Digital Policy Office

INFORMATION SECURITY

IT Security Guidelines

[G3]

Version 10.2

April 2025

COPYRIGHT NOTICE

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
1	The Revision Report is available at the government intranet portal ITG InfoStation		4.0	April 2003
2	Change "Information Technology Services Department" (or "ITSD") to "Office of the Government Chief Information Officer" (or "OGCIO")		4.1	July 2004
3	Enrich/enhance the document to include more detailed guidance in: – section 10.1.1 "Security Considerations in Application Design and Development" and section 10.7. "WEB APPLICATION SECURITY" for application security – section 10.4. "PROGRAM/SYSTEM TESTING" and section 11.3. "EMAIL SECURITY" for proper/restrictive disclosure of information – section 11.2. "INTERNET SECURITY" for proper restriction of network traffic/ports and system services Change "HKCERT/CC" to "HKCERT" as the revised acronym for Hong Kong Computer Emergency Response Team Coordination Centre	10-2, 10-3 10-7 10-5 11-4 11-3 2-3, 11-15, 13-1	4.2	September 2004
4	Updates were made accordingly to comply with the revised government security requirements	9-3, 9-11, 11-2	4.3	November 2004
5	The Revision Report is available at the government intranet portal ITG InfoStation		5.0	May 2006

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
6	Updated Appendix B accordingly based on the revised government security requirements. Appendix C was updated and all six data protection principles were included.	B-2 C-1	5.1	November 2008
7	The Revision Report is available at the government intranet portal ITG InfoStation		6.0	December 2009
8	The Revision Report is available at the government intranet portal ITG InfoStation		7.0	September 2012
9	The Revision Report is available at the government intranet portal ITG InfoStation		8.0	December 2016
10	The Revision Report is available at the government intranet portal ITG InfoStation: (https://itginfo.ccgo.hksarg/content/itsecure/review2021/documents.shtml)		9.0	March 2021
11	Updated Section 9.1(c) accordingly based on the establishment of Civil Service College. Updated Section 10.3(b) on the flexibility of configuration of degaussing products. Updated Section 11.4(b) and 11.4(c) on the strong password policy. Updated Section 16.1(b) in accordance with a new version of the document.	25 32,34 40-41 85	9.1	August 2022
12	The Revision Report is available at the government intranet portal ITG InfoStation		10.0	April 2024

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
13	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. Updated Section 9.1 (c) and 14.7(b) on the examples of threat intelligence platforms and sources.		10.1	July 2024
14	Updated Section 5.2, 16.1(f), 18.1(b), and 20.2(a) and Appendix C and D to align with the General Circular No. 6/2024. Updated Section 7.2(b) and 16.1(a) to include the timing of determining information system classification. Updated Section 11.5(b) on the use of remote desktop software within the government internal network. Updated Section 14.3(b) on the physical transportation of backup media for offsite storage. Made editorial changes.		10.2	April 2025

TABLE OF CONTENTS

1 PURPOSE

This document elaborates on the policy requirements, sets out the implementation standards for the security requirements specified in the Baseline IT Security Policy, and provides implementation guidance for the effective implementation of the corresponding security measures.

The materials included in this document are prepared irrespective of computer platforms. Bureaux and departments (B/Ds) shall comply with the guidance in this document to implement security controls to satisfy the relevant security requirements. B/Ds may need to customise the security measures appropriate to their circumstances without prejudice to the security level.

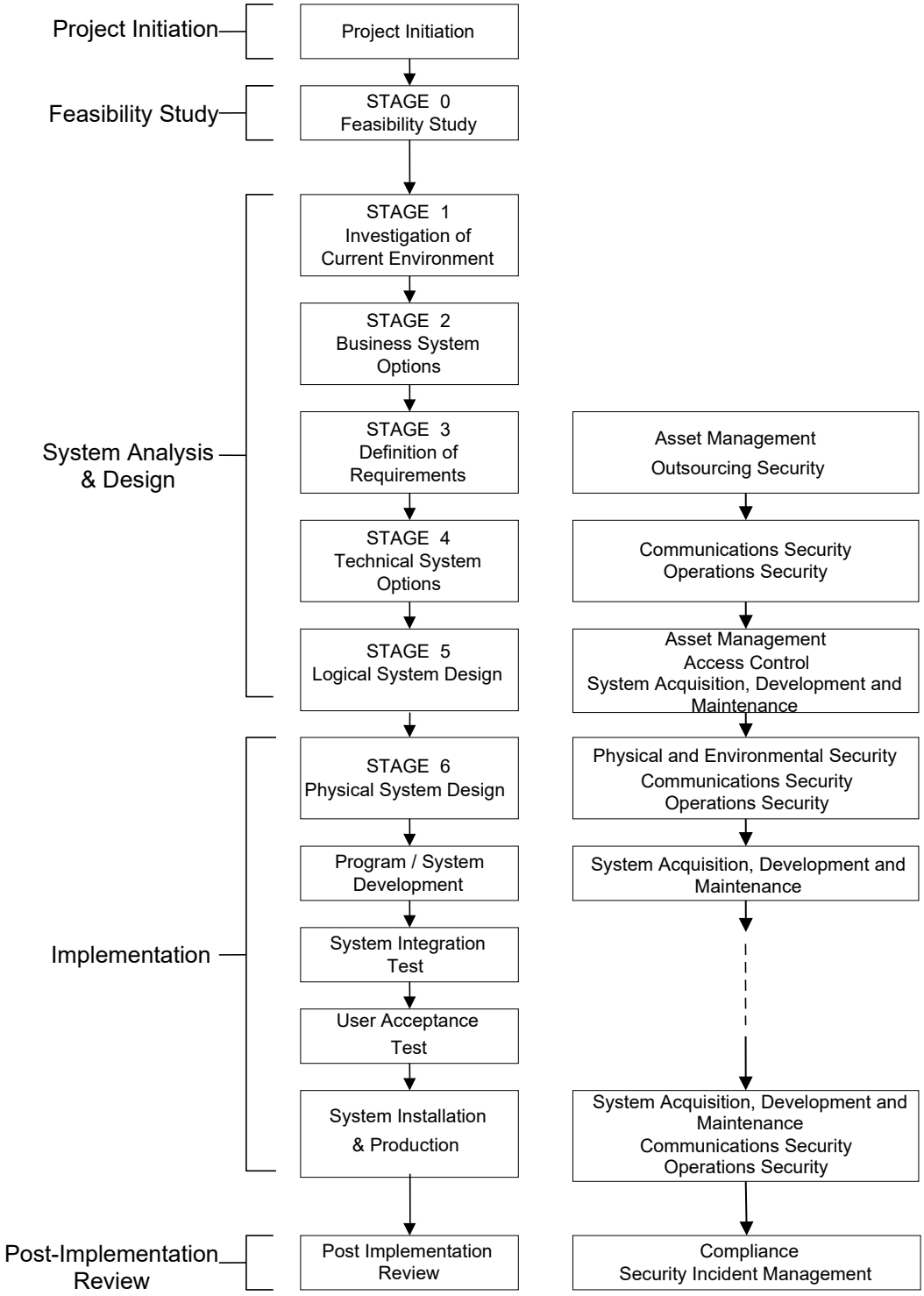
2 SCOPE

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 describes the 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).

Basically, these considerations should be taken into account in all phases of the System Development Life Cycle (SDLC). There are, however, specific areas in certain SDLC phases which need special attention. These areas are highlighted in the chart on the following page.



Security Considerations Related to Different Phases of System Development Life Cycle

2.2 Target Audience

The document is 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 document to understand and comply with it in order to implement the security requirements effectively.

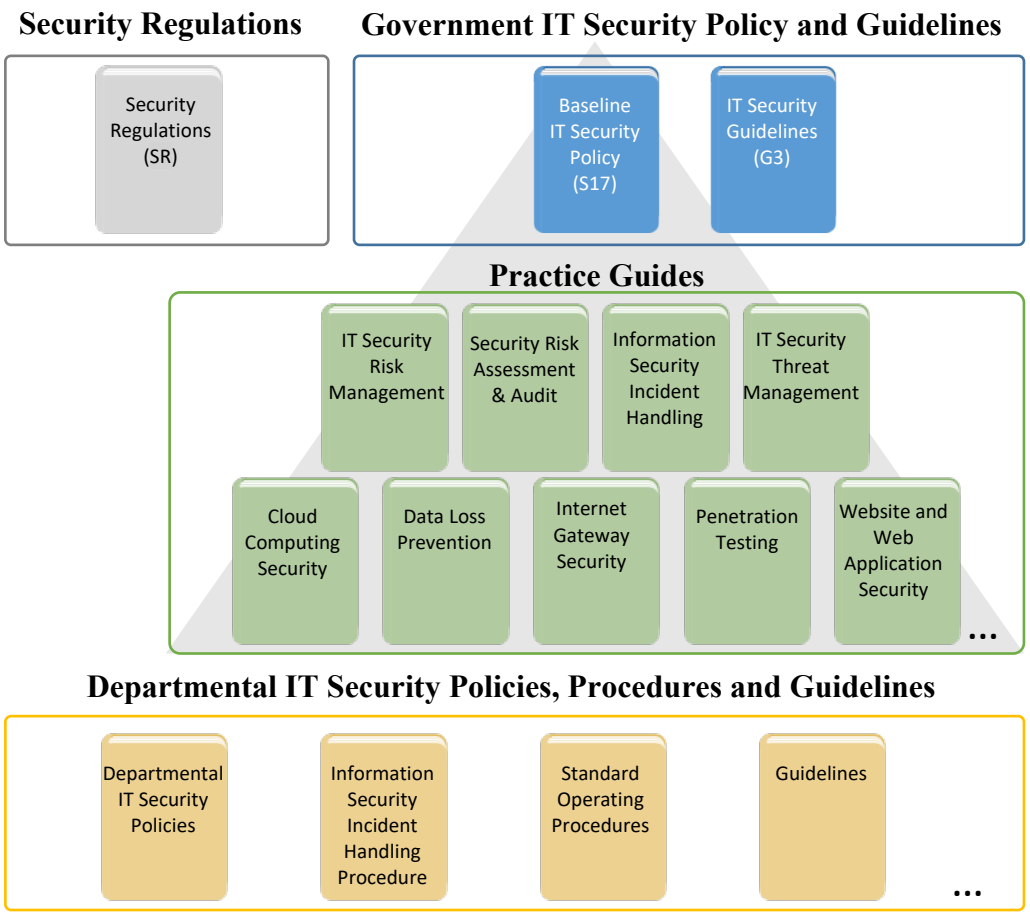
In addition, the document is intended for use by vendors, contractors and consultants who provide IT services to the Government.

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.

B/Ds shall adopt all the mandatory security requirements set out in this document for Tier 1 information systems and additionally adopt the more stringent security requirements set out in Appendix C for Tier 2 and Tier 3 information systems to achieve classified protection of IT security, which ensures that all government information systems are duly protected by security controls which are commensurate with the risk levels of information systems.

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.

In addition, there are a number of practice guides that are supplementary documents to the IT Security Guidelines. They provide guidance notes on specific security areas to help B/Ds address and mitigate risks brought by emerging technologies and security threats. Examples of these practice guides include Practice Guide for Internet Gateway Security, Practice Guide for IT Security Risk Management, Practice Guide for IT Security Threat Management, Practice Guide for Security Risk Assessment & Audit, Practice Guide for Information Security Incident Handling, etc.

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) Baseline IT Security Policy [S17]

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

f) The HKSARG Interoperability Framework [S18]

g) General Circular No. 6/2024 – Strengthening the Governance and Security of IT Systems, dated 6 August 2024

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.

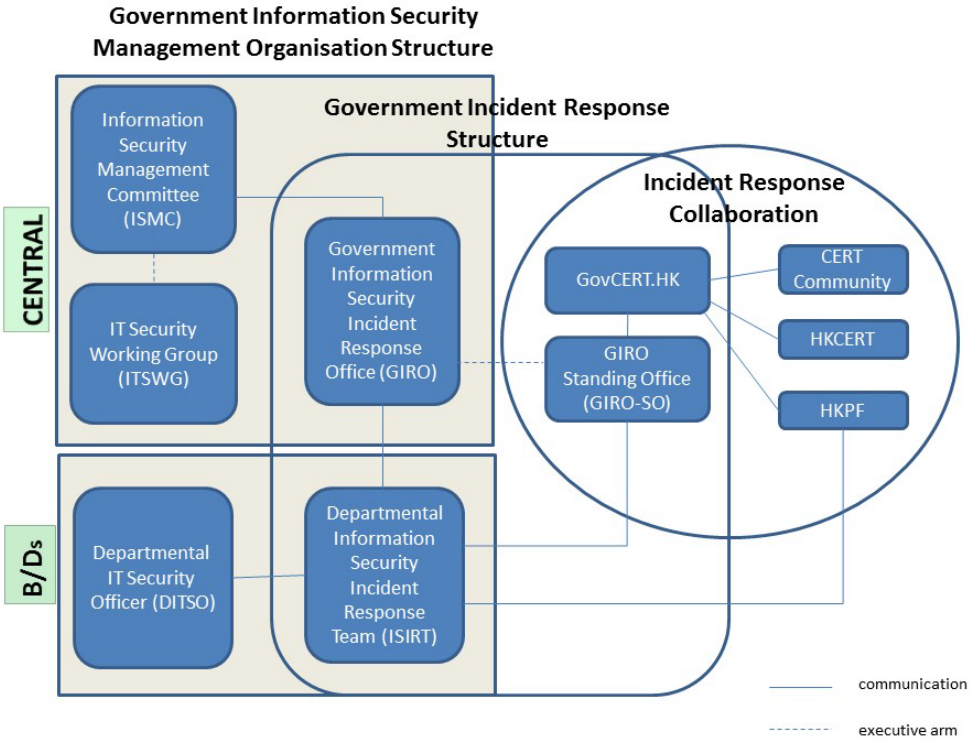
Shall	The use of the word ‘shall’ indicates a mandatory requirement.
Should	The use of the word ‘should’ indicates a best practice, which should be implemented whenever possible.
May	The use of the word ‘may’ indicates a desirable best practice.

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.

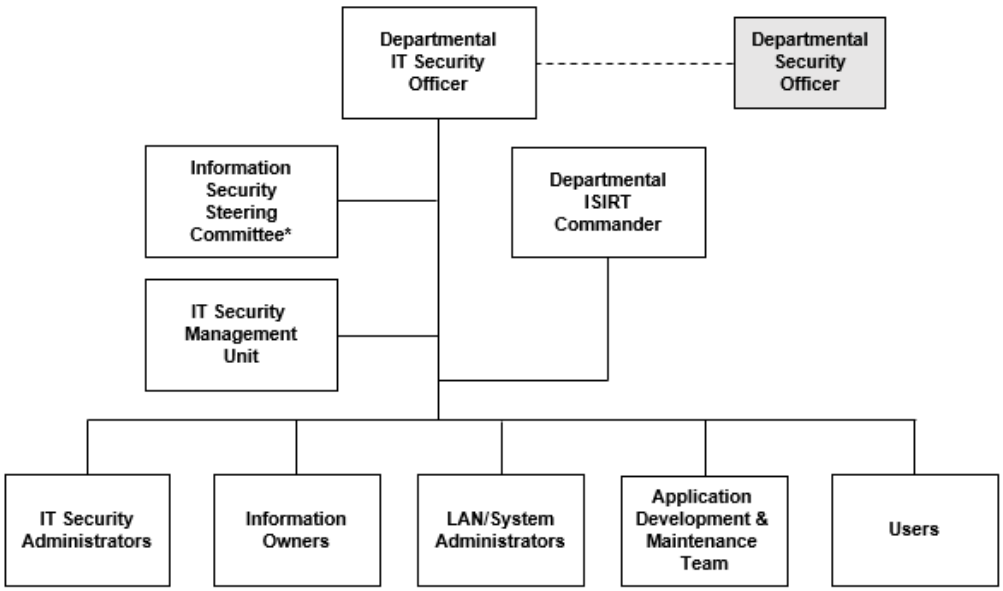
5.1.5 Bureaux/Departments

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 Departmental IT Security Officer (DITSO)

Head of B/D shall appoint an officer at D3 level or above from the senior management to be the Departmental IT Security Officer (DITSO) and responsible for IT security. As the senior management of the B/D, the DITSO shall participate in the overall steering of IT security matters of the B/D. The DITSO shall also understand the B/D's priorities, the importance of the B/D's information systems

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

and data assets, and the level of security that shall be achieved.

If a B/D does not have a directorate officer at D3 level or above, the highest rank directorate officer of the B/D shall assume the position of DITSO so as to uphold the principle of ensuring accountability in IT security.

To better equip the designated DITSOs with security management and related technology knowledge or skills, 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, including overseeing the satisfactory completion of security audit exercises of the B/D;
- 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 overseeing the satisfactory completion of information security risk assessments and privacy impact assessments as well as subsequent rectifications and responding to the evolving risk landscape, regulatory changes, technological advancements, and the system criticality;
- Oversee the IT security threat detection and monitoring process and the threat intelligence activities of the B/D, including dissemination of security alerts on impending and actual threats from the GIRO to responsible parties within the B/D and relevant project teams; and
- Initiate investigation and rectification in case of breach of security and co-ordinate the required submission of incident reports to the Director of Bureau.

5.2.2 Information Security Steering Committee

The senior management of B/Ds shall have an appreciation of IT security, its problems and resolutions. Senior management should consider setting up of an information security steering committee which reports to DITSO, or including

information security as one of the regular discussion items in management meetings. The responsibilities of the committee 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;
- Foster the proper, orderly and secure functioning of all information systems of the B/D;
- 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.

If B/Ds choose not to set up an information security steering committee, DITSO should undertake the responsibilities of the committee.

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 overseeing the security governance process for the IT security related activities within the B/D;
- Assist DITSO in the IT security management process for all IT operations of the B/D;
- 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;
- Co-ordinate security incident investigation and rectification;
- Liaise with other B/Ds and parties on IT security matters; 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.

  These security objectives guide the standards, procedures and controls used in all aspects of security design and security solutions. In short, for an information system, only authorised users shall be allowed to know, gain access, make changes to, or delete the information stored or processed by the information system. The system shall also be accessible and usable upon demand by the authorised users.

- **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 (b) to protect information assets and systems and mitigate security risks to an acceptable level.

  The risk based approach usually involves a risk assessment process and a risk treatment process which can be embedded within different processes, such as project management, vulnerability management, incident management, problem management, or even on an impromptu basis for a given identified specific topic. The risk assessment process involves:

  (a) establishing and maintaining the risk acceptance criteria and criteria for performing the information security risk assessment;
  (b) identifying the risk owners and the risks associated with the loss of confidentiality, integrity and availability of information;
  (c) analysing the risks by determining the risk levels based on the potential impact and likelihood of occurrence;
  (d) evaluating the risks by comparing the results of risk analysis with the established criteria and prioritising the analysed risks for treatment.

  The risk treatment process shall be applied to select appropriate risk treatment options and determine the necessary controls to implement the chosen options. The risk based process shall ensure all necessary controls are included,

formulate a risk treatment plan and obtain the risk owner's approval of the plan and acceptance of the residual information security risks.

A risk owner is responsible for the assessment, management, and monitoring of an identified risk as well as implementation of selected controls to the risk.

- **Security by Design Approach**

  Security by design shall be adopted to incorporate security requirements into the 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.

  Security by design is a software and hardware development approach that seeks to minimise system vulnerabilities and reduce the attack surface through designing and building security in every phase of the SDLC. This includes incorporating security specifications in the design, continuous security evaluation at each phase and adherence to best practices. Specific to IT security, security by design addresses the IT protection considerations throughout a system's lifecycle. This includes security design specifically to strengthen the IT resiliency of the system. Therefore, B/Ds shall adopt the security by design approach as far as possible.

- **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.

  Prevention is the first line of defence. Deployment of proper security protection and measures helps to reduce the risks of security incidents. However, when the prevention safeguards are defeated, B/Ds shall be able to detect security incidents rapidly and respond quickly to contain the damage. The information systems and data shall be recovered in a timely manner. Therefore, B/Ds shall designate appropriate personnel to manage IT security as well as plan for the information security incident handling.

- **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[2]. As an example, wireless communication without protection is vulnerable to attacks, and security measures shall be adopted when transmitting classified information.

When B/Ds formulate security measures, they shall carefully consider and assess the risk of unauthorised modification, destruction or disclosure of information and denial of access to information in different states.

- **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.

  The external systems may not be designed, developed and maintained according to government security requirements. Therefore, B/Ds shall consider implementing multi-level defence when information assets or information systems connect with external systems. Consider any data you receive from an external system, including input from users, that may be a potential source of attack. Information systems shall be partitioned or segregated accordingly, and different access controls and levels of protection should be applied commensurate to the required security level of the systems.

- **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.

  Damage containment means the implementation of security controls to limit the impact of damage arising from a security incident. The resilience of an information system refers to its ability to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state while maintaining essential operational capabilities. It also includes the recovery of the system to an effective operational posture in a time frame consistent with business needs.

[2] For the purpose of this document, "information in storage" refers to those data stored in non-volatile media that retains the information when power is shut off. Non-volatile media includes, but is not limited to, hard disk, solid state drive, optical disk, magnetic tape, USB flash drive and Non-Volatile Random Access Memory (NVRAM). The data residing in non-volatile media of any IT equipment like servers, workstations, notebooks, mobile devices, printers, network devices are regarded as information in storage. For those data that stored in volatile media (e.g. RAM) which gradually loses its information when power is shut off, they are not regarded as information in storage.

- **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.

  Auditability helps to reconstruct the complete behavioural history of a system and, hence, is useful for discovering and investigating a system during a security incident. Accountability is often accomplished by uniquely identifying a single individual so as to enable tracing his/her activities on an information system.

- **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.

  B/Ds shall identify the information security processes and controls to be monitored and measured and determine the methods for monitoring, measuring and evaluating the results. Regular reviews shall be performed on the security measures to ensure its continuing suitability, adequacy and effectiveness. The output of security reviews shall include decisions related to continual improvement opportunities and any need for changes to the security measures where appropriate.

7. MANAGEMENT RESPONSIBILITIES

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

7.1 General Management

(a) Roles and Responsibilities

B/Ds shall apply core security principles and best practices concerning the issue of checks and balances in information security management. Information security shall be considered in all stages of the project management, regardless of the project type.

Regardless of the sources of funding of information systems, B/Ds shall ensure all of their information systems, including infrastructure facilities and departmental shared IT services, are properly protected in accordance with their risk levels. The classified protection of IT security mentioned in Section 7.2 (b) shall be adopted to enable effective IT security risk management for information systems. In addition, B/Ds shall ensure that security protection is responsive and adaptive to changing environments and technology.

B/Ds shall define their own departmental IT security management framework with reference to Section 5.2 Departmental IT Security Organisation. A senior and key personnel in the B/D should be assigned the responsibility for ensuring that appropriate policies and procedures are developed and applied and that necessary checks and balances on proper administration and operation of the policies and procedures are in place. B/Ds should make reference to the departmental IT security management framework, policies and procedures when assigning responsibilities.

Staff with assigned responsibilities may delegate security tasks to others, but they remain ultimately accountable for ensuring that adequate security measures have been implemented. However, staff with assigned responsibilities should ensure that the delegated tasks are performed by appropriate staff in terms of capability, knowledge, experience and seniority. They should check that any delegated tasks have been performed properly. The details of delegation shall be documented and periodically reviewed.

(b) Segregation of Duties

Segregation of duties is the practice of dividing the steps in a function among different individuals so as to keep out the possibility of a single individual from subverting a process. There shall be sufficient segregation of duties with roles and responsibilities clearly defined so as to minimise the chance that a single individual will have the authority to execute and control all security functions and/or crucial operations of an information system.

In situations where segregation of duties is not practicable due to reasons such as a limited number of staff available or other technical limitations, compensating controls should be put in place to provide the equivalent safeguards, e.g. by maintaining appropriate logging on critical operations conducted by the staff together with random inspection and/or regular review on the log file by an appropriate level of authority.

(c) Budgeting

B/Ds shall control the budget to ensure sufficient resource allocation to support the implementation of necessary security safeguards for security protection. Management should develop information security budget plans, projections and resource allocations based on short-term and long-term objectives or goals. Resources should be allocated to protect information systems according to their risk levels.

(d) Rights for Information Examination

B/Ds shall reserve the right to examine all information stored in or transmitted by government information systems, including emails, file directories, and access records to discussion boards, newsgroups and websites, in compliance with the Personal Data (Privacy) Ordinance. This examination helps assure compliance with internal policies, supports internal investigations, and facilitates security management of government information systems.

7.2 Security Risk Management

(a) Risk-based Approach

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 in facing the changing environment and technologies. By applying some simple measures, B/Ds should be able to effectively mitigate and control potential information security risks associated with human and/or operation problems to an acceptable and manageable level. B/Ds shall consider the best practices for possible adoption with regard to their individual business and operation environments.

(b) Classified Protection of IT Security

To ensure all government information systems are duly protected by security controls which are commensurate with the risk levels of information systems, 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, which include Tier 1, Tier 2 and Tier 3 information systems. B/Ds shall adopt all the mandatory security requirements set out in this document for ordinary information systems and additionally adopt the more stringent security requirements set out in Appendix C for Tier 2 and Tier 3 information systems. B/Ds shall ensure that the classifications of information systems align with their business objectives across the entire life cycle of the information systems.

Tier 2 information systems refer to the 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. B/Ds should consider the data classification and the consequences of service disruption when determining the criticality. The criticality should be assessed on various aspects including:

- Defence/security risks (e.g. harm to human lives or properties, personal privacy, inability to carry out statutory duties and maintain law and order).
- Financial implications (e.g. the potential to reduce economic growth, financial loss of the Government).
- Government Image (e.g. effect on government reputation, public confidence).
- Interdependency (e.g. degradation of services of one system might result in service disruption to another information system).

In addition, B/Ds should include other aspects that apply to their information systems in the assessment of system classification. The assessment should be made with respect to the scope (i.e. number of users affected), severity (i.e. the consequences of disruption or destruction), downtime tolerance (i.e. the point that the service disruption could have a serious impact) and the largest potential business impact that would result from the failure or disruption of the information system.

Furthermore, there are a number of essential services that are critical to the functioning and security of a society and its economy. Tier 3 information systems refer to the 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.

B/Ds shall determine the classifications of information systems during the project initiation stage. When assessing the classifications of information systems, B/Ds shall make reference to the considerations in Appendix B. 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.

(c) IT Security Risk Management Framework

To ensure security risk assessments of B/Ds are performed and monitored in a structured manner, B/Ds should adopt the following IT security risk management framework, which encompasses a series of risk management processes and utilise risk registers to achieve effective management and communication about IT security risks. A highlight of the framework is given below for reference.

- Departmental context establishment – establishing the B/D's IT security risk management context, which includes the B/D's risk appetite and tolerance.
- Risk assessment – performing security risk assessments specified in Section 20.2 (a) for all information systems of the B/D, which identify IT security risks of an information system according to risk sources (e.g. vulnerabilities, threats) and events (e.g. incident scenarios), determine the level of identified risks based on their impact and likelihood, prioritise the analysed risks for risk treatment, and document the prioritised risks in the risk registers of information systems.
- Risk treatment – determining the appropriate risk treatment (e.g. risk reduction, avoidance, transfer, and acceptance) for each risk of information systems to reduce it to a level within the B/D's risk appetite and documenting the treatment in the risk registers of information systems.
- Risk correlation, aggregation and normalisation – consolidating individual risk registers of information systems into a departmental IT security risk register by performing risk correlation, aggregation, and normalisation in the departmental context to facilitate the monitoring and communication about IT security risks in a B/D.
- Risk monitoring and reporting – monitoring the departmental IT security risks and the corresponding risk treatment and reporting them to DITSO and other relevant parties.

For more information about the IT security risk management framework, please refer to the following document for details:

- **Practice Guide for IT Security Risk Management**
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

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

(a) Departmental IT Security Policy

Essentially, IT security policy shall set the minimum standards of a security specification and state what aspects are of paramount importance to the organisation. Thus, IT security policy shall be treated as the basic rules to be observed as mandatory while there can still be other desirable measures to enhance security.

B/Ds shall establish the departmental IT security policy based on the Baseline IT Security Policy as the basis for development.

The departmental IT security policy shall cover the proper use of the information systems, data assets, network resources, IT services and facilities, as well as the procedures to prevent and respond to security incidents. Drafting of the policy shall consider the following:

- B/Ds' own requirements on security.
- Prevailing government IT security requirements as specified in Section 2.3.
- Personal Data (Privacy) Ordinance.
- Code on Access to Information.
- Information on Record Management in the Manual of Office Practice.

The drafting of the policy shall additionally consider the following:

- Goals and direction of the Government of HKSAR.
- Existing policies, rules, regulations and laws of the Government of HKSAR.
- B/Ds' own requirements and needs.
- Implementation, distribution and enforcement issues.

B/Ds should set up procedures to provide prompt assistance in investigative matters relating to breaches of security and policy implementation issues. Establishing a Departmental Information Security Incident Response Team (ISIRT) and setting up a security incident response plan can improve the effectiveness of the policy.

(b) Evaluation and Periodic Review

Review of information security policies, standards, guidelines and procedures shall be conducted periodically. Results and proposed changes from reviews shall be evaluated and endorsed by related parties to ensure the necessary requirements are incorporated. B/Ds may consider hiring external qualified IT security auditors or consultants to review or assist in the development of the information security documents to improve the quality and completeness of the documents.

The development of information security documents without ongoing support will eventually leave them unattended and even outdated over time. In fact, some issues may diminish in importance while the new ones continually appear. Hence, frequent reviews of the information security documents can help ensure that the policy meets the latest requirements and copes with technological changes.

(c) Communication with Users

B/Ds shall promulgate their own IT Security Policy. A mechanism for the delivery of the policy shall be established to ensure ease of accessibility and availability to all staff, functional groups and management. B/Ds shall ensure that they are fully aware of the IT security policy so that they can carry out their duties and meet the government security requirements.

No policy shall be considered implemented unless users or related parties have commitment and communication. Hence, B/Ds should make sure that users and related parties:

- Are informed of the policy by briefing or orientation when they newly join.
- Are invited to participate in developing the policy proposals.
- Are trained with the skills needed to follow the policy.
- Are periodically reminded of and refreshed for security threats or issues.
- Are provided with policy guidance in manageable units.

In order to help an end user understand his / her responsibilities in IT security, B/Ds should develop a departmental end user instruction document on IT security, which highlights the security requirements that are related to an end user in a simple instruction format. A sample template is available in Appendix A – Sample IT Security End User Instructions.

9. HUMAN RESOURCE SECURITY

Positively cultivating a strong security culture is crucial for enhancing B/D's security posture, reducing risks, complying with regulations, and building a resilient and trusted environment across the Government. B/Ds shall ensure that staff 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

(a) IT Security Responsibilities

IT security roles and responsibilities shall be communicated to all staff when they are assigned a new post, and periodically throughout their term of employment. B/Ds shall ensure that all staff:

- are informed of the departmental IT security policy by briefing or orientation when they newly join; and
- are aware of and periodically reminded of their IT security responsibilities and the government security requirements.

(b) Information Dissemination

An effective information dissemination mechanism shall be in place to ensure all personnel involved are fully aware of the respective policies and procedures governing their authority and usage of information systems.

(c) Training

Proper security training and updates on IT security policy shall be provided to all staff regularly, including users, developers, system administrators, and security administrators who are engaged in government work to strengthen their awareness of information security. The awareness training may be in any form, such as classroom training, computer based training or self-paced learning. Users should be made aware of the training resources available on the Cyber Learning Centre Plus (CLC Plus) of the Civil Service College, which also includes general IT security related courseware and a self-assessment package for participants.

B/Ds may make reference to the resources when providing tailor-made training and materials to their staff or contractors in accordance with their own business and operation requirements. More information about CLC Plus is available at https://www.clcplus.csc.gov.hk.

Staff may also raise their security awareness by participating in security drills, attending seminars, showcases or visiting theme pages containing security intelligence information and general security information (e.g. Cyber Security Information Portal, InfoSec website). B/Ds shall participate in the IT security awareness activities designated by DPO.

Proper education and training should also be provided to the system administrators in implementing the IT security procedures. System administrators should know how to protect their systems from attack and unauthorised use. System administrators shall have a defined procedure for reporting security problems.

B/Ds should consider formulating an IT security training programme to enable the provision of targeted and structured IT security awareness activities to their staff.

An IT security training programme should include but is not limited to the following:

(i) Programme objectives

B/Ds should establish objectives for the IT security awareness programme. The objectives should be aligned with the overall IT security strategy of the B/D.

(ii) Target Audience

B/Ds should identify the specific groups or roles required to participate in the training activities. B/Ds should consider different levels of technical expertise, job functions, and needs to tailor the training content accordingly.

(iii) Training Approach

The design of training materials and content should be aligned with the objectives and target audience. Examples of training topics include phishing awareness, incident response, regulatory compliance, data privacy, social media platform awareness, etc. Appropriate delivery methods should also be adopted having regard to the B/D's size, risks, resources, and the target audience's needs. The training approach may include presentations, videos, interactive modules, practical exercises, and case studies.

(iv) Evaluation of the effectiveness of training activities

B/Ds should review the effectiveness of the training activities. An assessment may be conducted to ensure user awareness of information security requirements and responsibilities. This can be done through methods such as post-training quizzes, feedback surveys, simulation exercises, and observing changes in behaviour or the number of security incidents to evaluate knowledge gain, behavioural changes, and participant satisfaction.

(v) Regular review and update

B/Ds should continuously review and update the training programme to reflect the evolving threat landscape, new technologies, and changes in regulations and

compliance requirements. In addition, B/Ds should make reference to the feedback to identify improvement areas and adjust or fine-tune the training programme.

(d) Personnel Security

Classified information shall be protected from unauthorised access or unauthorised disclosure. Officers shall not publish, make private copies of or communicate to unauthorised persons any classified document or information obtained in their official capacity unless they are required to do so in the interest of the Government. The "need to know" principle shall be applied to all classified information, which shall 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, classification or information, the Departmental Security Officer should be consulted.

B/Ds shall ensure that personnel security risks are effectively managed. B/Ds shall assess the risk of allowing an individual to access classified information.

Access to classified information higher than RESTRICTED is restricted to civil servants who have undergone appropriate integrity checks. B/Ds should consult the departmental personnel section about the Integrity Checking Instructions. 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. Background verification checks may include the following having addressed any personal privacy issues:

- Independent identity check (Hong Kong Identity Card or passport).
- Confirmation of claimed academic and professional qualifications.
- Completeness and accuracy check of the provided curriculum vitae.
- Availability of employment references.
- More detailed checks, such as credit checks or checks of criminal records, if considered necessary.

(e) Clear Policies and Procedures

Management shall establish clear policies and supporting procedures regarding the use of information systems so as to set out clearly the allowed and disallowed actions on their information systems. These actions should normally be covered in the departmental IT Security Policy. The departmental IT Security Policy shall include a provision advising staff that if they contravene any provision of the policy, they may be subject to different levels of disciplinary or punitive actions depending on the severity of the breach. Staff shall be formally notified of their authorisation to access an information system as well as their responsibilities and duties on these information systems.

(f) IT Security Responsibilities after Termination or Change of Employment

Post-employment responsibilities and duties shall be defined in the terms and conditions of employment. The communication of termination responsibilities to the staff shall include continuing information security requirements and legal responsibilities. The communication of termination responsibilities should also include responsibilities stipulated in any confidentiality agreement and the terms and conditions of employment continuing for a defined period after the end of employment. Changes of responsibility or employment shall be managed as the termination of the current responsibility or employment followed by the commencement of the new responsibility or employment.

10. ASSET MANAGEMENT

B/Ds shall maintain appropriate protection of all the hardware, software and information assets and ensure that information receives an appropriate level of protection.

10.1 Responsibility for Assets

(a) Inventory of Assets

Inventory of assets helps ensure that effective protection takes place and identifies lost assets. Regardless of the source of funding of information systems, an inventory shall be drawn up of all information systems including infrastructure facilities and departmental shared IT services (with their system classifications), hardware assets, software assets, valid warranties, service agreements and legal/contractual documents (e.g. public domain name registrations and related IP addresses, physical locations of data storage, etc.). Periodic review of the inventory shall be conducted to ensure that the assets are properly owned, kept and maintained. To better manage the software supply chain, B/Ds should gather as much information as possible about the associated components of the software assets (e.g. supplier, component name, version, dependency relation, etc.).

In particular, DITSO shall maintain an up-to-date inventory of all Internet-facing services of their B/Ds. The inventory shall be comprehensive and include at least the description, IP addresses, domain names, and network ports opened of the services which are exposed to the Internet.

Asset ownership shall be assigned when assets are created or transferred from other parties. The asset owner shall be responsible for proper asset management to ensure that:

- Assets are inventoried.
- Assets are appropriately classified and protected.
- Access restrictions to assets are defined and reviewed periodically.
- Assets are handled properly for their disposal or reuse.

(b) Protection of Information about Government Information Systems

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. Information about information systems shall not be disclosed where that information may compromise the security of those systems, such as network diagrams with IP addresses and security audit reports, except on a

need-to-know basis and only if authorised by the DITSO. Such information shall also be classified and protected according to its classification.

This kind of information can be put at risk by external service providers with inadequate information security management. If there is a need to disclose the information to external service providers, a non-disclosure agreement or its equivalent shall be used to protect the information. The non-disclosure agreement should define the information that is protected against disclosure and how the parties are to handle such information. If the non-disclosure agreement is signed between a B/D and an external service provider that is at the organisation level, the agreement should require the external service provider to bind its staff, directors, agents, associates or contractors, etc., to the same obligations of confidentiality.

(c) Return of Assets

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 hand over and return computer resources and information to the Government. A termination process shall be developed to ensure the return of all previously issued assets owned by the B/D.

If the outgoing officer or staff of external parties possesses knowledge that is important to the B/D's operations, that knowledge should be documented and transferred to the B/D.

10.2 Information Classification

(a) Information Classification and Labelling

Before determining security measures, the data to be protected needs to be identified and classified. For instance, data which has a monetary value or which, if lost, can cause interruptions to the daily operation. Data should be classified based on the level of sensitivity of that data.

B/Ds should develop procedures for labelling classified information and handling information in accordance with the classification. B/Ds shall observe and follow the requirements of information classification and labelling, such as markings of classifications, regrading and downgrading of documents. In addition, B/Ds shall observe the following requirements for classified information handled by information systems:

- Users given access to classified information on information systems shall be alerted of the type(s) of classified information they are accessing or going to access.
- The Subject field of a classified electronic mail document shall include the classification category of the document.

- Removable media on which classified information is stored shall have clearly legible identification and conspicuous classification markings on labels fixed firmly to them and on their protective containers.
- Removable media on which a key is stored and is not used for backup purposes need not have its classification marked on a fixed label.

(b) Overall Data Confidentiality

All stored information classified as RESTRICTED or above shall be encrypted irrespective of the storage media. For the implementation options of encryption, B/Ds are advised to adopt a risk-based approach to assess the security risks and determine the appropriate security measures and configurations for their information systems based on their business needs. If a system contains both RESTRICTED and unclassified information, the requirement can be met no matter whether the RESTRICTED information is encrypted by application or other means at field, database, file or disk storage level.

Some systems, such as network devices (e.g. firewall, router) and proprietary appliances, may not support encryption for their configurations, rule sets and log records, which may be considered classified data. If there is no viable solution available, B/Ds shall implement complementary measures such as strengthened access control and obtain approval from Heads of B/Ds taking this constraint into consideration.

Information without any security classification should also be protected to preserve its confidentiality and integrity. Release of information outside the Government should be controlled by the officer responsible for the specific subject of work with which the information is concerned in line with the principles of the Code on Access to Information. B/Ds should always bear in mind to protect the confidentiality, integrity and availability of data. Security measures should 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.

Similar protections shall also be applied to interim material and information produced in the course of processing. All government data and system disks shall be removed whenever the computer equipment is no longer used.

The general principle is that classified messages/data/documents in whatever form shall bear the same classification as they would be for the paper equivalent and they shall be protected in accordance with government security requirements.

B/Ds shall advise their business partners, contractors, or outsourced staff to comply with the government security requirements in storing, processing and transmitting data owned by the Government, and put in place a mechanism to check their compliance.

10.3 Storage Media Handling

(a) Equipment and Media Control

B/Ds shall manage the use and transportation of storage media containing classified information. To protect the information during transportation, B/Ds should:

- Provide sufficient packaging to protect the storage media from physical damage during transit.
- Keep the record for identifying the contents of the storage media, the protection applied, the times of transfer to the transit custodians and receipt at the destination.

It is risky to store data on mobile devices and removable media as they are small and can be easily lost or stolen. Storing classified information on these devices should be avoided. Staff should justify the need to store classified information on these devices. Mobile devices and removable media provided by the B/D shall be used. Staff should seek proper authorisation before storing the minimum required classified data on the mobile device and removable media. To minimise the risk of data leakage, only devices with encryption features suitable to protect classified data should be used. Staff shall remove classified information from the mobile device and removable media as soon as it no longer needs to be stored there to minimise the exposure. Staff shall also ensure all classified data has been completely cleared or destroyed prior to disposal or re-use of the mobile device and removable media.

Some electronic office equipment, including multi-function printers and photocopiers, may have storage media embedded as auxiliary devices whose existence may not be readily apparent to the users. B/Ds should review their inventory and make suitable arrangements to ensure the data is handled in accordance with government security requirements. Equipment shall be used and managed with care if classified information is likely to be stored or processed by them. Where necessary, the file storage features of this equipment should be disabled to avoid storing any classified information.

All storage media containing classified information shall be handled strictly in accordance with the procedures set out in government security requirements. In case of problems, advice from the Department Security Officer or the Government Security Officer should be sought.

(b) Information Erasure

All classified information shall be completely cleared or destroyed from media before disposal or reuse by means of (a) Sanitisation or (b) Physical Destruction to ensure that the classified information cannot be recovered:

(a) Sanitisation: refers to the process of removing the data on the media to ensure that the original data cannot be retrieved. Sanitising may be accomplished by overwriting or degaussing:

(i) Overwriting

For any media which has been used for the storage of classified information, the procedure of overwriting ALL addressable locations with a character, its complement, then a random character and verify shall be performed before disposal or re-use. It is very important that every bit of storage space in the media shall be overwritten. For flash memory devices such as solid-state drives (SSDs) or flash drives, the manufacturers normally provide built-in commands[3], which provide effective sanitisation that destroys the entire drive data and not just overwrite or erases the cryptographic keys. Such functions should be used. Nevertheless, if it is not possible to verify that the media has been effectively sanitised and ensure that the original data cannot be retrieved, alternative sanitisation or physical destruction methods that can be verified shall be used.

(ii) Degaussing

Degaussing or demagnetising is considered an acceptable technical solution for the destruction of classified information stored on magnetic media such as hard disks, floppy disks and magnetic tapes if properly employed. For degaussing hard disks, all shielding materials (e.g. castings, cabinets, and mounting brackets), which may interfere with the degausser's magnetic field shall be removed from the hard disks before degaussing. Hard disk platters shall be in a particular position or direction as specified by the degausser during the degaussing process.

Sufficient checks and balances mechanisms shall be in place, such as requiring the individual who performs the degaussing to certify the completion of the degaussing. A sample check of the degaussed media shall also be performed by another party to ensure that the degaussing is done properly.

(b) Physical Destruction: storage media that cannot be sanitised shall be physically destroyed by means of shredding, disintegration or grinding.

For flash memory devices, the media shall be shredded or disintegrated into particles that have nominal edge dimensions of 2 millimetres or less.

For optical storage media (CDs, DVDs, Blu-ray discs and MO disks), the media shall be shredded or disintegrated into particles:

[3] B/Ds are advised to take into consideration of the availability of data sanitisation functions when procuring flash memory devices, particularly SSDs.

- that have nominal edge dimensions of 0.5 millimetres or less and surface area of 0.25 square millimetres or less if the media has been used for the storage of information classified as higher than CONFIDENTIAL; or
- that have nominal edge dimensions of 2 millimetres or less if the media has been used for the storage of CONFIDENTIAL or RESTRICTED information.

Alternatively, the CD media can be destroyed by grinding to remove the information bearing surface.

For any media which has been used for the storage of information classified as higher than CONFIDENTIAL, apart from the above procedure of sanitising the media, the media should also be physically destroyed before disposal.

In order to comply with the requirements, appropriate tools shall be used to overwrite the storage area where the classified information was originally stored in the media. Commercial software for secure deletion of information is available, which conforms to the industry best practice of writing over the storage area several times, including writing with different patterns, to ensure complete deletion. Whole disk sanitisation should be used instead of individual file sanitisation to ensure complete erasure of information for flash-based solid state disks or USB flash drives as completely overwriting a particular file may not be feasible.

Cryptographic erasure may be considered as an alternative approach for data sanitisation, which overwrites the cryptographic keys used to encrypt the data, but it is susceptible to risks such as vulnerable encryption algorithms, undeleted backup keys and sanitisation assurance problems. B/Ds shall assess the associated risks and possible impacts before implementing cryptographic erasure. Cryptographic erase shall not be used alone as a sanitisation method for the destruction of classified information. Cryptographic erasure can be used in combination with other sanitisation and physical destruction methods for the destruction of classified information.

A system of checks and balances shall be maintained to verify the successful completion of the secure deletion process. A sample check of the storage media should be performed by another party to ensure all classified information is properly cleared or destroyed.

Users should adopt erasure procedures which are similar for RESTRICTED information if they believe that the computer or storage media to be disposed of or re-used contains information which will cause data privacy problems.

For more information about destruction and disposal of storage media, please refer to the following document for details:

- **Practice Guide for Destruction and Disposal of Storage Media**
  Available at ITG InfoStation.
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

11. ACCESS CONTROL

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

11.1 Business Requirements of Access Control

(a) Principle of Least Privilege

B/D shall ensure that the least privilege principle is followed when assigning resources and privileges of information systems to users as well as technical support staff. This includes restricting a user's access (e.g. to data files, to IT services and facilities, or to computer equipment) or type of access (e.g. read, write, execute, delete) to the minimum necessary to perform his or her duties.

(b) Access to Information

B/Ds shall ensure that access rights to information are not granted unless authorised by relevant information owners. Information owners should determine appropriate access control rules, access rights and restrictions for specific user roles on their information. The level of detail and control restrictions should reflect the associated information security risks.

(c) Access Control of Classified Information

Access to classified information without appropriate authentication shall not be allowed. Authentication can be achieved by various means, including passwords, smartcards, tokens, biometrics and one-time passwords. Multi-factor authentication shall be used for accessing an information system that stores information classified as CONFIDENTIAL or above.

Logical access control refers to the controls to IT resources other than physical access control, such as restricted access to the physical location of the system. In general, logical access control refers to four main elements: users/groups of users, resources, authentication and authorisation:

- Users/groups of users refer to those people who are registered and identified for accessing the IT resources.
- People will be granted rights to access the system resources such as networks, files, directories, programs and databases.
- Authentication is to prove the identity of a user. Usually, it is done based on three major factors. They are: something you know (e.g. PIN or username/passwords), something you have (e.g. a token or a smart card) or something you are (e.g. biometrics characteristics such as fingerprint, facial

characteristics, retina of eye and voice). A combination of at least two of these factors, often called multi-factor authentication, can be applied to strengthen the authentication control.

- Upon user authentication, authorisation to access will be granted by mapping the user/group of users to the system resources.

11.2 User Access Management

(a) Data Access Control

Access rights to information shall be granted on a need-to-know basis and shall be clearly defined, documented and reviewed periodically. All administrative privileges and data access rights, including temporary access, shall be regularly reviewed (e.g. at least once annually, preferably twice per year) in order to identify and revoke unnecessary or excessive privileges. This regular check/audit on usages of some high privilege system accounts should be performed by an independent party to ensure the use of these accounts is for legitimate purposes. Records for access rights approval and review shall be maintained to ensure proper approval processes are followed, and the access rights are updated when personnel changes occur.

Access rights to information processing facilities, such as the physical premises where information systems are located, should also be managed based on the same principle.

Formal procedures shall be in place to control the allocation of access rights to information systems and services. The procedures shall cover all stages in the life cycle of user access, from the initial registration of new users, password delivery, and password reset to the final de-registration of users who no longer require access to information systems and services.

(b) Controlling the Use of Special Privileges

For accounts or user access with privileged access rights (such as an administrator or system account), the following are requirements to restrict and control the use:

- Special privileges and data access rights associated with each system or application, and the users to whom they need to be allocated shall be identified.
- Special privileges and data access rights shall be granted to users based on the principle of least privilege and segregation of duties.
- Special privileges and data access rights shall be granted to a user ID different from those used for regular business activities.
- Regular business activities (including but not limited to email reading, Internet browsing, and file downloading) shall not be performed by privileged accounts.
- Specific procedures should be established to avoid the unauthorised use of default administration user IDs.

- Multi-factor authentication should be adopted for high risk access.

(c) Removal of Access Rights

All user privileges and data access rights, including temporary and emergency access, shall be revoked after a pre-defined period of inactivity. This requirement should be enforced by B/Ds by means of security checking by the system/application automatically or periodical review manually (e.g. check on last login time).

In addition, user privileges and data access rights shall be revoked when they are no longer required, e.g. upon a staff's termination of employment or change of employment. Documentation which identifies user privileges and data access rights shall be updated to reflect the removal or adjustment of access rights. If a departing staff has known passwords for user IDs which will remain active, these passwords shall be changed upon termination or change of employment.

User privileges and data access rights may be granted on a group basis instead of an individual basis (e.g. a group access list). In this case, B/Ds shall remove the departing staff from the corresponding group access lists as well as inform other parties not to share any information with the departing staff.

(d) User Identification

Individual accountability should be established so the respective staff is responsible for his or her actions. For information systems, accountability can be accomplished by identifying and authenticating users of the system with the use of a user identity (user-ID), which uniquely identifies a single individual such that subsequent tracing of the user's activities on the system is possible in case an incident occurs or a violation of the IT security policy is detected.

Unless it is unavoidable due to business needs (e.g. demonstration systems) or it cannot be implemented on an information system, shared or group user-IDs shall be prohibited. Any exemption to this requirement shall obtain explicit approval from the DITSO with supporting reason. B/D shall justify the usage of shared accounts against the security risks that a system may be exposed to. B/Ds shall review the need for shared or group accounts periodically and remove them when the justifications are no longer valid.

11.3 User Responsibilities

(a) User Accountability

Users shall be responsible for all activities performed with their user-IDs. They shall only use their user-IDs to perform authorised tasks and functions. Shared user-IDs without approval shall be prohibited. For more information on user-IDs, please refer to Section 11.2 (d), "User Identification".

(b) Risk of Sharing Password

Password sharing can defeat user accountability and the non-repudiation principle of access control. Passwords shall not be shared or divulged unless there is a measure of determining user identification to enforce user accountability. If passwords need to be shared (e.g., helpdesk assistance, shared PC and shared files) and user accountability cannot be enforced, explicit approval from the DITSO shall be obtained with supporting reasons. B/Ds shall justify the usage of shared passwords against the security risks that a system may be exposed to. Shared passwords should be reset immediately when no longer used and should be changed frequently if sharing is required on a regular basis to minimise the risk of security breaches.

(c) Password Protection

Passwords shall always be well protected. When held in storage, security controls such as access control and encryption shall be applied to protect passwords. As passwords are considered key credentials for logging into a system, passwords shall be encrypted when transmitting over an un-trusted communication network. If password encryption is not implementable, B/Ds shall implement compensating controls such as changing the password more frequently.

11.4 System and Application Access Control

(a) Information Access Restriction

B/Ds shall ensure that their information systems are implemented with appropriate authentication mechanisms and measures that are commensurate with their security requirements and the sensitivity of the information to be accessed. A Risk Assessment Reference Framework for Electronic Authentication has been promulgated, which aims to introduce a consistent approach for B/Ds' reference in deciding the appropriate authentication method for their e-government services. The framework has a view to providing citizens/staff with a consistent experience and interface when transacting electronically with the Government for services of similar authentication requirements. B/Ds should follow the framework as far as possible in determining and implementing the electronic authentication requirements of their e-government services. For details of the framework, please refer to:

- **'e-Authentication Framework' theme page**
  ITG InfoStation (https://itginfo.ccgo.hksarg/content/eauth/index.html)

Depending on the level of security control required, one simple way of authentication is to use a password. The usage of a password checker on the authentication system should be considered to enforce password composition criteria and to improve password selection quality, such as avoiding the selection of passwords that are weak or suspected of being compromised. Another way to perform authentication is to use multi-factor authentication, such as smart cards or tokens that function as a secure container for user identification and other security related information, such as encryption keys or one-time passwords that provide

additional authentication. For example, a protected system cannot be activated until the user presents a token (something possessed) and a valid password (something known). Multi-factor authentication should be adopted for high risk access, such as remote access to the internal networks and should be considered as a standard to be abided by all newly implemented or upgraded systems. For some applications, a challenge-response scheme may be chosen to generate some information or challenges to the user and request for a correct response before allowing a successful log-in to proceed.

To reduce the possibility of passwords being compromised by password guessing activity such as brute-force attacks, consecutive unsuccessful log-in trials shall be controlled and the number of log-in trials, account lock-out duration and lock-out timer reset duration should be defined and enforced. This can be accomplished by disabling the account upon a limited number of unsuccessful log-in attempts. Alternatively, the mechanism of increasing the time delay between each consecutive login attempt may also be considered to prevent password guessing activity. In addition, user access log analytic tools may be used together with a central log server for maintaining the integrity of log records, monitoring user access activities, and facilitating incident investigation.

(b) Password Policy

A password is a secret word or code used to serve as a security measure against unauthorised access to data. There might be various categories of computer accounts designed for information systems, including service accounts or user accounts created for B/D users or citizens using government services. B/Ds shall carefully define and document password policy for each category of accounts, balancing the security requirements and operational efficiency. The password policy shall be enforced for all information systems.

The password policy shall at least include minimum password length, initial assignment, restricted words and format, password life cycle, and a good set of rules for password selection in combination with controls such as password history, account lockout and regular password change. The minimum password length of at least eight characters shall be enforced unless it is technically infeasible or there is genuine operational constraint for implementation. These controls mitigate the risks of password guessing activity such as brute force attacks and should be implemented as far as practicable. The password policy should be audited regularly.

The following strong password policy shall be enforced in all information systems containing classified data. In addition, if any information system, when compromised, could affect the security of the aforementioned systems (e.g. an information system sharing the same network segment with an information system containing classified data or specific machines which are allowed to perform administrative functions on information systems containing classified data), the following strong password policy shall also be enforced. If any of the controls of the following strong password policy cannot be implemented due to technical or operational constraints, DITSO's explicit approval shall be obtained, and the corresponding adjusted password policy, as well as the rationale, shall be

documented. All other information systems should also adopt the following strong password policy as far as possible.

Strong Password Policy:

Controls	Settings
Complexity and Length	• At least eight characters with upper-case alphabets, lower-case alphabets, numbers and special characters or • At least ten characters from at least three categories of characters[4].
Password history	At least eight passwords remembered
Account lockout	After five or fewer invalid logon attempts
Regular password change	Every six months or more frequent

(c) Password Selection

B/Ds should define a good set of rules for password selection and distribute these rules to all users. If possible, the software which sets user passwords should be modified to enforce password rules according to the departmental IT security policy.

Some guidelines for password selection are provided below:

DON'Ts

- Do not use your login name in any form (as-is, reversed, capitalised, doubled, etc.).
- Do not use your first, middle or last name in any form.
- Do not use your spouse's or child's name.
- Do not use other information easily obtained about you. This includes ID card numbers, licence plate numbers, telephone numbers, birth dates, the name of the street you live on, etc.
- Do not use a password with the same letter like "aaaaaa".
- Do not use consecutive letters or numbers like "abcdefgh" or "23456789".
- Do not use adjacent keys on the keyboard like "qwertyui".
- Do not use a word that can be found in an English or foreign language dictionary.
- Do not use a word in reverse that can be found in an English or foreign language dictionary.

[4]The categories include 1) upper-case alphabets, 2) lower-case alphabets, 3) numbers, 4) special characters (e.g. symbols shown on keyboard) and 5) other characters not covered in the (1) to (4) (e.g. Unicode characters of languages other than English).

- Do not use a well-known abbreviation. This includes abbreviations of B/D name, project name, etc.
- Do not use a simple variation of anything described in 1-10 above. Simple variations include appending or prepending digits or symbols or substituting characters, like 3 for E, $ for S, and 0 for O.
- Do not use a password with fewer than eight characters.
- Do not reuse recently used passwords.

DOs

- Do use passphrases, which consist of a sequence of words that are both lengthy and easy to remember, like 1Apple&2orange&3banana, to significantly increase the difficulty of password cracking through brute-force.
- Do use different passwords for different systems with respect to their different security requirements and the value of information assets to be protected.
- Do use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard, so that passers-by cannot see what you are typing.

Examples of bad passwords:

“password”	the most easily guessed password
“administrator”	a user’s login name
“cisco”	a vendor’s name
“peter chan”	a person’s name
“aaaaaaaa”	repeating the same letter
“abcdefgh”	consecutive letters
“23456789”	consecutive numbers
“111111”	repeating numbers
“1q2w3e4r5t”	Adjacent keys on the keyboard
“qwertyui”	Adjacent keys on the keyboard
“computer”	a dictionary word
“computer12”	simple variation of a dictionary word
“c0mput3r”	simple variation of a dictionary word with ‘o’ substituted by ‘0’ and ‘e’ substituted by ‘3’
“superman”	a fictional character’s name

(d) Compromising Password

B/Ds should remind staff about the prohibition on the following activities, which could lead to unauthorised access to information systems or a compromise of the security of information systems:

- Interactive attempts including password guessing and brute force attacks.
- Obtaining passwords through social engineering or phishing.
- Compromising passwords through oversight, observation, cameras, etc.
- Cracking through network traffic eavesdropping.

(e) Password Handling for System/Security Administrators

DON'Ts

- Do not disclose or reset a password on a user's behalf unless his/her identity can be verified.
- Do not allow the password file to be publicly readable.
- Do not send passwords to users unencrypted, especially via email.

DOs

- Do choose good passwords as initial passwords for accounts according to the departmental password policy.
- Do use different passwords as initial passwords for different accounts.
- Do technically enforce or request the user to change the initial password immediately upon receiving the new password.
- Do change all system or vendor-supplied default passwords, including service accounts, after installation of a new system.
- Do technically enforce or request users to change their passwords periodically or immediately in case of password compromises.
- Do encrypt passwords during transmission over un-trusted networks.
- Do scramble passwords with one-way functions. If possible, do use "salting" to scramble passwords so that the same passwords will produce different scrambled outputs.
- Do deactivate a user account if the logon fails for multiple consecutive times.
- Do remind the responsibilities of the users in protecting their passwords.

System Security Features

Following are desirable security features available in some operating and application systems which assist in enforcing some of the recommended password selection criteria. Such features should be enabled whenever possible.

- Automatically suspend a user account after a pre-defined number of invalid logon attempts.
- Restrict a suspended account to only allow reactivation with manual interventions by the system/security administrator.
- Prevent users from using passwords shorter than a pre-defined length or re-using previously used passwords.
- All accounts shall be revoked or disabled after a pre-defined period of inactivity by means of security checking by the system/application automatically or periodical review manually (e.g. check on last login time) by the IT security administrator.

(f) Password Handling for End Users

The password mechanisms are subjected to the same vulnerabilities as those of the operating system, namely, poor password selection by users, disclosure of passwords and password guessing programs.

DON'Ts

- Do not write down your password unless with sufficient protection.
- Do not tell or give out your passwords, even for a very good reason.
- Do not display your password on the monitor.
- Do not send your password unencrypted, especially via Internet email.
- Do not select the "remember your password" feature associated with websites that contain your personal particulars (e.g. ID card number), and disable this feature in your browser software. People with physical access to your system may access the information contained in these sites.
- Do not store your password in any media unless it is protected from unauthorised access (e.g. protected with access control or have the password encrypted).
- Do not store access codes for encryption (e.g. passwords, passphrases, PINs) in mobile devices.

DOs

- Do change your password regularly, for example, every 90 days.
- Do change the default or initial password the first time you log in.
- Do change your password immediately if you suspect that it has been compromised. Once done, notify the system/security administrator for further follow up actions.
- Do change the password immediately once the maintenance and support are completed if the password is disclosed to vendors for maintenance and support.

11.5 Mobile Computing and Remote Access

(a) Mobile Computing and Communications

A formal usage policy and procedures shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities. The usage policy and procedures shall take into account the risks of working with mobile computing equipment in unprotected environments.

The usage policy and procedures should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and malware protection. The usage policy and procedures should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public areas.

There shall also be policy, operational plans and procedures developed and implemented for remote access. B/Ds shall authorise remote access only if appropriate security arrangements and controls are in place and comply with the security requirements. Appropriate protection for remote access shall be in place, e.g., physical protection against theft of equipment and information, proper access controls against unauthorised disclosure of information, and multi-factor authentication for remote access to the B/D's internal systems. Users should be briefed on the security threats and accept their security responsibilities with explicit acknowledgement.

(b) Remote Access / Home Office

Remote access or home office enables users to work remotely at any time. While improving productivity, this introduces security risks as they are working on non-government premises.

B/Ds should not use remote access software to connect to a departmental server or user workstation directly. Such usage of remote access software can be a backdoor access by attackers to bypass firewall/router protection to the information system. To maintain the security of government infrastructure and information assets, B/Ds should set up a policy to advise users on how to work remotely and securely. If there is a business need to use remote access software, proper security controls shall be in place, including but not limited to,

- Providing secured network connection channels with strong end-to-end security (e.g. Virtual Private Network (VPN) connections, using encryption with personal certificate/key protection).
- Restricting network access control.
- Implementing proper network management, segmentation and monitoring.
- Enabling idle timeout control to avoid unauthorised access.
- Enabling logging features.
- Monitoring the access log to find out brute force analysis

- Always applying latest patch
- Setting up a white list for registered users and endpoints with proper authentication.
- Maintaining the communication requirements with other networks as specified in Section 15.1(c).
- Regularly reviewing users' need for remote access and removing the access rights that are no longer needed.

Notwithstanding the above requirements, B/Ds shall not allow direct access to government resources by remote access software (e.g. remote desktop software) through the Internet.

For remote access to the B/D's internal network via Virtual Private Network (VPN) connections or B/D's internal email systems via the Internet, multi-factor authentication shall be implemented.

Notwithstanding the above requirements, the use of remote desktop software within the internal network also poses a significant risk on information security, including potentially facilitating unauthorised lateral movement across internal network, etc. The use of remote desktop software within the government internal network should also be carefully planned to mitigate the risk. Where the use is justified by operational necessity, B/Ds should assess the relevant security risks and implement compensatory security measures, including network segmentation, strong password policy, restricted access to designated users or IP addresses, multi-factor authentication, etc.

Remote computers should be properly protected, such as by installation of a personal firewall, anti-malware software and malware detection and repair measures. All these security features should be activated at all times and with the latest malware signatures and malware definitions applied. Besides, the latest security patches shall be applied to these remote computers. A full system scan should be performed to detect any malware in these remote computers before connecting to the government internal network.

To avoid information leakage, users should minimise storing government information on remote or portable computers. Classified information shall not be stored or processed in any computer, IoT device, mobile device or removable media which is owned privately. Viewing or interacting with RESTRICTED information using privately-owned IT equipment through virtual desktop infrastructure (VDI) should generally not be allowed as these devices are not subject to government requirements. B/Ds shall assess the security risks and obtain approval from the Heads of B/Ds for such exceptional access requests, and regularly review the access to revoke or limit access without genuine needs and legitimate purposes. B/Ds shall, technically or administratively, ensure that robust control measures are effectively implemented on such privately-owned devices, which include implementing effective antivirus software to safeguard against malicious threats, enabling automatic system updates to ensure the latest security patches are applied promptly, and enforcing strong password policies to enhance access control. The VDI shall be placed in separate network segments outside the B/Ds' internal network and

accessed with multi-factor authentication. Restriction of screen capture and paste out from VDI should be applied. Terms and conditions of use can be considered to prevent end users from taking screenshots or photographs of the VDI on the device. B/Ds should provide secured network connection channels with strong end-to-end security (e.g. Virtual Private Network (VPN) connections, using encryption with personal certificate/key protection) for the access of VDI and implement Mobile Device Management (MDM) tools to manage the devices if feasible to reduce the risk of man-in-the-middle attack and unauthorised access of the device.

When working in public areas, users should avoid working on sensitive documents to reduce the risk of exposing to unauthorised parties. Users should also avoid using public printers. If printing is necessary, the printout should be picked up quickly. Furthermore, users should protect the remote computers with password-enabled screen savers and never leave the computers unattended.

For remote access to an information system containing classified information, B/Ds should log the access activities on the information system with regular review to identify any potential unauthorised access.

Users should make reference to the guidelines in Section 13.2 when using mobile devices at remote offices.

Practical advice to enhance the protection of personal data, which can also apply to other sensitive information under work-from-home arrangements, is available at the Office of the Privacy Commissioner for Personal Data (PCPD)'s website:

- for organisations
  (https://www.pcpd.org.hk/english/resources_centre/publications/files/gn_wfh_employers.pdf)
- for employees
  (https://www.pcpd.org.hk/english/resources_centre/publications/files/gn_wfh_employees.pdf)

11.6 IoT Devices

(a) Utilisation

The utilisation of IoT devices requires a holistic view of the end-to-end security, adopting risk based approach to identify, prioritise and address the security risks of IoT devices, including but not limited to asset management, authentication and authorisation, communication network, software and application, backend infrastructure, device security, physical security, etc. In particular, B/Ds shall maintain and review the inventory of IoT devices that handle sensitive data or connect to internal/external networks and make suitable arrangements to ensure that data is handled in accordance with government security requirements.

(b) Usage Policy and Procedures

A formal usage policy and procedures shall be in place, and appropriate security measures shall be adopted to protect against the risks to IoT devices. The usage policy and procedures should include but not be limited to the requirements for physical protection, access controls, network segmentation, cryptographic protection, log management, device management such as applying security patches and firmware upgrades, malware detection and prevention, as well as data protection, in particular personal data. The usage policy and procedures should also include rules and advice on how to connect IoT devices to government networks securely, as well as avoid being controlled by malicious attackers.

(c) Deployment

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. Moreover, unnecessary functionalities of IoT devices shall be disabled to avoid collection of sensitive information as well as connection to unauthorised devices or networks.

Appropriate security controls should be taken into consideration for accessing and managing IoT devices, including but not limited to:

- Implement proper logical access control mechanisms, such as changing the default username and password, use of strong passwords and periodic change of password
- Disable unnecessary connection or network port, and restrict device connection on a need basis
- Enable multi-factor authentication if available
- Encrypt data at rest and in transit for classified data
- Manage cryptographic key properly, such as avoiding the use of common encryption key for multiple endpoints
- Install the latest security patches as recommended by product vendors for vulnerability management
- Grant user access rights based on the principle of least privilege and segregation of duties
- Enforce secure booting in IoT devices

For IoT devices in use, B/Ds should avoid collecting and storing classified information in these IoT devices. If there are business needs to process classified information, the data shall be encrypted and transmitted to secured backend storage where security controls conform to the relevant government security requirements. If it is unavoidable to store classified information in IoT devices without staff attending due to business needs, proper physical protection with compensating measures such as data wiping and network disconnection shall be implemented when an attempt of breaking-in of physical protection is detected and confirmed.

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

(a) Data Encryption

Encryption techniques are used to protect the data and enforce confidentiality during transmission and storage. Many schemes exist for the encryption of files, such as using the program's own encryption feature, external hardware device, secret key encryption, and public key encryption.

The primary use of an application's password-protection feature is to provide protection on the file and prevent unauthorised access. Users should encrypt the file instead of using only a password in order to protect the information for confidentiality as appropriate. When a password is used, it is also important to follow the practices in password selection and handling described in Section 11.4(b) Password Policy and 11.4(c) Password Selection.

B/Ds shall comply with the government security requirements in relation to the use of encryption for the protection of classified data.

User passwords used for authentication or administration should be hashed or encrypted in storage. For hashing algorithms, at least Secure Hash Algorithm 2 (SHA-2) or the equivalent should be used. Subject to operational needs, SM3 can also be used for hashing algorithms. SHA-1 shall not be used unless it is for legacy systems. If encryption is used, keys used for performing encryption (symmetric key only) or decryption shall be kept secret and shall not be disclosed to unauthorised users.

B/Ds are encouraged to conduct their own research and evaluation in selecting the most suitable solutions that meet their business requirements. The theme page "Catalogue of IT Security Solutions" provides some encryption solutions for reference by B/Ds. It may serve as a starting point for users looking for relevant security solutions. You may access the theme page via the following URL:

- **Catalogue of IT Security Solutions**
  Available at ITG InfoStation (https://itginfo.ccgo.hksarg/content/coss)

(b) Cryptographic Key Management

The term 'key' here refers to a code that is used with respect to classified information for authentication, decryption or generation of a digital signature. This code is usually generated by mathematical algorithms. These kinds of algorithms are often called "cryptographic algorithms"; the generated keys are called "cryptographic keys".

For information classified as CONFIDENTIAL or above, the symmetric encryption key length shall be at least 128-bit for the AES encryption or equivalent. Subject to operational needs, the requirement can also be met by SM4. Whereas the asymmetric encryption key length shall be at least 2048-bit for the RSA encryption. Alternatively, the requirement can be met by Elliptic Curve Cryptography (ECC) encryption with a key length of at least 224-bit or equivalent, as well as SM2 subject to operational needs. For RESTRICTED information, the above key length should also be adopted. B/Ds should have a plan to upgrade their existing systems containing RESTRICTED information to meet the key length requirements and review the plan regularly to ensure the upgrade is implemented in accordance with the pre-defined schedule.

For keys that are used for the processing of information classified CONFIDENTIAL or above, they shall be stored separately from the corresponding encrypted information. These keys may be stored inside chips of smart cards, tokens, disks, etc., and are used for authentication and/or decrypting information. It is very important to ensure the protection and management of keys. Furthermore, it is dangerous to distribute the decryption key along with the encrypted file during file distribution since one may obtain the decryption key and easily open the file.

Key management should be documented and performed properly in accordance with:

(i) Key generation
- Equipment used to generate keys should be physically protected.

(ii) Key storage
- The master cryptographic key should be stored securely, such as by placing it within a hardware security module or a trusted platform module, and should not leave the security storage for the master key's service life.

(iii) Key recovery
- Assess the need to have a recoverable key. If considered necessary, cryptographic keys should be recoverable by authorised personnel only.
- The key recovery password should be protected by at least two levels of independent access controls and limited to personnel authorised for the task of information recovery.

(iv) Key backup
- The cryptographic key should be backed up with proper protection.
- A documented process should be established to access the backed up keys.

(v) Key transfer

- Cryptographic keys should never be transported together with the data or media containing encrypted data.

(vi) Retirement of key

- Activation and deactivation dates for the cryptographic key should be defined to reduce the likelihood of key compromise arising from security threats, including brute-force attacks, personnel turnover, open office environment, etc.
- Processes for key revocation and replacement should be established.

(vii) Logging transactions

- All access to the key recovery passwords should be recorded in an audit trail.
- All access to the backed up key should be recorded in an audit trail.

With different implementations of encryption technology, a key may be used to encrypt and decrypt data (sometimes called data encryption key) and is further protected by another key (called key encryption key). As such, the ultimate key encryption key should be protected in accordance with relevant government security requirements.

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

(a) Site Preparation

As most of the critical IT equipment is normally housed in a data centre or computer room, careful site preparation of the data centre or computer room is therefore important. Site preparation shall include the following aspects:

- Site selection and accommodation planning.
- Power supply and electrical requirement.
- Air conditioning and ventilation.
- Fire protection, detection and suppression.
- Water leakage and flood control.
- Physical entry control

To start with, B/Ds should make reference to existing site selection and preparation guidelines for the general requirements and best practices, including, but not limited to:

- **Practice Guide to Data Centre Design and Site Preparation**
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/itop/itm_site_preparation.htm)

B/Ds shall comply with the physical security requirements[5] according to the classification of information system(s) housed in a data centre or computer room. In situations where office premises cannot fulfil the physical security requirements, B/Ds shall seek advice from the Government Security Officer (GSO) on individual merits.

If a wireless communication network is to be set up on the site, a site survey shall be conducted to ensure proper area coverage of wireless signal and to determine the appropriate placement of wireless devices.

[5] For building works or fitting-out works on any government accommodation involving construction or conversion of a room into one that provides secure storage for classified data, B/Ds shall refer to government security requirements and spell out the required security level to Architectural Services Department, who shall carry out the necessary works in commensurate with security level as defined in prescribed guidelines. There is no need for B/Ds to obtain the detailed specifications of the guidelines, which will not normally be disclosed due to security reason.

(b) Fire Fighting

A fire fighting party should be organised in each operating shift with well-defined responsibilities assigned to each officer in concern. Regular fire drills shall be carried out to allow the officers to practice the routines to be followed when a fire breaks out.

Those operators not being members of the fire fighting party shall be taught how to operate the fire detection, prevention and suppression system and the portable fire extinguishers.

Hazardous or combustible materials should be stored at a safe distance from the office environment. Bulk supplies such as stationery should not be stored in the data centre or computer room. Stocks of stationeries to be kept inside the data centre or computer room should not exceed the consumption of a shift.

Hand-held fire extinguishers should be in strategic locations in the computer area, tagged for inspection and inspected at least annually.

Smoke detectors should be installed to supplement the fire suppression systems. Smoke detectors should be located high and below the ceiling tiles throughout the computer area and/or underneath the raised floor. Heat detectors may be installed as well. Heat detectors should be located below the ceiling tiles in the computer area. Heat detectors should produce audible alarms when triggered.

Gas-based fire suppression systems are preferred. Where water-based systems are used, dry-pipe sprinkling systems are preferred rather than ordinary water sprinkling systems. All fire suppression systems should be inspected and tested annually. Fire suppression systems should be segmented so that a fire in one area will not activate all suppression systems in the office environment.

(c) Physical Access Control

All access keys, cards, passwords, etc., for entry to any of the information systems and networks, shall be physically secured, subject to well-defined and strictly enforced security procedures. Staff should be educated to enter the password not in front of unauthorised personnel and to return the card keys or access devices when they resign or when they are dismissed. The acknowledgement of passwords and receipt of magnetic card keys shall be confined to authorised personnel only, and records of passwords shall be securely stored. Cardkeys or entrance passwords should not be divulged to any unauthorised person.

All staff shall ensure the security of their offices. Offices that can be directly accessed from public areas should be locked up any time when not in use, irrespective of how long the period might be, to protect information systems or information assets inside.

A list of authorised personnel to access the data centres, computer room or other areas supporting critical activities shall be maintained, kept up-to-date and reviewed

periodically. If possible, ask the cleaning contractor to assign a designated worker to perform the data centre or computer room cleaning and the personal particulars of whom shall be obtained. During the maintenance of the information system, works performed by external parties shall be monitored by the staff responsible.

Entry by visitors, such as vendor support staff, maintenance staff, project teams or other external parties, shall not be allowed unless accompanied by authorised staff. People permitted to enter the data centre or computer room shall have their identification card properly displayed so that intruders can be identified easily. Moreover, a visitor access record shall be kept and properly maintained for audit purposes. The access records may include the name and organisation of the person visiting, signature of the visitor, date of access, time of entry and departure, purpose of visit, etc.

All protected and secured areas in the computer area shall be identified by conspicuous warning notices so as to deter intrusion by strangers. On the other hand, the passage between the data centre/computer room and the data control office, if any, should not be publicly accessible in order to avoid the taking away of material from the data centre/computer room without being noticed.

All protected and secured areas in the computer area should be physically locked and periodically checked so that unauthorised users cannot enter the computer area easily. Examples of acceptable locks are, but are not limited to, bolting door locks, cipher locks, electronic door locks, and biometrics door locks.

B/Ds should consider installing video cameras (or closed-circuit TVs) to monitor the computer area hosting critical/sensitive systems and have video images recorded. The view of cameras should cover the whole computer area. The recording of the camera should be retained for at least a month for possible future playback. Besides, intruder detection systems should be considered to be installed for areas hosting critical/sensitive systems.

13.2 Equipment

(a) Equipment Siting and Protection

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. For IoT devices, security controls shall be enforced to protect the device against loss, theft and damage according to the classification of information being stored, processed and transmitted by the IoT devices.

Proper controls should be implemented when taking IT equipment away from sites. For mobile devices and removable media, B/Ds shall keep an authorised equipment list and periodically perform inventory checks for the status of such IT equipment. Besides, B/Ds shall adopt a check-in check-out process or inventory documentation measures to identify which mobile devices and removable media has been taken away. Nevertheless, staff taking IT equipment off-site should also ensure that IT

equipment is not left unattended in public places or is properly locked up when not attended to protect against loss and theft. Staff shall safeguard their approved possessions, such as mobile devices and removable media, for business purposes and shall not leave business possessions unattended without proper security measures.

Whenever leaving the workplace, re-authentication features such as a password protected screen saver on their workstations shall be activated, or the logon session/connection shall be terminated to prevent illegal system access attempts. For a prolonged period of inactivity, the workstation shall be switched off to prevent unauthorised system access.

Staff shall carefully position the display screen of an information system on which classified information can be viewed to prevent unauthorised persons from viewing the classified information. Staff should consider using a privacy screen filter to limit the view angle of the display screen.

14. OPERATIONS SECURITY

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

14.1 Operational Procedures and Responsibilities

(a) Principle of Least Functionality

Information systems should be configured to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services. The functions and services provided should be carefully reviewed to determine which functions and services are candidates for elimination. Administrators should consider disabling unused or unnecessary physical and logical ports and protocols (e.g. USB port, FTP, SSH) on information system components to prevent unauthorised connection of devices, unauthorised transfer of information, or unauthorised tunnelling.

Both the least functionality principle and least privilege principle shall be adopted when performing system hardening, assigning resources and privileges and accessing networks or network services. For details of least privilege principle, please refer to Section 11.1(a) “Principle of Least Privilege”.

(b) Change Management

Changes affecting existing security protection mechanisms shall be carefully considered. Changes to information systems should be controlled. Operational systems and application software should be subject to strict change management control, and the following should be considered:

- Identification and recording of significant changes.
- Planning and testing of changes.
- Assessment of the potential impacts, including security impacts.
- Formal approval procedure for proposed changes.
- Communication of change details to all relevant parties.
- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
- Provision of an emergency change process to enable quick and controlled implementation of changes for resolving an incident.

(c) Operational and Administrative Procedures

Operational and administrative procedures shall be properly documented, followed, maintained, reviewed regularly and made available to users who need them.

Documentations should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and shut-down, backup, equipment maintenance, media handling, computer room management, etc. B/Ds should develop, maintain and review regularly the baseline configuration of their information systems.

(d) Capacity Management

The use of resources should be monitored for capacity management. Capacity requirements should be identified according to the business requirements of the concerned system.

A capacity management plan should be in place for information systems to outline B/D's approach and processes for monitoring, analysing and adjusting information system capacity over time. It helps ensure that the IT infrastructure has sufficient capacity to handle current and planned business workloads. Staff in charge of budgeting should take into account the demands in a capacity management plan.

14.2 Protection from Malware

(a) User's Protection

To protect against malware, users should ensure malware detection and recovery protection measures have been installed and run on their workstations and mobile devices to protect against threats from malware. Some products will also provide a certain degree of protection against spyware/adware.

But, if the malware definition is not updated, the protection software will not be able to detect and guard against the latest malware attacks. Users shall regularly update malware definitions and detection and repair engines. Updates should be configured as automatic, and update frequency should be at least on a daily basis. If automatic updates are not possible (e.g. mobile devices not often attached to networks), updates should be done manually at least once a week. Users should also note that from time to time, there could be ad hoc and serious malware outbreaks. If so, users shall follow the instructions and immediately update with the latest malware definitions in order to protect against malware outbreaks.

The following are security guidelines to protect against malware:

- Enable real-time detection to scan malware for active processes, executables and document files that are being processed. Also, schedule full-system scans to run regularly based on operational needs.
- Check any files on storage media and files received over networks against malware before use.
- Avoid opening suspicious electronic messages, and do not follow URL links from un-trusted sources to avoid being re-directed to malicious websites.
- Check attachments and downloads against malware before use.

- Before installing any software, verify its integrity (e.g. comparing checksum value) and ensure it is free of malware. Prior approval from the officer as designated by the B/D should be obtained before installing any executable/software, including those received via electronic message or downloaded from web browsing.
- Always boot from the primary hard disk. Do not allow booting workstations from removable devices without permission.
- Do not use storage media and files from unknown sources or origin unless the storage media and files have been checked and cleaned for malware.
- Follow the guidance in Section 14.3 (a) Data Backup and Recovery to backup data.

Users shall not intentionally write, generate, copy, propagate, execute or be involved in introducing malware. User should be responsible for protecting their workstations and mobile devices by taking the appropriate actions for malware protection.

(b) LAN/System Administrator's Protection

To protect against malware, LAN/System Administrators shall ensure servers, workstations and mobile devices are installed with malware detection and recovery protection measures. Malware definition updates should be configured as automatic, and the update frequency should be at least on a daily basis. If automatic update is not possible, LAN/System Administrators should perform manual updates at least once a week and whenever necessary.

The malware detection and recovery protection measures should support enterprise management to facilitate central management. Please refer to Section 15.1(b) Network Security Controls for more details about enterprise management.

LAN/System administrators should implement the following technical controls:

- Enable anti-malware protection on all local area network servers, personal computers, mobile devices, and computers connecting to the government internal network via a remote access channel.
- Enable anti-malware protection to scan all incoming traffic from the Internet. The gateway should be configured to stop traffic with malicious content, quarantine / drop them, and create audit logs for future reference.
- Apply information security considerations and procedures to computer equipment and software under development or being used for testing purposes. A less stable environment is likely to be more vulnerable to attacks unless proper control is applied.
- Perform full system scans for all computers of staff, contractors or outsourced staff before the machines are connected to the government networks.
- Request an external vendor to scan for malware (with the latest malware definition) on the user's hard disk after new machine installation, service maintenance or installation of software.

While managing servers, LAN/system administrators should observe the following security guidelines:

- Boot the server from the primary hard drive. If the machine should be booted from removable media like floppy diskettes, USB flash drives or hard drives, optical disks, etc., the removable media must be scanned for malware before booting. This can eliminate boot sector viruses from infecting the server.
- Protect application programs in the server by using an access control facility, e.g. directories containing applications should be set to 'read only'. In addition, access rights, especially the right to 'Write' and 'Modify', should be granted with least privilege on a need-to-have basis.
- Consider using a document management solution to share common documents with proper access controls and protections.
- Scan all newly installed software before they are released for public use.
- Schedule preferably a full-system scan to run immediately after the file server start-up.
- Follow the guidance in Section 14.3 (a) Data Backup and Recovery to backup data.
- In addition, LAN/system administrators should keep updated with security advisories and educate users on the best practices to protect against malware:
- Subscribe to notifications / advisories so that they can receive critical malware alerts at the earliest possible moment.
- Disseminate promptly the security alert issued by DPO to all end users and take necessary actions.
- Educate users to understand the impact of massive malware attacks and recognise ways of infecting with malware (e.g. educate users that the sender of an electronic message containing malware can be forged as friends or colleagues) in order to prevent malware infection.

(c) Detection and Recovery

The following can be symptoms of a computer infected with malware:

- Program takes longer time than usual to execute.
- Sudden reduction in system memory available or disk space.
- Unknown / new files, programs or processes in the computer.
- Popping up of new windows or browser advertisements.
- Abnormal restart/shutdown of the computer.
- Increase in network usage.

If a computer is suspected to be infected with malware, users should stop all activities because continually using the infected computer may help spread the malware further. Users should report any suspected malware incident to the management and LAN/system administrator immediately. If necessary, DITSO should be informed to determine if it is a security event or a security incident. The

DPO Central Computer Centre Helpdesk (ccc_hd@digitalpolicy.gov.hk) can provide technical assistance in investigating suspected malware incidents. With the assistance or advice of LAN/system administrators, users may also use anti-malware software available in the market to clear the malware on their own.

Removing malware does not necessarily imply that contaminated or deleted files can be recovered or retrieved. The most effective way to recover corrupted files is to replace them with the original copies. Therefore, regular backups should be done, and sufficient backup copies should be kept to facilitate file recovery whenever necessary.

After removing malware from a computer, users should perform a complete scan of the computer and other storage media to ensure that they are free of malware. Failure to rescan a computer for malware may lead to the resurrection of the malware.

(d) Use of Content Filtering

B/Ds should consider the value versus inconvenience of implementing technologies to block access to non-business websites. The ability to connect with a specific website does not in itself imply that users of systems are permitted to visit that site. B/Ds should consider using web page content filtering software to prevent staff from abusing resources, for example, downloading files in bulk from the Internet or browsing harmful websites. These activities not only consume bandwidth and waste resources but also increase the risk of malware infection.

Creating and enforcing a whitelist of allowed websites is a strong content filtering method. Only allowing access to websites with business needs can reduce the attack surface of the system. Alternatively, B/Ds can prevent users from browsing websites by using a blacklist approach. Some content filtering tools come with a database on the categorisation of web pages, which will be periodically reviewed and updated by the supplier to determine whether a web page is suitable for viewing by categorisation and scoring based on the web content. B/Ds should conduct research and identify suitable content filtering solutions for their business needs.

14.3 Backup

(a) Data Backup and Recovery

B/Ds shall carry out backups at regular intervals. B/Ds shall establish and implement backup and recovery policies for their information systems. Users should perform backups for the data stored in their workstations, mobile devices and removable storage media regularly. The backup frequency should be based on the impact of loss of availability of the data. Backup restoration tests shall be conducted regularly. The frequency of backup reviews and restoration tests shall be defined and documented. B/Ds should follow the best practices when establishing their backup and recovery policies:

- Backup copies should be maintained for all operational data to enable reconstruction should they be inadvertently destroyed or lost.
- The backup copies shall be taken at regular intervals such that recovery to the most up-to-date state is possible.
- Backup activities shall be reviewed regularly. Procedures for data backup and recovery shall be well established. Wherever possible, their effectiveness in real-life situations shall be tested thoroughly.
- The backup restoration test should be combined with a test of the backup media, associated tools, and restoration procedures and checked against the restoration time required.
- Backup software for servers should be server-based so that the data transfer can be faster and no traffic overhead is added to the network. Moreover, the software should allow unattended job scheduling, thus backup process can be done in non-office hours.
- It is advisable to store backup copies at a safe and secure location remote from the site of the systems. In case of any disaster which destroys the systems, the systems could still be reconstructed elsewhere.
- Should software updates, besides backup copies of the data, be necessary to recover an application system, the updates (or backup copies of them) and the data backup should be stored together.
- Multiple generations of backup copies should be maintained. This would provide additional flexibility and resilience to the recovery process. A "grandfather-father-son" scheme for maintaining backup copies should be considered such that two sets, viz, the last and the last but one, of backup copies are always maintained together with the current operational copy of data and programs. The updates to bring the backup copies to the current operational state shall, of course, also be maintained and stored with the backup copies.
- At least three generations of backups should be kept. However, if daily backups are taken, it may be easier administratively to retain six or seven generations. For example, a Monday's daily backup should be kept until the following Monday, when it can be overwritten. Month end and year end copies of files may be retained for longer periods as required.
- Magnetic tapes, magnetic/optical disks or cartridges used for backup should be tested periodically to ensure that they can be restored when needed.
- If an auto tape changer is implemented, it should be noted that the delivery turnaround time for an off-site storage location will be lengthened as tapes are not immediately relocated. A balance point should be struck between the operational convenience and the availability of backup data, especially for crucial information.

In some unexpected situations where data is deleted accidentally before performing a backup or data resides on a failed hard disk that cannot be accessed through the system, a hard disk data recovery service may be required. If an adopting external data recovery service is required, B/Ds should follow the best practices to mitigate the risk of data leakage:

- Use on-site data recovery service as far as practicable and ensure the contractor is aware of the protection requirements for the classified information during the recovery process.
- Escort the contractor's staff and take due care to ensure that classified information is not disclosed.
- Sanitise the residual user data in the equipment tools and the associated media used for the data recovery.
- Obtain a non-disclosure agreement from the contractor.
- Observe the government security requirements, in particular, on outsourcing security.

(b) Devices and Media for Data Backup

Proper procedures shall be established for the storing and handling of backup data. 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. Where physical disconnection is not possible, B/Ds should consider disconnection through logical means such as disabling the network port in the network device, using a tape library with autoloader, which has a mechanical means to move tapes into and out of the drives, or maintaining a non-updatable backup copy that cannot be accessed by malware (e.g. ransomware) so as to ensure the last backup copy is secured even if the production system is compromised.

Backup media should be stored and maintained properly. The backup media should be properly labelled and placed in their protective boxes with the write-protect tab, if any, in the write-protect position. The backup media should be kept away from magnetic/electromagnetic fields and heat sources and follow the manufacturer's specifications for the storage environment.

Access to the backup media shall only be done via authorised persons according to the established mechanism. Unauthorised access to the media library or off-site storage room shall not be allowed.

Physical transportation of backup media for offsite storage can be subject to risks of theft, loss, and unauthorised access. Where offsite storage of backup media is required, B/Ds should consider implementing alternative technology solutions that ride on secure network data transfer. In circumstances where physical transportation is deemed necessary, B/Ds should assess the relevant security risks and properly handle physical transportation of backup media to and from off-site, including securing containers with backup media onto escort personnel physically to maintain constant custody and controls, maintaining comprehensive chain-of-custody logs to ensure accountability, and employing appropriate tracking measures for better response in the event of loss. The cases carrying the media should be shockproof, heatproof, and water-proof and should be able to withstand magnetic interference. B/Ds should consider protecting the media from theft – by encrypting the data in the storage media. Movement of media IN/OUT of a library or off-site storage shall be properly logged. Unless permission is granted, any staff shall not be allowed to leave the data centre or computer room with any media. To facilitate the detection

of lost media, the storage rack can indicate some sort of markings/labels at the vacant slot positions. Periodic inventory checks shall be conducted to detect any loss or destruction of backup media.

There are quite a lot of devices available for data backup and recovery, such as magnetic disks, optical disks and digital data storage tapes.

The most commonly used medium for server backup is tape, as it is relatively cheap for the capacity provided. A tape magazine or automatic tape changer may also be used if the data volume is very large and spans multiple tapes in one backup session. To take advantage of tape changers, your backup software must have a tape changer option to support them.

For workstation backup, many devices are available as the amount of data that is required to be backed up will be generally less than that of a server. Tape is still the relatively cheapest device when a large amount of data is going to be backed up. Most workstation backup software supports both backup to tape and backup to removable optical storage media.

The tape drive's head should be cleaned regularly. The cleaning frequency depends on factors like the operating environment and operational (backup, restore, scan tape, etc.) frequency. Some tape drives have indicators to remind the user to clean their head after a certain number of runs. Documentation of the tape drive should be referred to for more information.

14.4 Logging

(a) Log Collection and Retention

An audit trail shows how the system is being used from day to day. Depending upon the configuration of the audit log system, audit log files may show a range of access attempts from which abnormal system usage can be derived.

More complicated applications should have their own auditing or tracing functions in order to give more information on individual use or misuse of the application. This mechanism is virtually essential for highly secure applications, as the tracing functionality of the operating system may not have a fine enough granularity to record critical functions of the application.

There is virtually no limit to the recording of access to records by individual users and the actual updates made. However, logging routine use can result in a waste of resources and may even obscure irregularities because of the volume generated. Therefore, self-developed audit trails should focus on failed transactions and attempts by users to access objects for which they do not have authorisation.

Transaction logs can contain the following information but are not limited to:

- Unauthorised update/access.
- Starting/ending date and time of activity.
- User identification (for illegal logon).
- Sign-on and sign-off activity (for illegal logon).
- Connection session or terminal.
- Computer services such as file copying and searching.

B/D shall define and document policies relating to the logging of activities of information systems (including the retention period) according to its business needs and data classification. The policies shall include but not be limited to the requirement to log:

- Attempts for log-in.
- Attempts for password changes.
- Access attempts to critical files (e.g. software configuration files, password and key files, etc.).
- Use of privileged rights such as addition and deletion of user accounts.
- Changes to user access rights.
- Modification to audit policy.
- Activation and de-activation of protection systems, such as anti-malware systems and intrusion detection systems.

Failure to log the above activities shall be justified and documented.

Information logged should meet the above requirement at a minimum to audit the effectiveness of the security measures (e.g. logical access control) in case a violation of the IT security policy (e.g. attempt of unauthorised access to a resource) is detected. The logging details should be commensurate with business needs and data classification. Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity or incident handling as approved by a Directorate officer.

Logs of the Approved Email System and Internet access service centrally provided by DPO or B/Ds shall be recorded. For the email log, the fields shall include but are not limited to sending date/time, client IP address, sender and recipient email addresses, and total email size. Other valuable fields (such as email subject, name and size of email attachment) and events (such as access to email including read, delete, unauthorised access) should also be logged. For the Internet access log, the fields shall include but are not limited to access date/time, client IP address, access website or URL.

The uncontrolled use of removable media and printers poses a risk of data leakage. B/Ds should prevent classified data from being transferred through printers or removable media for unauthorised use. Security controls, including but not limited to blocking connection of unauthorised removable media such as USB storage devices, logging printing activities and file transfer activities to removable media, should be applied. Depending on system criticality, data sensitivity and subsequent

impact in case of an incident, B/Ds shall have an upgrade plan for implementing endpoint protection solutions to strengthen security protection and support incident assessment on the use of removable media and printers for servers, workstations and mobile devices, in particular crucial systems, if such security controls cannot be implemented for existing systems.

Logs shall be retained for a period commensurate with their usefulness as an audit tool. The information and retention period of the logs shall also be sufficient to support the investigation of a breach of security. The retention period for a log of Approved Email System and Internet access service centrally provided by DPO or B/Ds shall be no less than six months. During the retention period, logs shall be secured such that they cannot be modified and can only be read by authorised persons. B/Ds should consider managing their logs through centralised log management. B/Ds shall regularly review the log retention period and storage capacity to ensure that log data is retained appropriately and that sufficient storage space is available.

B/Ds should take the following considerations into account when defining and reviewing their logging policies:

(i) Log generation
- Types of IT equipment and their components (e.g. applications, database, etc.) to generate logs.
- Types of events to be logged.
- Details for each type of event to be logged (e.g. username, source IP address, time stamps, etc.).
- Clock synchronisation requirements (e.g. trusted time source, date and time format, synchronisation method and frequency, etc.).

(ii) Log transmission
- Types of IT equipment and their components to transfer logs to central log management infrastructure.
- Log delivery requirements (e.g. network protocols, etc.).
- Frequency of logs to be transferred (e.g. real-time, every hour, etc.).

(iii) Log storage and disposal
- Log protection requirements (e.g. access control, etc.).
- Log storage space.
- Criteria for log rotation.
- Log retention period based on risk level of information system.

(iv) Log analysis
- Roles and responsibilities.
- Type of events to trigger alerts to responsible parties.
- Type of events to be analysed.
- Log review frequency.
- Handling procedures for suspicious and abnormal activities.

If shared accounts are used in a B/D, the system/security administrator should maintain and periodically update an account inventory list for shared/group accounts with information including, but not limited to, system name, user name (in person) who can share the account, shared user-ID, permission(s) granted, account valid period, and reason for sharing. The account inventory list can be used to trace the individual who has shared access to a particular system at a given time for an investigation if required.

Systems containing information classified as CONFIDENTIAL or above shall enable an audit trail on all shared access to the data.

Audit trail and logging features shall be enabled on a standalone PC or workstation when classified data is stored on its hard drive. Sufficient hard disk size shall be made available for log retention based on the retention period defined in the departmental logging policies.

Information systems shall synchronise their clock with a trusted time server periodically (at least once per month). B/Ds should use the clock synchronisation service from GNET or the time server of Hong Kong Observatory via the Network Time Protocol (NTP). Authentication in NTP can be considered to enhance security in the clock synchronisation process. System time for all machines may not necessarily be identical. Depending on the type and precision requirements of an information system, time deviation should be controlled within a reasonable limit. With a synchronised clock, audit trails can then have a trusted timestamp, and event correlation can be made easier. Besides, audit trails will be more credible during incident investigations.

Information about the clock synchronisation service of GNET is available at ITG InfoStation (https://itginfo.ccgo.hksarg/content/gnet/servicevas.htm#ntp).

Information about the time synchronisation service of Hong Kong Observatory (HKO) is available at HKO's website (https://www.hko.gov.hk/en/nts/ntime.htm).

14.5 Control of Operational Environment

(a) Installation of Computer Equipment and Software

Installation of computer equipment and software shall only be done by authorised staff, after obtaining approval from the system owner or the responsible manager. Equipment or software shall only be installed and connected if it does not lead to a compromise of existing security controls. All changes made to either equipment or software should be fully documented and tested, and an audit trail of all installations and upgrades should be maintained.

(b) Control of Changes

Changes to facilities, information systems, as well as business and security processes that affect IT security shall be controlled. Change control procedures and associated roles and responsibilities shall be defined and in place to ensure proper control of

changes. Change records shall be maintained to keep track of the applied changes. In addition to the operational environment, environments for development, testing and disaster recovery should also be subject to adequate change control. For details of change management control, please refer to Section 14.1(b) "Change Management".

14.6 Technical Vulnerability Management

(a) Vulnerability Management Process

B/Ds shall implement vulnerability management processes, which include identifying, evaluating, mitigating, and tracking of vulnerabilities. Integrating these processes into regular routines helps ensure that any new vulnerabilities are promptly identified and fixed before being exploited. The effective management of vulnerabilities also contribute to the effective IT security risk management in B/Ds.

(i) Vulnerability Identification

B/Ds shall implement a vulnerability identification process to continually discover potential vulnerabilities within their information systems. The process should involve different vulnerability identification activities, including vulnerability scanning, penetration testing, source code reviews, configuration reviews, simulated attacks, etc. to identify potential security loopholes and vulnerabilities. On the other hand, the vulnerability identification process should also involve monitoring of sources (e.g. GovCERT.HK) which would disseminate security news, alerts, reports and other publications to enable timely identification of new attack methods and unpatched vulnerabilities. The vulnerability identification activities used in this process may also be leveraged in the risk identification process during the security risk assessments to identify vulnerabilities that may contribute to IT security risks.

(ii) Vulnerability Evaluation

B/Ds shall implement a vulnerability evaluation process to assess the potential impact and severity of the vulnerabilities once they are identified. This evaluation should account for factors such as the sensitivity of the data or systems, the potential damage or disruption caused by successful exploitation, and the complexity of exploiting the vulnerability.

(iii) Vulnerability Mitigation

B/Ds shall implement a vulnerability mitigation process to take action to address and mitigate vulnerabilities timely upon assessing them. The process involves implementing a robust patch management process to apply necessary updates and adjusting configuration settings to secure the information systems. Implementing additional security controls to prevent exploitation and ensuring the use of authorised software are also integral to this mitigation process. In cases where immediate mitigation is not possible, B/Ds should implement temporary workarounds or compensating controls.

(iv) Vulnerability Tracking

B/Ds shall implement a vulnerability tracking process to ensure continuous tracking and monitoring of the identified vulnerabilities and their respective mitigation efforts. This involves maintaining a vulnerability inventory, regularly updating the status of vulnerabilities, and providing regular updates to DITSO.

(b) Vulnerability Scanning

Vulnerability scanning is part of vulnerability identification activities that should be adopted in the vulnerability management process. It uses specialised tools to systematically examine information systems for known vulnerabilities and aims to identify weaknesses before malicious actors can exploit them.

B/Ds shall maintain a record of vulnerability scanning results and remediation actions taken. This documentation will be helpful for future security audits and risk assessments. Furthermore, B/Ds should regularly review and update their vulnerability scanning schedule and tools to ensure they remain effective against evolving threats and vulnerabilities.

All personnel involved in the vulnerability scanning process should receive appropriate training and support to carry out their tasks effectively. This includes understanding how to configure and use scanning tools, interpret results, and remediate identified vulnerabilities. The GovCERT.HK Technology Centre provides vulnerability scanning facilities for B/Ds to conduct vulnerability scanning to their Internet-facing websites with the necessary assistance from the GovCERT.HK.

(c) Penetration Testing

Penetration testing is part of vulnerability identification activities that should be adopted in the vulnerability management process. While vulnerability scanning attempts to discover vulnerabilities without exploiting the vulnerability, penetration testing utilises automatic and manual techniques to discover vulnerabilities and simulate cyber-attacks to exploit the vulnerabilities. Penetration testing is an essential way to ensure effectiveness implementation of security measures of information systems, allowing B/Ds to better understand their systems' weaknesses and take proactive steps to address them. During the security risk assessments for information systems, penetration testing may also be incorporated in the corresponding risk identification process to discover vulnerabilities in information systems.

Before performing penetration testing, B/Ds should clearly define the scope and goals of the tests, which include an agreement with the penetration tester about the methods to be used and how the results should be reported. Penetration testing shall be carried out from the position of an external potential attacker, and can involve active exploitation of possible vulnerabilities. The penetration testing shall include network security, system software security, client-side application security, and server-side application security. The penetration tester should also understand the

scope and potential operational implications of the test. B/Ds may consider engaging external vendors specialising in penetration testing to conduct these tests.

Threat intelligence can be utilised to enhance the effectiveness of penetration testing by providing insights into the latest tactics, techniques, and procedures (TTPs) that threat actors use. This information can guide the design and execution of the test, enabling it to emulate real-world attacks better and identify vulnerabilities that current and emerging threats might exploit.

Similar to vulnerability scanning, B/Ds shall document all penetration testing results and follow-up actions. This documentation will be critical for future security audits. It can provide valuable insights into the ongoing security posture of the B/D.

Please refer to the Practice Guide on Penetration Testing for guidance on penetration testing.

(d) Configuration Review

Configuration reviews are part of the vulnerability identification activities that should be adopted in the vulnerability management process. A configuration review aims to identify potential misconfigurations that could introduce vulnerabilities and compromise the security of information systems. Configuration reviews may leverage automated scanning tools or manual review exercises to ensure the configurations of information systems are properly set up and aligned with security best practices.

(e) Source Code Review

Source code reviews is part of the vulnerability identification activities that should be adopted in the vulnerability management process. A source code review refers to the process of examining code with automated scanning tools or through a manual process to identify bugs, errors, and security flaws in information systems. B/Ds should utilise source code reviews to identify, classify, and prioritise repairs for bugs that present in the source code of information systems. Code modifications, applying secure coding practices, and implementing security controls are common mitigation measures for the identified source code issues.

(f) Simulated Attack

A simulated attack exercise, being intelligence driven and threat based, is a pivotal aspect of technical vulnerability management. Simulated attacks are part of the vulnerability identification activities that can be adopted in the vulnerability management process. A simulated attack exercise is also known as the red team exercise, which is designed to imitate authentic attacks to validate the overall strength of a B/D's security controls and their ability to withstand actual attacks. The exercise leverages a variety of methods to test different vulnerability points, ranging from social engineering to sophisticated technical exploits. While

penetration testing is designed to attempt discovering as many vulnerabilities as possible, simulated attacks are performed from the perspective of an external threat actor with a specific agreed objective (e.g. gaining access to a specific database of Tier 2 information systems).

The objectives, scope, and rules of engagement for the exercise should be clearly defined before conducting a simulated attack exercise. The results of the simulated attacks should be analysed to assess the B/D's ability to detect, respond to, and recover from the attacks. This analysis should be all-encompassing, taking into account both the technical and departmental aspects of the response. The findings should be documented, and recommendations for remediation should be made. The final report should be detailed, providing actionable insights to help strengthen the B/D's security posture. After implementing remediation measures, a re-test should be conducted to validate that the identified vulnerabilities are effectively addressed.

B/Ds can utilise threat intelligence in the simulated attack. For example, the reconnaissance phase can be enhanced with threat intelligence, as it facilitates the identification of likely attack vectors based on known TTPs of potential threat actors. This allows the simulated attack to mirror real-world threats more accurately, testing the B/D's defences against attacks they are most likely to encounter.

On the other hand, there is another type of attack simulation exercise, the purple team exercise, which also involves the blue (defensive) team in the simulated attack process. The blue team participates in the exercise with an aim to learning about the security loopholes which the red team finds and improving the overall defensive capabilities of the B/D.

(g) Patch Management

Patch management is the process of installing software updates and fixes in a timely manner to address vulnerabilities and resolve issues in information systems. It is an important vulnerability mitigation component to promptly address the vulnerabilities identified.

To avoid attacks through known issues or vulnerabilities, LAN/system administrators shall apply the latest security patches/hot-fixes released by product vendors to the information systems, including the operating systems, database software, programming libraries and applications running on them, or implement other compensating security measures. B/Ds should ensure that their LAN/system administrators are well informed of the latest release of security patches/hotfixes.

A responsive patch management process is critical in maintaining the security of information systems. With the increase in vulnerabilities discovered and the corresponding patches released, it is essential that LAN/system administrators should manage the patching process in a systematic and controlled way.

Successful patch management requires a robust process. This process, the patch management lifecycle, includes multiple steps that are described below:

- Patch acquisition – select and download appropriate patches and prepare them for deployment.
- Testing – perform testing to determine whether the patches contain components that conflict with other patches, key enterprise applications or even entire environment "baselines".
- Risk assessment – assess the risks and impacts associated with installing the patch and identify actions to be taken. Asking questions such as will the functionality of the system application be affected? Does the system require a reboot after installing the patch, which affects service availability?
- Deployment – deploy patches to the target machines and make sure that patches are only installed on machines where they are required.
- Compliance – verify that all machines are functioning properly and comply with the related security policies and guidelines.

In addition, the following guidance should be followed regarding patch installation and management:

- Create and maintain an inventory record of hardware equipment and software packages (including the patch management system itself) and version numbers of those packages mostly used within the B/Ds. This inventory record is essential to the patch management process and will enable system administrators to easily monitor and identify relevant vulnerabilities and patches.
- Define roles and responsibilities associated with patch management, including vulnerability monitoring, patching, etc.
- Consider standardising the configuration of their information systems. Standardised configuration can simplify the patch testing and installation process.
- Monitor IT security resources for vulnerabilities and patches which are relevant to the B/Ds.
- Define a timeline to react to security advisories relating to the technical configurations of the systems.
- Identify the associated risks and actions to be taken once a security vulnerability has been confirmed.
- Regularly review the patch management process to measure its effectiveness and efficiency.
- Check the end-of-support date for software products at the official website of the software vendor and prepare a viable migration plan beforehand.
- Uninstall end-of-support software products or upgrade to another software product that has security updates.
- Educate users to be highly aware of the importance of IT security and patch management to their daily operations.

- Perform vulnerability identification regularly, e.g. using vulnerability scanning tools (host-based or network-based) to identify patch inadequacy or system mis-configuration.
- Consider the acquisition of a patch management system that supports the full patch management cycle to ease the manual administration work and reduce patch deployment/testing time. Proper security measures should also be applied to the patch management system.

When a security patch is available, B/Ds shall assess the impacts in association with such installation. The patches shall be tested and evaluated before they are installed to ensure they are effective. The security patches shall be applied through an established change control process. If installing a patch is not feasible, an upgrade of the concerned product to eliminate security problems should be planned, or alternate security controls should be implemented and documented.

For end-of-support software, security updates to fix vulnerabilities to identified risks will no longer be available. This will increase the chance of successful intrusion into the systems or networks. If there is a need to use end-of-support software, B/Ds shall assess the security risks of using end-of-support software and implement appropriate security measures to protect the information systems and related data. To mitigate the impact of end-of-support issues, the migration plan should be in place at least six months before the end-of-support date, and the associated security measures should be in place no later than the end-of-support date. The migration plan should include but not be limited to the risk assessment in using such software, the planned date to replace such software, and security measures (such as physical isolation from the departmental network, whitelist applications and USB devices) when using end-of-support software.

Depending on the nature of information systems, their risk level can be different. For example, an information system for internal use faces fewer threats than an information system directly facing the Internet serving the public. 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. All known vulnerabilities of Internet-facing information systems should be fixed within a month after the release of security patches. In essence, information systems of high risk should be addressed first. B/Ds shall follow the recommendations stipulated in the security alerts issued by GovCERT.HK to mitigate the vulnerabilities of their information systems.

When evaluating whether to apply a security patch, the risks associated with installing the patch should be assessed by comparing the risk posed by the vulnerability with the risk of installing the patch. If a B/D decides not to apply a patch due to whatever reasons or if no patch is available, DITSO should be consulted, and the case shall be properly documented. B/D should also implement other compensating controls such as:

- Turning off services or capabilities related to the vulnerability.
- Adapting or adding access controls.
- Increased monitoring to detect or prevent actual attacks.

(h) Using Authorised Software

The control of software installation is one of the important vulnerability mitigation components to prevent the occurrence of potential vulnerabilities from unauthorised software. B/Ds shall define and maintain a list of authorised software, including freeware, open source software, mobile apps, programming libraries and related applications based on operational needs. Proper approval from an officer as designated by the B/D shall be obtained if installation of any software not in the authorised software list is required.

As for sourcing software downloaded from the Internet, it is important for B/Ds to note that that software can contain malware that is installed along with the legitimate software. B/Ds shall obtain the software from official sources and verify its integrity using the vendor supplied checksums. Furthermore, B/Ds should take the following considerations into account before deploying the software:

- Need of use of the software / product.
- Past record of the product.
- Patch frequency and the response time of product vendor to address the product's vulnerabilities.
- Characteristics of the product that may impose risks to the B/D (e.g., data synchronisation to cloud services).
- Security risks to the B/D in case the software / product is exploited.
- Technical support issues of the software / product.

Software Asset Management (SAM) tools are used to automate software inventory scanning and software metering. They help in detecting unauthorised software, ensuring sufficient licence coverage and revealing unused or under-utilised software licences. B/Ds should consider deploying SAM tools to assist in managing their software assets.

There are different products and technologies for SAM. For example, some desktop operating systems provide a means to maintain software asset inventory and prevent the loading of unauthorised software. B/Ds should choose the best SAM tool that fits their own IT environment. Alternatively, B/Ds may engage a service provider to implement SAM measures, conduct software audits, as well as install SAM tools.

14.7 IT Security Threat Management

(a) Threat Management Mechanism

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. The mechanism shall at least cover the regular monitoring of log records for information systems (e.g. servers, VPN gateways, firewalls) and a prompt response plan to IT security threats that are detected by the related security installations in the B/Ds (e.g. anti-malware systems, intrusion detection systems, endpoint detection and response (EDR) solutions, etc.).

(b) Threat Identification and Intelligence Gathering

Threat intelligence is the threat related information that is collected and analysed for reducing harm to information systems caused by threats. Threat intelligence can be operational details about specific attacks, information on attacker tactics (e.g. methodologies, tools), and strategic information on the changing threat landscape (e.g. types of attacks and attackers).

B/Ds shall be well aware of the emerging security threats and associated risks that are relevant to their business and daily operation by subscribing to security news, alerts, reports and other information security publications. GovCERT.HK is one of the sources to disseminate security alerts on impending and actual threats to B/Ds. B/Ds can also obtain threat information (e.g. malicious IP addresses and domains) in threat intelligence platforms.

B/Ds should consider establishing a mechanism to acquire threat intelligence, by collecting threat related information from different sources (e.g. GovCERT.HK) and analysing its significance to the B/Ds, and communicate the acquired threat intelligence to relevant parties within their B/Ds.

(c) Threat Monitoring and Detection

Once potential threats have been identified, continuous detection and monitoring on information systems becomes paramount. Regular checking on log records, especially on system/application where classified information is processed/stored, shall be performed according to the defined checking frequency, not only on the completeness but also the integrity of the log records. Any irregularities or system/application errors which are suspected to be triggered as a result of security breaches shall be logged and reported. Detailed investigation should be carried out if necessary.

Log records should also be correlated across different repositories to identify potential security incidents and operational and security issues. In addition to the application log, network device and server system logs (e.g. firewall logs, web access logs, system event logs) shall also be reviewed regularly to detect anomalies, including those attacks / intrusions on system software or web applications targeting on end users. All unauthorised accesses to an information system should be

reported, and the security violation report should be checked, preferably on a daily basis. It is also important to establish tight change control procedures for system software for detecting unauthorised usage.

Most operating systems have log files. Examination of these log files on a regular basis is often the first line of defence in detecting unauthorised use of the system. The following serves as some clues for identifying unauthorised access:

- Most users typically log in and out at roughly the same time each day. An account logged in outside the "normal" time for the account may be in use by an intruder.
- Accounting records, if any, can also be used to determine usage patterns for the system; unusual accounting records may indicate unauthorised use of the system.
- System logging facilities should be checked for unusual error messages from system software. For example, a large number of failed login attempts in a short period of time may indicate someone trying to guess passwords.
- Operating system commands that list currently executing processes can be used to detect users running programs they are not authorised to use, as well as to detect unauthorised programs which have been started by an intruder.

Other monitoring tools would be constructed using standard operating system software by using several, often unrelated, programs together. For example, checklists of file ownership and permission settings can be constructed and stored off-line. These lists can then be reconstructed periodically and compared against the master checklist. Differences may indicate that unauthorised modifications have been made to the system.

A host-based intrusion detection system (IDS) or intrusion prevention system (IPS) analyses several areas to determine misuse (malicious or abusive activity inside the network) or intrusion (breaches from the outside). Host-based IDS/IPS consult several types of log files (kernel, system, server, network, firewall, and more) and compare the logs against an internal database of common signatures for known attacks. Host-based IDS/IPS can also verify the data integrity of important files and executables. The IDS/IPS will check a database of classified files pre-selected by the user and create a checksum of each file with a message-file digest utility such as sha2sum. The IDS/IPS then stores the sums in a plain text file and periodically compares the file checksums against the values in the text file. If any of the file checksums do not match, then the IDS/IPS will alert the administrator by email, phone call, Short Message Service (SMS), or pager.

Other tools would also be available from external vendors and public software distribution sites. B/Ds should select suitable security monitoring and detection tools based on their objectives and specific requirements.

B/Ds shall deploy EDR solutions in all servers, workstations, and mobile devices where technically feasible to provide real-time identification of unusual or suspicious activities and give early warnings for potential security incidents. EDR solutions help detect and respond to threats in real time, reducing the potential

impact of security incidents. In addition, EDR solutions focus on the individual devices within the network (e.g. endpoints) and provide deep visibility into every action taken while monitor traffic to identify suspicious patterns and anomalies. B/Ds may also consider Network detection and response (NDR) solutions which can continuously monitor network traffic for signs of security incidents.

(d) Continuous Improvement and Adaptation

B/Ds should conduct regular evaluations and updates to their threat detection and monitoring process based on lessons learnt from security incidents and changes in the risk landscape. B/Ds should also leverage the vulnerability identification activities commonly used in the vulnerability management process, including vulnerability scanning, penetration testing, and simulated attacks, to verify B/Ds' ability to detect and respond to a realistic attack and integrate this as part of their continuous improvement and adaptation strategy. Please refer to Section 14.6 for more information about the vulnerability identification activities.

For more information about IT security threat management, please refer to the following document for details:

- **Practice Guide for IT Security Threat Management**
  Available at ITG InfoStation.
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

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

(a) General Network Protection

With networked or distributed applications, the security of multiple systems and the security of the interconnecting network are equally important, especially if public access wide area networks are used.

The risks of connecting to outside networks shall be weighed against the benefits. It may be desirable to limit connection to outside networks to those hosts that do not store sensitive material and keep vital machines isolated.

Some network protection guidelines are provided below:

- Keep the network simple (i.e. minimise the number of network interface points between the "secured" network and other networks).
- Allow only authorised traffic to enter the "secured" network.
- Use multiple mechanisms to authenticate the user (e.g. password system plus pre-registered IP address and/or pre-registered MAC address).
- Encrypt data with a proven encryption algorithm before transmitting over the network.

Up-to-date system or network information, in particular, the network diagrams, internal network addresses, and configurations, shall be maintained to reflect the latest network environment for effective security control. Such information shall be appropriately classified and securely stored. Disclosure of such information to unauthorised parties may lead to security breaches, and thus, it shall only be disclosed to users or parties on a need-to-know basis with proper records maintained. B/Ds shall ensure that such information will not be publicly released without prior approval.

(b) Network Security Controls

Users shall never connect unauthorised computer resources, including those privately-owned and those owned by external service providers, to the government internal network unless approved by the DITSO for operational necessities. B/Ds shall ensure that such usage of computer resources which have been approved by DITSOs conforms to the same IT security requirements.

If there is a need to participate in a wide area network, consider restricting all access to the local network through a dedicated gateway. That is, all access to or from the local network shall be made through a dedicated gateway that acts as a firewall

between the local network and the outside world. This system shall be rigorously controlled and password protected, and it should be configured to allow only legitimate network traffic from external users to the networks protected by it. The compromise of the firewall could result in compromise of the network behind it.

In addition, a two-tier firewall architecture should be considered to further protect information systems. In this architecture, two firewalls are used – an external firewall and an internal firewall. The external firewall protects a demilitarized zone (DMZ) from the Internet, and the internal firewall further protects the internal networks. In this design, even if external users compromise the servers in the DMZ, the internal firewall can still protect the servers/workstations in the internal networks.

Other than the firewall system, considerations should also include encryption algorithms for passwords sent across networks and a secure process identification system so that applications dispersed throughout a network can know "who" they are talking to.

B/Ds shall implement an intrusion detection strategy to detect abnormal activities on the network by installing a network intrusion detection system (NIDS) or network intrusion prevention system (NIPS) at critical nodes of the network. An IDS monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack). An alert will be sent to the IT administrator once an attack is detected by the IDS such that the system downtime and potential service impact can be minimised. IPS performs similar functions as IDS, but in addition, it provides a proactive response to stop the source of attacks or to minimise the impact of the attacks. Configuration of IDS and IPS requires tuning of signature and recognition patterns to reduce false alarms.

B/Ds have the overall responsibility to protect data, information systems and networks. B/Ds shall ensure that the information/communication systems are properly configured and securely managed, including turning off all unused services and setting security configurations properly. The configurations shall be reviewed regularly and updated if necessary. B/Ds should also acquire security software (e.g. firewall, malware detection and repair software, etc.) for enterprise management. Enterprise management means that the software uses a centralised management console to manage all agents (of the security software) in the organisation. It usually provides features like remote updates, policy enforcement, status queries, report generation, security functions, etc. It can save deployment time of policy / signatures / updates, enforce a standardised organisational security policy, assist in compliance assessment, and save the effort of LAN/system administrators and IT security administrators.

B/Ds shall divide their networks into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain). The segregation can be done by physical means or logical means (e.g. virtual private networking). Moreover, cross-network connectivity should only be provided on a need basis.

The perimeter of each domain shall be well defined. Access between network domains is allowed but should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for the segregation of networks into domains and the access allowed through the gateways should be based on an assessment of the security requirements of each domain. The assessment should be made in accordance with Section 11, "Access Control" on access requirements, value and classification of information processed and should also take account of the relative cost and performance impact of incorporating suitable gateway technology.

Mobile devices often possess network connection capabilities. For these devices connecting to the government internal networks without proper protective measures, they can become a point to breach security, such as disclosure of classified information and spreading malware into the government internal network or attacking devices controlled by malware. Users shall not connect their workstations or mobile devices to the external network if these workstations or mobile devices are simultaneously connected to a government internal network, unless with the approval from the DITSO.

Administrative consoles and management interfaces of information systems shall not be accessed directly from the Internet where technically feasible.

For access to classified information via wireless communications, consideration should be made to treat all wireless access as un-trusted connections. Thus, access to internal systems via wireless communications shall be granted only through a designated gateway (e.g. VPN gateway) with proper authentication, encryption, user level network access control and logging implemented.

(c) Communications with other networks

Connections made to other networks shall not compromise the security of information processed at another, and vice versa. The B/D shall communicate with other B/D or external parties on the security requirements before the network connection is established. 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. The security requirements should be based on the principle that stronger security protection is adopted on both sides if the security protection level of the two parties is different.

Some B/Ds may enforce stronger security requirements than others (e.g. client-side program configuration/settings, network transmission requirements, user identification and authentication, session handling, transaction integrity, etc.). There will be cases where the security requirements of two B/Ds are different, but they need to inter-communicate with each other. The following principles should be observed if there are security requirement discrepancies in inter-departmental communication:

- The security requirements of an information system provider are STRONGER than the security requirements of users from other B/Ds

  Under this scenario, the security requirements of the information system provider should dominate, with the fact that the B/D as the information system provider has legitimate business concerns to raise its security requirements. Users of other B/Ds will need to follow.

- The security requirements of an information system provider are WEAKER than the security requirements of users from other B/Ds

  Under this scenario, the information system provider should perform a security risk assessment to determine if it needs to refine its security requirements. If the outcome is that there is no need to change its security requirements, B/D of the information system provider should reconcile with users of other B/Ds with higher security requirements to either devise alternative access channels for their access or request these users to accommodate laxer security requirements.

  If the outcome is that B/D of the information system provider needs to strengthen its security requirements, additional security controls should be implemented accordingly. After strengthening its security requirements, if there are still users of other B/Ds having higher security requirements, B/D of the information system provider should reconcile with these users to either devise alternative access channels for their access or request these users to accommodate its laxer security requirements.

When a B/D implements an information system for users of other B/Ds to use, the B/D should treat the incoming requests as coming from un-trusted networks. Sufficient security controls should be implemented according to the application-specific requirement. Additional measures to ensure proper user behaviour should also be implemented (e.g. auto session timeout) instead of assuming users of other B/Ds will behave and follow their own IT security policy.

(d) Wireless Communication

Wireless communication involves the transmission of information over a distance without connecting wires, cables or any other forms of electrical conductors. Wireless communication is used in devices such as cordless telephones, mobile phones, GPS units and wireless computers. Wireless Local Area Network (WLAN) is a common wireless communication technology used in the Government. It is a type of local area network that uses high-frequency radio waves rather than wires to communicate between devices. WLAN is a flexible data communication system used as an alternative to or an extension of a wired LAN. Wireless information communication has enabled people to interact more easily and freely. With the advent of technology and advances in price/performance, wireless accessibility is increasingly deployed in the office or in public places.

WLAN is based on the IEEE 802.11 standard. Different standards, such as 802.11a, 802.11b, 802.11g and 802.11n, have evolved, supporting different frequency spectrums and bandwidths.

There are two related IEEE standards - 802.1X and 802.11i. The 802.1X, a port-based network access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard was created for wireless-specific security functions that operate with IEEE 802.1X.

Wireless communications with connection to the government internal network shall be used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.

(e) Threats and Vulnerabilities of Wireless Local Area Network

One characteristic of a wireless signal is that it generally fills the air within the WLAN's coverage and can penetrate beyond building walls and windows. Thus, there is a potential security risk that anyone can pick up and read such signals unless security measures have been incorporated to guard the wireless transmissions against offensive "listening". In fact, the risks in WLAN are equal to the sum of the risks of operating a wired network plus the new risks introduced by weaknesses in wireless protocols. The following are some of the risks associated with WLAN:

- Malicious entities may gain unauthorised access to the government internal network through wireless connections, potentially bypassing firewall protections and launching attacks.
- Computer malware may corrupt data on a wireless device and be subsequently introduced to a wired network.
- Malicious entities may deploy unauthorised equipment (e.g. client devices and access points) to surreptitiously gain access to or modify information.
- Classified information that is not encrypted (or that is encrypted with poor cryptographic techniques) and transmitted among wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- A fake wireless access point may be established to collect the information travelling across the WLAN.

WLAN technology has been continually evolving. B/D shall review their Wi-Fi infrastructure to assess the impact of the vulnerability found in Wi-Fi communication standards and protocols periodically. Protection by a stronger wireless security protocol such as Wi-Fi Protected Access 3 (WPA3) should be considered, but by no means should such wireless security protocol be solely relied upon to protect data confidentiality and integrity, as new weaknesses of these protocols may be discovered in the future. B/Ds should deploy Virtual Private Network (VPN) on top of WLANs if classified data is to be communicated over WLANs.

(f) Security Controls to Protect Wireless Local Area Network

B/Ds are reminded to not just rely on technical security measures to safeguard their WLANs but also adopt proper management controls to effectively protect their WLANs. The following are some management and technical security controls for consideration:

Management Controls

- Define a wireless security policy to address the usage of WLAN and the type of information that can be transmitted over WLAN.
- Develop and securely keep a coverage map of the WLAN, including locations of respective access points and SSID information, so as to avoid excessive coverage by the wireless signal.
- Ensure the hardware and software are properly patched.
- Search regularly for rogue or unauthorised wireless access points.
- Perform regular IT security risk assessments and audits to identify security vulnerabilities.
- Keep a good inventory of all devices with a wireless interface. Once a device is reported missing, consider modifying the encryption keys and SSID.
- Implement strong physical security controls and user authentication to complement the physical security deficiencies of wireless devices.
- Install access points far from a window or a door to prevent network tapping from publicly accessible areas.

Technical Controls

- Change network default name at installation; SSID should not reflect the name of any B/Ds, system name or product name/model.
- Change product default access point configuration settings, which are considered unsecured most of the time, for easy deployment.
- Disable all insecure and unused management protocols on access points and configure the required management protocols with the least privilege.
- Ensure that all access points have strong, unique administration passwords and change the passwords regularly.
- Enable and configure security settings, including SSID, encryption keys, and Simple Network Management Protocol (SNMP) community strings.
- Disable SSID broadcasting to prevent the access points from broadcasting the SSID so that only authorised users whose configured SSID matches that of the access point can connect to the network.
- Disable DHCP and assign static IP addresses to all wireless users to minimise the possibility of an unauthorised user obtaining a valid IP address.
- Use MAC address filtering for configuring access points so that they allow only clients with specific MAC addresses to access the network or allow access to only a given set of MAC addresses.
- Do not directly connect WLAN and wired networks. Install a firewall or router with access control lists (ACLs) between the access point and the B/D's network to filter connections.

- Enable threshold parameters, such as inactivity timeouts.
- Activate logging features and redirect all log entries to a remote logging server if possible. The log records should be checked regularly.
- Install a wireless intrusion detection system (WIDS) or wireless intrusion prevention system (WIPS) to monitor the WLAN.
- Deploy VPN on top of WLAN for connection to departmental network.
- Use client-side digital certificates for mobile devices with limited Wi-Fi defences so only authorised devices are allowed to access departmental networks or resources.
- Segment the access point's coverage areas to balance the loading and minimise the probability/impact of a Denial-of-Service (DoS) attack.
- Erase all sensitive information, such as system configurations, pre-shared keys, digital certificates and passwords, on the devices upon disposal of wireless components.
- Disable Universal Plug and Play (uPnP) on access points to prevent malware from bypassing the firewall via the connected devices.

End-user Controls

- Install a firewall on wireless clients (e.g. mobile devices).
- Turn off sharing or tethering at wireless clients.
- Don't attach the wireless clients to the departmental network while it is connected to a third party WLAN.
- Connect to departmental network resources using a VPN.
- Keep strict control of the wireless interface device (e.g. USB token for laptop) as access credentials such as SSID and/or encryption key are commonly stored on the card.
- Only enable wireless connections when users need them; disable them when they are no longer in use.
- Follow the guidelines in Section 14.2, Protection from Malware and Section 4, Mobile Device Security of the Practice Guide for Mobile Security.

(g) Transmission over Wireless Communication

WLAN is generally considered an un-trusted network and shall not be used to transmit classified information without proper security controls. Network traffic between the WLAN and the internal trusted network shall be encrypted and authenticated. The adoption of VPN is a viable option to achieve this kind of end-to-end security.

The following table summarises the applicability of wireless communication with respect to the transmission of various categories of information.

Category of Information	Applicability of Using Wireless Communication for Transmission
Higher than CONFIDENTIAL	Not allowed
CONFIDENTIAL	Allowed, provided that it is transmitted using a designated device with approval of Head of B/D, there are sufficient authentication and transmission encryption security controls and that it has attained the level of encryption required for CONFIDENTIAL information. VPN should be used to provide strong authentication and encryption tunnel over WLAN connection. In addition, proper key management and configuration policies should also be established to complement the technical solution. Wireless keyboards do not necessitate approval from the Head of B/D if they can meet the industry security standards for authentication and encryption, and the compliance is confirmed by the DITSO.
RESTRICTED	Allowed, provided that there are sufficient authentication and transmission encryption security controls and have attained the level of encryption required for RESTRICTED information. Recommend to adopt the same level of encryption required for CONFIDENTIAL information, and with proper key management and configuration policies similar to those for CONFIDENTIAL information.
Unclassified	Allowed. Following the principle that only authorised parties are permitted to access the network where information is stored, wireless communication with sufficient authentication and transmission encryption measures where appropriate is considered suitable for use by B/Ds. Similar to that for CONFIDENTIAL and RESTRICTED information, proper key management and configuration policies should also be established to complement the technical solution.

(h) Internet Security

The Internet is a world-wide "network of networks" that often uses the TCP/IP protocol suite for communication. Internet connectivity offers enormous benefits in terms of increased access to information. However, the Internet suffers from significant and widespread security problems.

The fundamental problem is that the Internet was not designed to be very secure. A number of TCP/IP services are vulnerable to security threats such as eavesdropping and spoofing. Electronic messages, passwords, and file transfers can be monitored and captured using readily available software.

Internet services need stronger authentication and cryptography mechanisms, and these mechanisms shall be truly interoperable. To enforce the authenticity of government Internet resources, the resource records of the government Internet domains shall be protected by prevailing security controls, i.e. Domain Name System Security Extensions (DNSSEC). Similarly, for Internet mail services, all government Internet mails to the public shall be protected by prevailing email authenticity standards, including Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) or Domain-based Message Authentication, Reporting & Conformance (DMARC) protocol. Moreover, encrypted transmission, e.g. HyperText Transfer Protocol Secure (HTTPS), shall be implemented for all Internet services, including informational websites, so as to strengthen the authenticity of the government Internet services and also the content integrity. Internet information enquiry or transaction processing requires user authentication. One-time password and multi-factor authentication may be required for secure access. Audit and backup of authentication information may be required.

In general, Internet security covers a wide range of issues such as identification and authentication, malware protection, software licensing, remote access, dial-up access, physical security, firewall implementation and other aspects relating to the use of the Internet.

Therefore, B/Ds should promote staff awareness of information security through regular and ad hoc training, with emphasis on the proper use of Internet services. All staff members shall be aware that the improper use of the Internet can bring security risks that may be harmful to government IT infrastructure and/or adversely affect the government reputation. Also, all staff members in B/Ds should understand the obligations and responsibilities when using the Internet services provided by the Government and should strictly follow the terms of usage of the Internet services provided.

The use of personal webmail, public cloud storage and web-version of instant messaging services introduces significant security risks, including the potential for unauthorised disclosure of sensitive information and data breaches during transmission. Therefore, B/Ds shall critically review the necessity of access to these services by users regularly. Access shall be granted only when justified by genuine needs and legitimate purposes with the approval from the Heads of B/Ds or their explicitly delegated officer at directorate level, and promptly revoked when no longer required. B/Ds should employ technical controls, such as web content filtering, to prevent unauthorised access to personal webmail, public cloud storage and web-version of instant messaging services.

Subscribing to online services with government email addresses together with passwords that are used in government information systems may allow attackers to gain access to the systems if the subscription services are compromised. Other information provided in the subscription may also be leaked and leveraged for phishing activities and cyber attacks. While there may be genuine needs for subscribing to online services, B/Ds should consistently remind users about the associated risks and promote the adoption of security best practices, such as using strong and unique passwords, exercising caution when handling personal information, enabling multi-factor authentication if available, maintaining a constant

state of vigilance against phishing attempts, and using email alias for online service subscriptions.

(i) Gateway-level Protection

Any B/D that supports Internet facilities shall protect its information and information resources from unauthorised access or public break-ins. All Internet access from the departmental network shall be made through centrally arranged Internet gateways or B/D's own Internet gateway. The gateway can provide both security and authentication protection by means of screening routers, firewalls or other communication facilities. The Internet gateway should deny all Internet services unless specifically enabled. All unused configurations, services, ports and unnecessary traffic, e.g. unnecessary daytime service, incoming or outgoing ICMP traffic, etc., should also be disabled or blocked. A direct dial-up connection to an Internet services provider should not be established. For technical guidelines on Internet gateway security, please refer to the following document for details:

- Practice Guide for Internet Gateway Security
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

If a B/D decides to install broadband connections on standalone (i.e. not connected to the government or departmental network) computers without going through centrally arranged Internet gateways or B/D's own Internet gateway, sufficient security controls such as firewall, anti-malware program, and user permission restriction shall be implemented on these computers to avoid potential security breaches and system misuse. An approval and control mechanism at the appropriate level shall also be in place. Computers that can simultaneously access a broadband Internet connection and an internal network poses great risk to the government network and shall be strictly prohibited except with proper security safeguard and approval from the DITSO.

To reduce the risks of users' access to phishing websites or websites that contain malicious content, B/Ds shall block users' access to any IP address or websites that are known or suspected to be malicious.

(j) Client-level Protection

Personal firewalls are effective measures to protect user's workstations from unauthorised network traffic, which can be network worms or other forms of malware attacks. A personal firewall resides on the user's workstation and provides firewall services between the workstation and the network. A personal firewall controls network traffic by asking for the user's authorisation before allowing the network traffic to enter into or leave the user's workstation. Some even provide application-level protection that ensures only authorised processes will run on the user's workstation.

LAN/System administrators shall install personal firewalls on computers that may directly connect to un-trusted networks like the Internet or third-party networks.

Most personal firewalls can act in either stand-alone configuration or in agent configuration, where the personal firewall policy can be centrally managed and enforced.

Besides considering personal firewall protection, web browsers running on the user's workstation should be properly configured. As web browsers are the primary interface with the Internet, poorly configured web browsers can allow malware to be downloaded onto user's workstations. B/Ds can refer to the following guidelines when configuring web browsers:

- Disable any active content options, e.g. Java, JavaScript and ActiveX, in the electronic message application or browser, except when communicating with a trusted source.
- Use up-to-date browser versions and apply the latest security patches.
- Disable password auto-complete or password remembering feature.
- Enable pop-up blocking feature, except when communicating with trusted sites.
- Remove regularly cache files or temporary files of the browsers to protect data privacy.
- Disable automatic installation of plug-ins, add-ons or software.

User education and awareness training are also important to alert users to the importance of using properly configured web browsers.

15.2 Information Transfer

(a) Transmission of Classified Information

Information classified as higher than CONFIDENTIAL shall be transmitted only when encrypted and inside an isolated wired LAN approved by the Government Security Officer with the technical endorsement of DPO. An isolated LAN refers to a local area network in a single controlled environment that has no connection with other network, including connection to other government networks, Internet connection, and remote access.

Transmission of CONFIDENTIAL/RESTRICTED information should be encrypted to protect the information during transmission in any communication network. CONFIDENTIAL/RESTRICTED information shall be encrypted when transmitted over an un-trusted communication network. Examples of un-trusted communication networks include:

- Internet.
- Network that uses a public telecommunication line (e.g. leased line, dial-up connection).
- Wireless communication.
- Metro Ethernet.

To be considered as a trusted communication network, the network should be:

- Protected within a physically secured area to prevent the data passing through the network from being accessed, modified or deleted by an unauthorised person.
- Secured well from unauthorised tampering, for example, through locking of network equipment and protection of LAN ports.
- Equipped with a well-defined IT security policy to control the proper configuration and administration of network equipment and settings.

Networks that do not fall under the definition of trusted communication networks are considered as un-trusted communication networks. In general, the transmission of information over any communication network could be exposed to security risks because a malicious attacker may capture classified information and even break into the government network by exploiting vulnerabilities of the communication networks. B/Ds should conduct a security risk assessment to ascertain the trustworthiness of the communication network in use and identify the associated risks. B/Ds should consider implementing encryption at the data, application or network level to minimise the risks of unauthorised access.

(b) Electronic Messaging Security

Electronic messaging (e.g. email, instant messaging) is a key enabling technology for internal and external communication. For internal users, there are various mailing products running on the government internal network. A formal request shall be made to apply for an email account. Authentication, encryption and digital signature services should be available for email over the Internet as well as email on internal networks. The electronic messaging containing classified information shall be encrypted during transmission or storage.

Use of public email should be restricted unless it is unavoidable due to business needs. Email transmission of classified information shall be transmitted only on an information system approved by the Government Security Officer. For internal communication, the Confidential Mail System (CMS), the Confidential Messaging Application (CMSG), the Mobile Confidential Mail Service (MCMS), and approved sub-systems of Centrally Managed Messaging Platform (CMMP) are designated email systems in the Government to facilitate the exchange of email messages and documents with CONFIDENTIAL classification within the government network. The exchange of email over the Internet, whether signed or encrypted, shall not be assumed to be of equivalent security status as the CMS or CMMP. This is because the Internet's electronic messaging services may not fulfil the government security requirements for handling CONFIDENTIAL information. For relevant configuration and operation procedures on CMS and CMMP, please refer to the documents posted on the government intranet CCGO website at http://cms.host.ccgo.hksarg/ and https://itginfo.ccgo.hksarg/content/cmmp respectively.

(c) Email Server and Client Security

Email servers and clients should be properly configured before connecting to the Internet. Standard SMTP mail provides no integrity checking. Internet email

addresses are easily spoofed. There is usually no guarantee of delivery with Internet mail. If technically and operationally feasible, information revealing the specific details of internal systems or configurations should be avoided in email headers to avoid the disclosure of system information to external parties.

B/Ds may consider enabling audit trails for any access to email to keep a record of each trial of reading or updating by authorised users and for those unauthorised ones. A systematic process for recording, retention, and destruction of electronic messages, as well as accompanying logs, shall be established and clearly documented. Alert reports or alarms should be used to report security incidents. In addition, the user email address list shall be properly maintained by authorised administrators and protected from unauthorised access or modification.

To enhance the security of the government email system, user authentication, such as passwords, shall be used for workstations and email accounts to prevent unauthorised access and use.

Email clients should not automatically process attachments, as an attachment may contain hostile scripts or malware. Please refer to Section 15.1(j) - Client-level Protection for details.

LAN/System administrator should arrange automatic updating of malware definition for users who use the government email system. Users should make sure that the auto-protection of the anti-malware in their workstation is always enabled whenever they use the system to access any document or information. Please refer to Section 14.2 – Protection from Malware for details.

Users should safeguard and change their passwords regularly. Users should not open or forward any email from unknown or suspicious sources. If users suspect or discover an email containing malware or suspicious content, they should report the incident to the management and LAN/System Administrator immediately and follow the corresponding incident response plan. User should also verify the identity of the email sender through alternate channels if in doubt (e.g. by phone).

In addition, users should not auto-forward official emails to external email systems unless the security of the email system can be assured. There is a possibility that some emails with classified content may also be automatically forwarded. If those emails with classified content are not encrypted but auto-forwarded, it may violate the government security requirements for transmission of classified information. Email systems that are not under the direct control of the Government pose additional security risks for the stored information.

For more details on email management and email security in the government email system, please refer to the following document:

- **Practice Guide on the Use of Electronic Mail (email)**
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp)

(d) Communication with External Parties

Network communication with external parties, such as non-government organisations (NGO), government related organisations, outsourcers or external service providers, should be treated as un-trusted. B/Ds should follow relevant IT security policy when connecting to or exchanging information over communication networks with external parties. Sufficient security controls should be implemented according to the application specific requirement.

Information shall be passed to external parties only on a "need to know" basis. B/Ds shall ensure that arrangements for the protection of classified information comply as far as possible with the standards adopted within the Government.

Agreement on the secure transfer of classified information between a B/D and an external party shall be established and documented. Information transfer agreements with external parties should include at least the following:

- Obligation not to disclose the classified information to third parties or indemnity with the Government as appropriate.
- Measures to protect classified information, such as cryptography and access control, from unauthorised access.
- Responsibilities and liabilities in the event of information security incidents, such as data leakage.
- Technical standards for recording or reading the classified information.

Policies, procedures and standards should be established and maintained to protect information and physical media in transit, and should be referenced in the information transfer agreements.

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

(a) Security by Design

The concept of security by design is important for identifying potential risks for the application system and taking appropriate remediation before development / acquisition. Good application design not only provides workable solutions to users' problems but also provides a secure environment for them to work in. Security and privacy should be introduced early and throughout all phases of the development process. The security facilities provided by the operating system should be utilised. Other than that, the application itself should build in additional security measures, depending on the vulnerability and criticality of the system and the sensitivity of the data it is dealing with.

The security shift-left approach integrates security considerations early and throughout the SDLC to ensure necessary security requirements are duly identified and incorporated. B/Ds should consider implementing a security shift-left approach, including adopting of secure coding practices and conducting security reviews for their information systems in the system design stage.

B/Ds shall determine the classifications of information systems during the project initiation stage and should define IT security requirements in the system design stage for new information systems or enhancements to existing information systems. If security requirements are defined properly and identified risks are addressed in the early stage, the rework effort is expected to be immensely reduced. B/Ds should conduct a security review in the design stage of an information system, which serves as a checkpoint to ensure necessary security requirements are identified and incorporated in the system design stage or other phases appropriately.

The review should assess the security requirements based on the business needs, legal and regulatory requirements (e.g. the Personal Data (Privacy) Ordinance) and government security requirements, and review the system design by identifying possible compliance issues as well as security risks with reference to the security considerations in application design and development. After performing the review, the identified risks and recommendations should be documented and addressed in the design stage or other phases appropriately. The review should include a role in the development team for assessing security risks, proposing potential security-related issues, and performing security reviews of the system design and programming code. The pre-production Security Risk Assessment should verify the completion of follow-up actions for the security review and the programming code

review to ensure necessary security measures and controls are implemented in the system properly before production rollout.

For more information about security by design, please refer to the following document for details:

- **Practice Guide for Security by Design**
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

(b) System Specification and Design Control

In the system specification and design phase, checking should be performed to:

(i) Ensure that the system designed complies with acceptable accounting policies, accounting and application controls to enforce adequate authentication, authorisation and accountability, and with all appropriate legislative measures.

(ii) Ensure a threat model is built, and threat mitigations are present in all design and functional specifications. A minimal threat model can be built by analysing high-risk entry points and data in the application.

(iii) Review the system design with the user to check out if there are any loopholes in maintaining the integrity of information. The user should be encouraged to suggest corrective measures for any deficiency detected.

(iv) Evaluate with the users how they will be affected if there is a loss to the data processing capability. A contingency plan should be formulated following the evaluation. For details on developing a contingency plan, please refer to Section 19.1(a) - Contingency Management.

(v) Evaluate with the Information Owner about the sensitivity of their data. Information to be discussed includes:
- Level of security to be achieved
- Origin of the source of data
- Data fields that each grade of staff in the user department is allowed to access
- The way that each grade of staff in the user department is allowed to manipulate the data in the computer files
- Level of audibility required
- Amount of data to be maintained and the purpose of maintaining it in the information system
- Data files that need to be backed up
- Number of copies of backup to be maintained
- Frequency of backup and archive

(vi) Conduct a Privacy Impact Assessment to examine the adequacy, effectiveness and practicability of the planned protection measures for the protection of personal data for systems having potential privacy implications. PCPD has

published an information leaflet on privacy impact assessment, which is available on PCPD's website.

(https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf)

The user requirements may be assembled into some form of security statement. The user's security statement should then form part of the system's functional specification and be reflected in the system design.

Agile development methodologies are gaining acceptance in the software industry. However, due to its characteristics, mismatches between agile methodologies and conventional methods for security assurance are quite obvious. There are some suggestions to adapt security assurance to fit agile software development:

(i) Document the security architecture.
(ii) Include a role in the development team for assessing security risks, proposing potential security-related issues, and performing security reviews of the system design and programming code.
(iii) Document security related programming activities.
(iv) Conduct code review, if necessary.

(c) Security Considerations in Application Design and Development

Listed below are some security principles which should be observed when designing and developing applications:

- ***Secure architecture, design and structure.*** Ensure that security issues are incorporated as part of the basic architectural design. Detailed designs for possible security issues should be reviewed, and mitigations for all possible threats should be designed and developed. In relation to personal data protection, B/Ds shall further refer to the mandatory requirements as specified in Data Protection Principles[6] of the Personal Data (Privacy) Ordinance.
- ***Least privilege.*** Ensure that applications are designed to run with the least amount of system privileges necessary to perform their tasks.
- ***Segregation of duties.*** Ensure that the practice of segregation of duties is followed in such a way that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process.
- ***Need to know.*** The access rights given for system documentation and listings of applications shall be kept to a minimum and authorised by the application owner.
- ***Secure the weakest link.*** Ensure that proper security protections are in place in all areas to prevent attackers from penetrating through loopholes caused by

[6] https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

negligence in coding since applications and systems are only as secure as the weakest link.

- ***Proper authentication and authorisation.*** Ensure that proper access control is implemented to enforce the privileges and access rights of the users. The use of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) should be considered for public web services providing controls for input submission.
- ***Proper session management.*** Ensure that applications have proper and secure session management to protect the sessions from unauthorised access, modification or hijacking. Protection measures include generating unpredictable session identifiers, securing the communication channel, limiting the session lifetime, encrypting sensitive session contents, applying appropriate logout function and idle session timeout, and filtering invalid sessions.
- ***Input validation.*** Ensure that strict validation is applied to all input of the application whenever the source is outside the trust boundary such that any unexpected input, e.g. overly long input, incorrect data type, unexpected negative values or date range, unexpected characters such as those used by the application for bounding character string input etc., are handled properly and would not become a means for an attack against the application.
- ***Proper error handling.*** Ensure that the application will provide a meaningful error message that is helpful to the user or the support staff while ensuring that no classified information will be disclosed. Ensure that errors are detected, reported, and handled properly.
- ***Fail securely.*** Ensure that security mechanisms are designed to reject further code execution if application failure occurs.
- ***Proper configuration management.*** Ensure that the application and system are properly and securely configured, including turning off all unused services and setting security configurations properly.
- ***Remove unnecessary items.*** Ensure that unused or less commonly used services, protocols, ports, and functions are disabled to reduce the surface area of attack. Unnecessary content such as platform information in server banners, help databases and online software manuals, and default or sample files should also be removed from production servers to avoid unnecessary disclosure of system information.
- ***Data confidentiality.*** Ensure that the classified data is encrypted in storage or during transmission. Mask the classified information when being displayed, printed or used for testing, where applicable.
- ***Data authenticity and integrity.*** Ensure that the authenticity and integrity of data are maintained during information exchange.
- ***Secure in deployment.*** Ensure a prescriptive deployment guide is ready outlining how to deploy each feature of an application securely.

  Log management. Maintain audit trails for important events, such as critical operation or processing of sensitive information, for routine control or investigation purposes; tampering with or changes to any audit trails should be prohibited; management attention should be drawn to exceptional circumstances.

(d) Programming Standard Establishment

The programming controls to be enforced shall achieve at least the following purposes:

- To ensure that the program conforms to the program specification and includes no undocumented features outside its functions.
- To ensure the program adheres to the necessary programming standards.
- To prevent and detect fraud.

A programming standard should be established to facilitate the development and maintenance of programs. Having established such a standard, the next important thing is to ensure that it is adhered to.

(e) Division of Labour

For risky and sensitive systems, it may be necessary to divide those programs dealing with very sensitive information into units of modules and segments. Assign the modules and segments to several programmers. This is to serve two main purposes:

- Separation of programming responsibilities makes it more difficult for the dishonest programmer to incur program faults in the system because he does not have control over the other units of the program. He has to work in collusion with others in order to be successful.
- The division of programs into smaller units also increases the opportunity for detecting programming fraud. The units can be analysed and reviewed in much greater detail.

(f) Program/System Testing

Firstly, the user department should carry out a user acceptance test in which they are responsible for preparing the test plan and test data. The user department should also examine all outputs in detail to ensure that expected results are produced. If error messages are encountered, they should be able to understand the messages and take corresponding actions to correct them.

The test plan should cover the following cases:

- Valid and invalid combinations of data and cases.
- Data and cases that violate the editing and control rules.
- Cases for testing the rounding, truncation and overflow resulted from arithmetic operations.
- Cases for testing unexpected input, e.g. overly long input, incorrect data type, unexpected negative values or date range, unexpected characters such as those used by the application for bounding character string input, etc.

Besides the user acceptance test, there are other tests that are useful to validate the correctness of system functionalities. Unit test is the testing of an individual program or module to ensure that the internal operation of a program performs according to specification. An interface test is a hardware or software test that evaluates the connection of two or more components that pass information from one to another. System test is a series of tests designed to ensure that the modified program interacts correctly with other system components. A stress test or load test is used to determine the stability of a given system by loading the system beyond its normal operational capacity in order to observe the results. A regression test is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. Each test record should be documented, stating the content of the record and its purpose during testing. The documentation for the transaction file should also contain a section on the expected results after the application of the transactions, which are then used for system testing. Whenever the system is changed, the same files are used for rerunning, and the two sets of outputs are compared. The amendment would only be accepted if no discrepancy is identified.

The information systems supporting large-scale public-facing digital services selected by DPO are subject to additional tests as stipulated in OGCIO Circular No. 5/2023 – Strengthening the Preparation for the Rollout of IT Systems with Large-Scale Public-Facing Services. Furthermore, the “Specified IT Systems” of B/Ds are also subject to additional tests by independent third-parties prior to their rollout as stipulated in the General Circular No. 6/2024 – Strengthening the Governance and the Security of IT Systems.

16.2 Security in Development and Support Processes

(a) Secure Development Environment

B/Ds should assess risks associated with individual application development efforts and establish secure development environments for specific application development efforts. B/Ds should consider:

- The sensitivity of data to be processed, stored and transmitted.
- Applicable internal and external requirements from regulations or policies.
- Security controls for application development are already established.
- Trustworthiness of working staff.
- The level of outsourcing associated with application development.
- Whether segregation between different development environments is necessary.
- Control of access to the development environment.
- Monitoring of change to the program code and the development environment.
- Secure storage of backups at offsite locations.
- Control for data moving in and out of the environment.

When the protection level is determined for a specific development environment, B/Ds should document the corresponding processes in secure development procedures, which should be provided to the staff who need them.

(b) Control of Documentation, Program Source Code and Listings of Applications

Documentation, program source code (including program scripts which can be executed directly without compilation) and listings of applications shall be properly maintained and restricted for access on a need-to-know basis with strict access control and properly managed according to established procedures. The access rights given for system documentation, program source code and listings of applications shall be kept to the minimum and authorised by the application owner. These documents should be suitably classified.

Program source code could be stored centrally as program source libraries, and the following additional guidelines should be observed to control access to the libraries:

- Program source libraries should not be held in a production system.
- All accesses to program source libraries should be recorded in the audit log and maintained.
- Strict change control procedures should be followed when maintaining the program source libraries.

(c) Testing and Review of Security Measures

B/Ds should ensure that thorough testing and verification of security measures are carried out during the development processes for any new and updated applications before production rollout, including the preparation of a detailed schedule of activities, test inputs and expected outputs under a range of conditions. The extent of testing should be in proportion to the nature and criticality of the system.

(d) Application Integrity

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.

A version control mechanism should be established to record changes to program source code over time during application development so that specific versions can be retrieved when necessary, e.g. program fallback. The version convention should be defined, documented and followed. For example, use 1.0 to indicate the first major release and 1.1 to indicate the first revision to the first major release. A change history should be maintained to describe the changes from the previous version. B/Ds may consider using version control tools to improve the effectiveness and reduce human errors in version control.

Development, system testing, acceptance testing, and live operation environments should be separated to reduce the risks of accidental change or unauthorised access to operational data and applications with the following considerations:

- Classified information shall not be copied to the testing environment unless approved by the Information Owner and equivalent security controls are implemented in the testing system.
- Rules for move of data and applications from development to operational status should be defined and documented.
- Development and operational software should run on different systems and in different domains.
- Changes to operational systems and applications should be tested in system and acceptance testing environments before production rollout.
- For testing and development systems, access should be restricted from unauthorised persons and unnecessary network connections, such as the Internet. Besides, system names which attract attackers' attention, such as those producing the impression of a development or testing environment, should be avoided for systems exposed to the Internet.
- For operational systems, other system utilities such as compilers should be restricted from unauthorised access unless such access is technically or operationally necessary, and when such access is allowed, a control mechanism should be in place.

- Users should use different user accounts for testing and operational systems, and the applications should display appropriate identification information to prevent the risk of error.

(e) Program/System Change Control

Changes to all information processing facilities should be authorised and well tested. All proposed program/system changes or enhancements should be checked to ensure they are not compromising the security of the system itself or its operating environment. Staff should receive appropriate training to ensure sufficient awareness of their security responsibilities and the impact of any security changes and usage on the information systems.

The objectives of maintaining program/system change controls (including changes on operating systems, databases and middleware platforms) are:

- To maintain the integrity of the program or system.
- To reduce the exposure to fraud and errors whenever a program or system is amended.

All changes related to security controls should be identified, documented, tested and reviewed to ensure that the system can be effectively protected from attacks or being compromised. Notification of changes should be provided in time to allow sufficient time for tests and reviews to be conducted before implementation. There should be an established procedure for requesting and approving program/system change. Changes should only be processed after formal approval as different levels of authority (some external to the project team) may be established. The authorisation should be commensurate with the extent of the changes. In any case, all changes should go through a change coordinator. The change coordinator should ensure the information quality and completeness of the change requests and that the requests are approved by the appropriate person(s). Operational and administrative procedures, business continuity plans, and audit trail, if applicable, should also be updated to reflect the changes made.

Changes to vendor-supplied software packages should be avoided as far as possible. If there is really a need to modify a software package, the following points should be considered:

- Whether the built-in controls and integrity processes will be compromised.
- Whether it is necessary to obtain the consent of the vendor.
- Whether it is possible to obtain the required changes from the vendor as standard program updates.
- Whether there is an impact if B/Ds are responsible for the future maintenance of the software.
- Whether the change is compatible with other software in use.

(f) Program Cataloguing

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

The basic principle with program cataloguing is that staff of the development or maintenance team are not allowed to introduce any program source or object into the production library nor to copy from the production library. Such activities should be performed by a control unit.

When amendments need to be made, production programs are copied to the development library under the custody of the control unit. Upon completion of the amendments, the project team should request the control unit to catalogue the program in the production library. To facilitate program fallback, version control should be in place, and at least two generations of software releases should be maintained.

Hardening of the program or system should be performed before production rollout. The hardened program/system should then be used as a baseline for any further changes.

For the effective maintenance of an application system, guidelines on the system maintenance cycle in terms of organisation structure, procedures, and products can be referred to the following document for details:

- Guidelines on System Maintenance Cycle (G22)
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/sm/docs/G22.doc)

16.3 Test Data

(a) Protection of Test Data

Test data shall be carefully selected, protected and controlled commensurate with its classification. Production data shall not be used for testing purposes. The use of operational databases containing personal or classified information for testing purposes should be avoided. If this cannot be avoided, the process shall be reviewed and documented, and proper approval shall be obtained from the Information Owner. The following controls should be applied:

- Personal data shall be de-personalised before use.
- Classified information shall be removed or modified beyond recognition before use.
- All these data should be cleared immediately after testing.

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

(a) Outsourcing Security

Outsourcing refers to making an arrangement with an organisation outside the Government to provide services that could be undertaken by B/D itself. When an information system is outsourced to an external service provider, proper security management processes shall be in place to protect the data as well as to mitigate the security risks associated with outsourced IT projects/services. External service providers, when engaged in government work, shall observe and comply with B/Ds' departmental IT security policy and other information security requirements issued by the Government. B/Ds utilising external services or facilities shall identify and assess the risks to the government data and business operations. All data to be handled shall be clearly and properly classified. Information transferring to external service providers may adopt data masking with appropriate techniques according to the nature and use case of the data. 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 with the defined security responsibilities of those external service providers. Security privileges for access shall only be granted on a need-to-know basis.

Furthermore, B/Ds shall not allow their external service providers with access right to government information systems and data in a production environment. If deemed necessary, e.g. for system maintenance and support, the access must be closely supervised by authorised personnel and under controlled environment in order to protect government information assets. Remote access to production systems and data by external service providers for carrying out day-to-day management and operation shall be strictly prohibited.

The security roles and responsibilities of the external service provider, B/Ds and end users pertaining to the outsourced information system should be clearly defined, agreed and documented. B/Ds should note that although the development, implementation and/or maintenance of an information system can be outsourced, the overall responsibility of the information system remains under B/Ds.

B/Ds should ensure the adequacy of the contingency plan and backup process of the external service provider. B/Ds should also ensure that external service providers employ adequate security controls in accordance with government regulations, IT security policies and guidelines. The staff of external service providers should receive appropriate awareness training to enable them to be aware of their responsibilities for information security.

The information or system owner should be aware of the location of the data being hosted by the service provider and ensure that measures are implemented to comply with relevant security requirements and local laws.

(b) Security Requirements in Contracts

Controls shall be in place to administer access to information systems by external consultants, contractors, and temporary staff. Security requirements resulting from third party access or internal controls shall be reflected in the third party contract or other forms of agreement.

B/Ds shall not allow access by external consultants, contractors, outsourced staff, and temporary staff to information and information systems owned or in the custody of the B/D until the appropriate controls have been implemented and a contract has been signed defining the terms for access.

When preparing the outsourcing service contract, B/Ds shall define the security requirements of the information systems to be outsourced. These requirements shall form the basis of the tendering process and are used to determine the compliance of the tenderers.

The outsourcing contract should include requirements for the staff of external service providers to sign a non-disclosure agreement to ensure the personnel from external service providers undertake the obligation of confidentiality where access to classified information is required. The contract should also include a set of service level agreements (SLAs). SLAs are used to define the expected performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. SLAs should address liability issues, reliability of services and response times for the provision of services. The external service providers shall also commit not to transfer or disclose the classified government data to any third parties without the Government's prior written consent. In case special requests for disclosing classified data are received from third parties while such requests cannot be rejected directly, the external service providers shall immediately inform and redirect the requests to B/Ds for handling. Moreover, they shall put in place the procedures for securely erasing government data in all their platforms with written confirmation after such data erasure. Besides, the contract should include the escalation process for problem resolution and incident response such that the contractor should be required to follow in order to minimise the impact on the B/Ds.

(c) Indemnity against Damage or Loss

Appropriate and effective indemnity clauses should be included in all contracts for external services to protect the Government from damage or loss resulting from disruption of services or malpractice of contractors' staff.

17.2 Outsourcing Service Delivery Management

(a) Monitoring and Review of Outsourcing Service

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.

B/Ds should use contractual means to reserve the audit and compliance monitoring rights to ensure sufficient controls have been implemented on government information systems, facilities and data. The contract should allow B/Ds to audit responsibilities defined in the SLA, to have those audits carried out by an independent third party, and to enumerate the statutory rights of auditors. Otherwise, the external service providers shall provide satisfactory security audit/certification reports periodically to prove that the measures put in place are satisfactory.

To manage the delivery of outsourcing services, B/Ds should establish processes to:

- Monitor the performance of services according to the service agreement.
- Conduct regular progress meetings and review the service activities performed by external service providers.
- Review security issues, operational problems, security audit reports, and follow up on issues identified.
- Retain sufficient overall control and visibility into the security activities of the outsourcing services, such as change management, vulnerability management and incident monitoring and response.

(b) Control for Contract Expiry or Termination

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. The destruction of data shall comply with the government security requirements in accordance with its data classification. The staff of external service providers shall return all government assets in their possession upon termination of their services to the Government. The termination process shall be defined and documented. For details about information erasure and return of assets, please refer to Section 10.3(b) “Information Erasure” and 10.1(c) “Return of Assets”, respectively.

17.3 Cloud Computing Security

(a) Shared Responsibilities

Shared responsibilities in cloud computing refer to the division of security and management responsibilities between the Cloud Service Provider (CSP), including both public cloud or private cloud services providers, and the cloud customer. This shared responsibility model ensures accountability and helps define the roles and obligations of both parties in ensuring the security and protection of data and resources in the cloud environment.

Before signing an agreement with a CSP, B/Ds shall ensure that the shared responsibilities of both parties are clearly defined, documented, and understood. B/Ds should carefully review the terms of service, the data protection policy, and the security measures implemented by the CSP.

After the agreement is signed, B/Ds should ensure continuous compliance with the shared responsibilities defined in the contract. Regular review should be conducted to verify that the CSP is adhering to their part of the shared responsibility model. This approach enables B/Ds to secure the workloads they put in the cloud, thereby ensuring the overall security of the outsourced information system.

While the development, implementation, and/or maintenance of an information system can be outsourced, the overall accountability of the information system remains under the B/Ds.

For more information about shared responsibility in cloud services, please refer to the following document for details:

- **Practice Guide for Cloud Computing Security**
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

18. SECURITY INCIDENT MANAGEMENT

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

18.1 Management of Information Security Incidents and Improvements

(a) Incident Monitoring and Detection

A sufficient level of security measures for incident monitoring and detection shall be implemented to protect the system during normal operation as well as to monitor potential security incidents. The level and extent of measures to be deployed will depend on the importance and sensitivity of the system and its data, as well as its functions.

Listed below are some typical measures for security incident monitoring and detection:

- Install firewall devices and apply authentication and access control measures to protect important system and data resources.
- Install intrusion detection tool to proactively monitor, detect and respond to system intrusions or hacking.
- Install anti-malware tools and malware detection and repair tools to detect and remove malware and prevent it from affecting system operations.
- Perform periodic security checks by using security scanning tools to identify existing vulnerabilities and perform a gap analysis between the stated security policy and the actual security arrangement.
- Install a content filtering tool to detect malicious contents or codes in emails or web traffic.
- Enable system and network audit logging to facilitate the detection and tracing of unauthorised activities.
- Develop programs and scripts to assist in the detection of suspicious activities, monitoring of system and data integrity, and analysis of audit log information.

(b) Security Incident Reporting

A reporting procedure shall be established and documented to clearly define the steps and processes in reporting any suspicious activities to all parties involved in a timely manner. Comprehensive contact information, such as telephone numbers (office hours, non-office hours and mobile), email addresses, and fax numbers, should be set out in the reporting procedure to ensure effective communication among responsible personnel.

B/Ds are welcome to seek advice from the GIRO Standing Office in case of any suspected system abnormalities for early detection of IT security threats and

incidents across the Government. It benefits the Government in safeguarding collective security and creating a resilient and secure environment.

To facilitate an effective reporting process, the following points should be noted:

- The reporting procedure should have a clearly identified point of contact and comprises simple but well-defined steps to follow.
- The reporting procedure should be published to all concerned staff for their information and reference.
- Ensure all concerned staff are familiar with the reporting procedure and are capable of reporting security incidents instantly.
- Prepare a security incident reporting form to standardise the information to be collected.
- Consider whether the reporting procedure should apply during and outside working hours, and if necessary, draw up a separate procedure for non-office hour reporting together with those non-office hour contacts in respect of the concerned staff.
- Information about incidents should be disclosed only on a "need to know" basis, and only the ISIRT Commander has the authority to share, or authorise others to share, information about security incidents with others.

To improve the efficiency and effectiveness of IT security incident handling, upon becoming aware of an information security incident (i.e. having a reasonable degree of certainty that an information security event has caused harm to the confidentiality, integrity or availability of government information systems or data assets or has compromised their operations), the departmental ISIRT shall:

(i) Report to the GIRO Standing Office within 60 minutes by phone and submit a completed Preliminary Information Security Incident Reporting Form within 48 hours;

(ii) Share with the GIRO Standing Office the following information upon availability if the security incident involves critical e-government services, has significant security implications, or might attract media attention:
   - type of the incident with an assessment of its scope, damage and impact;
   - actions being taken or to be taken to contain the damage and rectify the problem;
   - line-to-take if the case may attract media attention; and
   - enquiries from media and suggested responses, if any.

(iii) Update the recovery status to the GIRO Standing Office on a daily basis for those affected critical e-government services until the services are resumed.

(iv) Notify GIRO Standing Office for any security incident reported to HKPF, PCPD[7], or issued to media organisations.

A post-incident report should be submitted to GIRO Standing Office no later than one week after the incident is resolved. For those cases that require a longer time to complete the investigation, the concerned departmental ISIRT shall submit interim reports to the GIRO Standing Office on the latest recovery and investigation status according to the following:

- Submit to the GIRO Standing Office the first interim report no later than 14 days after the incident was first reported; and
- Submit to the GIRO Standing Office the progress of the incident investigation on a three months' interval until the case is closed to keep management informed on the status.

Under the General Circular No. 6/2024 – Strengthening the Governance and the Security of IT Systems, in the event of the occurrence of an IT security incident in respect of a government IT system of a B/D which the Director of Bureau considers has embarrassed the Government or undermined the image of its monitoring role, the Project Person-In-Charge (PPIC) (in respect of "Specified IT System") or the DITSO (in respect of B/D's all other information systems) shall submit an initial government IT security incident report to the Director of Bureau within two calendar days from the onset of the incident, to be followed by a full government IT security incident report in seven calendar days. The full incident report, with recommended follow-up actions and endorsement of the Director of Bureau, shall be submitted to the DPO for record, monitoring and technical advice as appropriate. B/Ds should refer to the circular and its thematic website (https://sgsits.host.ccgo.hksarg) for more details.

(c) Security Incident Response

Proper and advanced planning ensures the incident response activities are known, co-ordinated and systematically carried out. It also facilitates the B/D concerned to make appropriate and effective decisions in tackling security incidents and, in turn, minimises the possible damages.

A security incident response plan shall be established and documented. The security incident response plan shall cover at least the following:

- Structure of the incident response team and the corresponding roles and responsibilities;
- Reporting procedures as stipulated in Section 18.1 (b);

[7] If the incident involves personal data breach, the incident shall be reported to the PCPD as soon as possible via the PCPD's Data Breach Notification Form: https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

- Procedures for mitigating the impact of an incident, preserving evidence, investigating the cause and impact of an incident;
- Recovery plan;
- Communication plan with stakeholders and the general public; and
- Post-incident review procedures.

Regular review for security incident response plan shall be conducted at least once every two years, or when there is any material change in the operating environment of the B/Ds. B/Ds shall ensure all relevant personnel are familiar with the plan, and the plan should be made known to all staff, including management personnel, for their reference and compliance. The plan should be clear, straightforward and easily understood so that all personnel have clear knowledge about what they need to do. The plan shall be regularly tested and updated to ensure a quick and effective response to information security incidents. B/Ds shall conduct drills at least once every two years, preferably annually, to assess the effectiveness of the plan. The incident response team members shall participate in the drills to familiarise themselves with their roles in the incident response plan to ensure quick and effective response to security incidents.

All security incidents, actions taken, and the corresponding results shall be recorded. This can facilitate incident identification assessment and provide evidence for prosecution and other useful information for subsequent stages of incident handling. Logging should be carried out throughout the whole security incident response process. An incident reference number may be assigned to each incident to facilitate follow up and tracing during the whole incident handling process.

As a minimum requirement, the following information shall be logged:

- System events and other relevant information, such as audit logs.
- All actions taken, including the date, time and personnel involved.
- All external correspondence, including the date, time, content and parties involved.

In case a security incident happens during non-working hours, 7x24 contact points are crucial for instant communication and swift incident handling which can effectively minimise any damage and loss incurred. B/Ds shall appoint two 7x24 contact points for receiving emergency calls on IT security issues. The contact points shall be capable of handling security incidents or relaying emergency security messages to responsible personnel in a timely manner.

For detailed guidelines and procedures in handling an incident, please refer to:

- Practice Guide for Information Security Incident Handling
  Available at ITG InfoStation
  (https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices.shtml)

The document provides a reference for the B/Ds to facilitate the development of a departmental security incident handling planning and to be used for preparation for, detection of, and response to information security incidents. For the plan to be effective, drills should be arranged and exercised regularly.

(d) Training and Education

B/Ds shall ensure all staff observe and follow the security incident response plan for information systems accordingly. Staff should be familiar with the procedures to handle the incident, from incident reporting, identification and taking the appropriate actions to restore the system to normal operation. Drills on incident handling should also be organised regularly for staff to practise the procedures. B/Ds shall also participate in security drills designated by DPO.

In addition, sufficient training for system operation and support staff on security precaution knowledge is also important in order to strengthen the security protection of the system or functional area and reduce the chance that an incident may occur.

(e) Disclosure of Information about the Incident

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.

Any disclosure of information about incidents, including how to compromise and the background of the system, such as physical location or operating system, may encourage hackers to intrude on other systems with the same vulnerabilities. Moreover, the disclosure may influence the forensic and prosecution processes under Police investigation.

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

(a) Contingency Management

IT contingency planning refers to interim measures to recover information systems and IT services following an emergency or system disruption. Interim measures may include the relocation of information systems and operations to an alternate site, the recovery of IT services using alternate equipment, or the performance of IT services using manual methods. The IT contingency plan should be fully documented and regularly tested. B/Ds should also assess the security risks in the business continuity site or alternate work site to ensure that sufficient security controls are in place to protect the classified government data.

There are different types of contingency plans for information systems. The two most common ones are Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). BCP focuses on sustaining an organisation's critical business processes during and after a disruption. In BCP, system owners from the business side should assess the criticality of the systems and data concerned, conduct business impact assessments, identify recovery time objectives and recovery point objectives, and define minimum service levels. DRP provides detailed procedures to facilitate the recovery of IT capabilities. It will be further elaborated in the next section.

(b) Disaster Recovery Planning

Disaster recovery planning is a process to create a DRP for an information system. DRP includes a well-planned document to deal with situations when a disaster occurs to an information system and/or its primary site, whereby the systems and data are totally lost. DRP should include a detailed backup procedure of the information system and a recovery procedure of the information system to an alternate site. Consideration should be given to the possibility that the primary site of the information system may not be available for a prolonged period of time after the disaster and that the information system at the alternate site will not be run at an optimal performance level (e.g. the performance degradation may be supplemented by manual procedures). The plan should consist of a clear identification of the responsibilities, persons responsible for each function and contact information.

The plan should include a recovery strategy with detailed and well-tested procedures for data recovery and verification. As the purpose of the test is to increase confidence in the accuracy and effectiveness of the procedure, it is important to

define what is being tested, how the test is conducted, and the expected result from the test.

In addition, all necessary materials and documents for recovering the data should be prepared. Arrangements for telecommunication network services at the alternate site should be made beforehand. The plan should also include a procedure to resume data back to the primary site when the primary site is restored after the disaster.

B/Ds should determine if their DRPs are adequate to address possible disasters. DRP should be maintained with updated information, especially when there are changes to the information system at the primary site. A scheduled disaster recovery drill is a good way to test the accuracy and effectiveness of DRP. However, since carrying out a disaster recovery can be time-consuming and may affect normal operations, B/Ds need to determine the frequency of conducting drills according to their business environment.

(c) IT Security Continuity

B/Ds shall plan, implement, and regularly review disaster recovery plans to ensure adequate security measures under such situations. B/Ds should define the roles and responsibilities, information security requirements and the continuity of information security in the disaster recovery plans. In the absence of disaster recovery and contingency plans, B/Ds should assume that the information security requirements remain the same in any situation compared to normal operational conditions.

19.2 Resilience

(a) Availability of Information Systems

B/Ds should identify business requirements for the availability of their information systems. All information systems should be implemented with resilience sufficient to meet the availability requirements. If the availability cannot be guaranteed with the existing system architecture, resilient IT services and facilities should be considered. Resilient information systems should be tested to ensure the component failover works as intended. When designing resilient information systems, B/Ds need to consider and address the risk to the integrity or confidentiality of associated information.

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

(a) Identification of Applicable Legislation and Contractual Requirements

To avoid breach of legal and contractual requirements, B/Ds shall explicitly identify, document and keep up-to-date with all relevant statutory, regulatory and contractual requirements applicable to the operations of each information system. The specific controls and individual responsibilities to meet these requirements should be defined and documented. The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies, and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

(b) Intellectual Property Rights

Copyright law restrictions shall be respected at all times. Only approved software and hardware with purchased licences are allowed to be set up and installed following all licensing agreements and procedures. Staff shall observe and follow these terms. Unauthorised copying, modification or unlicensed use of the software or hardware shall be strictly prohibited. Security control procedures should be developed to ensure compliance with all software licences, purchase agreements and the existing legislation on copyright.

An inventory of all installed software should be audited against the licence agreements on a regular basis, e.g. once a year. Licences, software manuals, and procurement documentation should be stored in a secure location, such as in a closed file cabinet, and the inventory list shall be maintained regularly. When upgrades of software are purchased, the old version may be required to be disposed of depending on the purchase agreement.

- All software to be installed or run in a computer should be acquired officially from an authorised dealer/supplier.
- B/Ds should be aware that the licence of freeware may not cover business usage.
- Regular reviews of the software inventory of systems should be conducted. It is necessary to investigate the installation of unapproved software or unauthorised amendments to production files.

(c) Documented Records

B/Ds shall keep records to evidence compliance with security requirements and support audits of effective implementation of corresponding security measures. The documented information should be protected from loss and unauthorised access. A lack of such information will hinder any security assessment or auditing activities that are part of the governance and assurance of information security within a B/D and the Government.

B/Ds should consider establishing a list of documented information as evidence of security compliance based on their own departmental IT security policy and guidelines documents. For a sample list of documented information as evidence of compliance, please refer the Practice Guide for Security Risk Assessment & Audit.

(d) Data Protection

It is the responsibility of the B/D to understand and follow the regulations stated. To protect classified data from unauthorised access or unintended disclosure, B/Ds should identify the possible avenues of data breaches and consider implementing data leakage prevention solutions to monitor and protect classified data while at rest in storage, in use at endpoint, or in transit with external communications.

B/Ds should also be aware of the possible impact of the regulatory frameworks in other economies (e.g., General Data Protection Regulation (GDPR), Mainland's Personal Information Protection Law) where applicable. 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. B/Ds shall ensure compliance with the Personal Data (Privacy) Ordinance, particularly the Data Protection Principle 4 (on the security of personal data), when handling personal data. For details on the six Data Protection Principles, please refer to Personal Data (Privacy) Ordinance at PCPD's website. (https://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html)

For information systems that may involve personal data, appropriate measures should be implemented throughout the whole data lifecycle in order to effectively handle the following:

- Limit the collection of personal data to the minimum that is relevant and necessary for the identified purposes.
- Limit the processing of personal data to the extent that is adequate, relevant and necessary for the identified purposes.
- Minimise the exposure of personal data by applying anonymisation techniques (e.g. removing or masking the identity of individuals).
- Ensure that the personal data is erased when no longer necessary.

When designing information systems containing personal data, appropriate technical and organisational security measures should be adopted to protect personal data from unauthorised or accidental access, processing, erasure or other use, including but not limited to ensuring compliance with all applicable laws and regulations, conducting privacy impact assessment to identify and manage data protection risks, ensuring the processes and systems are designed such that the collection and processing of personal data are limited to what is necessary for the identified purpose, and improving staff awareness of the possible consequences (such as violation of security policies, damage of government image, disciplinary actions) when personal data is breached.

For better protection of personal data in the information systems, B/Ds should observe the following guidelines as developed by PCPD.

- Guide To Data Protection by Design for ICT Systems (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf)
- Privacy Management Programme (https://www.pcpd.org.hk/pmp/pmp.html)

20.2 Security Reviews

(a) Security Risk Assessment

Security risk assessments aim to assess the IT security risks to information systems by identifying risks according to their sources (e.g. threats, vulnerabilities) and events (e.g. incident scenarios), determining the level of risks based on their impact and likelihood, and prioritising risks for treatment. In addition, during security risk assessments, vulnerability identification activities (e.g. vulnerability scanning, penetration testing) are conducted to aid the identification of IT security risks. Upon the completion of the security risk assessments, the outstanding risks identified that have not yet been fully addressed should be documented in the risk registers of information systems. A privacy impact assessment is also a risk assessment process that evaluates an information system in terms of its impact upon personal data privacy with the objective of avoiding or minimising adverse impacts.

Security risk assessments for information systems and production applications as well as privacy impact assessments for information systems and production applications involving personal data shall be performed at least once every two years. For the avoidance of doubt, (a) the interval between two consecutive assessment exercises is the period between either (i) the commencement dates of the two exercises after funding approval or (ii) the release dates of the reports of the two assessments on the identified risks, and such interval shall not be longer than two years; and (b) the time for implementing security protection and safeguards against identified risks would not be included in the calculation of the interval. A security risk assessment for information systems as well as a privacy impact assessment for information systems involving personal data shall also be performed before production rollout and prior to major enhancements and changes associated with these systems or applications.

B/Ds should identify and document their information systems with certain criteria, including data classification, Internet-facing information, personal data involvement, outsourcing arrangement and availability requirements applicable to each information system.

Due to the high demand for expert knowledge and experience in analysing the collected information and justifying security measures, a security risk assessment and privacy impact assessment should be performed by qualified security expert(s) independent of the area under review. When engaging service providers for security risk assessments and privacy impact assessments, the details (e.g. assessment scope, methodology, report format) shall be determined and agreed before commencement of the assessments. The security risk assessments and privacy impact assessments shall be conducted according to industry best practices. In particular, security risk assessments shall include on-site review, encompassing thorough inspection of IT infrastructure and interviews with key personnel, to gain a comprehensive understanding of the environment and identify any risks that may not be evident from off-site review. The privacy impact assessments shall be performed in accordance with PCPD's prevailing guidelines. B/Ds shall properly document all the assessment details as evidence of the satisfactory completion of security risk assessments and privacy impact assessments.

B/Ds shall hold regular check-point meetings with service provider during the security risk assessments and privacy impact assessments to monitor progress, provide feedback, and address unexpected issues promptly. B/Ds shall oversee the security risk assessments and privacy impact assessments and ensure the quality of work complies with the service agreement. While completing self-assessment checklists can be a useful tool for ongoing monitoring, they are not sufficient to be considered as thorough and unbiased security risk assessments and privacy impact assessments and shall not be used as a substitute for comprehensive security risk assessments and privacy impact assessments.

A security risk assessment and privacy impact assessment can only give a snapshot of the risks of the information systems at a particular time. B/Ds should consider conducting security risk assessments and privacy impact assessments more frequently according to the risk levels of information systems. For avoidance of doubt, B/Ds may arrange to perform these assessments internally in an independent and quality manner.

For guidance on security risk assessment, please refer to the Practice Guide for Security Risk Assessment & Audit. For guidance on privacy impact assessments, please refer to the Personal Data (Privacy) Ordinance and the information leaflet on privacy impact assessment, which are available on PCPD's website.

(b) Security Audit

Security Audit is a process or event with the IT security policy or standards as a basis to determine the overall state of the existing protection and to verify whether

the existing protection has been performed properly. It targets finding out whether the current environment is securely protected in accordance with the defined IT security policy. It shall be performed at least once every two years to ensure the compliance of the security policies and effective implementation of security measures. B/Ds shall maintain updated documentation for security related processes and procedures to facilitate the auditing process.

B/Ds should consider whether the appointed security auditor is appropriate for the nature of the planned security audit. An independent and trusted party shall be chosen to ensure a true, fair and objective view. The hiring of internal or external security auditors should be carefully planned, especially when dealing with classified information. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work. Moreover, B/Ds should avoid engaging the same security auditor for a prolonged period to avoid the degradation of independence.

The audit shall be performed by auditors with sufficient skills and experience accompanied by system administrators. The roles, responsibilities and accountabilities of each involved party should be clearly defined and assigned.

The security audit shall be conducted by independent security auditors who possess relevant professional qualifications (e.g. Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP) and Certified Information Security Professional (CISP)). The auditor should also have relevant experience in auditing similar systems or industries.

The security audit shall evaluate the compliance of information systems against the government information security requirements and B/Ds' information security policies and guidelines. The security audit shall not be considered a verification process for the rectification recommended in security risk assessment exercises. The security audit shall include interviews with various stakeholders and reviews of system settings, logs, policies, procedures, and other relevant documents.

When any non-compliance is found, B/Ds shall:

- Determine the causes of the non-compliance.
- Evaluate the need for action.
- Implement any action needed.
- Review the effectiveness of any corrective action taken.
- Document and maintain the results of the audit and corrective action taken.
- Review whether similar issues will be applicable to other information systems.

For guidance on security audit, please refer to the Practice Guide for Security Risk Assessment & Audit.

(c) Technical Compliance Review

Use of software and programs for performing security risk assessment or security audit shall be restricted and controlled. All changes to the information system for the use of such software and programs should be subject to strict change management control. B/Ds should assign dedicated user accounts with appropriate access rights for vulnerability scanning, penetration testing, configuration reviews, and source code reviews based on the least privilege principle. The involved accounts should be removed or password reset immediately after the completion of the exercises or activities.

B/Ds shall conduct vulnerability scanning for all Internet-facing information systems at least annually, before production rollout and prior to the major enhancements and changes associated with those information systems. Vulnerability scanning should also be incorporated in the risk identification process of the security risk assessments for information systems. Penetration testing shall be included in the respective security risk assessment exercises for all Internet-facing information systems. B/Ds should conduct configuration reviews and source code reviews for all Internet-facing information systems regularly, before production rollout and prior to major enhancements and changes associated with those information systems. The identified vulnerabilities and issues should be evaluated and addressed with appropriate corrective actions before system live-run or production rollout.

Vulnerability scanning, penetration testing, configuration reviews, and source code reviews should be planned, documented and exercised with caution since such activities could compromise the security of the information systems. Vulnerability scanning, penetration testing and source code reviews should only be carried out by competent, authorised persons or under the supervision of such persons.

For details about technical vulnerability management, please refer to Section 14.6 Technical Vulnerability Management.

(d) Information Security Compliance Monitoring and Audit Mechanism

B/Ds shall follow the mechanism introduced by the Government which streamlines the various processes of monitoring and assessing B/Ds' information security compliance status as stipulated in Appendix D.

For details on the mechanism, please refer to the IT Security Theme Page at the ITG InfoStation (https://itginfo.ccgo.hksarg/content/itsecure/isc_new/index.asp).

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 ***

APPENDIX A SAMPLE IT SECURITY END USER INSTRUCTIONS

The document aims to help end users understand their responsibilities in IT security.

B/Ds should make use of the enclosed sample End User Instructions to produce one for their own organisation. The Instructions should be customised based on their departmental IT security policy and computer environment. B/Ds should distribute the document to all existing staff and new staff at first entry and remind the staff regularly to read the document.

This End User Instructions document, however, is not intended as a replacement for the existing security documents in the B/D or the Government. Users are required to read and follow all existing security documents in full.

END USER INSTRUCTIONS ON INFORMATION TECHNOLOGY (IT) SECURITY

[YOUR DEPARTMENT NAME]

[***Name of an officer***] has been appointed as the Departmental IT Security Officer (DITSO) to oversee the IT security of the [***name of Bureau/Department***]. Security is the personal responsibility of staff. End user diligence is necessary to protect the information or the information systems commensurate with the data classification. Each user is accountable for all of his/her activities on the information systems.

To protect classified or personal information from unauthorised access or unauthorised disclosure, prevailing government IT security requirements, including Security Regulations and Baseline IT Security Policy, shall be observed. No officer 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 shall be provided only to persons both within the Government and outside it, 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.

Users shall safely keep and protect computers and storage devices from unauthorised access or disclosure of information under their custody. Appropriate security measures shall be implemented to protect government information assets and information systems. If a user discovers any suspicious activities or suspects a security breach, the user shall report the case promptly to the [***help desk***] during office hours. If a security incident occurs after office hours, the officers to contact are: [***add names and contacts here***]

Failure to comply with the information security requirements may result in disciplinary proceedings.

The following are lists of DOs and DON'Ts actions that you should be aware of when handling government information or using information systems. Note that the lists are not exhaustive, you should refer to the departmental IT security policy, the Security Regulations and the Baseline IT Security Policy (S17) where appropriate.

DOs

- The classification category shall be clearly marked, for example, adding [RESTRICTED] before the subject title for an email containing RESTRICTED information.
- All stored classified information shall be encrypted. All classified information should be encrypted during transmission over any communication network. Transmission of CONFIDENTIAL or RESTRICTED information over un-trusted communication networks shall be encrypted.
- For transmission of CONFIDENTIAL information by electronic mail within the Government, the Confidential Mail System, Confidential Messaging System, Mobile Confidential Mail Services and approved sub-systems of Centrally Managed Messaging Platform shall be used.
- Check the email addresses of recipients carefully before sending emails, especially when the emails contain classified or personal information.
- Check for suspicious activities in mailboxes and unfamiliar changes to email account settings. For example, mail rules have been configured without notice, the inbox no longer receives incoming emails, or the "Sent" folder contains outbound emails that you did not write.
- Verify the authenticity of received messages and contents by examining the email address, URL, and spelling used in any correspondence.
- Back up critical data frequently and retain an offline copy of backups with sufficient protection measures in place.
- Minimise processing and storage of classified or personal information in mobile phones.
- Keep mobile phones under continuous and direct supervision when in use, and store them in physically protected areas commensurate with the classification of data stored when not in use.
- Safeguard any equipment, device or user identity in your possession with proper security measures, for example, password protected, log-off or power-off, locked in cabinet/drawer when unattended.
- Ensure a safe and secure working environment to prevent accidental disclosure of sensitive information and avoid eavesdropping, for example use a privacy screen filter.
- Release information and grant the data access rights based on a need-to-know basis.
- Select passwords in accordance with the departmental password management requirements, e.g. at least eight characters with upper-case alphabets, lower-case

alphabets, numbers and special characters and change your password periodically. If you suspect a password has been compromised, change it immediately and report it to your supervisor.

- Use a unique and sufficiently complex password for each system or service account, e.g. the password of your official email account should be different from your personal email account.
- Enable multi-factor authentication for online accounts to minimise the risks of credential theft if available.
- Apply the latest security patches and regularly remove cache files or temporary files to protect data privacy.
- Install malware detection measures with the latest signatures and definition files to perform scanning, including email, downloaded files, and files in removable media or mobile devices before use.
- Spam email[8] should be ignored or deleted. Beware of phishing emails[9], which could lead to malware infection or even security breaches.
- Protect wireless or mobile devices against unauthorised usage by use of encryption to protect data transmitted and use of password-protected features.
- Disable wireless and mobile services when there is no need to use them.
    - Turn off wireless connections such as Wi-Fi, Near Field Communication (NFC), Bluetooth and infrared connectivity when not in use.
    - Disable automatic Wi-Fi connection to avoid connecting to unsecure networks, for example, in public places, automatically.
    - Follow the Guiding Principles on the Use of Internet Services[10] when using the Internet services provided by the Government.

<u>DON'Ts</u>

- Don't store classified information in privately-owned mobile devices, removable media or IoT devices.
- Don't leave your workstation and computer equipment unattended without sufficient physical access controls, e.g., an opened door, left on a desk.
- Don't keep a written record of your password anywhere near your work (e.g. a memo stuck on screen), nor use any information that is easy to guess (e.g. a dictionary word) or related to you (e.g. name, birthday or post) as your password, nor share your password with others.
- Don't disclose information about your own, your system or your department to any unauthorised person.

[8] Spam email refers to flooding of an email account with many unwanted message, such as advertisement.
[9] Phishing email refers to email imitating to be sent from a person you knew, which attempts to steal information.
[10] https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices/Guide_use_of_Internet.htm

- Don’t connect your own device to the government internal information system or network.
- Don’t connect workstations to external networks by means of a dial-up modem, wireless interface or broadband link.
- Don’t give responses, open attachments or click links in unsolicited and any suspicious electronic messages, including but not limited to emails, instant messages, and SMS.
- Don’t download and open files from websites that have not been confirmed to be credible.
- Don’t use government email address to register non-work related online services.
- Don’t reuse the same password of your government email account for subscribing other online services.
- Don’t use any private e-mail service for official communication, in particular the case when communicating with the public or external parties in official capacity.
- Don’t install software in your workstation without proper approval.
- Don’t disable existing endpoint protection for government owned devices.
- Don’t access files from unknown removable media with your workstation.
- Don’t install and run unauthorised software in your workstation without prior approval from the officer as designated by the B/D

APPENDIX B GUIDANCE ON CLASSIFICATION ASSESSMENT

B/Ds should make reference to the below considerations when assessing the classifications of information systems.

1. Tier 2 Information Systems

Tier 2 information systems refer to the 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.

In general, the impact on the Government in case of failure or disruption of the information systems can be categorised into three levels of severity as follows:

Impact Level	Description
High (H)	Major loss / serious damage or prejudicial to the Government
Medium (M)	Medium loss / some damage to the Government
Low (L)	Minor loss / little damage to the Government

The following table summarises some factors for consideration when determining the impact. These factors can be grouped into four different aspects. B/Ds should critically consider the Impact Level on different aspects in case of system failure or disruption.

Aspect	Considerations if failure or disruption of the information system may cause	Impact Level (H/M/L)
Defence / Security Risks	(a) Endanger human lives or properties (b) Inability to maintain law and order (c) Inability to carry out statutory duties (i) In a sufficiently timely manner (ii) With sufficient confidence and/or correctness (iii) With planned resource constraints, etc. (d) Lead to damaging or loss of physical / information assets (i) Physical facilities, systems, or networks (ii) Equipment, component parts or supplies (iii) Data, personal information, intellectual property, etc. (e) Relaxed security controls, etc.	
Financial Implications	(a) Direct or probable financial loss of the Government (i) Direct financial loss (ii) Loss of revenue or delay in the collection of revenue (iii) Delay in review of Government fees and charges (iv) Additional expenditure to carry out follow-up action such as cleaning up and/or tidying up of data (v) Delay in payment process which would incur additional expenditure / compensation, etc.	
Government Image	(a) Affect Government reputation (b) Affect public confidence, etc.	

Services to Users	Based on the type of end users and the user population, how severe is the impact if the service is unavailable or degraded? (a) Affect a huge number of users or only a few users? (b) The targeted end users are the general public, within the B/D only, or other B/Ds? (c) Disruption in the analysis of information and decision making process of senior government officers? etc.	
Others	Please include any other additional area(s) that is / are applicable to the information system.	
	Overall Impact Level:	

(Remark: Please also consider any impact of the service disruption to other interdependent information systems.)

In general, if there are one or more aspects in which the impact level was assessed as "High", you should consider the Overall Impact Level of your system or service as "High". The information system should be considered Tier 2 information system if the overall impact level is "High".

2. Tier 3 Information Systems

There are a number of essential services that are critical to the functioning and security of a society and its economy. Tier 3 information systems refer to the 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.

To identify Tier 3 information systems, B/Ds should identify their provided essential services and subsequently determine the Tier 3 information systems according to the definition. In general, essential services usually spread across sectors that have a significant impact to a society (e.g. aviation, banking and finance, broadcasting, communications, energy, healthcare, land transport, maritime, media, security and emergency services, water and sewerage, etc). When identifying essential services, B/Ds should consider the criticality of their provided services based on the service nature and the service impact to the functioning and security of a society and its economy. With the essential services identified, B/Ds should subsequently identify the Tier 2 information systems which are directly related to the provision of essential service concerned. The identified information systems are considered as the Tier 3 information systems.

The above considerations serve as a reference for B/Ds to determine the classifications of their information systems. B/Ds should conduct own evaluations which make reference to the above guidance. When in doubt, B/Ds are encouraged to consult DPO regarding the assessment on system classification.

APPENDIX C CLASSIFIED PROTECTION OF IT SECURITY FOR INFORMATION SYSTEMS

The following more stringent security controls shall be adopted by Tier 2 and Tier 3 information systems respectively to achieve classified protection of IT security for information systems according to their system classifications. The security controls for Tier 2 information systems shall also be adopted by Tier 3 information systems.

Government Organisation Structure on Information Security (Section 5)		
Tier 3 Information Systems	a)	For B/Ds with Tier 3 information systems, an information security steering committee with the participation of senior management and DITSO shall be set up to ensure adequate resources and attention are devoted to information security. There shall be regular meetings for the information security steering committee. The outcome of the discussion for the committee, including management directive on information security related issues, shall be properly documented to facilitate follow-up actions. The committee's structure and roles and responsibilities shall also be documented.
	b)	For B/Ds with Tier 3 information systems, at least one of the members of the IT security management unit shall possess at least one of the industry-recognised IT security certifications (e.g. CISA, CISSP, CISP, etc.).
Management Responsibilities (Section 7)		
Tier 3 Information Systems	a)	For B/Ds with Tier 3 information systems, the B/Ds shall adopt the IT security risk management framework specified in Section 7.2 (c). B/Ds shall maintain risk registers for their Tier 3 information systems. The risk registers shall at least document the IT security risks being identified, the likelihood and severity of the occurrence, the risk mitigation measures and monitoring required.

Human Resource Security (Section 9)		
Tier 3 Information Systems	a)	For B/Ds with Tier 3 information systems, the B/Ds shall formulate an IT security training programme to enable the provision of targeted and structured IT security awareness activities to their staff. The training programme shall also ensure that all personnel involved in the support and operation of Tier 3 information systems, including vendors, contractors and service providers, are familiar with the IT security requirements and the prevailing IT security threats, impacts and mitigation measures. In case it is infeasible to formulate or provide training programmes for vendors, contractors or service providers, B/Ds shall impose contractual obligations on those parties to provide relevant IT security training to their staff.
Access Control (Section 11)		
Tier 2 Information Systems	a)	Regular check/audit by an independent party on the usages of privileged accounts shall be conducted at least once every six months to ensure the use of these accounts is for legitimate purposes.
	b)	Administrative procedures shall be adopted to manage the access (e.g. obtaining passwords from a sealed envelope kept by another designated person, login by two staff members using split password) if there is no technical solution to limit the access to data in the systems and applications through privileged accounts.
	c)	The strong password policy as specified Section 11.4(b) shall be enforced. In addition, if any information system, when compromised, could affect the security of Tier 2 information systems (e.g. an information system sharing the same network segment with a Tier 2 information system or specific machines which are allowed to perform administrative functions on Tier 2 information systems), the strong password policy shall also be enforced.
	d)	Multi-factor authentication shall be implemented for any interactive logon to privileged accounts of Tier 2 information systems where technically feasible.

Operations Security (Section 14)		
Tier 2 Information Systems	a)	Local and off-site backups shall be maintained. Off-site data backup shall be stored at a secure and safe location remote from the site of the equipment.
	b)	A capacity management plan shall be in place and documented.
	c)	To mitigate the impact of end-of-support issues of software, a migration plan shall be in place at least six months before the end-of-support date, and the associated security measures shall be in place no later than the end-of-support date.
	d)	All known vulnerabilities shall be fixed as soon as possible, typically within a month after the release of security patches. B/Ds shall perform risk assessments to determine the vulnerability mitigation approach and schedule by considering the potential impact and the possibility of the vulnerabilities being exploited. The risk assessment results shall be properly documented. If the vulnerabilities cannot be mitigated within one month, B/Ds shall inform their DITSOs of the rationale, the associated risks, and the mitigation approach and schedule to enhance the visibility of the vulnerability mitigation status. B/Ds shall also provide monthly interim updates to DITSOs regarding the mitigation status of the vulnerabilities until they are mitigated.
Tier 3 Information Systems	e)	For B/Ds with Tier 3 information systems, the B/Ds shall establish information security monitoring processes which includes 24 x 7 information security surveillance. The information security monitoring processes allows B/Ds to consolidate data from multiple sources (e.g. firewalls, IDS/IPS, EDR/NDR solutions), providing a holistic view of the security landscape and enabling a more rapid and effective response to potential security events. In addition, the security monitoring processes shall facilitate monitoring of the activities in the network and systems and provide continuous threat detection, monitoring, and incident response capabilities, which include the utilisation of security information and event management (SIEM) tools to aid in comprehensively analysing and correlating security event data from multiple sources.

System Acquisition, Development and Maintenance (Section 16)		
Tier 2 Information Systems	a)	Security shift-left approach, including secure coding practices and conducting of security reviews as specified in Section 16.1(a) in the system design stage shall be adopted. The pre-production security risk assessment shall verify the follow-up actions of the security review to ensure necessary security measures and controls are implemented in the system properly before production rollout.
	b)	System hardening shall be performed before production rollout, and the system hardened shall then be used as a baseline for any further changes.
IT Security Aspects of Business Continuity Management (Section 19)		
Tier 2 Information Systems	a)	An IT contingency plan shall be developed to enable sustained execution of Tier 2 information systems in the event of a disastrous disruption (e.g. fire, natural disasters such as floods) or emergency situation (e.g. terrorism, mass demonstrations or bomb threats requiring the evacuation of a site). Plans for disaster recovery shall be fully documented, regularly tested and tied in with the business continuity plan.
Tier 3 Information Systems	b)	Sufficient resilience shall be implemented to prevent disruption of the essential services provisioned. The resilience shall be tested regularly to ensure the component failover works as intended.

Compliance (Section 20)	
Tier 2 Information Systems	a) Vulnerability scanning shall be conducted for Tier 2 information systems at least once a year, before production rollout and prior to the major enhancements and changes associated with those information systems. b) Penetration testing shall be included in the respective security risk assessment exercises for all Tier 2 information systems. For Internet-facing Tier 2 information systems, B/Ds shall ensure penetration testing is conducted at least once a year.
Tier 3 Information Systems	c) Security risk assessments shall be conducted for Tier 3 information systems at least annually, before production rollout and prior to the major enhancements and changes associated with those information systems. The security risk assessments shall include vulnerability scanning, penetration testing, configuration reviews and source code reviews. The penetration testing included in the security risk assessment shall be conducted by an independent service provider having professional accreditations or certifications (e.g., Certified Information Security Professional - Penetration Test Engineer (CISP-PTE), CREST Certified Web Applications Tester (CCT APP), GIAC Penetration Tester Certification (GPEN), Offensive Security Certified Professional (OSCP)). Upon the completion of security risk assessments, the security risk assessments reports, including the risk registers of the systems, the corresponding vulnerability scanning reports, penetration testing reports, and rectification plans for vulnerabilities, shall be endorsed by DITSO.

APPENDIX D INFORMATION SECURITY COMPLIANCE MONITORING AND AUDIT MECHANISM

The following Information Security Compliance Monitoring and Audit mechanism is introduced by the Government to streamline the various processes of monitoring and assessing B/Ds' information security compliance status:

1. For B/Ds with Tier 3 information systems, the B/Ds shall submit the establishment, reporting mechanism, and roles and responsibilities of their IT security management unit to DPO. If necessary, DPO may request B/Ds to clarify the information. Where there is any material change to the information, B/Ds shall notify DPO within 30 days.
2. B/Ds shall submit the list of their Tier 2 information systems, Tier 3 information systems, and the assessment details of the system classification, with the endorsement from the Heads of B/Ds or their explicitly delegated officer at directorate level, to DPO. B/Ds shall also inform DPO within 30 days in case of any changes to the submitted list, including the change in system classifications. DPO may require B/Ds to submit further information to ensure that the assessment by B/Ds on the system classification is aligned with the classified protection of IT security specified in Section 7.2 (b).
3. Upon request, the incident response plan of Tier 3 information systems shall be submitted to DPO for inspection and review.
4. B/Ds shall furnish the DPO with relevant documentation for record and monitoring regarding their security risk assessment, security audit, and privacy impact assessment exercises. DITSOs shall oversee the satisfactory completion of the exercises as well as subsequent rectifications and arrange to submit the relevant documentation, assessment results and the corresponding rectification status of the exercises to DPO upon regular requests.
5. The reports of security risk assessments for Tier 3 information systems, including the risk registers of the systems, the corresponding vulnerability scanning reports, penetration testing reports, and rectification plans for vulnerabilities, shall be submitted to DPO within 30 days after the assessment completion for inspection and review.
6. The security audit reports for Tier 3 information systems shall be submitted to DPO within 30 days after the audit completion and further submit the rectification plans within 30 days after the submission of the audit report in case of non-compliance.
7. B/Ds shall participate in the government-wide IT security compliance audits conducted by DPO and accord priority to complete the audit within the agreed schedule. This exercise assesses the security compliance status of B/Ds against the government information security requirements and the follow-up status arising from the previous compliance audit.
8. B/Ds shall complete security surveys conducted periodically by DPO for the collection of security status information. This enables an understanding of B/Ds' plans, practices and actions related to information security. The information reveals the readiness of B/Ds in response to security policies, security threats or other security issues.