The Office of the
Government Chief Information Officer

IT SECURITY GUIDELINES

[G3]

Version : 7.0

September 2012

The Government of the Hong Kong Special Administrative Region

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. PURPOSE

This document aims at introducing general concepts relating to Information Technology (IT) security. In referencing the Baseline IT Security Policy, this document elaborates relevant security concepts and best practices related to the usage of IT. Readers will also find guidelines and considerations in defining security requirements in the system development process.

The materials included in this document are prepared irrespective of computer platforms, and may not be applicable to all types of systems. Individual project owners should consider and select only those applicable to their environment.

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

In addition to the Baseline IT Security Policy and this document, there are three other IT security guideline documents:

a. Internet Gateway Security Guidelines (G50)
b. Security Risk Assessment & Audit Guidelines (G51)
c. Information Security Incident Handling Guidelines (G54)

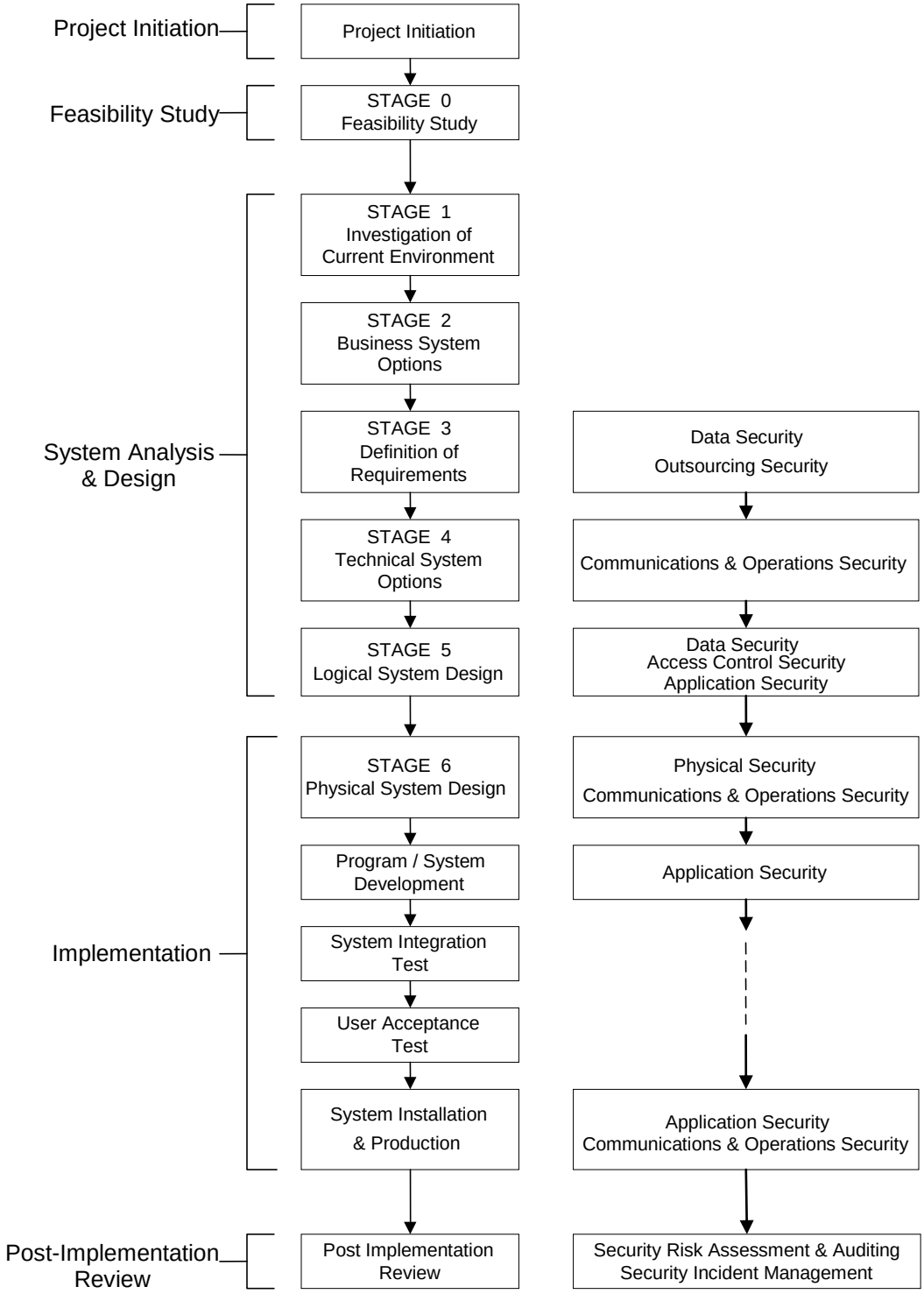
Section 2.1 – IT SECURITY DOCUMENT OVERVIEW describes in details the purpose and relationship of these documents.

2. SCOPE

This guideline describes security considerations in the following eight areas:

- Management responsibilities
- Physical security
- Access control security
- Data security
- Application security
- Communications and operations security
- Security risk assessment and auditing
- Security incident management

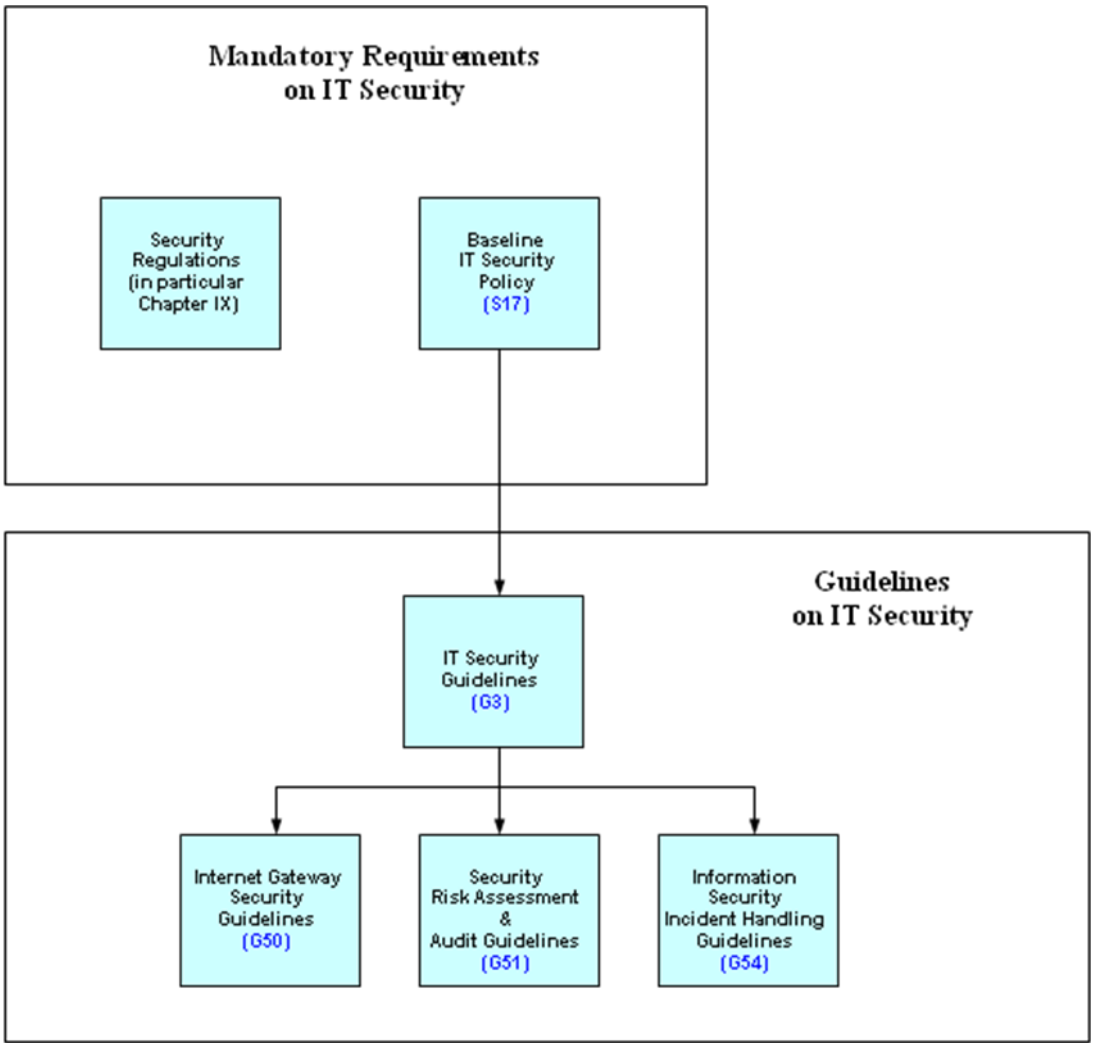
Basically, these considerations should be taken into account in all phases of the System Development Life Cycle (SDLC). There are, however, specific areas in the SDLC phase which needs special attention. These areas are highlighted in the chart in the following page.



Security Issues Related with Different Phases of System Development Life Cycle

2.1 IT SECURITY DOCUMENT OVERVIEW

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



IT Security Documents

The purpose and overview of the five core IT security documents are described below:

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 must be observed as mandatory while there can still be other desirable measures to enhance the security.
IT Security Guidelines: (G3)	Introduces general concepts relating to IT security and elaborates interpretations on the *Baseline IT Security Policy*. It also provides readers some guidelines and considerations in defining security requirements.
Internet Gateway Security Guidelines: (G50)	Acts as a supplementary document to *IT Security Guidelines* to provide general guidelines on Internet gateway security. These guidelines represent what are regarded as best practices to maintain security risks at an acceptable level under the Internet open platform. It is intended for staff who are involved in the operational and technical functions of Internet gateway services.
Security Risk Assessment and Audit Guidelines: (G51)	Acts as a supplementary document to *IT Security Guidelines* to give an introduction to a generic model for IT security risk assessment and security audit. This document does not focus on how to conduct a security risk assessment or audit. Rather, it provides a reference model to facilitate the alignment on the coverage, methodology, and deliverables of the services to be provided by independent security consultants or auditors.
Information Security Incident Handling Guidelines: (G54)	Acts as a supplementary document to *IT Security Guidelines* to provide a reference for the management, administration and other technical and operational staff to facilitate the development of security incident handling plan, and to be used for preparation for, detection of, and responding to information security incidents.

3. REFERENCES

3.1 STANDARDS AND GUIDELINES

a) Baseline IT Security Policy [S17]
http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/s17_pub.pdf

b) Internet Gateway Security Guidelines [G50]
http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g50_pub.pdf

c) Security Risk Assessment & Audit Guidelines [G51]
http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g51_pub.pdf

d) Information Security Incident Handling Guidelines [G54]
http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g54_pub.pdf

e) The HKSARG Interoperability Framework [S18]
http://www.ogcio.gov.hk/en/infrastructure/e_government/if/doc/s18.pdf

f) Guidelines on System Maintenance Cycle [G22]
http://www.ogcio.gov.hk/en/infrastructure/methodology/others/doc/g22_pub.pdf

3.2 OTHER REFERENCES

a) Asia Pacific Economic Cooperation Telecommunications and Information Working Group
http://www.apectelwg.org

b) SecurityFocus
http://www.securityfocus.com/

c) SANS Institute
http://www.sans.org/

d) Site Security Handbook
http://www.ietf.org/rfc/rfc2196.txt?number=2196

4. DEFINITIONS AND CONVENTIONS

4.1 DEFINITIONS

a)	Information System	a related set of hardware and software organised for the collection, processing, storage, communication, or disposition of information.
b)	Confidentiality	only authorised persons are allowed to know or gain access to the information stored or processed by information systems in any aspects.
c)	Integrity	only authorised persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.
d)	Availability	Information Systems should be accessible and usable upon demand by authorised persons.
e)	IT Security Policy	a documented list of management instructions that describe in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorised disclosure, modifications or destruction.
f)	Classified Information	refers to the categories of information classified in accordance with the Security Regulations.
g)	Staff	persons employed by the Government irrespective of the employment period and terms.
h)	Data Centre	a centralised data processing facility that houses Information Systems and related equipment. A control section is usually provided that accepts work from and releases output to users.
i)	Computer Room	a dedicated room for housing computer equipment.
j)	Malicious Codes	programs intended to perform an unauthorised process that will have adverse impact on the confidentiality, integrity, or availability of an Information Systems. Examples of malicious codes include computer viruses, worms, Trojan horses, and spyware etc.

k)	Mobile Devices	portable computing and communication devices with information storage and processing capability. Examples include portable computers, mobile phones, tablets, digital cameras, audio or video recording devices.
l)	Removable Media	portable electronic storage media such as magnetic, optical, and flash memory devices, which can be inserted into and removed from a computing device. Examples include external hard disks or solid-state drives, floppy disks, zip drives, optical disks, tapes, memory cards, flash drives, and similar USB storage devices.

4.2 CONVENTIONS

N.A.

4.3 ABBREVIATIONS AND ACRONYMS

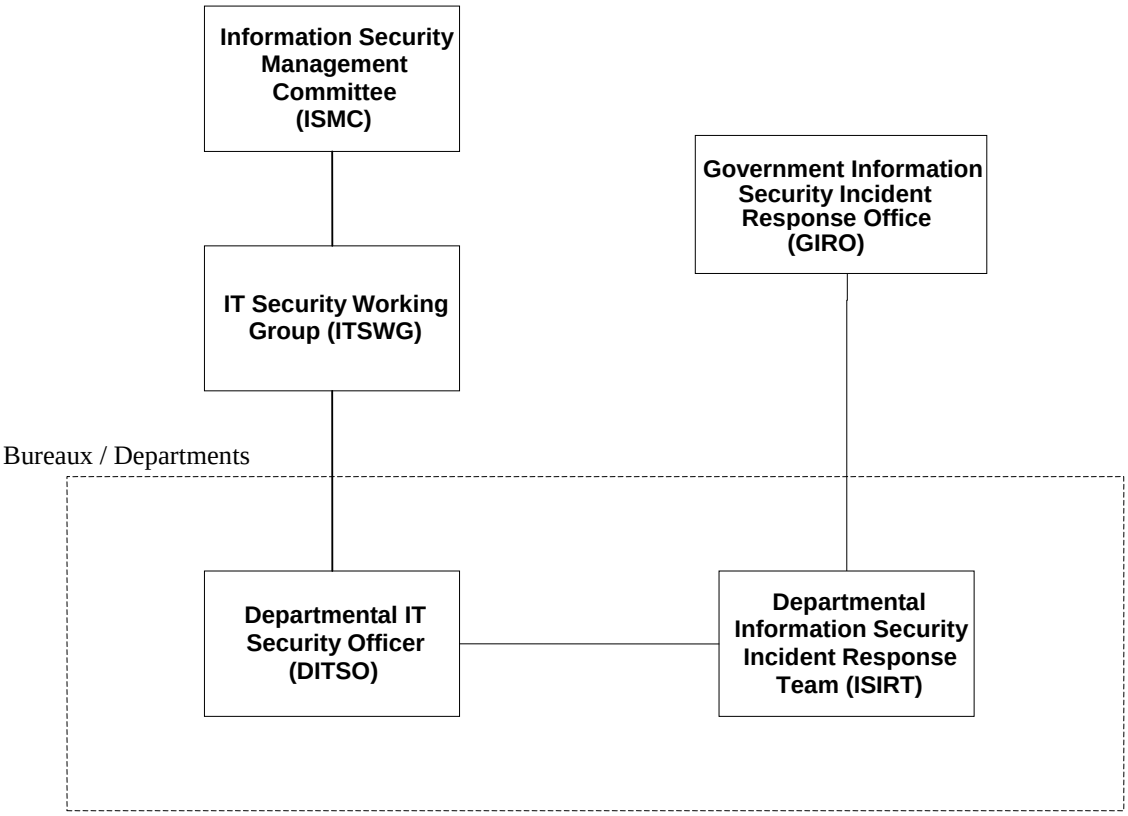
BCP	Business Continuity Plan
CD	Compact Disc
DMZ	Demilitarised Zone
DRP	Disaster Recovery Plan
IDS	Intrusion Detection System
IM	Instant Messaging
IPS	Intrusion Prevention System
LAN	Local Area Network
LUN	Logical Unit Number
NAS	Network Attached Storage
RFID	Radio Frequency Identification
SAM	Software Asset Management
SAN	Storage Area Network
SLA	Service Level Agreement
SNS	Social Networking Service
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

5. GOVERNMENT ORGANISATION STRUCTURE ON INFORMATION SECURITY

5.1 GOVERNMENT INFORMATION SECURITY MANAGEMENT FRAMEWORK

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

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



Government Information Security Management Framework

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

5.1.1 Information Security Management Committee (ISMC)

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

- Review and endorse changes to the Government IT security related regulations, policies and guidelines.
- Define specific roles and responsibilities relating to IT security.
- 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:

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

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

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.
- Promote IT security awareness within the Government.

The core members of ITSWG comprise representatives from:

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

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

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. Meanwhile, 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 has the following major functions:

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

The core members of GIRO comprise representatives from:

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

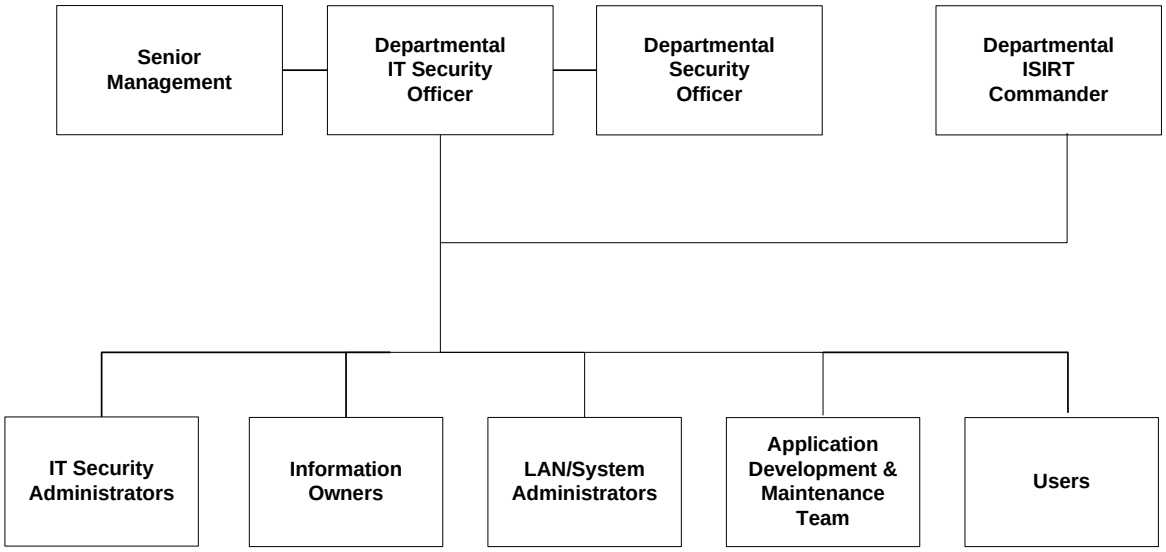
5.1.4 Bureaux/Departments

B/Ds are 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 role and responsibility 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 organisational framework:



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

5.2.1 Senior Management

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

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

Senior management should consider the setting up of an information security steering committee, or including information security as one of the regular discussion items in management meetings. This will provide an ongoing basis to ensure the alignment of security strategy with business objectives.

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

5.2.2 Departmental IT Security Officer (DITSO)

Head of B/D shall appoint a Departmental IT Security Officer (DITSO) to be responsible for IT security. To better equip the designated DITSOs with security management and related technology knowledge or skills, SB and OGCIO will provide training to DITSOs to facilitate them in carrying out their duties. B/Ds should ensure that the designated DITSOs have duly received such training. The roles and responsibilities of DITSO shall be clearly defined which include but are not limited to the following:

- Establish and maintain an information protection program to assist all staff in the protection of the information and information system they use.
- Lead in the establishment, maintenance and implementation of IT security policies, standards, guidelines and procedures.
- Coordinate with other B/Ds on IT security issues.
- Disseminate security alerts on impending and actual threats from the GIRO to responsible parties within the B/D.
- Ensure information security risk assessments and audits are performed as necessary.
- Initiate investigations and rectification in case of breach of security.

DITSO may line up an IT security working team within the B/D to assist in leading, monitoring and coordinating of IT security matters within the B/D.

5.2.3 Departmental Security Officer (DSO)

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

- Discharge responsibilities for all aspects of security for the B/D.
- 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 coordinating the handling of information security incidents occurring within the respective B/D. Heads of B/D should designate an officer from the senior management to be the ISIRT Commander. The ISIRT Commander should

have the authority to appoint core team members for the ISIRT. The responsibilities of an ISIRT Commander include:

- Provide overall supervision and co-ordination of information security incident handling for all information systems within the B/D.
- Make decisions on critical matters such as damage containment, system recovery, the engagement of external parties and the extent of involvement, and service resumption logistics after recovery etc.
- Trigger the departmental disaster recovery procedure where appropriate, depending on the impact of the incident on the business operation of the B/D.
- Provide management endorsement on the provision of resources for the incident handling process.
- Provide management endorsement in respect of the line-to-take for publicity on the incident.
- Collaborate with GIRO in the reporting of information security incidents for central recording and necessary follow up actions.
- Facilitate experience and information sharing within the B/D on information security incident handling and related matters.

5.3 OTHER ROLES

5.3.1 IT Security Administrators

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

- Maintain control and access rule to the data and system.
- Check and manage audit logs.
- Promote security awareness within the B/D.

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

Although IT Security Administrator is responsible for managing the audit logs, they should not tamper 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 assure that they perform their duties due diligently.

5.3.2 Information Owners

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

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

5.3.4 Application Development & Maintenance Team

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

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

5.3.5 Users

Users of information systems are the staff who actually use the information and shall be accountable for all their activities. Responsibilities of a user include:

- Know, understand, follow and apply all the possible and available security mechanisms to the maximum extent possible.
- Prevent leakage and unauthorised access to information under his/her custody.
- 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 changing. They are NOT stated here as security requirements but are provided as useful guiding references 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 are 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 solution. In short, for an information system, only authorised users are allowed to know, gain access, make changes to, or delete the information stored or processed by the information system. The system should also be accessible and usable upon demand by the authorised users.

- **Prevent, Detect, Respond and Recover**

  Information security is a combination of preventive, detective, response and recovery measures. Preventive measures are for avoiding or deterring the occurrence of an undesirable event. Detective measures are for identifying the occurrence of an undesirable event. Response measures refer to coordinated response to contain damage when an undesirable event (or incident) occurs. Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

  Prevention is the first line of defence. Deployment of proper security protection and measures helps to reduce risks of security incidents. However, when the prevention safeguards are defeated, B/Ds should be able to detect security incidents rapidly, and respond quickly to contain damage. The information systems and data should be recovered in a timely manner. Therefore, B/Ds are required to 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 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. Wireless network without protection is vulnerable to attacks, security measures must be adopted when transmitting classified information.

When B/Ds formulate security measures, they should 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 or entity that is not under your direct control should be considered insecure. Additional security measures are required when your information assets or information systems are located in or interfacing with external systems. Information systems infrastructure could be partitioned using either physical or logical means to segregate environments with different risk level.

  For example, consider any data you receive from an external system, including input from users, to be insecure and a source of attack. Multi-level of defenses should be considered. Information resources should be partitioned according to needs, different access controls and level of protections could be applied to defend potential attacks.

- **Resilience for critical information systems**

  All critical information systems need to be resilient to stand against major disruptive events, with measures in place to detect disruption, minimise damage and rapidly respond and recover.

  The resilience of an information system refers to its ability to continue to operate under adverse condition 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.

- **Auditability and Accountability**

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

  Auditability helps to reconstruct the complete behavioral history of a system, and hence is useful to discover and investigate for 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 the information system.

7. MANAGEMENT RESPONSIBILITIES

7.1 GENERAL MANAGEMENT

This section summarises some key principles and best practices concerning the issue of checks and balance in information security management, and aims to provide B/Ds with a focused appreciation of and references on the subject matter.

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 are advised to consider the following best practices for possible adoption with regard to their individual business and operation environments.

7.1.1 Clear Policies and Procedures

Management should 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. This should normally be covered in the departmental IT Security Policy. They should also include in their policies 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.

7.1.2 Assigning Responsibility

A senior and key personnel in the B/D should be assigned the responsibility for ensuring that the appropriate policies and procedures are developed and applied, and that the necessary checks and balance on the proper administration and operation of the policies and procedures are in place.

7.1.3 Information Dissemination

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

7.2 OUTSOURCING SECURITY

When an information system is outsourced to external service provider, proper security management processes must be in place to protect the data as well as to mitigate the security risks associated with outsourced IT projects/services. Outsourcing or 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 should be clearly and properly classified. Security protections commensurate with the data classification and business requirements shall be documented and implemented with the defined security responsibilities with those external services providers. Security privileges for access should only be granted on a need-to-know basis.

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 and documented. B/Ds should note that although development, implementation and/or maintenance of an information system can be outsourced, the overall responsibility of the information system remains under B/Ds.

When preparing the outsourcing service contract, B/Ds should define the security requirements of the information systems to be outsourced. These requirements should form the basis of the tendering process and as part of the performance metrics.

The outsourcing contract should include requirements for the staff of external service providers to sign non-disclosure agreement to protect sensitive data in the systems. Confidentiality and non-disclosure agreements shall be properly managed, and reviewed when changes occur that affect the security requirement. 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. Besides defining SLA, the contract should include an escalation process for problem resolution and incident response so that incidents can be handled according to a pre-defined process to minimise the impact to the B/Ds.

B/Ds should monitor security control compliance of the external service providers and users actively and periodically. B/Ds should reserve the audit and compliance monitoring rights such as to audit responsibilities defined in the SLA, to have those audits carried out by independent third party, and to enumerate the statutory rights of auditors. Otherwise the external service providers should provide satisfactory security audit/certification report periodically to prove the measures put in place are satisfactory.

In addition, B/Ds should ensure the adequacy of contingency plan and back-up 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 standards. Staff of external service providers are subject to equivalent information security requirements and responsibilities as Government staff.

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.

7.3 CONTINGENCY MANAGEMENT

Information systems are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, disk drive failure) to severe disruptions (e.g. equipment destruction, fire, natural disasters). While many of these vulnerabilities may be minimised or eliminated through management, operational and technical controls, it is virtually impossible to completely eliminate all risks.

B/Ds should develop an IT contingency plan to enable sustained execution of mission critical processes and information systems in the event of a disastrous disruption. IT contingency planning refers to interim measures to recover 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.

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 assessment, identify recovery time objectives and define minimum service levels. DRP provides detailed procedures to facilitate recovery of IT capabilities. It will be further elaborated in the next section.

7.3.1 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 detailed backup procedure of the information system, and 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 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 procedure for data recovery and verification. As the purpose of test is to increase the confidence of 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 in recovering the data should be prepared. Arrangement of telecommunication network services at the alternate site should be made beforehand. The plan should also include 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 for possible disasters. DRP should be maintained with updated information, especially when there are changes to the information system at the primary site. Scheduled disaster recovery drill is a good way to test for the accuracy and effectiveness of DRP. But 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.

7.4 HUMAN RESOURCES SECURITY

7.4.1 Training

Proper security training and updates on IT security policy should be provided to all staff regularly, including users, developers, system administrators, security administrators, and staff of external parties who are engaged in Government work to strengthen their awareness on information security. The awareness training can be in any form such as classroom training, computer based training or self-paced learning. An assessment may be conducted to ensure user awareness for information security requirements and responsibilities. There are handy training resources available on the Cyber Learning Centre Plus (CLC Plus) of the Civil Service Training and Development Institute providing general IT security related courseware as well as self-assessment package to participants. Moreover, B/Ds may make reference to the resources when providing tailor-made training and materials to their staff or contractors in accordance with its own business and operation requirements.

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 own systems from attack and unauthorised use. They should have a defined procedure for reporting security problems.

7.4.2 Personnel Security

To protect classified information from unauthorised access or unauthorised disclosure, relevant clauses in Security Regulations shall be observed. No officer may 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 should be applied to all classified information, which should be provided only to persons who require it for the efficient discharge of their work and who have authorised access. If in any doubt as to whether an officer has authorised access to a particular document or classification or information, the Departmental Security Officer should be consulted.

B/Ds shall ensure that personnel security risks are effectively managed. The risk of allowing an individual to access classified information should be assessed. For example, if classified data is properly encrypted and protected from unauthorised access, the perceived risk is low.

Civil servants authorised to access CONFIDENTIAL and above information shall undergo an integrity check as stipulated in Civil Service Branch Circular No.17/94 – Integrity Checking. For non-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 could 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.

For personnel from external service providers, a non-disclosure agreement should also be signed along with the employment contract if he/she will access classified information or system.

7.4.3 Security Requirements in Contracts

Controls should be in place to administer access to information systems by external consultants, contractors, and temporary staff. Generally, all security requirements resulting from third party access or internal controls shall be reflected in the third party contract or other forms of agreement. For example, if there is a special need in protecting the confidentiality of information, non-disclosure agreements should be established and signed.

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

As a basic principle, all security policies, procedures, as well as checks and balance of an information system adopted for in-house staff should also apply to all external consultants, contractors, outsourced staff and temporary staff engaged in Government work.

7.4.4 Indemnity Against Damage or Loss

It should be ensured that appropriate and effective indemnity clauses are 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.

8. PHYSICAL SECURITY

This section describes the best practices that can be utilised to physically protect classified information and IT resources in order to minimise the business and operational impact due to nature disasters and trespassing.

8.1 ENVIRONMENT

The following sections provide guidelines in building a well-protected computer environment and maintaining a computer room for operation.

8.1.1 Site Preparation

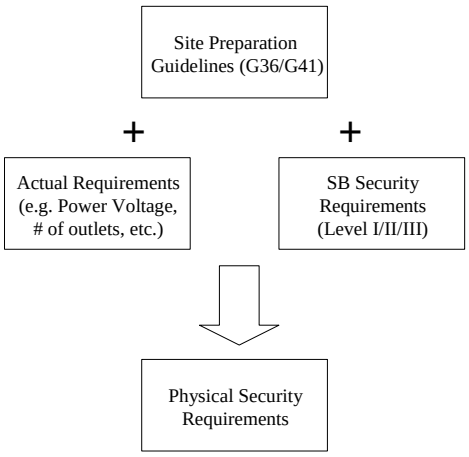
As most of the critical IT equipment are normally housed in a data centre or computer room, careful site preparation of the data centre or computer room is therefore important. Site preparation should include the following aspects:

- 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.

Together with the set of specific facility requirements and the Security Bureau security specification[2] (Level I/II/III), B/Ds can determine all the physical environmental requirements, including security requirements prior to construction. The following diagram illustrates the typical workflow in determining the physical security requirements:

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



Typical Workflow in Physical Security Requirements Determination

B/Ds should observe the physical security specifications from the Security Bureau. It is a mandatory standard for a data centre or computer room to conform to Level III security if the IT equipment involves handling of TOP SECRET/SECRET information, and Level II security if the IT equipment involves handling of CONFIDENTIAL information. Level II security is still recommended for physical facilities hosting IT equipment handling information classified as RESTRICTED or below. This requirement may be constrained by the existing office environment, building structures and/or leasing agreements for offices in non-government premises. B/Ds should evaluate the physical feasibility of the environment before building a data centre or computer room in/around its own office premise. In situations where an office premise cannot fulfil Security Regulations security level requirements, B/Ds must obtain exemption approval from the Government Security Officer (GSO). Details about Level II security specifications are available from SB-GSO or Architectural Services Department (ASD).

If wireless communication network will be set up in the site, a site survey should be conducted to assure proper area coverage of wireless signal and to determine the appropriate placement of wireless devices.

8.1.2 Housekeeping

Proper cleaning procedures for the data centre or computer room must be established. Such procedures should include at least the following:

- Regular cleaning of the external surfaces of the peripherals by operators.
- Daily emptying of the waste paper bin.
- Daily vacuum cleaning of the data centre or computer room floor.
- Daily mopping of the data centre or computer room raised floor.
- Periodic cleaning of the water pipes.
- Periodic cleaning of the in-house partitions, doors, lighting fixture and furniture.
- Periodic inspection and cleaning of the floor void.

B/Ds must regularly inspect the data centre or computer room to ensure the cleaning procedures are followed. Unused peripherals or equipment should be disposed of or written off according to Government rules and regulations. Hardware or workstation should be well covered when there is any cleaning or maintenance work that causes a lot of dust arouse. Eating and drinking in the data centre or computer room should be avoided as far as possible or even prohibited. Smoking in the data centre or computer room is strictly prohibited.

The service utilities must be regularly inspected to ensure continuous availability and failure detection. Besides, regular maintenance and testing should be arranged for all service utilities including air conditioning equipment, fire detection, prevention and suppression system, standby power supply system, power conditioning system, water sensing system and temperature sensing system. All maintenance work carried out must be recorded.

Apart from the service utilities, emergency exits, locks and alarms shall also be regularly checked.

8.1.3 Items for Emergency Use

The data centre or computer room should be equipped with the following things for emergency use:

- Plastic sheets large enough for covering the computer equipment in case of water seepage from the ceiling.
- Raised floor panel lifter/sucker.
- Battery supported fluorescent lanterns in case of power failure.

The locations of these items should be made known to all operations personnel and should not be removed from their designated locations without permission.

At least one telephone line must be installed in each of the console area and help desk area inside the data centre or computer room, production control office and operation management/support office.

8.1.4 Fire Fighting

A fire fighting party should be organised in each operating shift with well-defined responsibility 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 fire breaks out.

Those operators not being members of the fire fighting party shall be taught on 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. They should be tagged for inspection and inspected at least annually.

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

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

8.2 EQUIPMENT SECURITY

This section provides security guidelines in handling computer equipment in operation and disposal.

8.2.1 Equipment and Media Control

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.

Proper controls should be implemented when taking IT equipment away from sites. For non-fixture type of IT equipment such as mobile devices, B/Ds can consider keeping an authorised equipment list and periodically performing inventory check for the status of such IT equipment. For removable media such as universal serial bus (USB) flash drives stored with classified data, B/Ds can consider implementing similar controls. For fixture type of IT equipment, B/Ds can consider adopting a check-in check-out process or inventory documentation measures to identify which IT equipment has been taken away. Nevertheless, staff taking IT equipment off-site should also ensure that IT equipment is not left unattended in public places to protect against loss and theft.

It is risky to store data to mobile device and removable media as they are small and can be easily lost or stolen. Storing classified information to these devices should be avoided. Staff should justify the need to store classified information to these devices. Mobile device and removable media provided by the B/D should be used and staff should seek proper authorisation before storing minimum required classified data to the device. In order to minimise the risk and consequence of data loss, use devices which equip with security measures and use encryption for classified data. Staff should remove classified information from the mobile device and removable media once finished using and should ensure all classified data has been completely cleared prior to disposal or re-use.

Some electronic office equipment, including multi-function printers and photocopiers, may have storage media embedded as auxiliary devices which their existence may not be readily apparent to the users. B/Ds are reminded to review their inventory and make suitable arrangements to ensure the data is handled in accordance with the requirements of Security Regulations, and related policies, procedures and practices. In addition, the equipment should be used and managed with care if sensitive or classified information is likely to be stored or processed by them.

Proper procedures must be established for the storing and handling of backup media. Backup media containing business essential and/or mission critical information shall be stored at a secure and safe location remote from the site of the equipment. Access to the backup media should only be done via a librarian as far as possible. Other staff, including operators, programmers, and contractors, should not be allowed to have access to the media library or off-site storage room under normal circumstances.

Movement of media IN/OUT of a library or off-site storage should be properly logged. Unless permission is granted, any staff should not be allowed to leave the data centre or computer room with any media. To facilitate the detection of loss of media, the storage rack can indicate some sort of markings/labels at the vacant slot positions. Periodic inventory check is necessary to detect any loss or destruction.

Transportation of backup media/manuals to and from off-site must be properly handled. The cases carrying the media should be shockproof, heatproof, water-proof and should be able to withstand magnetic interference. In addition, B/Ds should consider protecting the media from theft – by encrypting the data in the storage media, splitting the media into multiple parts and transported by different people.

All media containing classified information must be handled strictly in accordance with the procedures set out in the Security Regulations. In case of problems, queries can be addressed to the Department Security Officer or Government Security Officer.

The construction of external media library should have the same fireproof rating as the data centre or computer room. The rating for fireproof safe for keeping vital media should reach the standard for keeping magnetic media.

To safeguard tape contents from being erased or overwritten when a tape is accidentally mounted for use, all write-permit rings should be removed from the tapes on the tape racks.

8.2.2 Disposal of Computer Equipment

Physical disposal of computer or electronic office equipment containing non-volatile data storage capabilities must be checked and examined to ensure all information has been removed. Destruction, overwriting or reformatting of media must be approved and performed with appropriate facilities or techniques. Procedures of destruction must comply with the regulations stated in the Security Regulations.

B/Ds are advised to follow the necessary steps below to ensure the secure deletion of information before the disposal or re-use of their equipment:

- Users should check whether classified information had previously been processed and/or kept in the equipment. If in doubt, it should be assumed that it had.
- User is responsible for removal of sensitive data from the equipment, when the data is no longer required, and secure storage of the equipment until disposal or for any other processing.
- User should acquire appropriate secure deletion software to completely clear or erase all the classified information in the equipment.
- B/D should maintain a system of checks and balances to verify its successful completion of the secure deletion process.

For details on disposing classified information, please refer to Section 10.9 – INFORMATION ERASURE in this document.

While there is no specific regulation on the disposal of unclassified information, as a good practice to protect data privacy, B/Ds are advised to adopt the above procedures if they believe that the equipment to be disposed of or reused contains information which may cause data privacy issue if it is not cleared properly.

8.3 PHYSICAL ACCESS CONTROL

Staff should be educated not to enter the password in front of unauthorised personnel and to return the cardkeys or access devices when they resign or when they are dismissed. Finally, the acknowledgement of password and receipt of magnetic cardkeys shall be confined to authorised personnel only and record of passwords shall be securely stored. Cardkeys or entrance passwords should not be divulged to any unauthorised person.

Whenever leaving the workplace, the re-authentication features such as a password protected screen saver in their workstations should be activated or the logon session/connection should be terminated in order to prevent illegal system access attempts. For a prolonged period of inactivity, the workstation should be switched off to prevent unauthorised system access. The display screen of an information system on which classified information can be viewed shall be carefully positioned so that unauthorised persons cannot readily view it. All staff shall ensure the security of their offices. Office that can be directly accessed from public area should be locked up any time when not in use, irrespective of how long the period might be.

A list of authorised personnel to access the data centres, computer room or other areas supporting critical activities must be maintained, kept up-to-date and be 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 party 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 purpose. The access records may include 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 not limited to, bolting door locks, cipher locks, electronic door locks, and biometrics door locks.

B/Ds can consider installing video cameras (or closed-circuit TV) 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 can be considered to be installed for areas hosting critical/sensitive systems.

Safekeeping of classified materials shall comply with the Security Regulations to prevent unauthorised access and disclosure. For example, TOP SECRET documents shall be kept in a safe with a combination lock inside a strong room while SECRET documents shall be kept either in a safe fitted with a combination lock or in a steel cabinet fitted with a locking bar and padlock inside a strong room. Classified information shall be handled strictly in accordance with the procedures set out in the Security Regulations.

8.4 ADDITIONAL REFERENCES

- "Data Center Physical Security Checklist", Sean Heare, The SANS Institute.
  http://www.sans.org/reading_room/whitepapers/awareness/data_center_physical_security_checklist_416
- "Protect Yourself", Justin Bois, The SANS Institute.
  http://www.sans.org/reading_room/whitepapers/physcial/protect_yourself_271
- "An Introduction to Computer Security - Physical and Environmental Security", Special Publication (SP) 800-12, NIST.
  http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter15.html
- "Operational Security Standard on Physical Security", Treasury Board of Canada Secretariat.
  http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=1232

9. ACCESS CONTROL SECURITY

9.1 DATA ACCESS CONTROL

B/Ds should ensure that access rights to information are not granted unless authorised by relevant information owners. Access rights shall be granted on a need-to-know basis and are clearly defined, documented and reviewed. 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 should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life cycle of user access, from the initial registration of new users, password delivery, password reset to the final de-registration of users who no longer require access to information systems and services.

9.1.1 Endpoint Access Control

Data access to end-user device including mobile devices or removable media should be properly controlled. According to different assessed risk levels, B/Ds may consider to apply appropriate measures for protection in the following aspects:

- Control the usage of different ports such as USB, FireWire, Wi-Fi, network, parallel port, serial port, PC Card slot (formerly known as PCMCIA slot), infrared and Bluetooth.
- Enforce and update security policy to all endpoints.
- Identify, control and manage the use of mobile devices and removable media.
- Prevent data copy to any unauthorised mobile devices and removable media.
- Apply data encryption on mobile devices and removable media issued to individuals.
- Provide audit trail information on the usage of mobile devices and removable media.
- Prevent introduction of malware to the corporate network.

9.1.2 Logical Access Control

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:

1. Users/groups of users refer to those people who are registered and identified for accessing the IT resources.
2. People will be granted with rights to access the system resources such as network, files, directories, programs and databases.
3. 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 two of these factors, often called 2-factor authentication, can be applied to strengthen the authentication control.
4. Upon user authentication, authorisation to access will be granted by mapping the user/group of users to the system resources.

9.2 AUTHENTICATION SYSTEM

An authentication mechanism that uniquely identifies users is the basis for security controls. Authentication process begins with identification that requires every user to enter a unique user identity. The person can then use conventional way of authentication by entering a password. Other ways of authentication include use of smart card, token or biometrics technology such as iris, retina, and fingerprint scanning.

Most information systems require the use of authentication system to gain access to the system and its files. Authentication systems can be as simple as allowing users to enter the system without the need of a password, or as complicated as requiring a combination of personal properties like biological recognition systems (e.g. fingerprint, handwriting, voice) and cardkey system such as smart card.

However, many of these authentication mechanisms not only control access to the application, but also facilitate better tracing or auditing of application use. Authentication can be divided into two types: weak or simple authentication mechanisms (e.g. use of passwords), or strong authentication mechanisms where an entity does not reveal any secrets during the authentication process (e.g. use of asymmetric cryptosystems where separate keys are used for encryption and decryption).

Depending on the level of security control required, the simplest way is to use password. Usage of a password checker on the authentication system can be considered to enforce password composition criteria and to improve password selection quality. Another way is to use two-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. A protected system cannot be activated until the user presents a token (something possessed) and a valid password (something known). For some applications, challenge-response scheme may be chosen to generate some information or challenges to the user and request for correct response before allowing log in.

To reduce the possibility of passwords being compromised using brute-force attack, consecutive unsuccessful log-in trials should be controlled. This can be accomplished by

disabling account upon a limited number of unsuccessful log-in attempts. Alternatively, the mechanism of increasing the time delay between each consecutive login attempt could also be considered to prevent password guessing activity.

B/Ds should 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 with 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.

9.3 USER IDENTIFICATION

Identity Management is a combination of processes and technologies to manage and secure access to the information and resources of an organisation while also protecting users' profiles. It includes the entire process of deciding who should get what access to which resources; providing, changing and terminating such access when appropriate; managing the process and monitoring it for compliance with policies.

For authentication, identity management supports the concept of single sign-on in which a user presenting with a single credential can be granted access to authorised data, applications and systems. Since a user essentially only needs to remember one credential for single sign-on, an attacker who can compromise the credential can break-in to all systems authorised to the user.

Therefore, extra security measures are required to protect the credentials when implementing single sign-on. Strong password policy and frequent password changes should be enforced to deter password attacks. Additional authentication methods, such as biometrics or two-factor authentication, could also be considered to strengthen the authentication process. Functions requiring another level of authorisation should implement re-authentication. To prevent illegal system access attempt, if there has been no activity for a predefined period of time, re-authentication should be activated or the logon session or connection should be terminated. Automatic time-out facility such as password protected screen saver should be deployed.

Individual accountability should be established so the respective staff be 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 are prohibited. Any exemption to this requirement must obtain explicit approval from the DITSO with supporting reason. B/D should justify the usage of shared accounts against the security risks that a system may expose to.

If a staff's user-ID/password becomes unusable and he/she requests for a new one, the legitimacy of the user should be confirmed before renewing or re-activating the account.

9.4 PASSWORD MANAGEMENT

A password is 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 should carefully define and document password policy for each category of accounts balancing the security requirements and operational efficiency.

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

9.4.1 Password Selection

It is important to 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 IT security policy.

Some guidelines for password selection are provided below:

DON'Ts

1. Do not use your login name in any form (as-is, reversed, capitalised, doubled, etc.).
2. Do not use your first, middle or last name in any form.
3. Do not use your spouse's or child's name.
4. 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.
5. Do not use a password with the same letter like "aaaaaa".
6. Do not use consecutive letters or numbers like "abcdefgh" or "23456789".
7. Do not use adjacent keys on the keyboard like "qwertyui".

8. Do not use a word that can be found in an English or foreign language dictionary.
9. Do not use a word in reverse that can be found in an English or foreign language dictionary.
10. Do not use a well known abbreviation. This includes abbreviation of B/D name, project name, etc.
11. 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.
12. Do not use a password with fewer than six characters.
13. Do not reuse recently used passwords.

DOs

1. Do use a password with a mix of at least six mixed-case alphabetic characters, numerals and special characters.
2. Do use different passwords for different systems with respect to their different security requirements and value of information assets to be protected.
3. Do use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
4. 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
"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'

9.4.2 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

1. Do not write down your password unless with sufficient protection.
2. Do not tell or give out your passwords even for a very good reason.
3. Do not display your password on the monitor.
4. Do not send your password unencrypted especially via Internet email.
5. 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 to the information contained in these sites.
6. 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).

DOs

1. Do change your password regularly, for example every 90 days.
2. Do change the default or initial password the first time you login.
3. 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.

9.4.3 Password Handling for System/Security Administrators

DON'Ts

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

DOs

1. Do choose good passwords as initial passwords for accounts according to the above password selection criteria.
2. Do use different passwords as initial passwords for different accounts.
3. Do request the user to change the initial password immediately upon receiving the new password.
4. Do change all system or vendor-supplied default passwords, including service accounts after installation of a new system.
5. Do request users to change their passwords periodically.
6. Do encrypt passwords during transmission over un-trusted networks.
7. Do scramble passwords with one-way functions. If possible, do use “salting” to scramble passwords so that same passwords will produce different scrambled outputs.

8. Do deactivate a user account if the logon fails for multiple consecutive times.
9. 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. It is highly recommended that such features be enabled whenever possible.

1. Automatically suspend a user account after a pre-defined number of invalid logon attempts.
2. Restrict a suspended account to only allow reactivation with manual interventions by the system/security administrator.
3. Prevent users from using passwords shorter than a pre-defined length, or re-using previously used passwords.
4. 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.

9.5 MOBILE COMPUTING AND REMOTE ACCESS

9.5.1 Mobile Computing and Communications

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

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

There should also be policy, operational plans and procedures developed and implemented for remote access. B/Ds should only authorise remote access if appropriate security arrangements and controls are in place and complying with the security requirements. Appropriate protection of the remote access should be in place, e.g., physical protection against theft of equipment and information, proper access controls against unauthorised disclosure of information, two-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.

9.5.2 Mobile Device Security

Mobile devices are information systems which are capable of storing and processing information, plus the fact that their physical locations are not fixed and can be carried around easily. Mobile devices often possess networking capabilities, such as wired or wireless network connection, e.g. Wi-Fi, GPRS, 3G, etc.

While mobile devices provide portability and convenience to users, they can introduce new security risks. Users should be aware that mobile devices are susceptible to theft easily. Users should therefore safeguard the devices and not leave them unattended without proper security measures. For instance, users should consider using laptop cable locks to physically secure laptop and portable computers.

Also, as mobile devices often possess network connection capabilities, they can be used to connect to the Government internal networks and can become a point to breach security such as disclosure of classified information and spreading computer viruses and malicious codes into the Government internal network. Users are prohibited from connecting their workstations or devices to external network if these workstations or devices are simultaneously connected to a Government internal networks, unless with the approval from the DITSO.

The following are some management, technical and end-user controls for consideration:

<u>Management and Operational Controls</u>

- Define a usage policy for mobile device to meet the business needs of the B/Ds that includes:
  i. The types of approved mobile devices and the approval mechanism.
  ii. The data classification permitted on each type of mobile device. Classified information must not be stored in privately-owned mobile devices.
  iii. The control mechanism that would be implemented to comply with the SR requirements based on the data classification.
  iv. The procedures to ensure timely sanitisation of government data stored in the mobile devices when staff posts out or ceases to provide services.
- Establish an asset management process for tracking all approved mobile devices. This includes, for example, the procedure of assigning a device to a staff, the inventory control of the device, and the procedure of returning a device when the staff no longer needs it.
- Perform risk assessments prior to deployment of new mobile devices, and implement a continuous risk monitoring program for evaluating changes in or new risks associated with mobile devices.
- Define incident handling procedures for lost or stolen devices, and in particular on the procedure of how to remotely wipe/erase the data stored on these devices.

- Provide security awareness training to staff before they use mobile devices at work. Customise awareness training for security topics related to the risks and policies associated with the approved mobile device and its security components being used.

Technical Controls

- Enable password-protection feature of mobile devices to protect against unauthorised access.
- Encrypt classified data stored in mobile devices in accordance with the Security Regulations requirements.
- Encrypt classified data before transmitting over an un-trusted network (e.g. wireless network) in accordance with the Security Regulations requirements.
- Implement proper security measures, such as enable with anti-virus and malicious code detection and repair mechanism to protect the devices against computer viruses and malicious codes.
- Perform full system scans on mobile devices for malware before connecting them to Government internal networks.
- Install personal firewall software, whenever feasible, to protect from network intrusions.
- Disable unnecessary network services such as Wi-Fi, infrared (IR) ports and Bluetooth when not in use to avoid being detected as attack points.
- Enable authentication, whenever feasible, when connecting to synchronisation software.
- Avoid storing passwords of other systems (e.g. email, ATM card, network login, etc.) on mobile devices without proper security measures.
- Consider using security measures such as biometric user authentication and tamper-proof smart cards to further protect the mobile devices, where applicable.
- Consider deploying a Mobile Device Management (MDM) solution to centrally manage all approved mobile devices to define, enforce and monitor the mobile device policies with the following features:

    i. Configure device settings according to access right of user group, operating system or model of mobile devices.
    ii. Enforce security controls such as access authentication (single or multilevel), inactivity timeout, strong password, storage encryption, or device wipe after specified number of failed login attempts.
    iii. Manage configuration profiles to simplify the provision of new devices and deactivation of devices, and to restrict the devices accessing to the Government internal networks.
    iv. Control installation, configuration, update and removal of mobile applications.
    v. Install and manage protective software (e.g. anti-malware system or firewall) to protect the devices from malicious websites or from attacks coming over other communications channels such as Short Message Service (SMS).
    vi. Disable unnecessary hardware components such as the camera, Wi-Fi, Bluetooth, GPS, and restrict the use of external storage media (e.g. SD cards).

vii. Maintain asset-tracking information such as serial number, inspect applications on devices, and keep track of them for audit.

End-user Controls

- Store the device in a secure place, preferably out-of-sight, when not in use. The physical security of the device is the responsibility of the staff to whom the device has been issued.
- Do not store classified or personal data on mobile device, except the data is protected with appropriate security measures.
- Install only approved applications ("apps") to mobile devices. Properly enable and configure security features of the operating system and installed "apps".
- Only take the minimal amount of data necessary to complete the work when working away from office.
- Erase the data according to the security requirements when the data is no longer required to be stored in mobile device.
- Do not synchronise unauthorised computer resources including those privately-owned (e.g. home computers) with mobile devices storing classified or personal data.
- Do not simultaneously connect to external network when the mobile device is connected to a Government internal network.
- Do not process sensitive data in the mobile devices unless with encryption feature turned on or with end-to-end connection secured.
- Do not open or follow URLs from un-trusted sources, emails, or electronic messages such as SMS/MMS.
- Do not allow wireless connections from unknown or un-trusted sources to mobile devices.
- Do not try to exploit the operating system of the mobile devices by using unauthorised software in order to gain root access (also known as "jailbreaking" or "rooting"). Such manipulation may introduce unexpected security risk and void the warranty.
- Promptly report and escalate if an information security incident occurs (e.g. loss of mobile device) in accordance with the security incident handling procedure.

9.5.3 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.

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. B/Ds should also provide secured channels, for example VPN connections, for users to connect to Government internal networks. Users shall never connect unauthorised computer resources, including those privately-owned to Government internal network unless approved by the Head of B/D for operational necessities.

Usage of remote access software to connect to a departmental server or PC directly is not recommended. This can be a backdoor access by attackers to bypass firewall/router protection to the information system. If there is a business need to use remote access software, proper security controls include logging feature should be in place. The remote access software should be enabled with idle timeout control to avoid unauthorised access.

Remote computers should be properly protected, such as by installation of personal firewall, anti-virus software and malicious code detection and repair measure. All these security features should be activated all the time and with the latest virus signatures and malicious code definitions applied. Besides, latest security patches shall be applied to these remote computers. A full system scan should be performed to detect any computer virus and malicious code in these remote computers before connecting to Government internal network.

To avoid information leakage, users should minimise storing Government information on remote or portable computers. Classified information shall not be stored in privately-owned computer, mobile devices or removable media. TOP SECRET or SECRET information shall not be processed in privately-owned computers or mobile devices. CONFIDENTIAL or RESTRICTED information shall not be processed in privately-owned computers or mobile devices unless authorised by the Head of B/D. All CONFIDENTIAL or RESTRICTED information shall be encrypted when stored in mobile devices or removable media issued to individual officer, authorisation from Head of B/D should be sought for storing CONFIDENTIAL information. 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 saver and never leave the computers unattended.

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

Users should reference the guidelines in Section 8.2 - EQUIPMENT SECURITY when using mobile devices at remote office.

9.5.4 Dial-up Access

Dial-up access is one form of remote access over a public telephone network. Only authorised persons should be allowed with dial-up access. B/Ds should keep an updated inventory of their dial-up access points and modem lines. Dial-up access is advised to be safeguarded by user authentication, and dial-up passwords should be changed regularly. In some cases, two-factor authentication may need to be implemented.

B/Ds should also consider using call-back security feature. With call-back security, the answering modem accepts the incoming call and authenticates the user. Once the user is

authenticated, the modem disconnects the call and then places a call-back to the user using a telephone number in a predefined database. The implementation assists in preventing unauthorised access or use of stolen credential. Although call-back improves security, it is susceptible to compromise by call forwarding and should be used together with other security controls such as two-factor authentication for dial-up connection to sensitive environment.

Access logs should be kept for every dial-up request. At least the following information should be recorded: date, time and duration of access, username, and the connected communication port. The access log should be made available for the inspection when necessary.

9.5.5 Virtual Private Network

Virtual Private Network (VPN) establishes a secure connection over un-trusted network by using a technique called tunnelling. Operating on layer 2 or layer 3's networking protocols, tunnelling encapsulates a message packet within an IP (Internet Protocol) packet for transmission across a network. There are three tunnelling protocols: Internet Protocol Security (IPSEC), Layer 2 Tunnelling Protocol (L2TP) and Point-to-Point Tunnelling Protocol (PPTP).

In addition to traditional layer 2 and layer 3 VPN, SSL-VPN (Secure Sockets Layer Virtual Private Network) is another VPN technology providing the tunnelling protection. In SSL-VPN, the tunnel rides on TLS (Transport Layer Security) communication sessions. SSL-VPN differs from traditional VPN because it can operate without the need of VPN client software while the traditional VPN usually requires client software.

Setup of VPN is considered to be a viable solution to establish secure communication channel for users to work outside office. Before implementing VPN, B/Ds should evaluate compatibility with the existing network and consider implementing the following VPN security guidelines:

- Authenticate with either one-time password authentication such as a token device or public/private key system with a strong passphrase.
- Disconnect automatically from Government internal network after a pre-defined period of inactivity. The user must then logon again to reconnect to the network.
- Disallow dual (split) tunnelling. Only one network connection is allowed.
- Protect all computers or devices connected to Government internal networks via VPN with personal firewall, latest security patches, anti-virus and malicious code detection and recovery software. All these security measures should be activated all the time and with the latest virus signatures and malicious code definitions.
- Seek approval from the Head of B/D before using privately-owned computer resources to access Government internal network or information assets. The usage of these computer resources shall comply with Government IT security requirements.

- Provide logging and auditing functions to record network connection, especially for failed access attempt. The log should be reviewed regularly to identify any suspicious activities.
- Remind users with VPN privileges that they are accountable for the proper use of the account, ensuring that unauthorised users cannot use the account to access Government internal networks.
- Educate LAN/system administrator, supporting staff as well as remote users to ensure that they follow the security best practices and policies during the implementation and usage of VPN.
- Install gateway-level firewalls to control network traffic from VPN clients to authorised information systems or servers.

9.6 ADDITIONAL REFERENCES

- "Information on Role Based Access Control (RBAC)", the National Institute of Standards and Technology (NIST) of the U.S. Department of Energy. http://csrc.nist.gov/groups/SNS/rbac
- "Authentication", related articles from The SANS Institute http://www.sans.org/reading_room/whitepapers/authentication/
- "Logging Technology and Techniques", related articles from The SANS Institute http://www.sans.org/reading_room/whitepapers/logging/

10. DATA SECURITY

Access to application and data, especially classified data, should be restricted to those who are authenticated and authorised to access. Proper protective measures such as access control and encryption should be adopted to ensure the confidentiality of the data. Backup and recovery of data shall be carefully planned to ensure the availability and integrity of the data and software when corruption occurs. Other measures like audit trail and network protection should also be adopted. The following are examples on protection mechanism:

Threat	**Protection System Examples**
Unauthorised access of the application or data.	Encrypted password system, magnetic cardkey system, challenge and response system, digital signature, file permission, access control, restricted access to backup data, audit log, or a combination of these.
Unauthorised access of the workstation or terminal.	Keyboard lock, screen saver with password protection, bootup password and proper access control.
Unauthorised access of mobile devices or removable media.	System with encryption capability, proper access control, and safe custody.
Disclosure of information on screen.	User profiles and views, screen saver with password protection, proper positioning of the display screen, timer to disconnect.
Disclosure of information on transmission.	Use network that are “secured”, use challenge and response system on password and encryption system on data.
No service due to server failure.	Tape backup system, mirror disk, redundant array of independent disks (RAID) system, server backup system, hot standby system.
No service due to communication link failure.	Multiple communication paths.
Spoofing of origin (someone sends the message in others name).	Multiple authentication mechanism, digital signature.
Spoofing of delivery (someone sends the message but denies afterwards or someone makeup the message which he did not send).	Transaction log, message time stamp, digital signature.
Spoofing of receipt (someone pretends he has not read the message in which he actually did).	Multiple authentication mechanism, transaction log, message send/read time stamp, return receipt.

Security usually means trade-offs in user friendliness, simplicity, flexibility, investment on time, effort and cost and ability to recover the information when keys are not available or not provided. User should be explicitly notified of such implication during the implementation of the IT security measures.

10.1 OVERALL DATA CONFIDENTIALITY

Before determining security measures, the data to be protected need to be identified and classified. For instance, data which worth money or which, if lost, can cause interruptions to the daily operation. How data should be classified depends on their level of sensitivity. In Government of Hong Kong Special Administrative Region, sensitive data are classified to following four categories according to the requirements of the Security Regulations:

- TOP SECRET
- SECRET
- CONFIDENTIAL
- RESTRICTED

The controls of classified documents are detailed in Chapter IV of the same document.

Chapter IX of the Security Regulations defines regulations related to, but not limited to, storage, transmission, processing and destruction of classified data. Essentially, 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.

In accordance with Security Regulations 161(d)(iii), all personal data should be classified RESTRICTED at least, depending on the nature and sensitivity of the personal data concerned and the harm that could result from unauthorised or accidental access, processing, erasure or other use of the personal data, a higher classification and appropriate security measures may be required. B/Ds shall ensure compliance with the Personal Data (Privacy) Ordinance, particularly the Data Protection Principle 4 (on security of personal data), when handling personal data. Appropriate security measures should be adopted to protect personal data from unauthorised or accidental access, processing, erasure or other use. For details of six Data Protection Principles, please refer to

Principles 1 to 3 at http://www.pcpd.org.hk/english/ordinance/section_76.html; and

Principles 4 to 6 at http://www.pcpd.org.hk/english/ordinance/section_77.html.

Information without any security classification should also be protected from unintentional disclosure. 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.

The key requirements in Chapter IX of the Security Regulations in regards to data handling are summarised in the following table:

Security Requirement	TOP SECRET / SECRET	CONFIDENTIAL	RESTRICTED
Encryption in storage	Mandatory	Mandatory	Recommended (Mandatory in mobile device / removable media issued to individual officer)
Shared access	Prohibited (unless authorised)	Prohibited (unless authorised)	Allowed
Shared access tracking	Audit trail and Logical access control software	Audit trail and Logical access control software	Recommended
Encryption in transmission over trusted network	Mandatory and only inside an isolated LAN	Recommended	Recommended
Encryption in transmission over un-trusted* network	Transmission prohibited	Mandatory	Mandatory
Email system for transmission		Information system approved by the Government Security Officer subject to the technical endorsement of OGCIO. Approved email system: - Confidential Mail System (CMS)	Information system approved by the Government Security Officer subject to the technical endorsement of OGCIO. Approved email system: (i) GCN with encryption feature enabled (ii) System with PKI encryption or with encryption methods as specified in the SR
Processing	Only on Information system complied with SR356	Only on Information system complied with SR363	Only on Information system complied with SR367
Computer room requirement	Level III	Level II	Locked room / cabinet

Remarks:

"*": For definition and examples of un-trusted network, please refer to Section 12.2.2 Transmission of Classified Information.

The above regulations should also be applied to interim material and information produced in the course of processing. Also, all sensitive 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 should bear the same classification as they would be for the paper equivalent and they should be protected accordingly as stated in the Security Regulations.

B/Ds shall advise their business partners, contractors, or outsourced staff to comply with the guidance in the Security Regulations in storing, processing and transmitting data owned by Government.

10.2 DATA LIFE CYCLE MANAGEMENT

Data life cycle management is a policy and procedure based approach to managing data throughout its life cycle: from creation and initial storage to the time when it becomes obsolete and is destroyed. It aims to provide framework for data management and provide cost effective solution for risk mitigation, and to reduce the risk of data loss or leakage. The life cycle includes six phases, namely create, store, use, share, archive and destroy. Appropriate procedures and practices should be deployed to properly protect the data at different phases.

Create: It applies to creating or changing a data or content element. Creation is the generation of new digital content or the alteration/updating of existing content, either structured or unstructured. In this stage the information should be classified and appropriate security measures should be determined.

Store: It refers to the act of committing data to structured or unstructured storage, such as database or files. Appropriate security controls, including access controls, encryption and rights management, commensurate with the classification of the data should be applied to managing content in storage repositories.

Use: It refers to the stage when the user is interacting with the data. Security controls should be deployed to ensure the access of data in a manner that conform to Government security requirements. Data access and usage activities should be properly monitored, and if possible with preventive measures to alert/stop policy violations.

Share: It refers to the stage when exchanging data with users or external parties. Secure sharing of data should be ensured by deploying appropriate encryption technology. A mix of detective and preventative measures, such as by deploying Data Leakage Prevention (DLP) or Content Management Framework solutions, should be considered to monitor

communications and block policy violations, in addition to monitor the activities related to data exchange.

Archive: It is a process of transferring data from active use into long-term storage. A combination of encryption and asset management should be used to protect the data and ensure its availability.

Destroy: When the data is no longer needed, it should be permanently destructed. Verification should be done to ensure the data in all active storage or archives has been destructed. Common techniques include shredding, disk/free space wiping or physical destruction.

Following are some of the security requirements for handling or using data in connection with a data life cycle:

Phases of Data Life Cycle	Security Requirements
Create	• Assign proper data classification to the data. • Specify necessary security measures for the data, commensurate with the data classification as well as other contractual or legal requirements. • Determine whether classification marking is needed. • Determine the retention period for the data.
Store	• Do not store classified information in privately-owned computer resources. • Encrypt classified information during storage, even for RESTRICTED information when stored in mobile devices or removable media issued to individual officer.
Use/Share	• Apply need-to-know and least privilege principles when need to access the data. • Encrypt classified information when transmitted over un-trusted network. • Track all activities in relation to share access of CONFIDENTIAL or above information by audit trail and logical access control software.
Archive	• Apply same security controls as “Store”, when putting classified information into archives. • Maintain a record of repositories where classified information being stored.
Destroy	• Perform proper data sanitisation / disposal on devices storing classified data.

10.3 INTEGRITY OF DATA

The source, destination and processes applied to the information must be assured. Untrustworthy software should not be used or held on computers or servers. Time stamps or sequence numbers may be employed to ensure the completeness of data or processing. Parity checks or control totals should be used to guard against errors in transmission.

To avoid data tampering during transmission, some cryptographic algorithms can be applied. Hashing technology can also be used to assure data integrity. Examples are digital signatures. A digital signature is a data structure which is generated by using some hashing algorithm associated with the public key algorithm. A digital signature is created using a private key and only the corresponding public key can be used to verify that signature was really generated by the private key. Examples of hashing algorithms are Secure Hash Algorithm[3] (SHA) and the Digital Signature Algorithm (DSA).

Papers analysing MD5 (Message Digest 5) have been published and revealed the weaknesses of MD5. Therefore, MD5 should not be used in new systems and MD5 in the existing systems should be replaced by stronger hashing algorithms, e.g. SHA-2.

10.4 STORAGE NETWORK SECURITY

Traditionally, all storage devices are directly attached to the computer that uses it. However, technologies like storage networks are growing popular. There are two major technologies in storage networks – storage area network (SAN) and network attached storage (NAS).

SAN is considered as a hard drive of a server computer. The SAN device is subject to the security requirements in accordance with the highest classification level of data the SAN device contains. If the SAN storage is attached to the server using network protocol (e.g. Gigabit Ethernet, SCSI over IP) in channel other than fibre channel, data transmission shall follow the same security requirements of SR according to the data classification.

Whereas, NAS can be considered as a server which shares files over a network using file sharing protocol, such as NFS (Network File System) or SMB/CIFS (Server Message Block/Common Internet File System). The NAS is usually attached with a local hard drive, or SAN for data storage. Again, the NAS server is subject to the security requirements in accordance with the highest classification level of data the NAS server contains.

Security guidance for storage network security includes, but not limited to the following:

- Change default passwords of storage devices.

[3] There are studies that mathematical weakness may exist in SHA-1, more secure algorithm such as SHA-2 (in particular the SHA-256) should be considered as far as practicable.

- Do not plug storage management interface into un-trusted networks.
- Protect the management interface of the storage devices so that only authorised staff can manage the devices from specific locations.
- Use segmentation or authentication for management access.
- Enforce strict access control on the file systems of the storage devices in the storage network.
- Use 'zoning' to enforce access control of all communication.
- Use 'LUN masking' to hide LUNs (Logical Unit Number) from specific servers.
- Secure any system connected to the storage network.

10.5 USER PROFILES AND VIEWS

In addition to user identification and authentication mechanisms, most database management systems also allow users to be classified such that individual users may be enabled to merely access data, or to perform a certain limited function. This permission can be given with respect to a whole database, or even to selected fields of a database.

Granularity of access is added to database access control by the use of logical "views" so that the user views only the part of the database he/she is authorised to access.

User profiles should be well protected and should not be accessed by unauthorised persons.

10.6 DATA ENCRYPTION

Encryption techniques are used to protect the data and enforce confidentiality during transmission and storage. Many schemes exist for 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 (e.g. word processor) password-protection feature is to provide protection on the file and prevent unauthorised access. Users should encrypt the file instead of using only password in order to protect the sensitive information as appropriate. When password is used, it is also important to follow the practices in password selection and handling described in Section 9.4 PASSWORD MANAGEMENT.

B/Ds shall comply with the requirements in Chapter IX of the Security Regulations to handle classified data. Please refer to Section 10.1 OVERALL DATA CONFIDENTIALITY for the summary of requirements for data handling.

Besides, user passwords that are used for authentication or administration should be hashed or encrypted in storage. If encryption is used, keys used for performing encryption (symmetric key only) or decryption must be kept secret and should not be disclosed to unauthorised users.

10.6.1 Cryptographic Key Management

The term 'key' here refers to a code that is used in respect of classified information for authentication, decryption or generation of a digital signature as defined in the SR350(c). This code is usually generated by mathematical algorithms. These kinds of algorithms are often called "cryptographic algorithms". These generated keys are called "cryptographic keys".

In accordance with the SR371, 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, or 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:

- 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.
- Key recovery
  - Assess the need on having 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.
- Key backup
  - The cryptographic key should be backed up with proper protection.
  - A documented process should be established to access the backed up keys.
- Key transfer
  - Cryptographic keys should never be transported together with the data or media.
- 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.

10.6.2 Encryption Tools

B/Ds should refer to the guidelines of Security Regulations to select encryption tools for their information systems. In some countries, the encryption software and hardware requires exporting licence or approval. The selection and use of encryption software or

hardware shall be considered carefully to avoid breaking these foreign regulations. Care shall be taken in selecting software programs or utilities such as the mailing system which may adopt different encryption algorithms. Nevertheless, the choice of encryption tools shall meet the requirements of Security Regulations; if acquisition of particular encryption tools may break the foreign regulations, B/D should seek alternatives to acquire similar encryption tools.

But there are trade-offs in using encryption including user friendliness of the application, simplicity of the application, performance of the application, the cost of the application, the time and effort spent on the application, and the ability to reveal the information in case the key is not available or provided.

Depending on the purpose of the encryption, there are products designed for encryption only while others support encryption and digital signature. Some are more suitable for encrypting documents for storage and some are better for transmission than others. B/D may consider the following during the selection of encryption products

- Encryption algorithms and key lengths supported.
- Operation requirements.
- Handling of temporary files.
- Ease of deployment.
- Ease of use.
- Key management and recovery.
- Future needs of access to the information by other staff.

Related information can be found in the Annex F of the Security Regulations for the recommended minimum encryption key length to be used.

10.7 SECURE PRINTING

Hardcopies are often found in the printing device's output tray unprotected, leaving unattended printed documents susceptible to unauthorised access. An uncontrolled printing environment may introduce risk to confidentiality of classified documents. B/Ds should take practical precautions to protect documents which are printed, scanned, copied or faxed.

Secure printing is to ensure that (a) printing devices are secured; and (b) printed or transmitted data meets the confidentiality, integrity and availability requirements. Following practices should be adopted to secure the documents when using such devices:

- Physically secure the printing device. In particular, prevent unauthorised access to the storage device, e.g. hard drive, if any.
- The global configuration should be protected from unauthorised access. It should be modified via the console by requiring a strong password.

- Limit print/copy/fax/scan services to required protocols. Disable all unnecessary protocols/services.
- Require user authentication for printing classified documents, if available.
- Enable available security features on the device. For example, configure the device to remove spooled files and other temporary data using a secure overwrite, or encrypt the disk for data processing.
- Follow requirements as stipulated in SR if the embedded storage will be used for processing classified information.
- Assign a static IP address for the device.
- Change all default password or Simple Network Management Protocol (SNMP) strings. Whenever possible, use SNMP v3.
- Only allow trusted hosts to manage the device. Disable unsecure protocols such as Telnet, File Transfer Protocol (FTP), Dynamic Host Configuration Protocol (DHCP), Hypertext Transfer Protocol (HTTP). Use Hypertext Transfer Protocol Secure (HTTPS) if remote management is needed.
- Enable secure network protocols and services (e.g. IPsec or Secure Internet Printing Protocol (IPP)) whenever possible to prevent unauthorised network interception.
- Access to file shares should be appropriately controlled (e.g. by password protection).
- Firmware should be upgraded as recommended by the manufacturer or support vendor.
- Enable audit logging and review the logs regularly, if available.

10.8 DATA BACKUP AND RECOVERY

A good backup strategy is essential for data security. File system backups not only protect data in the event of hardware failure or accidental deletions, but also protect information systems against unauthorised changes made by an intruder. With a daily copy of data backup, it would be easier to revert to the last secured state of information systems prior to the changes or modifications an intruder has made.

Backups, especially if run daily, can also be useful in providing a history of an intruder's activities. Looking through old backups can provide footprints when the system was first penetrated. Intruders may leave files around which, although deleted later, are captured on the backup media.

10.8.1 General Data Backup Guideline

- Backup copies should be maintained for all operational data to enable reconstruction should they be inadvertently destroyed or lost.
- The backup copies should 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 should be well established. Wherever possible, their effectiveness in real-life situations should be tested thoroughly.

- 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 the 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 period as required.
- Magnetic tapes, magnetic/optical disks or cartridges used for backup should be tested periodically to ensure that they could 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 operation convenience and the availability of backup data, especially for mission critical information.

10.8.2 Devices and Media for Data Backup

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. Tape magazine or automatic tape changer may also be used if the data volume is very large that spans multiple tapes in one backup session. To take advantage of tape changers, your backup software must have tape changer option to support them.

For workstation backup, many devices are available as the amount of data that requires to be backed up will be generally lesser 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.

Regular cleaning of tape drive's head is required. 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 user to clean its head after certain number of runs. Documentation of tape drive should be referred for more information.

Proper storage and maintenance of backup media are also important. The media should be properly labelled and placed in their protective boxes with the write-protect tab, if any, in the write-protect position. Keep them away from magnetic/electromagnetic fields and heat sources and follow the manufacturer's specifications for storage environment.

10.8.3 Server Backup

Local server tape drive backup is recommended over backing up of multiple servers through the network as backing up through the network will be much slower and time consuming if the amount of data is very large.

It would be better to use the differential[4] backup during night time on week days and use full backup on Saturday night, when no one will be accessing the server.

The following is a suggested labelling standard for backup tapes and the use of four sets of backup tapes is suggested:

Format**:**	**<File Server>_X_Day_N**
where	
<File Server>	= name of the file server (e.g. ITSX001)
X	= F / D (Full / Daily)
Day	= Mon / Tue / Wed / Thu / Fri / Sat
N	= backup set no.(1 / 2 / 3 / 4)
Example:	ITSX001_D_Tue_1

[4] Most backup software products on the market support both incremental backup and differential backup. Incremental backup means only the files modified since the previous full or incremental backup will be backed up. Differential backup means all the files modified since the previous full backup will be backed up (i.e. files backed up in the previous differential backup will also be included in the following differential backup).

Differential backup is highly recommended even though it may use more backup media because it is easier to rebuild the file server based on one full backup plus the latest differential backup.

In this case, 24 unattended backup schedules need to be created. This means that the LAN/system administrator will just have to mount the tape (write enabled) before leaving the office for the day, and check that the backup runs are successful on the following working day.

With automatic tape changers with adequate slots, manual mounting of tapes can be less frequent, say once a week. The LAN/system administrator should check the logs of the backup runs daily to ensure that everything is running fine.

There may be a need to keep a tape for each month or any special occasion in a safe when documents need to be deleted every month.

If the time required for backing up the server is too long that exceeds the site's allowable backup time frame, data on the production server to be backed up can be copied to a dedicated backup server and let the backup task run on the dedicated server. However, the security level of this dedicated backup server should be retained as the same of the production server to avoid any potential security breach or unauthorised access.

Server backup software is operating system version specific. Most backup software products also provide disaster recovery option for faster and more reliable system recovery.

10.8.4 Workstation Backup

There are many ways to back up a workstation, common options include:

a. Backup using local backup device

Workstation data can be backed up as frequent as required. Users can take the active role for backing up their data. Or a scheduler can be used to back up the data to local backup device (e.g. tape drive) at regular intervals.

b. Backup using workstation backup agent and central network backup

Most server backup software products provide the function to back up data that reside on connected workstations. Workstation data can be backed up to the server backup device following the client backup schedule defined by the LAN administrator. This can be done without interruption to user after office hours or lunch time, but the workstation will have to leave powered on during the backup.

c. Backup using central network backup with vital data copied to server

Workstation data can be copied to a server and the server will be backed up according to its regular backup schedule. Users can take the active role for copying their data to the server. Or a scheduler can be used to copy data to the server at regular intervals to match with the backup schedule on the server.

10.9 INFORMATION ERASURE

All classified and personal data must be erased before the media, computer equipment and electronic office equipment are to be reused, transferred or disposed. This includes equipment that may have storage media embedded as auxiliary devices whose existence may not be readily apparent to the users, including multi-function printers and photocopiers. Typical examples of erasure include degaussing or overwriting disks and tapes. Destruction or erasure of information resource must comply with the Security Regulations.

The Security Regulations provide clear guidelines and requirements on the classification and handling of government information. B/D should refer to SR377 and SR378 with regard to destruction of classified information stored in information systems. All classified information stored in information systems shall be completely cleared from the storage media before disposal or re-use. If for any reason this is not feasible, or the media contains damaged or unusable tracks and sectors which may inhibit the overwriting process, or overwriting is not possible (e.g. optical disk) or inadequate (e.g. magnetic tape, floppy disk), the media unit must be physically destroyed to prevent the recovery of the classified information.

Degaussing (demagnetising) reduces the magnetic flux of the magnetic media to virtual zero by applying a reverse magnetising field. Degaussing hard drives often destroys the drive's timing tracks and disk drive motor. Therefore, hard drives cannot be reused after degaussing. Below are major considerations regarding the use of degaussing:

- The resistance of a magnetic media to demagnetisation is the coercivity of the magnetic media and is measured in Oersteds. In order to completely erase the content on the magnetic media (e.g. hard drive), the degausser should produce a magnetic field, recommended to be at least 1.5 times, higher than the coercivity of the media.
- For degaussing hard drives with very high coercivity ratings, it may be necessary to remove the magnetic platters from the hard drive’s housing.
- Besides, the degausser should also be periodically tested accordingly to manufacturer's directions to ensure that it functions properly.
- If the degaussing process is outsourced, it should be ensured that comparable arrangements are in place to ensure that the same protections as above are provided.

During the degaussing process, the degaussers have to be operated at their full magnetic field strength. The product manufacturer’s directions must be followed carefully since deviations from an approved method could leave significant portions of data remaining on the magnetic media.

A normal “delete” command merely prevents further file access by deleting the pointer to the file in an electronic storage medium; the content of the file is not actually cleared or erased. Even a general disk formatting operation is not capable of completely erasing the data to an extent which prevents data recovery.

In order to comply with the SR requirements, appropriate tools should be used to overwrite the storage area where the classified information was originally stored in the media. Commercial software for such secure deletion 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. For flash-based solid state disks or USB flash drive, due to its different internal architecture, completely overwriting a particular file may not be feasible; it is suggested to sanitise the whole disk instead of individual file to ensure complete erasure of information.

A system of checks and balances should be maintained to verify the successful completion of the secure deletion process. Sample check of the erased media should be performed by another party to ensure all classified information was properly erased.

To support government computer users to comply with the SR requirements, OGCIO has set out the technical standards required regarding the destruction of classified information under the SR. For information about the requirements and technical controls for disposing classified information, please refer to Annex F of the Security Regulations.

While there is no specific regulation on the disposal of unclassified information, as a good practice to protect data privacy, users are advised to adopt similar erasure procedures for RESTRICTED or CONFIDENTIAL 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 if it is not erased properly.

10.10 ADDITIONAL REFERENCES

- "Backup Strategies", related articles from The SANS Institute. http://www.sans.org/reading_room/whitepapers/backup/
- "Encryption and VPNs", The SANS Institute. http://www.sans.org/reading_room/whitepapers/vpns/
- "Information Lifecycle Management", Cloud-Security Alliance. https://wiki.cloudsecurityalliance.org/guidance/index.php/Information_Lifecycle_Management
- "Information-centric Security", Securosis. https://securosis.com/tag/information-centric+security

11. APPLICATION SECURITY

Good application design not only provides workable solutions to users' problems but also provides a secured 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 of the system and the sensitivity of the data it is dealing with.

Security measures related to data, like password mechanisms, audit trails and data backup and recovery, have been discussed in Section 10 - DATA SECURITY. This section mainly discusses security issues related to application/system development and maintenance. The following topics will be covered in this section:

- System specification and design control
- Programming standard and control
- Program/system testing
- Change management and control
- Web application security
- Mobile application security

11.1 SYSTEM SPECIFICATION AND DESIGN CONTROL

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

- Ensure that the system designed complies with acceptable accounting policies, accounting and application controls, and with all appropriate legislative measures.
- 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.
- Review the system design with the user for checking out if there are any loopholes in maintaining the integrity of information. The user should be encouraged to suggest corrective measures on any deficiency detected.
- Evaluate with the users on 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 contingency plan, please refer to Section 7.3 - CONTINGENCY MANAGEMENT.
- Evaluate with the users 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 are allowed to access

  - The way that each grade of staff in the user department are 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
- Conduct privacy impact assessment if the system has significant privacy implications. The Privacy Commissioner for Personal Data has published an information leaflet on privacy impact assessment, which is available at http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.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:

- Document the security architecture.
- 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.
- Document security related programming activities.
- Conduct code review, if necessary.

11.1.1 Security Considerations in Application Design and Development

Listed below are some security principles for reference 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.
- ***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 the minimum and authorised by the application owner.
- ***Secure the weakest link.*** Ensure that proper security protections are in place in all areas to avoid attackers from penetrating through loophole caused by 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 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 meaningful error message that is helpful to the user or the support staff yet ensuring that no sensitive 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 contents 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 sensitive or personal data is encrypted in storage or during transmission. Mask the sensitive 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.

11.2 PROGRAMMING STANDARD AND CONTROL

11.2.1 Programming Standard Establishment

The programming controls to be enforced must 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 standard.
- 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.

11.2.2 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 into the system, because he does not have control over the other units of program. He has to work in collusion with others in order to be successful.
- The division of program into smaller units also increases the opportunity for detecting programming fraud. The units can be analysed and reviewed in much greater detail.

When reviewing each unit of a program, the one responsible should ensure that:

- Programming standards are observed.
- Controls specified in the program specification have been incorporated.
- The program meets the technical design as well as security requirements, and that there is no hard-to-follow, suspicious and unexplained code in the unit.

11.3 PROGRAM/SYSTEM TESTING

The need for comprehensive program/system testing is obvious. Therefore, this section will only focus on areas that need to be observed in order to increase the reliability and security of the program/system in concern.

Firstly, the user department should carry out user acceptance test in which they are responsible for preparing the test plan and test data. Test data should be selected, protected, and controlled commensurate with its classification carefully. All sensitive content contained in the test data should be removed or modified beyond recognition before use. The user department should 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 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. 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. 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. Regression test is 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 application of the transactions, which are then used for system testing. Whenever the system is changed, the same files are used for rerun and the two sets of outputs are compared. The amendment would only be accepted if no discrepancy is identified.

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, control mechanism should be in place.

Production data shall not be used for testing purposes. The use of operational databases containing personal or sensitive information for testing purposes should be avoided. If this

cannot be avoided, proper approval should be obtained. The following controls should be applied:

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

11.4 CHANGE MANAGEMENT AND CONTROL

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

11.4.1 Program/System Change Control

The objectives of maintaining program/system change controls are:

- To maintain 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, tested and reviewed to ensure that the system can be effectively protected from attacks or being compromised. 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 must go through a single coordinator. Operational and administrative procedures as well as audit trail, if applicable, should also be updated to reflect the changes made.

11.4.2 Program Cataloguing

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. On completion of the amendments, the project team should request the control unit to catalogue the program into 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 program or system should be performed before production rollout. The hardened program/system should then be used as baseline for any further changes.

11.4.3 Installation of Computer Equipment and Software

Installation of computer equipment and software should only be done by authorised staff, after obtaining approval from the system owner or the responsible manager. Equipment or software should 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.

11.5 WEB APPLICATION SECURITY

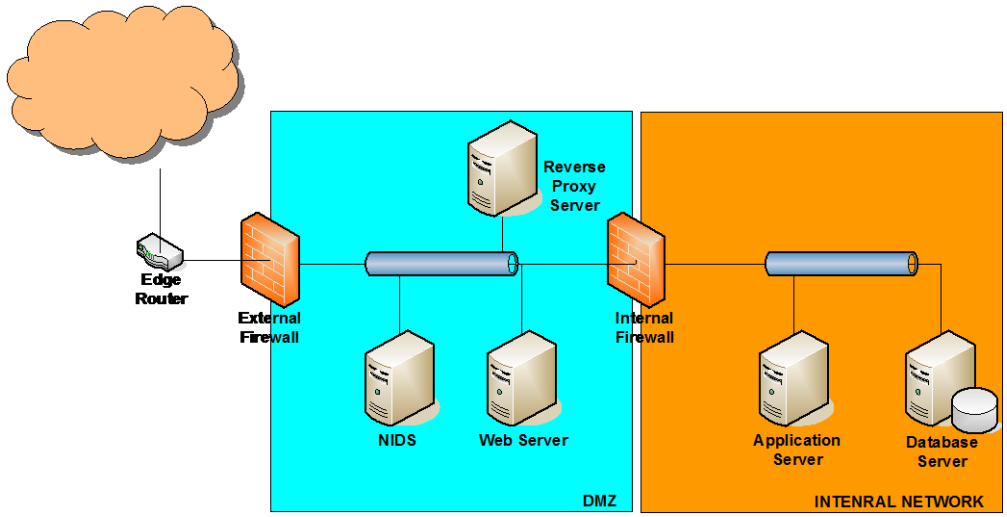
Web application is commonly used to provide services to the public and to the Government staff nowadays. Web 2.0 applications such as Wiki also create a platform for effective knowledge sharing and contribution. Although web application provides convenience and efficiency, it is faced with many security threats because the client access can be from anywhere over the Internet.

The threats originate from the untrustworthy client, session-less protocols, complexity of web technologies, and network-layer insecurity. In web application, the client software usually cannot be controlled by the application owner. Therefore, input from the client software cannot be completely trusted and processed directly as an attacker can forge as a legitimate client, masquerade a user identity, create fraudulent message and cookies, or include links of malicious sites. Besides, HTTP is a session-less protocol. It is susceptible to replay and injection attacks. Messages in HTTP can easily be modified, spoofed and sniffed.

Because of the complexity of web technologies, conducting a detailed security analysis is not easy and straightforward. Therefore, web application should be designed properly to mitigate the security risks. The following sections describe the web application security reference architecture, web server software security guidelines, web application development process and web application secure coding best practices.

11.5.1 Web Application Security Architecture

A typical web application architecture contains 3 tiers, separating an external facing web server, application server, and database server as shown in the diagram below. With such a tier-based architecture, even if an attacker compromises the external facing web server from outside, the attacker still has to find ways to attack the internal network.



The external facing web server should be confined within a demilitarised zone (DMZ) which is a special network segment containing servers with access to Internet services. Servers with sensitive information are located in the internal network with additional protection. The internal and external firewalls should be from different vendors or types so that the firewalls will not have the same vulnerability. For example, the external firewall can be a web application firewall while the internal firewall can be a network layer stateful inspection firewall.

Network intrusion detection system (NIDS)/intrusion prevention system (NIPS) should be installed to detect/prevent attacks or suspicious traffic in the DMZ. Alerts and reports from the NIDS/NIPS should be actively reviewed to identify attacks at the earliest possible moments. In addition, NIDS/NIPS should always be updated with latest attack signatures provided by the vendor.

Reverse proxy server may be considered. It acts as a single point to provide all web applications services to the users. Details such as the actual number and platform of the web or application servers are hidden from users. This provides additional security controls because the reverse proxy server can perform checks against security attacks at a centralised location. However, reverse proxy server is not easily scalable.

For web application servers which only serve internal users and have no connection to external network, since the level of external threats are limited, B/Ds may consider implementing fewer security protection measures such as implementing just one layer of firewall to segregate the web server from internal users. B/Ds are recommended to perform security risk assessment in order to determine the most appropriate security protection measures.

11.5.2 Web Server Security

The following guidance should be observed in enhancing the security of the web servers:

- Configure web server securely according to the vendor's security guidelines.
- Run web server processes with appropriate privilege account. Avoid running the web server processes using privileged accounts (e.g. 'root', 'SYSTEM', 'Administrator').
- Apply latest security patches to the web server software.
- Configure access rights such that the web server software cannot modify files serving the users. In other words, the web server software should have read-only access rights to those files.
- Disable all unused accounts, including user and default accounts.
- It is common for web application to store the hash value of users' password in database or file, however, a successful SQL injection attack or leaking of password file may yield easily crackable passwords. The hashing of password should be used with a secret salt to protect against dictionary attack or pre-computed lookup table (i.e. a rainbow table) of hashed values.
- Install host-based intrusion detection system (HIDS)/intrusion prevention system (HIPS) in web servers storing or processing sensitive information to monitor suspicious activities or unauthorised creation / deletion / modification / access of files. Alerts and reports from the HIDS/HIPS should be actively reviewed to identify security attacks at the earliest possible moment. In addition, HIDS/HIPS should always be updated with latest signatures provided by the vendor, if appropriate.
- Configure web server software to prevent leaking information like web server software version, internal IP address, directory structure, etc.
- Disable or remove unnecessary modules, and default or sample files from the web server software.
- Restrict web crawling for the contents which are not supposed to be searched or archived by public search engines.
- Identify application files on the web server and protect them with access control.
- Backup the private key for the server certification and protect it against unauthorised access when using SSL.

11.5.3 Web Application Development Process

The security controls of web application should be analysed and defined during early stage of the software development with the following considerations:

- Follow the security guidance of general application design and development in Section 11.1.1 - Security Considerations in Application Design and Development.
- Ensure that security requirements are well defined and prioritised for the web applications.

- Perform IT security risk assessment for critical systems during design and implementation stages.
- Define and adopt secure coding practices to avoid application defects introduced during development stage.
- Perform source code review to identify security bugs overlooked during development stage. It may focus on input validation, information leakage, improper error handling, object reference, resource usages, and weak session management.
- Perform functional security test to ensure that web application behaves as specified in the security requirements (such as control-flow/data-flow test). Similarly, perform risk-based test to ensure that common mistakes and suspected software weaknesses (such as cross-site scripting, SQL injection and buffer overflow) are mitigated.
- Include security controls in the system integration testing and user acceptance test.
- Prepare a security and quality assurance plan and adopt assurance methods such as code review, penetration testing, user acceptance tests, etc.
- Perform IT security audit before production launch and after major changes to the system.
- Review application log regularly.
- Maintain version control and separate environment for development and production at the maintenance and support stage.

11.5.4 Web Application Secure Coding

The security considerations and principles of a general application design and development described in Section 11.1.1 - Security Considerations in Application Design and Development also apply to web application development. But since web applications are subject to additional security threats as described in Section 11.5 - WEB APPLICATION SECURITY, the software development team should follow a set of web application secure coding practices that can help withstand common web application security vulnerabilities. Listed below are some secure coding practices to be observed when developing web application:

- Validate all input parameters to prevent attacks such as SQL injection and cross-site scripting attacks
  - Develop a centralised module to perform the input parameter validation.
  - Check each input parameter against a strict format (i.e. whitelist) that specifies exactly which types, length, and syntax of input will be allowed.
  - Filter special characters such as “~!#$%^&*[]<>’\r\n” from the input form, or replace them with escape sequence.
  - Do not rely exclusively on blacklist validation to detect malicious input.
  - Do not rely on client side script to perform the validation check. It should also be done at the server side.
  - Do not pass the HTML forms parameters directly to system call or database query.
  - Do not display the HTML forms parameters directly in the processing response.

- Sanitise application response
  - Develop a centralised module to perform the sanitisation.
  - Check all output, return codes and error codes from calls (e.g. calls to backend database) to ensure that the expected processing actually occurred.
  - Do not reveal sensitive information such as credit card number, HKID, personal telephone/mobile number, credentials and other sensitive information without proper control, e.g. masking.
  - Do not include comments about application logic in the HTML response.
  - Do not include unnecessary internal system information like internal IP address, internal host name, internal directory structure, etc. in the response.
  - Do not include verbose error messages of internal server errors (such as debug information, stack traces) to avoid exposing information to attackers. Most application/web server allows customisation of an error page in case of internal server error.
- HTTP trust issues
  - Do not trust and rely on HTTP REFERER headers, form fields or cookies to make security decisions as any of this data can be spoofed.
  - Do not trust these parameters from the client browser unless strong cryptographic technique is used to verify the integrity of the HTTP headers.
  - Do not pass HTTP header's parameters directly to system call or database query.
  - Do not display HTTP header's parameters directly in the processing response.
  - Do not assume hidden parameters cannot be changed by users as hidden parameters can be manipulated easily by attackers.
- Keep sensitive session values on servers to prevent client-side modification
  - Do not put sensitive information in any client browser's cookies.
  - Use strong cryptographic techniques to protect the confidentiality and integrity of the data, if sensitive values have to be stored in client browsers.
- Encrypt pages with sensitive information and prevent caching
  - Encrypt pages containing sensitive information with proper algorithms and keys during transmission; e.g. SSL, TLS.
  - Use signed Java applet or ActiveX to acquire and display sensitive information.
  - Set the appropriate HTTP header attributes to prevent caching, by browser or proxy, of an individual page wherein the page contains sensitive information.
- Session management
  - Use a session ID that is long, complicated, and with random numbers so that it is unpredictable.
  - Set duration of session ID to as minimum as appropriate to complete the session activity.
  - Do not store session ID in URL, persistent cookies, hidden HTML field nor HTTP headers. Consider storing session ID in client browser's session cookies with proper encryption.
  - Protect session ID by SSL/TLS, so that attacker cannot sniff from the network.
  - Do not share session ID for multiple connections.

  - Do not rely on checking IP address of the incoming connection with the session ID because the IP address can be proxied.
  - Implement a logout function for the application and idle session timeout. When logging off a user or expiring the idle session, ensure that not only is the client-side cookie cleared (if possible), but also the server side session state for that browser and connections to backend servers are cleaned up.
- Access restriction
  - Ensure that end-user account only has the least privilege to access those functions that they are authorised, and the account has restricted access to backend database, or to run SQL or other OS commands.
  - Do not make system calls directly to real file names and directory paths. If attackers have access to source codes, they may discover system-level information. Use mapping provided by web server as a layer of filtering.
  - Do not place data file, temporary or backup files in the same directories of web servers to prevent from unauthorised access.
  - Restrict access to application and web server system or configuration files.
  - Do not assume that users are unaware of special or hidden URLs or APIs.
- Logging
  - Use POST only to send request because GET request can leave verbose information in the web/application server logs.
  - Enable web server log and transactions log.
  - Build a centralised module for application auditing and reporting.
- Use the most appropriate form of authentication methods to identify and authenticate incoming user requests.
- Consider using server side programming platform with strong sandbox model to protect the application server and session variables, such as Java or .Net.
- Protect XML data at the same way as protecting HTML traffic and do not include sensitive data in XML document in clear-text.
- Restrict the types of files being uploaded to the server. Uploading executable programs or scripts should be controlled.
- Keep abreast of the emerging risks associated with new web technologies such as Asynchronous JavaScript and XML (AJAX), JavaScript Object Notation (JSON) and HTML5.

11.6 MOBILE APPLICATION SECURITY

As mobile devices are getting more popular, mobile applications may be developed for internal or public use. Mobile devices, as being mobile, have a higher risk of loss or theft. Adequate protection should be built in to minimise the loss of sensitive data on device. Mobile applications are subject to the same security considerations and risks as other applications, and thus most general coding best practices are also relevant to mobile coding, such as input validation and output encoding, run application with the minimum required privilege, and etc. However, due to wildly varying use cases, usage patterns and various mobile platforms, developers should consider more than just the “apps”. Developers of mobile applications should also take note of the remote web services,

platform integration issues and insecurity of the mobile devices. Some additional best practices for creating a secure mobile application are provided below:

- At the early design stage, mobile device management (MDM) features, such as remote locking/wiping, password enforcement, software/patch distribution, policy management, and jailbreak detection, should be incorporated with if available. Depending on the vendor of the target mobile device, different MDM functions are available in the market.
- Mobile devices are likely to contain or process information that is personal to the owners or tightly tied with them. A security in mind approach should be adopted in mobile application development to mitigate privacy risks in a proactive and preventive manner. Privacy should be embedded into design and integrated to system.
- Encryption should be provided for storing sensitive data. Assume that shared storage is un-trust, store sensitive data on the server instead of client-end device. Application should enforce appropriate encryption on the data downloaded or created. Data used by mobile application should be kept at minimum, e.g. geo-location data or contact information should be discarded after use for the sake of user privacy.
- Transmission of any sensitive data such as personal data or credit card information should be properly protected with encryption. If the mobile application needs to access or upload specific information stored in the device (contact list, location or calendar entries), it should be carried out on a permission basis and allow the user to decide whether to continue to use the application.
- OS level settings of the mobile device should be commensurate with the data security level. Do not directly manipulate the settings within the mobile application for privacy or security reasons. Such manipulation is easily taken for granted by attackers to gain access without knowledge of user.
- Users should be well-informed before they install or use an application on what information the application would access or upload, and for what purpose. If personal information is involved, a personal information collection statement should be provided.
- Assuming the potential risk of exposing personal information, such as contact data, associated with new web technologies, execution from un-trusted or unknown codes should be used with caution. For example, whenever possible, use JSON parser instead of Javascript inherent function for parsing and executing with data.
- It should be kept in mind that mobile device can easily be lost or stolen. Developers should ensure that user authenticator or session token can be revoked quickly in the event of reported lost/stolen device, and always make use of latest security mechanism provided by mobile platform; for instance, keychain management to protect user login credentials and hardware encryption that is keyed with combination of device key and user's chosen device lock code.
- Stolen password provides unauthorised access not only to backend service but also potentially many other services/accounts used by the user. Since a majority of the users store and reuse their passwords in the mobile device, mobile application should not store passwords or long term session IDs without appropriate encryption or hashing.
- Session of mobile application is generally longer than other application in the sake of user convenience. To circumvent privilege escalation, never use device ID or

subscriber ID as sole authenticator or session token. Developer should consider using authentication that ties back to the user identity rather than device identity, and using additional authentication factors for applications giving access to sensitive data or interface where possible.

- Most mobile applications interact with the backend services. All back-end services for mobile applications should be assessed for vulnerabilities periodically, and ensure that the back-end platform/server is running with a hardened configuration with the latest security patches applied. Security scan with latest virus signature should be provided on installation of the mobile native application to the mobile device.
- Since mobile device is capable of using multiple transport carriers including mobile telecommunication network, Wi-Fi or Bluetooth, applications should enforce the use of an end-to-end secure channel when sending sensitive on wire/air.
- Some mobile applications provide programmatic access to premium rate phone calls, SMS, roaming data etc. Developers should implement security controls, such as using a white list model by default for paid resource addressing or authenticate all API calls to paid resources, so to prevent unauthorised or unnecessary access to paid resources. If online payment is required, mobile application should provide alternate payment methods that require verification, for example, Visa - Verified, MasterCard - SecureCode and Payment by Phone Service (PPS).
- Use obfuscation software to protect source code leakage and hide the application details as far as possible in case the mobile native applications are not compiled to machine code format so as to prevent reverse engineering by external party to obtain the source code.
- Applications must be designed and provisioned to allow updates for security patches, taking into account the requirements for approval by app-stores and the extra delay this may imply.

11.7 ADDITIONAL REFERENCES

- "Application and Database Security", related articles from The SANS Institute http://www.sans.org/reading_room/whitepapers/application/
- "A Guide to Building Secure Web Applications and Web Services", The Open Web Application Security Project (OWASP) http://www.owasp.org/index.php/Guide_Table_of_Contents
- "Improving Web Application Security: Threats and Countermeasures", Microsoft Corporation http://msdn.microsoft.com/en-us/library/ms994921.aspx
- Writing Secure Code (2nd Edition), by Michael Howard and David LeBlanc from Microsoft Press
- "Security Considerations in the Information System Development Life Cycle", The National Institute of Standards and Technology (NIST) http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
- "The Trustworthy Computing Security Development Lifecycle", Microsoft Corporation. http://msdn.microsoft.com/en-us/library/ms995349.aspx

Application Design and Security

- "2011 CWE / SANS Top 25 Most Dangerous Software Error", The MITRE Corporate. http://cwe.mitre.org/top25/
- "Insecure Configuration Management", OWASP. http://www.owasp.org/index.php/Insecure_Configuration_Management
- "Web Application Firewall Evaluation Criteria, version 1.0", Web Application Security Consortium. http://www.webappsec.org/projects/wafec/
- "Security Development Lifecycle for Agile Development", Microsoft. http://msdn.microsoft.com/en-us/library/windows/desktop/ee790621.aspx
- "A Security Analysis of Next Generation Web Standards", ENISA. http://people.cs.kuleuven.be/~lieven.desmet/research/publications/docs/NG_Web_Security.pdf

Application Testing

- "Risk-based and Functional Security Testing", Michael, C. C. and Radosevich, W. https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/testing/255-BSI.html
- "OWASP Testing Guide, version 3.0", OWASP. https://www.owasp.org/images/8/89/OWASP_Testing_Guide_V3.pdf
- "OWASP Code Review Guide, version 1.1", OWASP. https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf

Security Best Practices

- "OWASP Best Practices: Use of Web Application Firewalls", OWASP. http://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls
- "Ten Best Practices for Enterprise Intrusion Prevention", Ryan, L., Information System Security Magazine. http://www.infosectoday.com/Articles/IPSChecklist.htm
- "Build Security In – Best practices", Department of Homeland Security. https://buildsecurityin.us-cert.gov/bsi/articles/best-practices.html

Mobile Application Security

- "Mobile security project", OWASP. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- "Mobile Web Application Best Practices", W3C. http://www.w3.org/TR/mwabp/
- "iOS5 Hardening Configuration Guide", Department of Defense, Australia Government. http://www.dsd.gov.au/publications/iOS5_Hardening_Guide.pdf

12. COMMUNICATIONS & OPERATIONS SECURITY

12.1 OPERATIONS MANAGEMENT

12.1.1 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 should 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 all security functions of an information system.

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

12.1.2 Principle of Least Privilege

B/D should 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.

12.1.3 Principle of Least Functionality

Information systems should be configured to provide only essential capabilities and specifically prohibits or restricts 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.

12.1.4 Change Management

Changes to information systems should be controlled. Operational systems and application software should be subject to strict change management control, 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.

12.1.5 Operational and Administrative Procedures

Operational and administrative procedures should 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.

12.1.6 Operations Controls

Control of Computer Operators

Operations controls relate to the computer operators' activities and to the running or operation of the computer equipment. The purpose of these controls is to reduce potential fraud in the computer room. These controls are usually preventive in nature.

The best way to keep track of operators' activities is to record all events on hard copy console logs. There are chances that operators' activities cannot be logged to an operator job journal file because of a file full condition. The console log should be produced on pre-numbered pages so that operators could not destroy any pages without being noticed. The console log or job journal file should be checked daily for the following:

- Missing pages.
- Abnormal activities, e.g. security violation messages, improper operating procedures, etc.

Besides, operators should provide explanations for all reruns and abnormal interventions made, such as overrides, interrupts, halts and restarts. Such occurrences can be plotted into a graph so that patterns of occurrences, which are indications of fraud perpetration, can be spotted.

Ideally, written logs should be prepared by operators to record information like date of execution, completion status and any relevant comments for all jobs run. The log should also reflect incidents such as equipment malfunctions, idle time and downtime. The cause of such incidents, if known, should be specified. Supervisors shall then review the logs regularly for monitoring purposes.

The responsibilities of operators should be, and only be, directly related to the operation of the computer equipment. Therefore, under no circumstances should operators be allowed to make program modification, even under the supervision of programmers, because this is a serious breach of segregation of duties. Besides, it provides opportunities for operators to perpetrate frauds.

Those opportunities can further be eliminated by rotating the operators among shifts, rotating their responsibilities and prohibiting them from working alone.

Control of System Programmers

System programmers, although responsible for maintaining the system software, should not be allowed to perform any update unless authorised.

Journal should also be available for logging every job being run in the system such that by going through the log, illegal actions taken by the system programmers can be identified.

While the system programmers shall be controlled for his activities, he should be encouraged to report any faults or loopholes detected in the system and how they can be manipulated for security violation.

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

Up-to-date network information, in particular, the network diagrams, should be maintained to reflect the latest network environment for effective security control and securely stored.

12.2.1 Network Security Controls

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 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. 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 mission-critical systems. In this architecture, two firewalls are used – external firewall and internal firewall. The external firewall protects a DMZ[5] from the Internet and the internal firewall further protects the internal networks. In this design, even if external users compromised 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.

Installation of a NIDS or NIPS on the network helps to detect if there is an attack happening on 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 proactive response to stop the source of attacks or to minimise the impact of the attacks. Configuration of IDS and IPS require tuning of signature and recognition patterns to reduce false alarms.

B/Ds have the overall responsibility to protect data, information system and network. A B/D should acquire security software (e.g. firewall, malicious code 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 feature like remote update, policy enforcement, status query, 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 effort of LAN/system administrators and IT security administrators.

[5] DMZ is a network added between a protected network and an external network, in order to provide an additional layer of security. Usually, servers providing services to users in the Internet are placed in DMZ.

12.2.2 Transmission of Classified Information

In accordance with the Security Regulations, TOP SECRET/SECRET information must be transmitted only when encrypted and inside an isolated wired LAN approved by the Government Security Officer subject to the technical endorsement of OGCIO. 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 must be encrypted when transmitted over an un-trusted communication network. Examples of un-trusted communication network include:

- Internet
- Network that uses public telecommunication line (e.g. leased line, dial-up connection)
- Wireless network
- 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 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.

Communication over un-trusted communication networks poses security risks because a malicious attacker may capture sensitive information and even break into the Government network by exploiting vulnerabilities of the un-trusted communication networks. Since the security requirements to communicate over a trusted and un-trusted network are different, it is important for B/Ds to differentiate the nature of a communication network in order to apply necessary security measures. Networks that do not fall under the definition of trusted communication network are considered as un-trusted communication networks.

12.3 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 message, passwords, and file transfers can be monitored and captured using readily available software.

Internet services need stronger authentication and cryptography mechanisms, and these mechanisms must be truly interoperable. Internet information enquiry or transaction processing requires user authentication. One-time password and two-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, computer virus protection, software licensing, remote access, dial-up access, physical security, firewall implementation and other aspects relating to the use of Internet.

12.3.1 Gateway-level Protection

Any B/D that supports Internet facilities must protect its information and information resources from unauthorised access or public break-ins. All Internet access from departmental network must 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, firewall 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. Direct dial-up connection to Internet services provider should not be established. For technical guidelines on Internet gateway security, please refer to the following document for details:

- **Internet Gateway Security Guidelines (G50)**
  http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g50_pub.pdf

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-virus program and user permission restriction should be implemented on these computers to avoid potential security breaches and system misuse. An approval and control mechanism at appropriate level should 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 are strictly prohibited except with proper security safeguard and approval from the DITSO.

12.3.2 Client-level Protection

Personal firewalls are effective measures to protect user’s workstation from unauthorised network traffic which can be network worms or other forms of malicious code attacks. It resides on user’s workstation and provides firewall services between the workstation and

the network. Personal firewall controls network traffic by asking for user's authorisation before allowing the network traffic entering into or leaving user's workstation. Some even provide application-level protection that ensures only authorised processes will run on user's workstation.

LAN/System administrators are recommended to install personal firewall 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 user's workstation should be properly configured. As web browsers are the primary interface with the Internet, poorly configured web browsers can allow malicious code 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 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 the importance of using properly configured web browsers.

12.3.3 Using Internet Services

Staff should be authorised to use the Government Internet access service only if the service can assist them in carrying out their official duties. By default, staff should be denied access for Internet service unless they are granted with authorisation.

B/Ds should define acceptable Internet usage behaviours for their users. Some recommended security guidelines for the acceptable usage behaviours are:

- Comply with the requirements in the Security Regulations in transmitting classified information.
- Beware that the privacy and confidentiality of information sent over the Internet cannot be guaranteed. Proper security measures should be used.
- Disable password remembering feature at web pages.
- Disable Internet connection when not in use.

- Beware that when accessing the Internet using IP addresses and domain names of B/Ds, they may be perceived by others to be representing the Government.
- Use only privately-owned email addresses or identities in public forums, newsgroup, etc. for personal purposes.
- Do not execute mobile code or software downloaded from the Internet unless the code is from a known and trusted source.
- Do not visit or download files from doubtful websites, all software and files downloaded from the Internet shall be screened and verified with anti-virus software.
- Follow the best practices in Section 12.5 –PROTECTION AGAINST COMPUTER VIRUS AND MALICIOUS CODE to protect against computer virus and malicious code.

12.3.4 Social Networking Services

- Using social networking services (SNSs) such as social networking sites, microblogging sites, video and photo sharing sites, wikis, collaboratively edited web pages, discussion forums and blogs are getting popular but they also bring privacy issues, security concerns and add new dimensions of security risks:
- Privacy threat: User may place too much personal information to the social networking sites, allowing a profile to be produced on an individual's behaviour on which decisions, detrimental to an individual, may be taken.
- Disclosure of sensitive information: Post internal or classified information that would bring discredit on or embarrass the Government.
- Malicious content: As usually SNSs are rich in content with many applications developed by different parties, there may not be sufficient controls or scrutiny before use. Attackers are able to create customised applications that appear to be legitimate while infecting the users' computer without their knowledge. Internal systems / data are exposed to risk if these unknown applications are used.
- Social-engineering attacks: SNS builds online communities of people with certain level of interpersonal trust. Malicious people might impersonate a trusted person of the users and then convince them to disclose sensitive information. In addition, attacks like viruses, Trojans or rumours can be spread easily and rapidly when some social-engineering skills are used.

In consideration of the high risk and unforeseeable threats that may be introduced by SNSs, B/Ds should seriously assess the associated risk and estimate the potential impact before using such services. When SNSs are used by B/Ds for official purpose, the following controls should be considered:

<u>Management Controls</u>

- Usage policies should be established, sensitive information should not be disclosed in SNSs. Any information that may cause embarrassment or discredit to Government shall not be revealed when engaged in SNSs.

- It is not recommended to treat the information published to SNSs as information of record or official. Disclaimers should be made on the profiles to state that official information can be found at B/D's official website.
- It is prohibited to use SNSs to gather personal information unless with sound justifications.
- Risk assessment for each SNS to use for official communications should be conducted so as to determine whether public comments are allowed or even necessary.
- Incident handling plan should be developed to handle possible compromises of passwords, content subject to attack and change, etc.

Operational Controls

- B/D may consider using a computer outside the B/D internal network for managing and maintaining their service in SNSs. Alternatively, the use of desktop virtualisation technologies will allow users to view potentially malicious websites in a virtualised "sandbox".
- The inclusion of third party applications on official profile pages is not recommended unless the application provider can be trusted, e.g. other governmental agency or well-known commercial vendor.
- The use of licensing agreements should be considered to help control distribution and use of the published content.
- Whenever possible, disclaimers should be made on the profiles in social networking sites to state that official information can be found at B/D's official website.

End-user Controls

- SNS users should have high security awareness about what information to share, with whom they can share it, and what not to share. Official data should not be shared or archived to SNSs unless with explicit approval from data owner.
- SNS users should avoid placing too much personal information to the sites, and set appropriate access control to personal profile where appropriate.
- Regular awareness training should be conducted to educate staff about B/D's IT Security Policy and strengthen security awareness around the risks associated.
- Moderation is required to filter out comment spam. Some of the SNSs may also provide spam control plug-ins for automatic filtering comment spam.
- SNS users should check whether providers have channels for reporting abuse and concerns.
- SNS users should use strong authentication where appropriate. Strong password should be used and the password should be regularly changed. Do not use the same password for various social networking sites.
- SNS users should remain cautious to messages sent by people that you do not know well, and should avoid clicking links coming from people or sources you do not know.
- SNS users who need to review the comments should be trained on how to look for suspicious code in a page, and the risk related to URL redirection.

- SNS users should regularly look for related news and updates released by the provider. The suggested security setting by respective providers should be followed.

12.4 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. Formal request must be made for applying an email account. Authentication, encryption and digital signature services should be available for email over the Internet as well as email on internal network. It is recommended that the electronic messaging containing sensitive information shall be encrypted during transmission or storage.

In accordance with the Security Regulations on internal communication, the Confidential Mail System (CMS) is a designated email system in the Government to facilitate exchange of email messages and documents with CONFIDENTIAL classification within the Government network. The exchange of email over Internet, whether signed or encrypted, shall not be assumed to be of equivalent security status as the CMS. This is because the Internet electronic messaging services may not fulfil the security requirements as stipulated in Security Regulations for handling of CONFIDENTIAL information.

12.4.1 Email Security

Email servers and clients should be properly configured before connecting to 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 record of each trial of reading or updating by authorised users and for those unauthorised ones. Alert report or alarm should be used to report on security incidents. In addition, 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 password, should 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 malicious codes. Please refer to Section 12.3.2 - Client level Protection for details.

LAN/System administrator should arrange automatic updating of virus signature and malicious code definition for users who use the government email system. Users should make sure that the auto-protection of the anti-virus in their workstation is always enabled whenever they use the system to access any document or information. Please refer to Section 12.5 - PROTECTION AGAINST COMPUTER VIRUS AND MALICIOUS CODE 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 email containing computer viruses or suspicious content, they should report the incident to the management and LAN/System Administrator immediately and follow the corresponding incident handling procedures.

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

12.4.2 Instant Messaging

Instant messaging (IM) is widely used nowadays for online communication, chatting and file sharing. Though IM is an effective means of communication, it introduces new security risks:

- Disclosure of sensitive information: Sensitive information can be read by or distributed to unauthorised users. This is especially the case when using public IM clients to communicate with individuals outside the Government.
- Security breaches: Malicious code can spread via the IM channel quickly.
- Monitoring and retention headaches: It is not trivial to monitor IM messages and retain the messages as business records.
- Accountability: Identity of IM message sender and receiver cannot be verified in public IM network.

Because of the potential security risks, usage of IM should be restricted for business purpose only and requires approval by DITSO.

If a B/D decides to use IM, the following security controls should be implemented:

- Develop IM acceptable usage policy and clearly disseminate to users of IM.
- Consider implementing an enterprise IM solution instead of using public IM clients. Also consider to integrate the enterprise IM system with the B/D’s existing authentication mechanisms, such as the Directory Service.

- Select enterprise IM products that provide strong encryption.
- Implement IM gateway to enforce IM policy by monitoring the usage, managing IM traffic and filtering content to block unwanted messages, computer viruses and offensive material, and log IM messages for audit trail purpose.
- Disable all unnecessary features and network services provided by the IM, enable all notifications when incoming/outgoing messages/call/files are received/sent, disable sharing of resources, and disable remote activation of microphone and video camera.

12.4.3 Spam and Phishing

In today's connected world, email and other messaging tools are critical business tools. However, behind the convenience, electronic messaging can carry viruses, spam, worms, inappropriate images and other damaging content that can seriously compromise your information assets and networks. Given the ease and power of electronic messaging tools and increasing popularity of Internet services such as SNS, B/Ds should be aware of the potential security threats associated with the use of these tools. Spammers and attackers are always using tricks such as spam and phishing scams to perform fraudulent activities.

Spam refers to bulk, unsolicited electronic messages sent in the form of email, fax or short message, etc. regardless of whether the recipients have given any consent to receive such or even after the recipients have requested not to receive such any more. In general, spammers send such messages to a big pool of recipients, expecting that some would be interested in their products or information, and respond to their messages/offers. Spam includes legitimate advertisements, misleading advertisements, and even phishing messages designed to trick recipients into giving up personal and financial information.

Phishing attacks involve the mass distribution of fraudulent electronic messages with return addresses, links, and branding which appear to come from legitimate organisations such as banks, insurance agencies, retailers or credit card companies. Phishing scams may be circulated in the same mass-mailing format as spam. It involves the use of social engineering techniques in an attempt to infect your system with malicious codes and/or ask you to provide your personal or sensitive information. They normally appear as important notices, urgent updates or alerts with a deceptive subject line to attract the recipient to believe that the electronic message has come from a trusted source. Even more, the electronic message may contain a fraudulent link enticing the recipient to a spoofed website, luring users to download malicious software onto their computer, allowing attackers to remotely control them for use in hacking exploits such as a Distributed Denial of Service (DDoS) attack.

Spam or phishing scams are sometimes nearly impossible to distinguish from one and the other, and in fact they are used by spammers or attackers as a vehicle to commit illegal activities. Spam and phishing messages can degrade network performance and consume substantial memory or disk space in the electronic messaging system. Substantial damage could also be resulted if those messages carry attachments that are infected by computer virus or malicious code. Both LAN/system administrators and end-users should consider some countermeasures and observe rules of thumb for protecting from these security threats.

LAN/System Administrators can consider the following security countermeasures to prevent spam or phishing email:

- Install spam filtering gateway to filter all spam electronic messages. Latest spamming lists / blacklists should be regularly updated.
- Prevent email address harvesting from websites.
- Stop third-party mail relay and use web proxy.
- Block by public and private DNS blacklists.
- Allow emails by whitelists.
- Filter by sender email address, email subject or email content, or use heuristic content filtering.
- Seek help from Internet service providers (ISPs) to prohibit spammers from using the ISPs' services for spamming activities.

Users should observe the following security guidelines against spam or phishing email:

- Use strong and unique passwords for electronic messaging accounts.
- Do not open or forward any electronic messages from unknown or suspicious sources. Ignore or delete all electronic messages from un-trusted sources.
- Do not follow URL links from un-trusted sources to avoid being re-directed to malicious websites or falling prey to phishing attacks.
- Handle the email addresses with care. When filling out web registration forms, surveys and other online documents etc, users are advised to check the privacy policy of the website before providing their email addresses, to ensure that the website provides proper protection for their email addresses.
- Use separate email addresses different from their office email addresses when participating in public newsgroup or chat rooms, to avoid their office email addresses and/or mail systems to become a target of spam.
- Do not reply to spam or phishing messages because most return addresses are not legitimate and would only result in the generation of non-delivery messages thus increasing the amount of undesired traffic, and allow the spammers to obtain a validated email address for future spamming.
- Use email filtering tools in email software to block or screen out spam by defining some simple filtering rules.
- Ensure that computer applied with the latest security patches and virus signature to reduce the chance of being affected by fraudulent electronic message or websites riding on software vulnerabilities.
- Report the incident to the LAN/system administrator immediately if users suspect or discover electronic messages containing computer viruses or phishing attacks.

12.5 PROTECTION AGAINST COMPUTER VIRUS AND MALICIOUS CODE

Malicious code refers to a broad category of software threats that can cause damages or undesirable effect to computers or networks. Potential damages include modifying data, destroying data, stealing data, allowing unauthorised access to the system, popping up unwanted screens, and doing things that user does not intend to do.

Examples of malicious codes include computer viruses, network worms, Trojan horses, logic bombs, spyware, adware and backdoor programs. As they pose serious threats to software and information processing facilities, precautions are required to prevent and detect malicious codes.

Computer virus is a common form of malicious code. It is a program that infects a computer by attaching itself to another program, and propagating itself when that program is executed. Another form of malicious code is network worm which is a computer program that can make copies of itself and spread itself through connected systems, consuming resources in affected computers or causing other damages. Trojans become a prominent malicious code threat that users unwittingly install onto their computers, through either opening email attachments or downloading from the Internet. Trojans are often downloaded and installed by other malicious code as well.

Traditionally, malicious codes are spread via two main channels:

(a) Data transmitted through network.
(b) Removable media.

Recently, the attacks have evolved to become more automatic and progressive. New forms of attacks can be a combination of several types of malicious actions. For example, some type of mass-mailing virus with spoofing characteristics may take advantage of reported system vulnerabilities and scan across the network for vulnerable systems. Upon infecting a compromised system, not only will the worm continue scan and exploit other systems at randomly generated IP addresses, it can also inject computer viruses and spyware programs onto the compromised system, and use its built-in mass mailing technique to spoof as legitimate email to further spread via email channel.

A hoax computer virus warning is an untrue virus-related warning/alert started by malicious individuals. Hoax message mixes itself together with true computer virus alerts, and enlists recipients to pass on to alert those unknowns. By forwarding such hoax alarms to others, it is likely to cause confusion to the recipients in their attending real computer virus alerts. Besides, it creates unnecessary traffic on the Government network as well as wastes people's time in reading them. Users should not forward any received hoax messages to avoid further spreading.

Besides relying on technical controls such as installing virus or malicious code detection and recovery protection measures, users should beware of their behaviour when using IT

services and facilities and take the responsibility to protect against computer virus and malicious code attacks.

12.5.1 User's Controls

To protect against computer virus and malicious code, users should ensure virus or malicious code detection and recovery protection measure has been installed and running on their workstations and mobile devices. Most of the major anti-virus software vendors should have equipped their products with the capability to deal with threats from computer worms, Trojan horses, etc. in addition to computer viruses. Some products will also provide a certain degree of protection against spyware/adware.

But if the virus signature, malicious code definition are not updated, the protection software will not be able to detect and guard against the latest computer virus and malicious code attacks. Users should therefore regularly update virus signature and malicious code definition and detection and repair engine. Update should be configured as automatic and update frequency should be at least on daily basis. If automatic update is not possible (e.g. mobile device which are often not attached to networks), update 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 virus outbreaks. If so, users should follow the instructions and immediately update with the latest virus signature and malicious code definition in order to protect against virus outbreak.

The following are other recommended security guidelines to protect against computer virus and malicious code:

- Enable real-time detection to scan computer virus and malicious code for active processes, executables and document files that are being processed. Also schedule full-system scan to run regularly based on operational needs.
- Check any files on storage media, and files received over networks against computer virus and malicious codes 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 electronic message attachments and downloads against computer virus and malicious code before use.
- Before installing any software, verify its integrity (e.g. comparing checksum value) and ensure it is free of computer virus and malicious code. Installation of any executable/software received via electronic message or downloaded from web browsing should be approved by DITSO.
- Avoid using personal Internet email which is more susceptible to computer virus infection. If private Internet email services must be used for business purpose, emails should be downloaded to an isolated computer with dedicated Internet connection for Internet mail exchange.
- Always boot from the primary hard disk. Do not allow booting workstations from removable device without permission.

- Do not use storage media and files from unknown source or origin unless the storage media and files have been checked and cleaned for computer viruses and malicious codes.
- Follow the guidance in Section 10.8 DATA BACKUP AND RECOVERY to backup data.

User should also note that it is their own responsibility to protect their workstations and mobile devices by taking the appropriate actions for computer virus and malicious code protection.

12.5.2 LAN/System Administrator's Controls

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

The virus or malicious code detection and recovery protection measures should support enterprise management to facilitate central management. Please refer to Section 12.2.1 - Network Security Controls for more details about enterprise management.

LAN/System administrators should also consider implementing the following technical controls:

- Enable anti-virus 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-virus protection to scan all incoming traffic from Internet. The gateway should be configured to stop traffic with malicious content, quarantine / drop them, and create audit logs for future references.
- 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 external vendor to perform a computer virus scan (with the latest virus signature) on user's hard disk after:
  - New machine installation.
  - Service maintenance.
  - 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 computer virus before booting. This can eliminate boot sector viruses from infecting the server.
- Protect application programs in the server by using access control facility, e.g. directories containing applications should be set to 'read only'. In addition, access right, especially the right to 'Write' and 'Modify', should be granted with least privilege on a need-to-have basis.
- Consider using document management solution to share common documents so as to minimise the propagation of infected files in an uncontrolled manner.
- Scan all newly installed software before they are released for public use.
- Schedule preferably full-system scan to run immediately after the file server start-up.
- Follow the guidance in Section 10.8 - DATA BACKUP AND RECOVERY to backup data.

In addition, LAN/system administrators should keep updated with security advisories and educate users the best practices to protect against computer virus and malicious code:

- Subscribe to notifications / advisories so that they can receive critical computer virus / malicious code alerts at the earliest possible moment.
- Disseminate promptly the computer virus alert issued by OGCIO to all end users and take necessary actions.
- Educate users to understand the impact of massive computer virus attacks, recognise ways of infecting with computer virus and malicious code (e.g. educate users that sender of electronic message containing computer virus and malicious code can be forged as friends or colleagues) in order to prevent computer virus and malicious code infection.

12.5.3 Detection and Recovery

The following can be symptoms of a computer infected with computer virus or malicious code:

- 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 a computer virus or malicious code, users should stop all activities because continually using the infected computer may help spreading the computer virus or malicious code further. Users should report the incident to the management and LAN/System Administrator immediately. The OGCIO Central Computer Centre Helpdesk (ccc_hd@ogcio.gov.hk) can provide technical assistance in investigating suspected computer virus and malicious code incidents. Users may also use anti-virus software available in the market to clear the computer virus on their own.

Clearing a computer virus or malicious code does not necessarily imply that contaminated or deleted files can be recovered or retrieved. The most effective way for recovering corrupted files is to replace them with the original copies. Therefore, regular backup should be done and sufficient backup copies should be kept to facilitate file recovery whenever necessary.

After clearing computer virus or malicious code from a computer, users should perform a complete scan on the computer and other storage media to ensure that they are free of computer virus and malicious code. Failure to do this may lead to resurrection of computer virus or malicious code.

12.6 SOFTWARE AND PATCH MANAGEMENT

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

12.6.1 Software Usage

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 is 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. Illegal software copy should not be installed or run under any circumstances since these software files may have been computer virus contaminated.

- Public domain software and freeware, according to past records, have a relatively higher chance of being contaminated with computer virus or spyware/adware. Use of such software should be avoided. If necessary, they should only be installed with the approval from DITSO. For close-source freeware, only those with a long history (at least more than 2 years) with good track record should be installed. Open-source freeware may be installed when they are carefully inspected and downloaded from trusted sites, such as the official website. Security patch should be applied when available. Nevertheless, users 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 installation of unapproved software or unauthorised amendments to production files.

12.6.2 Software Asset Management

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 technology for SAM. For example, some desktop operating systems provide a means to maintain software asset inventory and prevent loading of unauthorised software. B/Ds should choose the best SAM tool that fits to 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.

12.6.3 Patch Management

Many security advisories of vendors are publishing to announce software vulnerabilities. Therefore, a responsive patch management process becomes critical in maintaining the security of information systems. With the increase in vulnerabilities discovered and the corresponding patches released, it is essential that 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:

1. Patch acquisition – select and download appropriate patches and prepare them for deployment.
2. Testing – perform testing to determine whether the patches contain components that conflict with other patches, key enterprise applications or even entire environment "baselines".
3. 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 system application be affected? Does the system require reboot after installing the patch which affects service availability?

4. Deployment – deploy patches to the target machines and make sure that patches are only installed on machines where they are required.
5. Compliance – verify that all machines are functioning properly and comply with the related security policies and guidelines.

In addition, the following guidance should be observed 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.
- Identity the associated risks and actions to be taken once a security vulnerability has been confirmed.
- Assess the impacts associated with installing the security patch, when a security patch is available.
- Test and evaluate patches before they are installed to ensure they are effective; if installing patch is not feasible, upgrade of the concerned product to eliminate security problem should be considered or alternate security controls should be implemented.
- Apply the security patches through an established change control process.
- Regularly review the patch management process to measure its effectiveness and efficiency.
- Educate users to be highly aware of the importance of IT security and patch management to their daily operation.
- Perform security risk assessment regularly, e.g. using vulnerability scanning tools (host-based or network-based) to identify patch inadequacy or system mis-configuration.
- Consider 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.

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 should determine the appropriate patch management strategy including patch checking and

patching frequency for their systems. In essence, information systems of high risk should be addressed first.

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 should 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.

12.7 WIRELESS SECURITY

12.7.1 Wireless Network

Wireless Local Area Network (WLAN) 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 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.

WLAN should be used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.

12.7.1.1 Threats and Vulnerabilities of Wireless 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 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 Government internal network through wireless connections, potentially bypassing firewall protections and launch attacks.
- Computer viruses or other malicious codes 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.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.

Wired Equivalent Privacy (WEP) protocol was originally designed to give wireless networks an equivalent level of security as wired networks. It relies on a secret key to encrypt network packets transmitted between a wireless client and an access point. However, WEP has been proven to contain weaknesses. Attackers equipped with tools and a moderate amount of technical knowledge could gain unauthorised access to a WLAN even if it is protected by WEP.

Protection by a stronger wireless security protocol such as WPA (Wi-Fi Protected Access) or preferably WPA v2[6] (WPA2) 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. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal authenticates users for network access using a pre-shared password, while WPA2-Enterprise authenticates through a Remote Authentication Dial In User Service (RADIUS) authentication server. Although the setup for WPA2-Enterprise is more complicated, it is recommended because it provides additional security and offers better centralised control over access to the WLAN. WPA2-Personal is only recommended for small ad-hoc network such as guest WLAN for visitors. B/Ds should deploy Virtual Private Network (VPN) on top of wireless network if classified data is to be communicated over wireless networks.

[6] WPA (Wi-Fi Protected Access), which by default uses Temporal Key Integrity Protocol (TKIP) for data encryption, is a wireless security protocol to fix known security issues of WEP. However, vulnerability of TKIP has been discovered, and rendered TKIP encryption unsecure. WPA v2 (Wi-Fi Protected Access 2), based on IEEE 802.11i, has been proposed. With WPA v2, only authorised users can access their wireless network with the features of supporting stronger cryptography (Advanced Encryption Standard AES), stronger authentication control (Extensible Authentication Protocol EAP), key management, replay attack protection and data integrity.

12.7.1.2 Security Controls to Protect Wireless 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 wireless networks. The following are some management and technical security controls for consideration:

Management Controls

- Define a wireless security policy to address the usage of wireless networks and type of information that can be transmitted over wireless networks.
- Develop and securely keep a coverage map of the wireless network, including locations of respective access points and SSID information so as to avoid excessive coverage by the wireless signal.
- 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 wireless interface. Once a device is reported missing, consider modifying the encryption keys and SSID.
- Implement strong physical security controls and user authentication for complementing physical security deficiencies of wireless devices.
- Install access points far from a window or a door to prevent network tapping from publicly accessible area.

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 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, Simple Network Management Protocol (SNMP) community strings.
- Deploy WPA2-Enterprise, or change encryption keys regularly if WPA2-Personal is used.
- 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 wireless networks 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 wireless intrusion detection system (WIDS) or wireless intrusion prevention system (WIPS) to monitor the wireless networks.
- Deploy VPN on top of wireless network 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 network or resources.
- Segment the access point's coverage areas to balance the loading and minimise the probability/impact of 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.

End-user Controls

- Install firewall on wireless clients (e.g. mobile devices).
- Turn off sharing or tethering at wireless clients.
- Don't attach the wireless clients to departmental network while it is connected to a third party wireless network.
- Connect to departmental network resources using VPN.
- Keep strict control of the wireless interface device (e.g. PCMCIA card and 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 12.5 - PROTECTION AGAINST COMPUTER VIRUS AND MALICIOUS CODE and Section 9.5.2 – Mobile Device Security to protect the mobile device.

12.7.1.3 Data Transmission Considerations

WLAN is generally considered as an un-trusted network and should 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 network with respect to the transmission of various categories of information in accordance with the requirements specified in the Security Regulations.

Category of Information	Applicability of Using Wireless Network for Transmission
TOP SECRET	Not allowed
SECRET	Not allowed
CONFIDENTIAL	Allowed, provided that it is transmitted using designated device with approval of Head of B/D and there are sufficient authentication and transmission encryption security controls and have attained the level of encryption required for CONFIDENTIAL information. Usage of VPN is recommended 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.
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 network 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.

For technical guidelines in compiling such requirements, please refer to Annex F of the Security Regulations.

12.7.2 Radio Frequency Identification (RFID) Security

RFID technology is a non-contact, automatic identification technology making use of radio signals to identify, track, sort and detect a variety of objects such as people, vehicles, goods and assets without contact (as that of magnetic stripe technology) or line-of-sight (as that of bar code technology), and track the movements of these objects through a network of scanning devices over a distance of several meters. RFID technology is growing rapidly in different applications. More developers apply the technology not only to traditional applications but also to security applications and services that use together with other wireless technology.

Systems implementing RFID technology are typically composed of three key components:

- RFID tag, or transponder, carries object identifying data. Depending on the source of power, tags may come in three flavours: active, semi-passive and passive.
- RFID tag reader, or transceiver, reads and writes tag data.
- Back-end database stores records associated with tag contents.

Each of these three components can pose privacy and security issues with RFID systems. Unprotected RFID tags are especially vulnerable to physical attacks, counterfeiting, spoofing, eavesdropping, traffic analysis or denial of service attacks. In terms of privacy, RFID tags should not compromise the privacy of their holders. Information should not be leaked to unauthorised readers, nor should it be possible to build long-term tracking associations between tags and holders. In terms of security, RFID tag contents should be protected by access control. Mutual authentication between tags and readers is necessary to build trust relationship.

In general, the following security guidelines can be used as reference to mitigate the security risks regarding the usage of RFID:

- Use a password to protect the tag data to prevent tags from being read without owner's permission.
- Provide physical locking of tag memory so that the chip is read-only and has information stored on it during the manufacturing process to provide a proof of origin.
- Encrypt tag data using asymmetric cryptography to verify the authenticity of information.
- Protect readers by rejecting tag replies with anomalous response times or signal power levels according to the physical properties of tags.
- Verify reader's identity when transmitting data between the reader and the RFID application server.
- Equip RFID environments with special devices to detect unauthorised read attempts or transmissions on tag frequencies. These read detectors may be used to detect unauthorised read/update attempts on tags if they are used together with specially designed tags that can transmit signals over a reserved frequency indicating that they are being killed or modified.
- Consider using the "kill" tag approach to protect privacy of the user when the tag information is no longer in use. When a tag receives a "kill" command from a reader, it renders itself permanently inoperative. To prevent wanton deactivation of tags, this kill command can be PIN protected.
- Protect tagged products from being detected, by shielding RFID tags in a container made of metal mesh or foil, which is known as a "Faraday Cage".
- Protect back-end database with firewall, access control and encryption security controls.

Because RFID tags come in different flavours, there is no generic RFID security solution. Some low-cost passive and basic tags cannot execute standard cryptographic operations like encryption, strong pseudorandom number generation, and hashing. Some tags cost more than basic RFID tags, and can perform symmetric-key cryptographic operations. B/Ds wishing to use RFID should therefore evaluate the cost and security implications as well as understand the limitations of different RFID technologies and solutions.

12.7.3 Bluetooth

Bluetooth is an open standard based on IEEE 802.15 for short-range[7] transmission of digital voice and data that supports point-to-point and multipoint applications. Bluetooth can be used to establish a wireless personal area network to connect disparate devices (e.g. mobile phones, PDAs, printers, faxes, etc.) together wirelessly in a small environment such as an office or home.

Product developers that use Bluetooth wireless technology in their products have several options for implementing security. There are three modes of security for Bluetooth access between two devices.

- Security Mode 1: non-secure.
- Security Mode 2: service level enforced security.
- Security Mode 3: link level enforced security.

Devices and services also have different security levels. For devices, there are 2 levels, "trusted device" and "un-trusted device". A trusted device, having been paired with one's other device, has unrestricted access to all services. With regard to services, three security levels are defined: services that require authorisation and authentication, services that require authentication only and services that are open to all devices.

B/Ds using Bluetooth to connect mobile device to Government networks should ensure that the usage is controlled for business purposes only. The same management, operational and technical controls described in Section 9.5.2 – Mobile Device Security apply to Bluetooth security. In addition, B/Ds should implement the following technical controls:

- Select obfuscated device identity (ID) of the Bluetooth devices – the device ID should not reveal information about the Government or B/D.
- Enable proper authentication in the device to prevent connections from unauthorised devices. Only permit connection to known devices.
- Select hard-to-guess PIN and avoid weak PIN.
- Change default PIN (e.g. 0000).
- Configure encryption key sizes to the maximum allowable.
- Establish a "minimum key size" for any key negotiation process.

[7] About 10 meters (30 feet); can be extended to 100 meters.

- Put the Bluetooth device into a non-discoverable state so that the device is invisible to other Bluetooth devices.
- Un-pair the lost or stolen Bluetooth device with all the devices to which it was previously paired.
- Do not accept files transmitted via Bluetooth devices from unknown or suspicious entities.
- Ensure that mobile devices with Bluetooth interfaces are configured with power-on password to prevent unauthorised access if lost or stolen.

12.8 VOICE OVER IP (VOIP) SECURITY

Voice over IP (VoIP) technology unites the telephony and data worlds. It enables the transfer of voice data over a packet-switched network. VoIP allows phone calls, faxes and voice traffic to be relayed over Intranet and Internet. Current VoIP systems use either a proprietary protocol, or one of two standards, namely H.323 and the Session Initiation Protocol (SIP).

VoIP can provide more flexible service at lower cost, but there are tradeoffs that shall be considered. VoIP systems are considered to be more vulnerable than conventional telephone systems, because they are tied in to the data network, resulting in additional security weaknesses and avenues of attacks.

In a conventional office telephone system, intercepting conversations requires physical access to telephone lines or compromise of the office private branch exchange (PBX). But for VoIP, voices that converted into IP packets may travel through many network access points and therefore expose to more attack points for interception by intruders. In fact, all security risks associated with Internet protocol such as computer virus, Denial-of-Service and man-in-the-middle attacks also apply to VoIP.

B/Ds should understand and manage the risk associated with VoIP. B/Ds should develop appropriate network architecture to support the usage of VoIP with the following considerations:

- Separate voice and data on logically different networks if feasible.
- Separate servers for TCP/IP services such as DHCP and DNS for VoIP and data networks if feasible to minimise the impact if a server is out of service.
- Implement device authentication (e.g. using the MAC address) of an IP phone and user authentication (such as with a user ID and password, or a personal identification number) as far as appropriate to avoid unauthorised access to the services.
- Disallow H.323, SIP, or other VoIP protocols from the data network at the voice gateway, which interfaces with the public switched telephone network.
- Use strong authentication and implement access control to protect the voice gateway system.
- Protect VoIP traffic through firewalls.

- Use IPSEC or Secure Shell (SSH) for all remote management and auditing access.
- Use encryption at the router or voice gateway to provide for IPSEC tunnelling, if necessary.
- Ensure that adequate physical security should be in place to restrict access to VoIP network components. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to perform traffic analysis.
- Protect computers which use "softphone"[8] for VoIP connections with firewall, latest security patches, virus or malicious code detection measure with latest virus signature and malicious code definitions.
- Develop contingency plans of making voice calls if VoIP systems become unavailable.

12.9 COMMUNICATION WITH OTHER PARTIES

12.9.1 Inter-departmental Communication

It is becoming more common for B/Ds to have network communication with each other in order to exchange information and provide their information systems as IT services to users of other B/Ds.

Since Baseline IT Security Policy (S17) spells out the baseline security requirements, all Government information systems, regardless of providing services to users within its own B/D or to users of other B/Ds, should comply with the system requirements stated in S17. Users of Government information systems should also comply with the user requirements stated in S17.

Nevertheless, 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 of inter-departmental communication:

- Security requirements of an information system provider is STRONGER than security requirements of users from other B/Ds

  Under this scenario, 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.

- Security requirements of an information system provider is WEAKER than security requirements of users from other B/Ds

[8] "Softphone" systems, which implement VoIP using an ordinary computer with a headset and special software.

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 with laxer security requirements.

But 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.

In addition, 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. Moreover, additional measure 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.

12.9.2 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. Therefore 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 should be passed to external parties only on a “need to know” basis. B/Ds should ensure that arrangement for the protections of classified information comply as far as possible with the standards adopted within the Government. The external parties should be imposed the obligation not to disclose the classified information to third parties by entering into non-disclosure agreement and/or indemnity with the Government as appropriate.

12.10 INTERNET PROTOCOL VERSION 6 (IPV6) SECURITY

The prevailing Internet protocol standard is IPv4 (Internet Protocol version 4). There are well-known limitations of IPv4, including the limited IP address space and the security exposures. IPv4 specifies a 32-bit IP address field. Available address spaces are rapidly running out. As a result, the Internet Engineering Task Force (IETF) has been working on the IPv6 (Internet Protocol version 6) specifications in order to address these limitations, along with consideration on performance, ease-of-configuration, network management, and security issues.

The overall enhancements on IPv6 may provide better security in certain areas, but attackers might still be able to exploit part of the protocol.

Transitioning tools allow IPv4 applications to access IPv6 services, and vice versa. There are a variety of IPv6 transition technologies, such as 6to4 (defined in RFC 3056), Simple Internet Transition (SIT) tunnels, and IPv6 over UDP (e.g. Teredo). IPv6 traffic can enter networks via these methods while LAN/system administrators may not be aware that networks are vulnerable to IPv6 exploits. In addition, many firewalls permit UDP traffic, allowing IPv6 over UDP to get through firewalls such that LAN/system administrators are not aware of it. Attackers might also use 6to4 tunnels to evade IDS/IPS. Some firewall products are only capable of filtering IPv4 traffic but not IPv6. Attackers can exploit this loophole and hence compromise the network by using IPv6 packets.

Regarding host security on IPv4-IPv6 mixed networks, it should also be noted that applications are subject to attacks in both IPv6 and IPv4 versions. Therefore, if traffic blocking is required, it is necessary to act on both IP versions on any host control systems (firewall, VPN client, IDS/IPS, and so on).

In order to mitigate the threats associated with IPv6, the following measures should be taken when implementing IPv6:

- Make sure network devices are IPv6 aware and that the installed firewall and IDS/IPS can detect and enforce security policy on IPv6 traffic.
- Switch on IPv6 protection capabilities and security measures on both the firewall and IDS/IPS even it is working under an IPv4 environment.
- Provide IPv6 training to the LAN/system administrators.

12.11 DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC)

Domain Name System (DNS) is often subject to man-in-the-middle, spoofing, and cache-poisoning attacks that are hard to defend against. Domain Name System Security Extensions (DNSSEC) adds an additional layer of protection to the network by providing validation of DNS responses. It uses public key cryptography to verify the authenticity of a DNS record. By checking the digital signature, the client computers can trust that information they receive has not been modified or tampered. It protects users from being redirected to malicious sites.

DNSSEC is progressively rolled out to add security to the existing DNS infrastructure. B/Ds should plan and prepare for DNSSEC deployment. For DNSSEC implementation, B/D should consider:

- Designing a signing system – how to integrate the system with the existing DNS architecture and the changes to the existing procedures of DNS management have to be considered.

- Signing in a testing environment – before releasing the system to the external world, test the complete system, including all the defined procedures, under a testing environment.
- Checking DNS servers – verify the external authoritative name servers supporting DNSSEC.
- Key generating and management – the procedures to generate, publish and manage keys, as well as the size and lifespan of the keys should be planned.
- Establishing emergency procedure – the procedures to re-generate keys and re-sign the zone for should be established for case of key compromise.

12.12 VIRTUALISATION

Virtualisation refers to the technology of creating and managing one or more virtual machines (VMs) used for IT development, testing or operation. A VM could be served as a workstation, a server, a storage device or other network resource. There are several forms of virtualisation such as full virtualisation, server virtualisation, desktop virtualisation, application virtualisation and operating system virtualisation.

Before implementing virtualisation environment, security risks should be analysed by comparing with options without virtualisation. It should be treated as part of the risk management process before vendors or products are selected.

VMs on a physical machine are managed by a hypervisor (also called virtual machine monitor) which controls the flow of instructions between the VMs and the physical hardware (e.g. CPU, disk storage, memory and network interface cards). A hypervisor can run directly on the hardware, or runs as an application on top of an existing operating system (host OS). The VM running on top of the host operating system (host OS) is called the guest operating system (guest OS).

The security of a virtualised environment is heavily dependent on the individual security of each component, from the hypervisor and host OS (if applicable) to the VMs, applications and storage. In general, a virtualised environment should be secured in the same way as physical machine, and following security practices are recommended:

<u>Management Controls</u>

- Maintain up-to-date inventory records of a virtualised environment, including all relevant network and infrastructure components, and a list of VM images.
- Maintain configuration management procedures to cover all the physical and virtual machines in the virtualisation infrastructure.
- Segregate VM's and create security zones by type of usage (e.g. desktop vs server), development phase (e.g. development, testing and production), and sensitivity of data (e.g. classified data vs unclassified data).
- Ensure the connection of the virtualised environment to the Government network shall not compromise the existing security level.

- Review the resources requirement, such as disk spaces and network capacities, of VMs and applications.
- Establish recovery procedure to revert the VMs to known-good image.

Technical Controls

- Enable VM-specific network security features, such as host firewall on VMs, virtual network configuration and virtual firewall in hypervisor layer.
- Restrict access to the VMs using physical or virtual firewall commensurate with the business need, and regularly review the access policy to reflect new business needs.
- Implement hypervisor-based, network-based or host-based protection solution for each VM or a cluster of related VMs as appropriate, such as deploy anti-virus solution, firewall to monitor and block malicious traffic.
- Harden the hypervisor and VM instance. Configure the host OS with minimum required functions. Create a list of expected services and applications or white list for each VM.
- Disable unnecessary services (e.g. clipboard), communication ports and virtual hardware (e.g. virtual CDs, virtual network adapters) to reduce security vulnerabilities.
- Deploy patch management to the hypervisor and VM as if they are physical machines. Install all updates promptly to the hypervisor and all VMs, including online VMs (i.e. those in use) and offline VMs (i.e. those not in use but with their image files kept as backup).
- Use vulnerability management tools to regularly scan the host OS and VMs for vulnerabilities.
- Verify security status of each VM before putting into production or after restoring from a snapshot, including the updateness of the anti-virus solution and patching status.
- Protect against unauthorised access between two VMs. Enforce least privilege principle for communication between VMs, by disabling unnecessary VM-to-VM communication if possible.
- Restrict remote access to the management console by authorised personnel only.
- Manage VM images and snapshots with care, and encrypt VM images and snapshots whenever possible if sensitive data was involved.
- Log activities for privilege accounts of hypervisor and VM. Security logs should include events such as access to VM images and snapshots, changes to user access rights, modifications of file permission.
- Identify and delete all the image copies including the copies for backup or in failover system when the VM image is no longer needed.

12.13 CLOUD COMPUTING

Cloud computing can be viewed as a new way of delivering IT based services to enterprises, rather than a new technology on its own. For the most part, cloud computing uses similar management tools, operating systems, databases, server platforms, network infrastructure, network protocol, storage arrays, and so on. Therefore, security principles in cloud are largely similar to those in traditional IT environment. However, because of the cloud service models and deployment models used, and the technologies used to enable cloud services, certain risks in a traditional IT environment may become relatively more significant. Following security controls are recommended for handling such risks.

Management Controls

- Before engaging the service, plan the business needs, requirements on service and data confidentiality, integrity, availability and privacy aspects. Define a service level agreement (SLA) with the service provider, if applicable.
- Departmental security policy should be reviewed and modified with the necessary adjustments for protecting data to ensure the security controls are effective when deploying business applications in a cloud environment.
- Potential impacts of storing data in different physical locations and jurisdictions, as well as in a shared environment collocated with data from other clients, should be analysed in detail and the relevant procedures should be identified. Enhancement to the security measures should be considered to compensate for any areas outside B/D's direct control.
- Cloud services should be checked to ensure the compliance of globally recognised industry security standards, such as ISO 27001. Compliance certificates and reports should be requested from cloud service providers for verification on their validity.
- If possible, cloud service providers should be requested to provide third party audit reports, with documentation for remedial actions taken for dealing with security findings.
- When any part of the cloud service is outsourced, define clearly the security requirements, implement security measures so as to meet government security requirements commensurate with the involved data classification and sensitivity. Ensure external threats are properly addressed by the service provider. B/Ds should apply due diligence and oversight for external service providers satisfying the business, security and privacy needs.
- The ownership of the data stored in the cloud should be clearly defined and agreed with the service provider.
- Disaster recovery plan and business contingency plan should be developed to cater for unavailability of the cloud service. An exit strategy, including the arrangement of copying out and erasure of data, should be formulated.
- Roles and responsibilities should be clearly defined in a multi-tenancy cloud environment. Cloud service providers should be requested to have robust segregation of job duties. Request non-disclosure agreement from the external service providers and ensure they have proper human resource management. Internal and external staff

including subcontractors of the cloud service should be well trained in order to ascertain their security awareness and understanding of the security requirements.

- As with other in-house applications, a security risk assessment should be performed before production, and prior to major enhancements and changes associated with the cloud systems or applications. If a cloud service provider does not allow clients to directly conduct security risk assessment and audit on it, it should be requested to provide third party audit reports which meet industry standards and satisfy B/D's requirements.
- B/D and the cloud service provider need to agree in advance to what extent the B/D has accessibility to the cloud service provider to audit and verify the existence and effectiveness of security controls specified in the SLA. Both sides should agree how to collect, store, and share compliance evidence (e.g., audit logs, activity reports, system configurations).
- B/D should be well aware of the overall incident handling procedures of the service provider and should also ensure that the steps to be taken by the service provider and the timing of response in a security incident satisfy B/D's requirements. Information security incidents that originated from the cloud service provider's infrastructure might have an impact on the B/D's resources and they should be reported to the B/D with sufficient details.

Technical Controls

- Due to multi-tenancy nature in a cloud environment, the risks of unauthorised physical access by unknown co-tenants or third parties become one of the most security concerns. Adequate physical security measures in a cloud data centre could protect against trespassing activities to the computing resources at the physical layer. If there is special requirement of not sharing equipment or equipment racks with application systems of other B/Ds or application owners due to the sensitivity of data or other security requirements, an isolated area or equivalent measures should consider be provided by the premise provider to segregate the application owner's data and resources from others.
- In a cloud environment, authentication and authorisation on logical access control should be clearly defined, such as who should be granted with the rights to access the data, what their access rights are, and under what conditions these access rights are provided. The cloud services should enable support on various strong authentication options for use in accessing sensitive data.
- Regardless of public or private cloud, it is critical to acquire the log data that offers a clear view into the operational and security events. B/Ds should define the log requirements. For public cloud services, B/Ds should understand whether the provider could supply the required log data.
- Classified data should be protected through encryption both at rest and in transit in a cloud environment. The cryptographic keys should be managed and protected properly. Key management on storage should be enforced and keys are desirable to be managed in the custody of the B/D.
- The data on backup media held by the cloud service provider could commingle with other cloud tenant's data. Regular backup for all operational data at client side is

advised. Recovery tests should be conducted to assure that recovery to the most up-to-date state is possible.

- Secure software development lifecycle processes, e.g. security design review, should be applied to applications built on the cloud platform to make application less vulnerable to potential threats after release. Credentials should be kept securely to help prevent unauthorised access to as well as illicit tampering of application programs and control files.

End-user Controls

- Awareness training should be provided to end-users on the secure use of cloud services, such as the use of encrypted network or two-factor authentication to access the data on cloud.
- Staff should only use approved cloud services.
- Staff should not upload any classified or personal data without prior approval.

12.14 MONITORING

12.14.1 Logging

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

For more complicated applications, they 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 log 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, searching.

B/D should define policies relating to the logging of activities of information systems according to its business needs and data classification. The policies shall include but not be limited to the requirement to log successful and unsuccessful log-in attempts, activities of privileged user-IDs, changes to user access rights, details of password changes, modification to software etc. The information logged should meet the above requirement at minimum in order 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. Nevertheless, the logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity as approved by a Directorate officer.

Logs shall be retained for a period commensurate with their usefulness as an audit tool. During this period, such logs shall be secured such that they cannot be modified, and can only be read by authorised persons.

Regular checking on log records, especially on system/application where classified information is processed/stored, shall be performed, not only on the completeness but also the integrity of the log records. 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.

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 individual who has shared access to a particular system at a given time for an investigation if required.

In accordance with Chapter IX of the Security Regulations, systems containing information classified as CONFIDENTIAL or above require mandatory audit trail on all shared access to the data.

Audit trail and logging features should be enabled on standalone PC or workstation when classified data is stored on its hard drive.

Information systems shall synchronise its clock with a trusted time server periodically (at least once per month). B/Ds should use the clock synchronisation service from GNET or use the time server of Hong Kong Observatory via the Network Time Protocol (NTP). Authentication in NTP can be considered to enhance security in 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 investigation.

Information about the time synchronisation service of Hong Kong Observatory is available at

http://www.hko.gov.hk/nts/ntime.htm

12.14.2 Monitoring the System

In addition to the application log, server system log (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.

More and more vendors nowadays adopt or comply with international/industry standards, such as Common Criteria (http://www.commoncriteriaportal.org/), in building security facilities into their systems. Such standards usually have different certifications for systems attaining different levels of security requirements. B/Ds may consider such certification requirements when assessing the security measures provided by the systems based on their business needs.

On the other hand, all unauthorised accesses to an Information System must 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 unauthorised users of an information system can be detected via system monitoring. Monitoring a system, which must be done on a regular basis, involves looking at several parts of a system and searching for anything unusual.

12.14.3 Tools for Monitoring the System

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:

i. 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.
ii. 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.
iii. 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.
iv. Operating system commands which 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's 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 IDSes/IPSes 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 IDSes/IPSes can also verify data integrity of important files and executables. The IDS/IPS will check a database of sensitive files pre-selected by the user and creates a checksum of each file with a message-file digest utility such as md5sum or sha1sum. 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 files checksums do not match, then the IDS/IPS will alert the administrator by email or pager.

Other tools would also be available from external vendors and public software distribution sites.

12.14.4 Varying the Monitoring Schedule

Despite the advantages that regular system monitoring provides, some intruders will be aware of the standard logging mechanisms in use on systems they are attacking. They will actively pursue and attempt to disable monitoring mechanisms. Regular monitoring does not provide full guarantee that the system is secure, nor should monitoring be considered an infallible method of detecting unauthorised use. Varying the monitoring schedule should always be considered.

To minimise the chance of illegal access, monitoring commands should be executed more frequently and at different times throughout the day, making it hard for intruders to predict the actions.

12.15 ADDITIONAL REFERENCES

- "Email Issues", related articles from The SANS Institute. http://www.sans.org/reading_room/whitepapers/email/
- "Firewall & Perimeter Protection", related articles from The SANS Institute. http://www.sans.org/reading_room/whitepapers/firewalls/
- "Instant Messaging Rules – A Business Guide to Managing Policies, Security, and Legal Issues for Safe IM Communication", Nancy Flynn, American Management Association.
- "Threat Intelligence Library", McAfee Labs. http://www.mcafee.com/us/mcafee-labs/threat-intelligence.aspx

- "Security Response", Symantec Corporation.
  http://www.symantec.com/business/security_response/index.jsp
- "Hoax warning", F-Secure.
  http://www.f-secure.com/virus-info/hoax/
- "Security", Wi-Fi Alliance.
  http://www.wi-fi.org/security
- "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", SP 800-97, NIST.
  http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
- "Guide to Securing Legacy IEEE 802.11 Wireless Networks", SP 800-48 Rev 1, NIST.
  http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf
- "RFID Security and Privacy: A Research Survey", Ari Juels, RSA Laboratories.
  http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf
- "Security White Paper", RFID Journal.
  http://www.rfidjournal.com/whitepapers/5
- "Guide to Bluetooth Security", SP 800-121, NIST.
  http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf
- "Security", Bluetooth SIG Inc.
  http://developer.bluetooth.org/KnowledgeCenter/TechnologyOverview/Pages/Security.aspx
- "Security Considerations for Voice Over IP Systems", SP800-58, NIST.
  http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
- "A Complete Guide on IPv6 Attack and Defense", The SANS institute.
  http://www.sans.org/reading_room/whitepapers/detection/complete-guide-ipv6-attack-defense_33904
- "Good Practices Guide for Deploying DNSSEC", ENISA.
  http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec/at_download/fullReport
- "Guiding principles for Cloud Computing Adoption and Use", ISACA.
  http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Guiding-Principles-for-Cloud-Computing-Adoption-and-Use.aspx

13. SECURITY RISK ASSESSMENT AND AUDITING

13.1 OVERVIEW

Security Risk Assessment is a process of evaluating security risks, which are related to the use of information technology. It shall be performed at least once every two years and shall also be performed before production, and prior to major enhancements and changes associated with the systems or applications. It can be used as a baseline for showing the amount of change since the last assessment, and how much more change is required in order to meet the security requirements.

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 at finding out whether the current environment is securely protected in accordance with the defined IT security policy. B/Ds shall identify and document all relevant statutory, regulatory and contractual requirements applicable to the operations of each information system. 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.

Before performing a security assessment or audit, B/Ds should define the scope, the budget and the duration allowed for the assessment or audit.

For guidelines on assessment and auditing methods / model, please refer to document

- **Security Risk Assessment & Audit Guidelines (G51)**
  http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g51_pub.pdf

13.2 ADDITIONAL REFERENCES

- "Management Planning Guide for Information Systems Security Auditing", the National State Auditors Association and the U.S. Government Accountability Office. http://www.gao.gov/special.pubs/mgmtpln.pdf

14. SECURITY INCIDENT MANAGEMENT

14.1 OVERVIEW

An IT security incident is any adverse event that could pose a threat to the availability, integrity and confidentiality of an information system or information asset.

Examples of security incidents include malicious code attacks, unauthorised access or utilisation of services, denial of resources, compromise of protected system privileges, malicious destruction or modification of data, intrusion, computer virus and hoaxes.

Every B/D should set up its departmental Information Security Incident Response Team (ISIRT) and appoint a Commander to oversee the handling of all information security incidents. An ISIRT Commander is responsible for collaboration with the Government Information Security Response Office (GIRO), which provides centralised co-ordination to B/Ds, upon happening of an IT security incident in the B/D.

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

- **Information Security Incident Handling Guidelines (G54)**
  http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/doc/g54_pub.pdf

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, drill should be arranged and exercised regularly.

14.2 ADDITIONAL REFERENCES

- "Publications and Resources", Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT).
  https://www.hkcert.org/

15. IT SECURITY POLICY CONSIDERATIONS

15.1 WHAT AN IT SECURITY POLICY IS

Essentially, IT security policy sets the minimum standards of a security specification. It states what aspects are of paramount importance to the organisation. Thus, IT security policy can be treated as basic rules which must be observed as mandatory while there can still be other desirable measures to enhance the security.

Individual departments should identify appropriate opportunities to establish the departmental IT security policy. For instance, when conducting Information Systems Strategy Study (ISSS) or when preparing business plans.

An IT security policy should cover the department's expectations of the proper use of its computer and network resources as well as the procedures to prevent and respond to security incidents. During the drafting of the policy, the department's own requirements on security should be considered. Besides, the requirements as specified in the Security Regulation, Personal Data (Privacy) Ordinance, Code on Access to Information, and Information on Record Management in the Manual of Office Practice should also be addressed. In other words, the drafting of the policy should consider the following aspects:

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

In fact, IT security policy can be very high-level and technology-neutral or detailed and technology-specific. IT security policy can be categorised into three basic types:

- Program-level policy

  It is used to create an organisation's computer security program by assigning program management responsibilities and stating organisation-wide computer security purpose and objectives. It is a high-level policy and is usually broad enough that it requires little modification over time.

- Issue-specific policy

  It identifies and focuses on areas of current relevance and concern. It requires more frequent revision due to changes in technology. For example, a policy on the proper use of a cutting-edge technology (whose vulnerabilities are still largely unknown) within an organisation.

- System-specific policy
  It focuses on policy issues which management has decided for a specific system. It addresses only one system while the program-level policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organisation.

The choice of developing which type of policy depends on your organisation's requirements. However, the most important thing is that policy sets the direction. The direction can be used as the basis for making other lower level decisions. In later sections, the term 'IT SECURITY POLICY' refers to a general IT security policy instead of referring to any of the above particular type so as to provide a baseline guidance.

15.2 TOOLS TO IMPLEMENT IT SECURITY POLICY

Because policy may be written at a broad level, it is essential to develop standards, guidelines and procedures to offer users, administrators, computer personnel and top management a clearer approach to implementing IT security policy and meeting the departmental missions.

STANDARDS specify a uniform use of specific technologies, parameters or processes to be used to secure systems. Standardisation can act as a control for IT security policy implementation and are normally compulsory. They are mandatory statements which can be measured.

GUIDELINES are similar to STANDARDS but they are not mandated actions. They can assist users, administrators and other systems personnel in effectively interpreting and implementing IT security policy. They are recommended as effective security practices that should be implemented where such controls are applicable and enforceable. Although guidelines are often used to ensure that specific security measures are not overlooked, they cannot cover every instance.

PROCEDURES are the detailed steps or instructions to be followed by users, system administrators, and other system operations personnel to accomplish a particular security-related task, and assist in complying with IT security policy, standards and guidelines.

In order to promote flexibility and cost-effectiveness, a mixed use of POLICY, STANDARDS, GUIDELINES and PROCEDURES may be promulgated throughout a department as they are closely related to each other.

15.3 HOW TO DEVELOP AN IT SECURITY POLICY

Policy creation shall be a joint effort of technical persons, who understand the full ramifications of the proposed policy and the implementation of the policy, and decision makers who have the power to enforce the policy. A policy must be implementable and enforceable.

Since an IT security policy can affect everyone in an organisation, every user should be involved when establishing the policy, though in a variety of ways depending on their level of responsibility. The key element is making sure everyone knows their own responsibility in security related issues.

Developing an IT security policy requires to undergo a series of activities step by step. The first step is to form an IT security policy task force to assume an overall responsibility to define and upkeep the departmental IT security policy. Members of the task force may include as simple as one person or as structured as a well-organised IT Security Policy Group. It depends on the level of details and the scope covered. The policy task force may include empowered representatives from groups of staff or users such as:

- Human resources
- Legal and regulatory matters
- Information systems
- Public relations
- Security
- Line of business

Such task force can also be constructed with well-defined roles and responsibilities of each team member. The set of activities required to develop the IT security policy can then be defined and carried out under a properly managed environment.

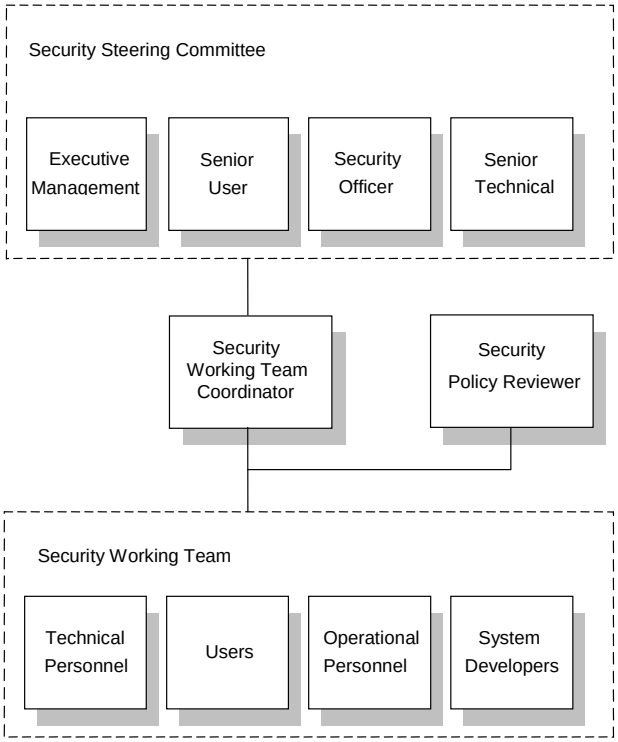
The development may consist of the following activities:

- Create a security task force such as an IT Security Policy Group
- Plan for the various activities and resources
- Determine the security requirements
- Construct an IT security policy framework
- Evaluate and review the IT security policy

The task force is expected to go through several iterations of review and refinement before a complete policy is developed. The following sections suggest a rather structured approach of forming IT security policy for reference. Organisation of the group and the development process may vary from one department to another according to specific departmental requirements.

15.3.1 Organisation of IT Security Policy Group

As policy drafting, review and enforcement involves the acceptance and support of various parties, the forming of a specialised team is particularly useful and effective. Below is a sample of such organisation model.



Sample Organisation Model of IT Security Policy Group

a) Security Steering Committee

A department can first organise a Security Steering Committee. A Security Steering Committee has the ultimate responsibility for developing the IT security policy. Its members have the responsibilities to decide the start and termination of the development, and to formulate a security working team. The Steering Committee is not involved in the detailed preparation activities but is the one who sets up high level guidelines and requirements, and who makes the key decision to evaluate and agree on the formulation of an IT security policy.

Examples of tasks performed by Security Steering Committee are:

- Determining requirements for policy.
- Meeting organisational or departmental policy needs.
- Getting agreement on security objectives.
- Identifying who should be involved in the developing process.
- Deciding on the developing schedule.

Only after the policy has been approved by the Steering Committee will it then be proposed and submitted to the management of the department or related parties for approval. This means that the policy so prepared shall conform to the department's own procedures for implementation and further approval.

Members of the committee may include:

i) Executive Management: who represents the interests of the departmental goals and objectives, and provides overall guidance and assessment of the IT security policy throughout the forming process. Examples are senior managers and principal officers from departments.

ii) Senior User: who represents the users of the related systems or applications which may be affected by the IT security policy. Examples are the senior officers, data/system owners and managers from departments.

iii) Security Officer: may be the DSO or any person who is responsible for the security issues of the department, and can state the high level security requirements with reference to the Security Regulations, law or rules of the Government such as the classification or sensitivity of information.

iv) Senior Technical: any personnel who can provide technical support for various security mechanisms or technological aspects. Senior Systems Manager from OGCIO is an example.

b) Security Working Team

A Security Working Team is a group of staff and users who are directly involved in developing the details of the IT security policy. They are required to produce the policy draft to the Security Steering Committee. The security working team members may change or vary depending on the needs and requirements of the department and the policy issues.

Team members include but are not limited to:

i) Technical Personnel: may refer to security administrators, network administrators, system administrators or technical support staff who are familiar with the technological aspects, and participate in all technical related issues.

ii) Users: are the user / staff who give detail user or business requirements related to user interests on the IT security policy.

iii) Operational Personnel: may refer to the system operators or any administrative staff who provide the day-to-day operation and monitoring support. Depending on the organisational establishment of the department and project, Operational Personnel may come from departments or the computer operations of OGCIO.

iv) System Developers: are the application or system developers such as the project team members, who may be affected by the IT security policy. Project team members may include Systems Managers and Analyst/Programmers from OGCIO, contract staff, or even external human resources for outsourced projects.

c) Security Working Team Coordinator

A Security Working Team Coordinator is responsible to coordinate among the security working team members for managing and controlling the preparation of the policy within the time set by the Security Steering Committee. This co-ordinator may be managers or officers from departments.

d) IT Security Policy Reviewer

It may include staff or group of staff from internal or appointed external qualified consultants who are responsible for reviewing the IT security policy including quality assurance and applicability of the IT security policy. The internal or external security consultants / auditors can assist in formulating the compliance measure of the IT security policy. Permanent establishment of this team may or may not be required depending on the department's own needs.

The above organisation model is used herein as a sample and individual department may tailor for its own structure or functional units. For some departments, they may only require a Security Working Team Coordinator to perform all the tasks and propose the policy to their senior management. Whilst for other departments, a Security Working Team may be sufficient.

15.3.2 Planning

Plans provide information that is a basis for decision making and controlling. By planning the necessary resources required and the activities to be undertaken, the development of the IT security policy can be monitored and under control. The Security Working Team Coordinator will be responsible for planning of the detailed activities which will be controlled and monitored by the Security Steering Committee.

a) Initial Planning

It focuses on the goals and objectives of the IT security policy. This can help to identify whether the activities undertaken are those necessary ones, and can ensure that a common understanding exists among all interested parties. The establishment process may be divided into different stages, which must be distinct and manageable.

This plan is probably prepared by the Security Steering Committee. The committee shall define the policy scope which may cover certain areas of use and responsibility. Examples are Internet IT Security Policy or Security Incident Response Policy.

b) Resource Planning

It is used to identify the details of various resources required for developing the IT security policy. It can highlight the type, amount and period of use of these resources

including personnel and administrators for different stages of the policy development process. Everything to be secured shall have an owner and they shall be involved in the preparation process.

c) Control Planning

It is used to control the whole development project by identifying the major control points or checkpoints for different stages of activities.

At each checkpoint, there will be meetings to review the progress and to make any refinements if necessary. Regular meetings will also be performed by the Steering Committee as control by reviewing the progress of the working team.

The planning activities vary a lot depending on how detailed the policy is, how sensitive the information is, and how much protection intended to have.

15.3.3 Determination of Security Requirements

One of the ways to identify security requirements is by means of risk analysis. Risk analysis involves determining what to protect, against what to protect it from, and how to protect it. It is the process of examining all of risks, and ranking those risks by level of severity. This process results in making cost-effective decisions on what is required to protect. The results of risk analysis, if performed, should be documented together with the "Audit, Control and Security Requirement" of the Feasibility Study or System Analysis & Design Technical Specification.

There are three major steps in risk analysis, namely:

- Identifying the assets (What to protect)
- Identifying the threats (Against what to protect from)
- Identifying the impacts (How much risk to bear)

a) Identifying the Assets

The essential point in this step is to list all the things that are subjected to security threats. The following is a list of categories for general reference:

- Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers, hubs, gateways, servers, modems.
- Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication program, firewall software.

- Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media, any information resident within the organisation.
- People: users, people needed to run systems.
- Documentation: on programs, hardware, systems, local administrative procedures.
- Supplies: paper, forms, ribbons, magnetic, optical or solid state devices.

Based on the list of assets, an information asset inventory can be prepared to keep an accurate inventory with the following information for each asset:

- Designated 'owner' of the information.
- General support system or critical/major application.
- Physical or logical location.
- Inventory item number if applicable such as bar code or serial number.

b) Identifying the Threats

Once the assets requiring protection are identified, it is necessary to identify threats to those assets. The threats can then be examined to determine what potential for loss exists. It helps to consider what threats to protect assets from. There are generally two basic types of threats: accidental threats and intentional threats.

Accidental threats can result in either exposure of sensitive information or causing an illegal system state to occur due to modification of information. An intentional threat is an action performed by an entity with the intention to violate the security. Examples are destruction, modification, fabrication, interruption or interception of data.

In general, threats to an asset should be considered in terms of the availability, confidentiality and integrity of the asset. The following sections describe some possible threats to an information system. It should be noted that the list is not exhaustive, and other threats may be identified depending on the assets one wants to protect.

i) Unauthorised Access

Unauthorised access may take many forms. One form of unauthorised access is the use of another user's account to gain access to a system. The use of any computer resource without prior permission may also be considered as another form of unauthorised access.

The seriousness of an unauthorised access will vary from site to site. For some sites, it may cause irreparable harm while for others, it may open the door for other security threats. Unauthorised access may be performed by both insiders and outsiders.

ii) Disclosure of Information

Another common threat is disclosure of information. The impact of disclosing valuable or sensitive information stored on the computers is unquestionable. Generally, there are three instances in which information is vulnerable to disclosure:

- When the information is stored on an information system.
- When the information is in transit to another system (on the network).
- When the information is stored on backup media.

The first type of instances can be controlled by file permissions, access control lists, and other similar mechanisms. The second type can be controlled by transmission through dedicated leased lines or password-protected dial-up lines and the last type by restricting access to the backup media (by locking them in a safe, for example). All three cases can be supplemented by using encryption mechanisms.

The advantage of using encryption is that, even if other access control mechanisms are compromised by an intruder, the data is still unusable. This is particularly important when there is external connection with the Internet or public network. The risk of disclosure may be higher then.

Information in transit may be vulnerable to interception as well. Several solutions to this exist, ranging from simply encrypting files before transferring them (end-to-end encryption) to special network hardware which encrypts everything it sends without user intervention (secure links).

iii) Denial of Service

Many people rely on services provided by the computers/computer networks to perform their jobs efficiently. If these services are not available, a loss in productivity results. Each site should determine which services are essential, and for each of these services determine the effect to the site if that service were to become disabled. Therefore, working out the security requirements together with users is very important.

c) Identifying the Impacts

After identifying the assets and threats, the impact of security attack should be assessed and appropriate security measures should be introduced. The following is a list of tasks for the process:

- Identifying the vulnerabilities of the system.

- Analysing the likelihood of threats aimed at exploiting these vulnerabilities.
- Assessing the consequences if each threat was to take place.
- Estimating the cost of each attack.
- Costing out potential countermeasures.
- Selecting the security mechanisms that are justified.

The consequence of a threat materialised in an organisation could result in one or more impacts on the organisation. For example, impacts can be from:

- Infringement of privacy
- Financial loss
- Disruption to activities

Impacts can be estimated in monetary terms of any loss of software and files, hardware damage, and manpower costs to restore altered files, reconfigure affected systems, and so forth. Intangible impacts may have even greater influence and should also be estimated in non-monetary terms. Examples of these impacts are staff morale, government prestige or public image. Violations of individual privacy rights may also violate the 'Personal Data (Privacy) Ordinance'. Details of the data protection principles in the Ordinance can be found at:

http://www.pcpd.org.hk/english/ordinance/section_76.html and

http://www.pcpd.org.hk/english/ordinance/section_77.html.

15.3.4 Construction of an IT Security Policy Framework

After gathering and ranking the security requirements, the policy can be grounded in good sense. A common way is to use a hierarchical approach by first defining the overall scope and then breaking the scope into various components.

Examples of events are:

- Describe the overall security program objectives or scope.
- Itemise the results of risk analysis, including the threats responding to and the corresponding safeguards.
- Define roles and responsibilities of various parties for the implementation and maintenance of such safeguards.
- Define appropriate and inappropriate behaviour for users so that the evidence can be used in court if security violations occur.
- Address internal and external issues.
- Be consistent and associated with a 'code of conduct', laws, regulations and policies for individuals or groups to make reference to, for example, the 'Code on Access to Information'.

IT security policy shall also address those procedures and behaviours that can be changed. It is also important to recognise that there are always exceptions to every security rule. Keep the policy as flexible as possible for an IT security policy to be viable in a longer term.

The major contents of the IT security policy can include the followings:

- What the policy objectives and scope are?
- Which information resources to protect?
- Whom the policy affects with?
- Who has what authorities and privileges?
- Who can grant authorities and privileges?
- What the minimum measures to protect the information resources are?
- Expectations and procedures for reporting security violations and crimes.
- Specific management and user responsibilities for making security effective.
- Policy effective date and revision dates or interval.

In order to fill in the above contents, below are some sample questions one may need to ask and answer. In addition, aspects of the particular department shall be considered as well.

- Who is allowed to use the resources?
  - To explicitly state who is authorised to use what resources.

- What is the proper use of the resources?
  - To provide guidelines for the acceptable use as well as unacceptable use of resources.
  - To include types of use that may be restricted.
  - To define limits to access and authority.

- Who is authorised to grant access and approve usage?
  - To state who is authorised to grant access to the services and type of access they are permitted to give.

- Who may have system administration privileges?
  - To determine very carefully who will have access to system administrator privileges and passwords for the services. One approach is to grant only minimal privilege to accomplish the necessary tasks.

- What are the user's rights and responsibilities?
  - To incorporate a statement on the users' rights and responsibilities concerning the user of the site's information systems and services.

- What are the rights and responsibilities of the system administrator versus those of the user?
  - To specify to what degree system administrators can examine user files to diagnose problems or for other purposes, and what rights you granted to the users.

- What do you do with sensitive information?
  - To determine the level of sensitivity of data that users should store on systems.

The style of the policy is better to have the following characteristics:

- Use colloquial language that is common and easy to read and understand.
- Don't be clumsy, i.e. simply explains the deal by clear sentence and wordings.
- Be brief and keep the sentence simple and short.
- Be concise and unambiguous.
- Easy to teach and use.
- Provide ease of access to everyone who are related, for example, stored in global database or public directory.
- Break up policy document into digestible bites instead of a big one.
- Conform to the departmental format or standard of other existing policies or procedures.

15.3.5 Evaluation and Periodic Review

Evaluate the proposed policy by inviting open discussion or arranging meetings among related parties or departments. Hiring external qualified IT security auditors or consultants to review or assist in the development of the policy is a possible way to improve the quality and completeness of the policy. If necessary, the policy may be reviewed by legal counsel.

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

15.4 HOW TO GET IT SECURITY POLICY IMPLEMENTED

Even if an IT security policy has obtained approval, putting the IT security policy in place is another story. It requires a series of activities to streamline the process. The paragraphs below list some of these major activities. Departments should also consider their procedures, rules and regulations during implementation.

15.4.1 Security Awareness & Training

Security Awareness is crucial to ensuring that all related parties understand the risks, and accept and adopt good security practices. Training and education can provide users, developers, system administrators, security administrators and any related parties with the necessary skills and knowledge in implementing the security measures.

No policy is considered to be implemented unless users or related parties have commitment and communication. This means 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 in the skills needed to follow the policy.
- Feel that security measures are created for their own benefit.
- Are periodically reminded of and refreshed for new issues.
- Have signed for acknowledgement.
- Are provided with policy guidance in manageable units.

15.4.2 Enforcement and Redress

It refers to the task of enforcement of rights arising from the policy implementation and redress for violations of those rights. Department should set up procedures to provide prompt assistance in investigative matters relating to breaches of security. Establish a Departmental Information Security Incident Response Team (ISIRT) and set up a security incident handling procedure can improve the effectiveness of the policy.

15.4.3 On-going Involvement of All Parties

An effective IT security policy will also rely on continuous exchange of information, consultation, co-ordination and co-operation among users and departments. Injection of knowledge on standards, methods, codes of practice and other expertise on IT security from the private sector will also help to keep the IT security policy up-to-date and relevant.

15.5 ADDITIONAL REFERENCES

- "Security Policy Issues" related articles from The SANS Institute. http://www.sans.org/reading_room/whitepapers/policyissues/

*** End ***

APPENDIX A SAMPLE IT SECURITY END USER INSTRUCTIONS

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

The Instructions are summarised from both the Baseline IT Security Policy (S17) and the Security Regulations such that, users can have a basic understanding of their security responsibilities related to information system usage.

B/Ds are recommended to 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 for reading the document.

This End User Instructions document, however, is not intended as a replacement of the existing security documents in the B/D or 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***]. End user diligence is necessary to protect the information or the information systems commensurate with the data classification. Each user is accountable to all of his/her activities on the information systems.

Security is the personal responsibility of every user. To protect classified or personal information from unauthorised access or unauthorised disclosure, prevailing Government security requirements, including Security Regulations and Baseline IT Security Policy, shall be observed. No officer may 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 should be applied to all classified information, which should be provided only to persons who require it for the efficient discharge of their work and who have authorised access. If in any doubt as to whether an officer has authorised access to a particular document or classification or information, the Departmental Security Officer should be consulted.

Users should safe keep and protect computers and storage devices from unauthorised access or disclosure of information under their custody. Appropriate security measures should be implemented to protect Government information assets and information systems. If a user discovers any suspicious activities or suspects a security breach, the user should 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

1. The classification category must be clearly marked, for example, adding [RESTRICTED] before the subject title for an email containing RESTRICTED information.
2. All stored CONFIDENTIAL information must be encrypted. Transmission of CONFIDENTIAL or RESTRICTED information must be encrypted.
3. For transmission of CONFIDENTIAL information by electronic mail within the Government, the Confidential Mail System should be used.
4. 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 drawer when unattended.
5. Release information and grant the data access right based on a need-to-know basis.
6. Select passwords in accordance with the departmental password management requirements, e.g. at least six alphabetic and non-alphabetic characters (numerals or punctuation) and change your password periodically. If you suspect a password has been compromised, change it immediately and report to your supervisor.
7. Use separate passwords for systems with different security requirements, e.g. the password of your official email account should be different with your personal email account.
8. Apply latest security patches and regularly remove cache files or temporary files to protect data privacy.
9. Be aware that it is dangerous to download files from the Internet unless the file is from a known and trusted source.
10. Install virus, malicious code detection measure with latest signatures and definition files to perform scanning including email, downloaded file, files in removable media or mobile device before use.
11. Spam email[9] should be ignored or deleted. Beware of phishing email[10] which could lead to virus infection or even security breach.
12. Protect wireless or mobile devices by use of encryption to protect data transmitted and use of password-protected features to protect against unauthorised usage.
13. Disable wireless and mobile services when there is no need to use them.

[9] Spam email refers to flooding of an email account with many unwanted message, such as advertisement.
[10] Phishing email refers to email imitating to be sent from a person you knew, which attempts to steal information.

DON’Ts

1. Don’t store classified information in your own mobile devices or removable media.
2. Don’t leave your workstation and computer equipment unattended without sufficient physical access controls, e.g. opened door, left on desk.
3. Don’t keep a written record of password anywhere near to your work (e.g. a memo stuck on screen), nor use any information that is easy to be guessed (e.g. a dictionary word) or related to you (e.g. name, birthday or post) as your password, nor share your password with others.
4. Don’t disclose information about your own, your system or your department to any unauthorised person.
5. Don’t connect your own device to Government internal information system or network.
6. Don’t connect workstations to external network by means of dial-up modem, wireless interface or broadband link.
7. Don’t open any suspicious emails or follow any links to avoid being redirected to malicious websites.
8. Don’t publish or use office email address when participating in public websites to avoid office email address and/or mail systems to become a target of attack.
9. Don’t install software in your workstation without prior approval of DITSO.