsecure/ review2016/amendments.shtml)		6.0	December 2016

5 PURPOSE

5 PURPOSE

With the effective use of Internet services and general adoption of cloud and mobile computing, the security and survivability of information systems are essential to the economy and the 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's 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, while in storage, and during transmission.

6

DEFINITIONS AND CONVENTIONS

6 DEFINITIONS AND CONVENTIONS

6.1. Definitions

Information System	A related set of hardware and software organised for the collection, processing, storage, communication, or disposition of information.
Confidentiality	Only authorised persons are allowed to know or gain access to the information stored or processed by information systems in any aspects.
Integrity	Only authorised persons are allowed to make changes to the information stored or processed by information systems in any aspects.
Availability	Information System is accessible and usable upon demand by authorised persons.
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 to protect these resources as well as the information stored or processed by information systems from any unauthorised disclosure, modifications or destruction.
Classified Information	Refers to the categories of information classified in accordance with the Security Regulations.
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 Clause 12 of S17.
Data Centre	A centralised 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.
Computer Room	A dedicated room for housing computer equipment.
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 etc.

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.
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 disks or solid-state drives, floppy disks, zip disks, optical disks, tapes, memory cards, flash drives, and similar USB storage devices.

7 CONVENTIONS

7 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.

8

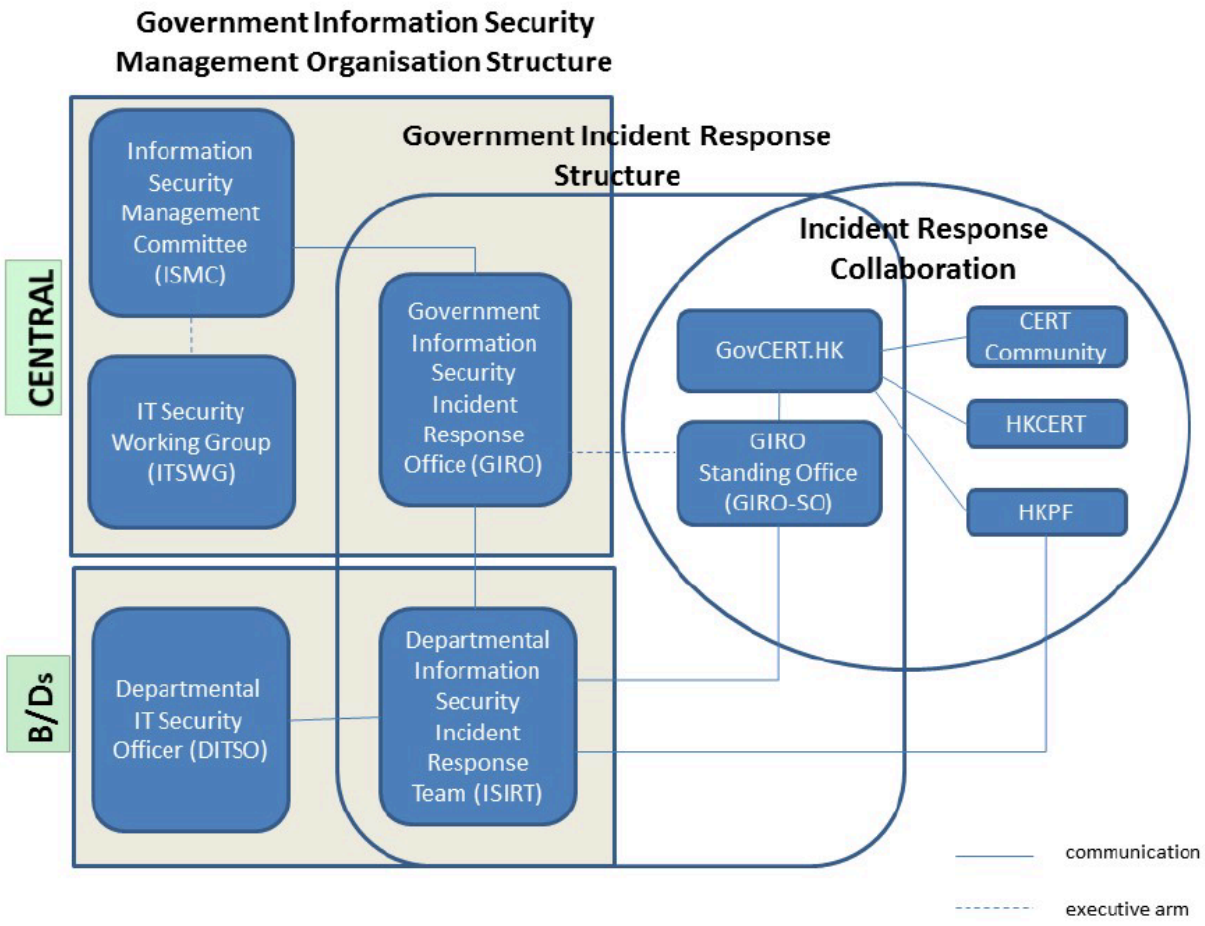
GOVERNMENT ORGANISATION STRUCTURE ON INFORMATION SECURITY

8 GOVERNMENT ORGANISATION STRUCTURE ON INFORMATION SECURITY

8.1. Government Information Security Management Framework

To coordinate and promote 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



Government Information Security Management Framework

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

8.1.1. 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 regulations, policies, and guidelines 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 B/Ds will be co-opted into the Committee on a need basis, in relation to specific subject matters.

8.1.2. 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 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 regulations, policies and guidelines;
- Monitor the compliance with the Baseline IT Security Policy at B/Ds;
- Define and review the IT security 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)

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

8.1.3. 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 coordination and support to the operation of individual ISIRTs of B/Ds. The GIRO Standing Office serves as the executive arm of GIRO.

The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) was established in April 2015. In addition to collaborating with GIRO Standing Office in coordinating 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 with a view to strengthening 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.

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 coordinate 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:

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

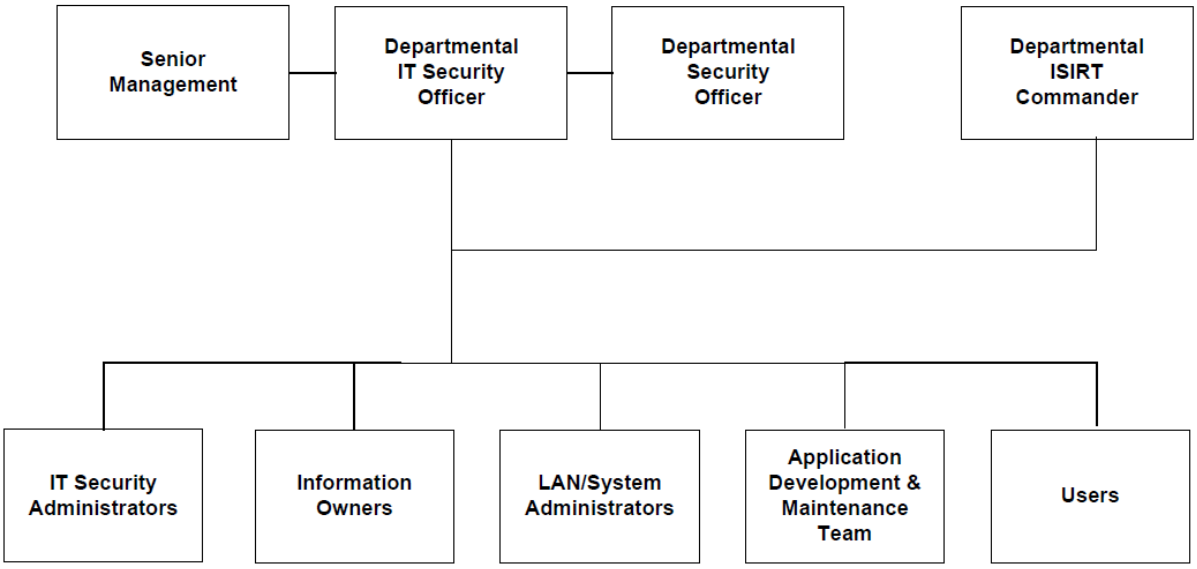
8.1.4. Bureaux/Departments

Bureaux and departments 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 Clause 8.2 — Departmental IT Security Organisation.

8.2. 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]

8.2.1. Senior Management

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

- 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.

8.2.2. 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 at directorate grade 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 OGCIO will provide training to DITSOs to facilitate them in carrying out their duties. B/Ds should ensure that the designated DITSOs have duly received such training. The roles

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

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 system they use;
- Establish proper security governance process to evaluate, direct, monitor and communicate the IT security related activities within the B/D;
- Lead in the establishment, maintenance and implementation of IT security policies, standards, procedures and guidelines;
- Monitor, review and improve the effectiveness and efficiency of IT security management;
- Coordinate with other B/Ds on IT security issues;
- Disseminate security alerts on impending and actual threats from the GIRO to responsible parties within the B/D;
- Ensure information security risk assessments and audits are performed as necessary; and
- Initiate investigations and rectification in case of breach of security.

8.2.3. Departmental Security Officer (DSO)

According to the Security Regulations, the Head of B/D will designate a Departmental Security Officer (DSO) to perform the departmental security related duties. A DSO will take the role as 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.

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

The Departmental Information Security Incident Response Team (ISIRT) is the central focal point for coordinating the handling of information security incidents occurring within the respective B/D. 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 etc.;
- 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 the reporting of 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.

8.3. Other Roles

8.3.1. 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 system vulnerabilities.
- Perform security administrative work of the system.
- Maintain control and access rules to the data and system;
- Check and manage audit logs; and
- Promote security awareness within the B/D.

The IT Security Administrator may 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.

8.3.2. 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.

8.3.3. 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 in accordance with procedures/guidelines established by the DITSO.

8.3.4. Application Development & Maintenance Team

The Application Development & Maintenance Team shall be responsible for producing the quality systems with 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.

8.3.5. 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:

- 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.

9

CORE SECURITY PRINCIPLES

9 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 to protect information assets and systems and mitigate security risks to an acceptable level.

- **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 coordinated actions to contain damage when an undesirable event (or incident) occurs. Recovery measures are for restoring 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, a wireless communication without protection is vulnerable to attacks, 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 critical information systems**
  All critical 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

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.

- **Continual Improvement**
  To be responsive and adaptive to a changing environment and to new technology, 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 IT security objectives are met.

10

MANAGEMENT RESPONSIBILITIES

10 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.

10.1. General Management

1. B/Ds shall define their departmental IT security organisational framework and the associated roles and responsibilities.
2. B/Ds shall ensure the confidentiality, integrity and availability of information assets and all other security aspects of information systems under their control including outsourced systems.
3. B/Ds shall ensure that security protection is responsive and adaptive to changing environment and technology.
4. B/Ds shall apply sufficient segregation of duties to avoid execution of all security functions of an information system by a single individual.
5. B/Ds shall ensure that the provision for necessary security safeguards and resources are covered in their budgets.
6. 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.

11

IT SECURITY POLICIES

11 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.

11.1. Management Direction for IT Security

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.
2. B/Ds shall conduct a review of their information security policies, standards, procedures and guidelines periodically.
3. B/Ds shall clearly define and communicate to users its policy in relation to acceptable use of IT services and facilities.

12

HUMAN RESOURCE SECURITY

12 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's interests in the process of changing or terminating employment.

12.1. During or Termination of Employment

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.

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 IT Security Policy.

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.

4. Civil servants authorised to access CONFIDENTIAL and above information 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.

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.

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.

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.

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

13

ASSET MANAGEMENT

13 ASSET MANAGEMENT

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

13.1. Responsibility for Assets

1. B/Ds shall ensure that an inventory of information systems, hardware assets, software assets, valid warranties and service agreements are properly owned, kept and maintained.
2. Information about information systems shall not be disclosed, where that information may compromise the security of those systems, except on a need-toknow basis and only if authorised by the Departmental IT Security Officer.
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.
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.

13.2. Information Classification

1. B/Ds shall comply with the Security Regulations in relation to the information classification, labelling and handling.
2. All stored information classified as CONFIDENTIAL or above shall be encrypted. RESTRICTED information shall be encrypted when stored in mobile devices or removable media.
3. All classified information shall be encrypted while in storage. For RESTRICTED information not stored in mobile devices or removable media, if data encryption cannot be implemented for whatever reasons, B/Ds shall have upgrade plan with approval from the Heads of B/Ds.

13.3. Storage Media Handling

1. B/Ds shall manage the use and transportation of storage media containing classified information.
2. Storage media with classified information shall be protected against unauthorised access, misuse or physical damage.
3. All classified information shall be completely cleared or destroyed from storage media before disposal or re-use.

14

ACCESS CONTROL

14 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.

14.1. Business Requirements of Access Control

1. B/Ds shall enforce the least privilege principle when assigning resources and privileges of information systems to users.
2. Access to information shall not be allowed unless authorised by the relevant information owners.
3. Access to information systems containing information classified CONFIDENTIAL or above shall be restricted by means of logical access control.
4. Access to classified information without appropriate authentication shall not be allowed.

14.2. User Access Management

1. Procedures for approving, granting and managing user access including user registration/de-registration, password delivery and password reset shall be documented.
2. Data access rights shall be granted to users based on a need-to-know basis.
3. The use of special privileges shall be restricted and controlled.
4. User privileges and data access rights shall be clearly defined and reviewed periodically. Records for access rights approval and review shall be maintained.
5. All user privileges and data access rights shall be revoked after a pre-defined period of inactivity or when no longer required.
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 Departmental IT Security Officer.

14.3. User Responsibilities

1. Users shall be responsible for all activities performed with their user-IDs.
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 Departmental IT Security Officer 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.
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.

14.4. System and Application Access Control

1. Authentication shall be performed in a manner commensurate with the sensitivity of the information to be accessed.
2. Consecutive unsuccessful log-in trials shall be controlled.
3. B/Ds 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.
4. Staff are prohibited from capturing or otherwise obtaining passwords, decryption keys, or any other access control mechanism, which could permit unauthorised access.
5. All vendor-supplied default passwords shall be changed before any information system is put into operation.
6. All passwords shall be promptly changed if they are suspected of/are being compromised, or disclosed to vendors for maintenance and support.

14.5. Mobile Computing and Remote Access

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.

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

15

CRYPTOGRAPHY

15 CRYPTOGRAPHY

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

15.1. Cryptographic Controls

1. B/Ds shall comply with the Security Regulations in relation to the use of cryptographic controls for protection of information.
2. B/Ds shall manage cryptographic keys through their whole life cycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

16

PHYSICAL AND ENVIRONMENTAL SECURITY

16 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.

16.1. Secure Areas

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.
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.
3. Data centres and computer rooms shall conform to Level II[2] security if the information system housed involves handling of CONFIDENTIAL information and conform to Level III2 security for handling of TOP SECRET/SECRET information.
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.
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.
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 purpose.
7. All staff shall ensure the security of their offices. Offices that can be directly accessed from public area and contain information systems or information assets should be locked up when not in use or after office hours.

[2]For detailed security specifications on Level I/II/III security, please refer to the document “Guidelines for Security Provisions in Government Office Buildings” published by the Security Bureau.

16.2. Equipment

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.
2. Staff in possession of mobile device 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.
3. IT equipment shall not be taken away from sites without proper control.
4. If there has been no activity for a predefined period of time, to prevent illegal system access attempt, re-authentication should be activated or 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.
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.

17

OPERATIONS SECURITY

17 OPERATIONS SECURITY

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

17.1. Operational Procedures and Responsibilities

1. B/Ds shall manage information systems using the principle of least functionality with all unnecessary services or components removed or restricted.
2. Changes affecting existing security protection mechanisms shall be carefully considered.
3. Operational and administrative procedures for information systems shall be properly documented, followed, and reviewed periodically.

17.2. Protection from Malware

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.
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.
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.
4. Users shall not intentionally write, generate, copy, propagate, execute or involve in introducing malware.
5. Computers and networks shall only run software that comes from trustworthy sources.
6. B/Ds should consider the value versus inconvenience of implementing technologies to blocking non-business websites.

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

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

17.3. Backup

1. Backups shall be carried out at regular intervals.

2. Backup activities shall be reviewed regularly. Backup restoration tests shall be conducted regularly.

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

4. 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 copy which is disconnected from information systems shall be stored in order to avoid corruption of backup data when an information system is compromised.

17.4. Logging and Monitoring

1. B/Ds shall define policies relating to the logging of activities of information systems under their control according to the business needs and data classification.

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

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.

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 rank officer.

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.

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

17.5. Control of Operational Environment

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

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.

17.6. Technical Vulnerability Management

1. B/Ds 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.

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

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

18

COMMUNICATIONS SECURITY

18 COMMUNICATIONS SECURITY

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

18.1. Network Security Management

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.

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

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

4. Connections made to other network 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.

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

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

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

8. 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[3], B/Ds may consider allowing Internet access through stand-

[3]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.

alone machines, provided that there is an approval and control mechanism at appropriate level in the B/Ds.

9. Staff are prohibited from connecting workstations and mobile devices to external network by means of communication device, such as 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 Departmental IT Security Officer.

18.2. Information Transfer

1. 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.

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.

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 OGCIO.

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

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

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

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

19

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

19 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.

19.1. Security Requirements of Information Systems

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

19.2. Security in Development and Support Processes

1. B/Ds shall establish and appropriately secure development environments for system development and integration efforts that cover the entire system development life cycle.
2. Documentation, program source code and listings of applications shall be properly maintained and restricted for access on a need-to-know basis.
3. Formal testing and review on the security measures shall be performed prior to implementation.
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.
5. Change control procedures for requesting and approving program/system changes shall be documented.
6. B/Ds shall ensure that staff are formally advised of the impact of security changes and usage on information systems.
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.

19.3. Test Data

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

20

OUTSOURCING SECURITY

20 OUTSOURCING SECURITY

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

20.1. IT Security in Outsourcing Service

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

20.2. Outsourcing Service Delivery Management

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.
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 report periodically to prove the measures put in place are satisfactory.
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.

21

SECURITY INCIDENT MANAGEMENT

21 SECURITY INCIDENT MANAGEMENT

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

21.1. Management of Security Incidents and Improvements

1. B/Ds shall establish an incident detection and monitoring mechanism to detect, contain and ultimately prevent security incidents.
2. B/Ds shall ensure that system logs and other supporting information are retained for the proof and tracing of security incidents.
3. B/Ds shall establish, document, test and maintain a security incident handling/reporting procedure for their information systems.
4. Staff shall be made aware of the security incident handling/reporting procedure that is in place and shall observe and follow it accordingly.
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.
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.

22

IT SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

22 IT SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

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

22.1. IT Security Continuity

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

22.2. Resilience

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

23

COMPLIANCE

23 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.

23.1. Compliance with Legal and Contractual Requirements

1. B/Ds shall identify and document all relevant statutory, regulatory and contractual requirements applicable to the operations of each information system.
2. B/Ds shall keep records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures.
3. B/Ds shall comply with the Security Regulations in relation to 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.
4. Personal Data (Privacy) Ordinance (Cap. 486) shall be observed when handling personal data. In accordance with Security Regulations 161(d)(iii), all personal data should be classified RESTRICTED at least, 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.

23.2. Security Reviews

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.
2. Audit on information systems shall be performed periodically 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.

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

24

CONTACT

24 CONTACT

This document is produced and maintained by the Office of the Government Chief Information Officer (OGCIO). For comments or suggestions, please send to:

Email: it_security@ogcio.gov.hk

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