For information
4 May 2006

Legislative Council Panel on Security

Guidelines on Information Security

Purpose

As requested by the Panel on Security, this note sets out the guidelines on information security of the Administration. Where appropriate these guidelines are applicable to information technology contracts.

The Guidelines

2. A list of relevant guidelines issued by the then Information Technology Services Department (ITSD), the Office of the Government Chief Information Officer (OGCIO) and the Security Bureau (SB), is as follows -

(a) ITSD Circular No. 1/96 on Guidelines on Microcomputer and Local Area Network Security, at **Annex A**;

(b) Baseline IT Security Policy issued by OGCIO, the content pages of which are at **Annex B**;

(c) IT Security Guidelines issued by OGCIO, the content pages of which are at **Annex C**;

(d) Security Risk Assessment and Audit Guidelines issued by OGCIO, the content pages of which are at **Annex D**;

(e) Information Security Incident Handling Guidelines issued by OGCIO, the content pages of which are at **Annex E**; and

(Given their bulk, the full versions of the guidelines at (b) to (e) above are not attached, but they may be viewed at www.infosec.gov.hk/english/itpro/guidelines.htm (English) and www.infosec.gov.hk/chinese/itpro/guidelines.htm (Chinese).)

(f) Security Regulations issued by SB, the more relevant extracts of which are at **Annex F**.

3. Members may also wish to refer to Paper CB(1)1097/05-06(01) entitled "Information Security" discussed at the meeting of the Panel on Information Technology and Broadcasting on 17 March 2006.

Security Bureau
Office of the Government Chief Information Officer
April 2006

Annex A

MEMO

From Director of Information Technology Services	*To* Heads of Branches and Departments
Ref. (13) *in* ITS 11/10 III	
Tel.No. 2582 4488 *Fax No.* 28024549	*Your Ref.* ____ *in* ____
Date 1 March, 1996	*dated* ____

ITSD Circular No. 01/96

Guidelines on Microcomputer and Local Area Network Security

~~(This circular sudersedes circular no. 4/88 dated 29.7.88)~~

The Guidelines on Microcomputer Security have been revised to become the Guidelines on Microcomputer and Local Area Network (LAN) Security to address issues of security in the use of microcomputers and their related equipment both on a *standalone* basis and when connected to a *LAN*.

2. A copy of the guidelines is enclosed herewith for your reference. The guidelines will also be included in our Microcomputer User Guide to be issued to individual users together with every microcomputer system purchased from the bulk contracts for microcomputers and LAN's.

3. These guidelines are issued for use by officers who need to manage and carry out the implementation of microcomputer and LAN security in their organizations.

4. Should you have any enquiry on the contents of the guidelines, please contact Mr. Nick Chan at 2582 4584 or:

TSSC Helpdesk Tel. No. : 2961 8383

Address: Technology Services Support Centre(TSSC)
Information Technology Services Department
20/F Wu Chung House
213, Queen's Road East
Wanchai, Hong Kong

(K.H. Lau)
Director of Information Technology Services

c.c. Judiciary Administrator
SMs and above, ITSD
ITS 61/39/14

Standards and Methods Document

GUIDELINES ON MICROCOMPUTER AND LOCAL AREA NETWORK SECURITY

Ref. No: G4
Version: 1.1

January 1996

TABLE OF CONTENTS

1. PURPOSE 1-1
2. SCOPE 2-1
3. REFERENCES 3-1
4. DEFINITIONS AND CONVENTIONS 4-1
   - 4.1 Definitions 4-1
   - 4.2 Conventions 4-2
5. PROTECTION AGAINST UNINTENDED EVENTS 5-1
   - 5.1 Access Control 5-1
   - 5.2 Systems Software Security 5-2
   - 5.3 Application Software Security 5-3
   - 5.4 Data Security 5-3
   - 5.5 Virus Considerations 5-5
   - 5.6 Disaster Recovery Plan 5-6
   - 5.7 Software Piracy 5-6
6. PROTECTION AGAINST UNAUTHORIZED ACCESS 6-1
   - 6.1 Access Control 6-1
   - 6.2 Systems Software Security 6-2
   - 6.3 Application Software Security 6-4
   - 6.4 Data Security 6-4
   - 6.5 Computer Crimes Legislation 6-5

1. PURPOSE

The guidelines in this document are meant to address from various aspects the major issues in implementing security upon microcomputers and their related equipment.

The target readers are assumed to have a fairly technical background in microcomputers. The guidelines would be suitable for these officers to carry out the implementation of microcomputer and local area network (LAN) security in their organizations.

2. SCOPE

The guidelines in this document are applicable to the protection of microcomputer equipment, their software systems, their application programs, and their data in standalone or local area network (LAN) environments.

Because of the widespread use of microcomputer equipment, the consequences of not having such Information Technology (IT) resources adequately protected may have financial or legal implications, and may lead to service interruption, data destruction, data disclosure, data modification, etc.

With respect to the LAN environment, the guidelines may not be fully applicable to systems demanding high resilience or high availability, or those involving midrange or mainframe systems. For such systems, project-specific security measures should be considered additionally.

3. REFERENCES

The following ITSD documents are related to, or referred to, in the guidelines:

- Microcomputer User Guide
- LAN Administrator's Guidelines for LANtastic
- LAN Administrator's Guidelines for LAN Manager
- LAN Administrator's Guidelines for NetWare.

Enquiries about the documents can be addressed to the TSSC Helpdesk at 2961-8383.

4. DEFINITIONS AND CONVENTIONS

4.1 DEFINITIONS

Security

From an IT perspective, security refers mainly to the protection of IT resources against unauthorized or unintended events. Examples of unauthorized events are: intentional interference or damage to programs or data, unauthorized program or data access and any misuse of a computer as defined in the Computer Crimes Ordinance 1993 (see 6.4.2). Examples of unintended events are: hardware or software faults, power interruptions, and virus infections.

Workstation

In these guidelines, workstation refers to a microcomputer operating either in standalone mode, or in a local area network as a network terminal.

Server

A server in the LAN environment is essentially a high performance microcomputer acting as a central service provider to the network. Examples of such services are: file sharing, data sharing, and gateway access to another computer; hence the names file server, database server, communications server respectively.

Systems Software

Systems software refers to operating systems of microcomputers such as DOS or Windows 95 and that of LAN file servers such as NetWare.

Application Software

Application software refers to the commonly used microcomputer packages such as spreadsheet and word processing software, as well as self-developed application programs running on microcomputers.

Virus

Virus is a subversive computer program that may corrupt or erase computer files and it may change the normal behaviour of the computer. Any of the following symptoms could be a signal of viral activity:

- The program takes longer than usual to execute.
- A sudden reduction in available system memory or disk space.
- A device light is on whilst there should be no activity with that device.

AVACS

The Anti-Virus and Access Control System developed by ITSD for enforcing security on microcomputer systems. Moreover, AVACS provides a customizable menu system to simplify microcomputer operations, a file encryption utility, a report program on system information, and a text-file viewer program.

TSSC

The Technology Services Support Centre set up by ITSD to provide Helpdesk and prototyping services to the Government users.

4.2 CONVENTIONS

Since IT security is about the protection of resources against unintended or unauthorized events, the guidelines are presented according to the following hierarchical format:

Protection Against Unintended Events
Access Control
- *General guidelines*
- *LAN Environment guidelines*

Systems Software Security
... (with sub-divisions where applicable as above)
Application Software Security
...
Data Security
...
Virus Considerations
...
Disaster Recovery Plan
...
Software Piracy
...
Protection Against Unauthorized Access
Access Control
...
(with sub-sections where applicable as above)

(Note The *General Guidelines* are also applicable to the LAN environment.)

5. PROTECTION AGAINST UNINTENDED EVENTS

5.1 ACCESS CONTROL

General

5.1.1 Office environment is in general acceptable for the operation of microcomputer equipment. However, for some equipment, there might be special requirements on site preparation and the operating environment. For such cases, advice can be sought from the equipment vendors and ITSD.

5.1.2 Sufficient space must be provided for the microcomputer equipment for both operating and access area.

5.1.3 Additional space must be allowed to cater for media storage, working area, and future expansion.

5.1.4 Microcomputer equipment must not be located near heat-generating areas or places where fire risk is high. Examples of such places are boiler rooms and canteen kitchens.

5.1.5 Smoking and drinking near the microcomputer equipment should be prohibited.

5.1.6 Portable fire extinguishers are preferred to be installed at sites with microcomputer equipment.

5.1.7 Direct sunlight upon the microcomputer systems should be avoided to prevent possible overheating or reflection from the monitor screens.

5.1.8 The operating environment should preferably be with low level of dust and dirt. The accommodation area is expected to be vacuum-cleaned regularly.

5.1.9 The microcomputer equipment should not be located in an area where there is high-frequency apparatus, or where there is excessive vibration.

5.1.10 The storage for microcomputer related magnetic media (such as tapes and floppy diskettes) should be away from any lightning conductor in the building as far as possible.

5.1.11 Provision of plastic covers for microcomputer equipment when they are powered off can, to a certain extent, protect the equipment from water damage.

5.1.12 All electrical installations should conform to the relevant standard specifications on electrical installation for Government buildings.

5.1.13 Electrical load surges or transient disturbance can cause system failures. Mains supply should not be shared with heavy, intermittent or switched loads.

5.1.14 Power sockets are recommended to be installed separately and dedicated to the microcomputer equipment. Appliances that are switched on and off frequently would be better not connected to dedicated power circuits.

5.1.15 Installation of hardware and software items to the microcomputer equipment should only be carried out by authorized personnel.

LAN Environment

5.1.16 If the LAN is to be installed on solid ground, ducts or trunkings (PVC or metal, covered by ramps) should, as far as possible, be used to protect the LAN cables from mechanical damage. Raised floors may be used optionally.

5.1.17 LAN cables should not be laid adjacent to mains electrical cables, telephone cables, paging system cables, etc. without suitable trunkings.

5.1.18 Uninterruptible power supply (UPS) should be considered for protecting the LAN servers against power surges and for the tidy close-down of the servers in case of prolonged power failure.

5.1.19 Connection of equipment to, or disconnection of equipment from, a LAN should only be carried out by authorized personnel.

5.2 SYSTEMS SOFTWARE SECURITY

General

5.2.1 Backup copies of the systems software and related configuration files should be taken periodically. Since systems software are the vital parts of any production service, the entire process of backup and restore should be well proven.

5.2.2 Wherever possible, backup copies of the systems software and related configuration files should be stored at a safe and secure location remote from the primary site, so that it would still be possible to reconstruct the operating environment should a disaster occur at the primary location.

5.3 APPLICATION SOFTWARE SECURITY

General

5.3.1 When two or more applications are to reside in the same microcomputer system, some measures must be devised to guard themselves against unintended interference by one another. For example, when data files are shared, each application should be aware of the possible risk in data corruption.

5.3.2 Similar to systems software, backup copies of the application software and related control files should be taken periodically. The entire process of backup and restore should be well proven. Wherever possible, the backup copies should be stored at a safe and secure location remote from the primary site, so that it would still be possible to reconstruct the operating environment should a disaster occur at the primary location.

LAN Environment

5.3.3 The need for process isolation is again emphasized for applications running in the LAN environment. Sufficient isolation schemes must be implemented to prevent unintended process interference.

5.3.4 It should be noted that in most cases, an existing single-user application on a microcomputer system would not work properly when directly migrated to run in a multi-user LAN environment.

5.4 DATA SECURITY

General

5.4.1 Backup copies should be maintained for all operational data to enable reconstruction should loss or destruction occur.

5.4.2 The backup copies should be taken at regular intervals such that recovery to the most up-to-date state is possible.

5.4.3 Procedures for data backup and recovery should be well established. Wherever possible, their effectiveness in real-life situations should be tested thoroughly.

5.4.4 It is advisable to store backup copies at a safe and secure location remote from the site of the microcomputer systems. In case of any disaster which damages totally the systems, the data could still be reconstructed on similar microcomputers elsewhere.

5.4.5 Multiple generations of backup copies should be maintained. This would provide additional flexibility and resilience to the recovery process.

5.4.6 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.

5.4.7 All data and documents of **Confidential** classification or above intended for processing by microcomputer systems should only be stored on removable media (e.g. floppy diskettes, removable hard disks) which can be stored away in a secure place after processing. Confidential data stored on the hard disk of a stand alone computer can be acceptable only if the computer can be stored in a secure place. Please refer to 6.4.3 of this document.

5.4.8 All media, including magnetic ones, containing classified information must be marked, handled and stored in the same way as their paper equivalent in accordance with **Chapter IV: Control of Classified Documents** of the **Security Regulations, REGULATIONS OF THE HONG KONG GOVERNMENT Volume 5.**

5.4.9 All intermediate material and information produced in the course of processing must also be accorded security protection of a degree commensurate with the highest classification of information contained in them.

5.4.10 Deletion of data files from microcomputer systems does not imply complete removal of the information. In most cases, the data are only made inaccessible by normal means. Thus it is advisable to either reuse the previously occupied area for storage of information of the same security classification, or reinitialize the area for storing data of a lower security classification.

5.4.11 Complete erasure of hard disk information can be accomplished through some common utility packages, a disk formatting function in the AVACS of ITSD, or physical destruction of the concerned disk.

5.4.12 All out-dated hardcopy printout or reports with classified grading should be downgraded and/or disposed in accordance with the relevant Security Regulations (Chapter III & IV).

LAN Environment

5.4.13 User data can be stored both in the LAN file server and in the workstations. There are many factors (e.g. backup and recovery set-up, physical security, server capacity) governing where private data should be stored, and the decision may vary from case to case. Advice can be sought from ITSD whenever necessary.

5.5 VIRUS CONSIDERATIONS

General

5.5.1 Illegal copies of software have been regarded as the most common source of viruses. It must be emphasized that in order to minimize the risk of contracting virus and to avoid infringement of copyrights, software products should only be acquired from authorized agents.

5.5.2 It is a good practice to check every floppy diskette (especially those of unknown origin) with a virus scanning program before use. However, it should be noted that new viruses are being discovered almost every day, thus a floppy diskette may contain a new virus that cannot be recognized by the scanning program.

5.5.3 Public domain software, according to past records, have a relatively higher chance of being virus infected. Use of such software should be avoided.

5.5.4 It is a good practice to write-protect all floppy diskettes that are not expected to be written. Also, it is a good practice to remove floppy diskettes from drive slots after use.

5.5.5 In a publicly accessed microcomputer or LAN server, a memory-resident anti-virus program should be used for continuous virus monitoring.

5.5.6 Programs of doubtful origin should never be used. If there is a doubt about a program in use, it is advisable to restrict its use to a microcomputer without hard disk or, if applicable, that having the hard disk write-protected through system setup. The concerned microcomputer should also be logged out from the network if it is connected to one. It should also be powered off after use for cleaning any possible virus in memory.

5.5.7 Connection to an external network (e.g. Internet) or any Bulletin Board System (BBS) should be controlled. A security scheme (e.g. checking of every downloaded file for virus) should be devised before any such connection is made. In this regard, advice can be provided by TSSC. Moreover, TSSC may be consulted regarding the background of any external BBS.

5.5.8 Any suspected virus case should be reported to the management immediately. The TSSC Helpdesk can provide assistance in investigating suspected virus cases, and in cleaning the virus. Virus cleaning can also be done through anti-virus software in the market.

5.5.9 If a machine is suspected to be infected by a virus, all activities on that machine should be stopped immediately. Continued usage of the machine may cause a serious deterioration of the situation.

5.5.10 Successfully cleaning a virus from a computer 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, sufficient backup copies should be kept to facilitate recovery from a virus attack.

5.5.11 If the output data from a microcomputer system are to be processed by another system (regardless of whether a microcomputer, mainframe or midrange system), consideration should be given to ensure that the output data are virus-free so as to prevent direct or indirect contamination to other computer systems.

5.6 DISASTER RECOVERY PLAN

General

5.6.1 A plan should be drawn up to deal with situations when a disaster occurs to the microcomputer systems or site, or both, whereby the systems and data are totally lost. A procedure must be devised and included in the plan such that any operational service which depends on the systems and data could still be provided, albeit not at an optimal performance level (e.g. supplemented by manual procedures).

5.6.2 The plan should complement the data backup and recovery procedures. Consideration must be given to the possibility that similar systems might not be available within a certain period of time after the disaster.

5.6.3 It is the department's own responsibility to ensure that a disaster recovery plan is in place and that its practicability is confirmed as far as possible through periodic drills.

5.7 SOFTWARE PIRACY

General

5.7.1 The copyrights of software programs, manuals and related literary works are protected by laws in Hong Kong. These laws prohibit, and impose penalties for, the unauthorized copying, duplication, and use of computer programs.

5.7.2 Any person who is found to be using, selling or distributing pirated software may be subject to trial under either civil or criminal law. It is an act of copyright infringement to release, reproduce, revise, translate, distribute or publish any software protected by copyright and without the consent of the software copyright owner.

5.7.3 As a software user, one must ensure that original and legitimate programs, and accompanying materials, have been acquired through proper channels. It is illegal, for any reason without the prior written consent of the software publisher, to purchase a single set of original software and use it on multiple machines, or to lend, copy or distribute software (or related literary works) without similar consent.

5.7.4 It should be noted that pirated software, besides associated with a legal risk, lacks the necessary quality in documentation, technical support, and upgradeability that are essential for the reliable, effective and efficient functioning of an organization.

6. PROTECTION AGAINST UNAUTHORIZED ACCESS

6.1 ACCESS CONTROL

General

6.1.1 Only authorized personnel should be allowed access to the microcomputer systems. In case a system is shared by many users, an administrator responsible for controlling access to the system is required.

6.1.2 Appropriate measures should be taken against theft at all times as microcomputer equipment and their components are fairly transportable. Some microcomputers, such as the notebook computers, are even designed for portability. If such portable microcomputers are allowed to be on loan for office duties, a suitable controlling scheme (e.g. on aspects such as the items on loan, their physical identification, the responsible officer, loan period) should be in force.

6.1.3 All microcomputer systems should require the use of passwords to gain access. Passwords can usually be set at both the hardware level (e.g. keyboard locking) and the software level (e.g. login systems, screen savers). Passwords must be used for access at all levels. The AVACS of ITSD, or equivalent login systems, are recommended to be installed.

6.1.4 Passwords should be so chosen that their meaning cannot be easily guessed or deduced. The length of passwords should be long enough (e.g. at least 6 characters) to prevent machine-assisted revelation. Also, they should be changed at least once every 3 months. Passwords of three or four characters are vulnerable to attack unless chosen from a large character set.

6.1.5 Users should exercise sufficient caution to prevent the exposure of their passwords at the moment of password input.

6.1.6 Hardcopies of passwords for record-keeping or other purposes are not advisable. If it is necessary to maintain such a hardcopy, adequate security measures (e.g. put in a sealed envelope and stored in a safe) accompanied by disclosure procedure should be devised.

6.1.7 Some equipment and physical devices that can restrict access to the microcomputer systems may be considered for enhancing security. The following are some examples: cabinets with locks, custom-made housing, diskette drive locks, disabled floppy drive for boot-up, smart cards for user authentication.

LAN Environment

6.1.8 If a diskette drive is not an operational necessity, as is the case for some workstations in a LAN environment, it can be removed or, "floppyless" workstations can be ordered, so that the risk of direct data retrieval is minimized.

6.1.9 A server room with locks is highly recommended for protecting the servers and the LAN equipment from unauthorized access. Moreover, it is advisable to have the servers locked inside cabinets.

6.1.10 Remote access, remote control or remote dial-in software are commonly used in the LAN environment. These software packages all offer security features to the users. These security features must be fully studied and used.

6.1.11 For all common LAN operating systems, a majority of the server operations can be done at a LAN workstation. Security of a LAN server can therefore be enhanced if, where affordable, the keyboard is locked or disconnected.

6.1.12 System security would be enhanced if the trunkings for LAN cables are, where applicable, sealed, locked, or accommodated in areas with high security.

6.2 SYSTEMS SOFTWARE SECURITY

General

6.2.1 Microcomputer operating system such as DOS provides minimal security features to the users. Users are thus recommended to enhance their workstation security by installing AVACS, or an equivalent security system in addition to DOS.

LAN Environment

6.2.2 The default settings for systems access should follow the spirit of "implicitly restricted until explicitly granted", as opposed to one of "implicitly granted until explicitly denied."

6.2.3 The alarm thresholds for access attempts should be appropriately adjusted to a level low enough to prevent intrusion, whilst high enough to avoid too many false alarms.

6.2.4 For systems access and control purposes, personal accountability should be the prime objective. Each user of the system must, as far as possible, be assigned a unique personal identifier. It is not recommended that two or more persons share the same identifier, even when they possess the same systems access privileges or share common data.

6.2.5 Today most LAN installations are using NetWare or LAN Manager as LAN operating systems. These operating systems offer security features in the form of matching user rights with resource locks. Files, directories, and hardware components are examples of the resources. The LAN Administrator should be aware of the security implications associated with the different settings of the resource locks.

6.2.6 In planning a LAN configuration, the LAN Administrator should appropriately match the settings of the resource locks with the user rights so as to arrive at a target security level. Samples of the settings can be found in the relevant **LAN Administrator's Guidelines** published by ITSD.

6.2.7 Where applicable, system security can be enhanced by restricting certain non-mobile LAN users to login through pre-defined workstations.

6.2.8 Intrinsic in the design of most common LAN operating systems, the user identifier (UserID) with the highest systems privileges is often implicitly assumed to be the security administrator. In this case the person (usually the LAN Administrator) in possession of the UserID would be responsible for two different roles. The Administrator should be of a rank in the senior cadre among the users of a LAN. He/She should hold a post listed in Appendices I and IV of the Integrity Checking Instructions issued by the Secretary for the Civil Service as per Security Regulation 113 so that clearance for access to classified information would have been made.

6.2.9 System access through a UserID with the highest systems privileges should be restricted to only one (or at most two, for mutual backup purpose) senior and responsible officer, as such privileged access has the potential of causing severe damage to the system. Considerations and guidelines for designation of any person who has high system privileges should be similar to those of the LAN Administrator set out in 6.2.8 above.

6.2.10 AVACS, or equivalent microcomputer security system, is recommended to be used in addition to whatever security features offered by the LAN operating system.

6.3 APPLICATION SOFTWARE SECURITY

General

6.3.1 The security requirements of every application system to be developed should be well specified before the commencement of design and implementation. This would facilitate the overall planning work and delivery of the custom functions.

6.3.2 Some guidelines stated in the SYSTEMS SOFTWARE SECURITY section above can be similarly applied to the application systems. The overall security of a microcomputer application would be greatly enhanced if thorough application security measures are built on top of the systems software.

LAN Environment

6.3.3 A basic technique in implementing security for a multi-user application is to maintain the mandate that, upon entry to the application, every user would identify himself according to a prescribed procedure, like responding to a prompt for password. The application would then execute an authentication procedure to confirm the user's identify and grant him the appropriate access rights.

6.4 DATA SECURITY

General

6.4.1 Encryption devices or programs should be considered for enhancing the security level of application data. It is advisable that sensitive data to be transferred from one workstation to another in a networked environment be encrypted before transfer. Some software, such as cc:mail, will encrypt mails that are transmitted over the network.

6.4.2 Classified data and documents should only be processed by microcomputer systems when nobody other than the authorized operating staff has access to the processing.

6.4.3 Storage of data and documents of a nature up to **Confidential** on the local hard disk of a standalone (i.e. not connected by any means to any network) microcomputer system is acceptable, provided that the system is in a secure place (e.g. in an office suitable for storing **Confidential** paper documents), since the system itself would be treated as a **Confidential** document.

LAN Environment

6.4.4 It is emphasized that potential risks exist in data exposure when different LANs are connected. Sufficient security measures (e.g. data encryption through software or hardware means) should therefore be planned in the network design stage. In this regard, advice should be sought from ITSD.

6.4.5 Stipulated rules and advice from Security Branch should be observed when considering the transmission of classified information over the network.

6.5 COMPUTER CRIMES LEGISLATION

General

6.5.1 The Computer Crimes Ordinance was effective as law in April 1993. Details of the Ordinance can be found in Computer Crimes Ordinance 1993.

6.5.2 In the Ordinance, the "misuse of a computer" is defined as:

"(a) To cause a computer to function other than it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of the data held in the computer;

(b) To alter or erase any program or data held in computer or in a computer storage medium;

(c) To add any program or data to the contents of a computer or of a computer storage medium,

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it."

6.5.3 In connection with the Computer Crimes Ordinance 1993, the Telecommunication Ordinance (Cap. 106) has also been amended to include, inter alia, the following:

"Any person who, by telecommunication, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence."

6.5.4 Similarly, the Theft Ordinance (Cap. 210) has also been amended to include, inter alia, the following:

"Unlawful damage to anything in a building includes –

(a) Unlawfully causing a computer in the building to function other than as it has been established by or on behalf of its owner to function, notwithstanding that the unlawful action may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;

(b) Unlawfully altering or erasing any program, or data, held in a computer in the building or in a computer storage medium in the building; and

(c) Unlawfully adding any program or data to the contents of a computer in the building or a computer storage medium in the building."

6.5.5 For the protection of programs and data held in a computer system, appropriate security measures, as suggested in this document, should be implemented.

The Office of the Government Chief Information Officer

BASELINE IT SECURITY POLICY

[S17]

Version : 2.3

Nov 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

1. PURPOSE 1-1

2. SCOPE 2-1

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

3. REFERENCE 3-1

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

4. DEFINITIONS AND CONVENTIONS 4-1

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

5. DEPARTMENTAL IT SECURITY ORGANISATION 5-1

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

6. MANAGEMENT RESPONSIBILITIES 6-1

6.1. MANAGEMENT 6-1

7. PHYSICAL SECURITY 7-1

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

8. ACCESS CONTROL SECURITY 8-1

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

9. DATA SECURITY 9-1

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

10. APPLICATION SECURITY 10-1

10.1. APPLICATION DEVELOPMENT & MAINTENANCE 10-1
10.2. CONFIGURATION MANAGEMENT & CONTROL 10-1

11. NETWORK & COMMUNICATION SECURITY 11-1

11.1. General Network Protection 11-1
11.2. Internet Security 11-1
11.3. Email Security 11-2
11.4. Software & Virus Management 11-2

12. SECURITY RISK ASSESSMENT & AUDITING 12-1

12.1. Security Risk Assessment 12-1
12.2. Security Auditing 12-1

13. SECURITY INCIDENT MANAGEMENT 13-1

13.1. Security Incident Monitoring 13-1
13.2. Security Incident Response 13-1

The Office of the Government Chief Information Officer

IT SECURITY GUIDELINES

[G3]

Version : 4.3

Nov 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

1. PURPOSE 1-1

2. SCOPE 2-1

2.1 GOVERNMENTAL INFORMATION SECURITY MANAGEMENT FRAMEWORK 2-3
2.1.1 Information Security Management Committee (ISMC) 2-3
2.1.2 IT Security Working Group (ITSWG) 2-4
2.1.3 Government Information Security Incident Response Office (GIRO) 2-4
2.1.4 Bureaux / Departments 2-4
2.2 IT SECURITY DOCUMENT OVERVIEW 2-5

3. REFERENCES 3-1

3.1 STANDARDS & GUIDELINES 3-1
3.2 OTHER REFERENCES 3-1

4. DEFINITIONS AND CONVENTIONS 4-1

4.1 DEFINITIONS 4-1
4.2 CONVENTIONS 4-1

5. DEPARTMENTAL IT SECURITY ORGANISATION 5-1

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

6. MANAGEMENT RESPSONSIBILITIES 6-1

6.1 CLEAR POLICIES AND PROCEDURES 6-1
6.2 ASSIGNING RESPONSIBILITY 6-1
6.3 INFORMATION DISSEMINATION 6-1
6.4 SEGREGATION OF DUTIES 6-1
6.5 LEAST PRIVILEGE PRINCIPLE 6-2
6.6 INTEGRITY CHECKING 6-2
6.7 SECURITY REQUIREMENTS IN CONTRACTS 6-2
6.8 INDEMNITY AGAINST DAMAGE OR LOSS 6-2

7. PHYSICAL SECURITY 7-1

7.1 ENVIRONMENT 7-1
7.1.1 Site Preparation 7-1
7.1.2 Housekeeping 7-2
7.2 EQUIPMENT SECURITY 7-3
7.2.1 Media Control 7-3
7.2.2 Disposal of Computer Equipment 7-4
7.3 PHYSICAL ACCESS CONTROL 7-4
7.4 MISCELLANEOUS 7-5
7.4.1 Training 7-5
7.4.2 Stationeries 7-5
7.4.3 Items for Emergency Use 7-5

7.4.4 Fire Fighting 7-6
7.4.5 Communication 7-6
7.4.6 Maintenance 7-6
7.5 ADDITIONAL RERERENCES 7-6

8. ACCESS CONTROL SECURITY 8-1

8.1 DATA ACCESS CONTROL 8-1
8.2 AUTHENTICATION AND IDENTIFICATION SYSTEM 8-1
8.3 PASSWORD MANAGEMENT 8-2
8.3.1 Password Selection 8-2
8.3.2 Password Handling for End Users 8-3
8.3.3 Password Handling for System/Security Administrators 8-4
8.4 AUDIT TRAILS 8-5
8.5 SECURITY OF SYSTEM SOFTWARE 8-6
8.5.1 Monitoring System User 8-7
8.5.2 Tools for Monitoring the System 8-7
8.5.3 Varying the Monitoring Schedule 8-8
8.6 ADDITIONAL REFERENCES 8-8

9. DATA SECURITY 9-1

9.1 CLASSIFIED DATA 9-2
9.2 DATA BACKUP AND RECOVERY 9-4
9.2.1 GENERAL DATA BACKUP GUIDELINES 9-4
9.2.2 DISASTER RECOVERY PLAN 9-5
9.2.3 DEVICES AND MEDIA FOR DATA BACKUP 9-6
9.2.4 SERVER BACKUP 9-7
9.2.5 WORKSTATION BACKUP 9-8
9.3 USER PROFILES AND VIEWS 9-8
9.4 DATA & FILE ENCRYPTION 9-8
9.4.1 Symmetric Key Encryption 9-9
9.4.2 Asymmetric Key Encryption 9-10
9.4.3 Cryptographic Key Management 9-10
9.4.4 Encryption Tools 9-11
9.5 INTEGRITY OF DATA 9-11
9.6 INFORMATION DISPOSAL 9-12
9.7 LICENSING 9-12
9.8 SOFTWARE ASSET MANAGEMENT 9-13
9.9 ADDITIONAL REFERENCES 9-14

10. APPLICATION SECURITY 10-1

10.1 SYSTEM SPECIFICATION AND DESIGN CONTROL 10-1
10.1.1 Security Considerations in Application Design and Development 10-2
10.2 PROGRAMMING CONTROLS 10-3
10.2.1 Programming Standard Establishment 10-3
10.2.2 Division of Labour 10-3
10.3 PROGRAM/SYSTEM CHANGE CONTROLS 10-4
10.4 PROGRAM/SYSTEM TESTING 10-4
10.5 PROGRAM CATALOGING 10-5
10.6 PERSONNEL CONTROL 10-5
10.6.1 Educating the System Administrators 10-5
10.6.2 Control of System Programmers 10-5
10.6.3 Operations Controls 10-5
10.7 ADDITIONAL REFERENCES 10-6

11. NETWORK & COMMUNICATION 11-1

11.1 GENERAL NETWORK PROTECTION 11-1
11.2 INTERNET SECURITY 11-2
11.3 E-MAIL SECURITY 11-3
11.4 SOFTWARE & VIRUS MANAGEMENT 11-5

11.4.1 Virus Prevention 11-5
11.4.2 Virus Detection 11-6
11.4.3 Virus Recovery 11-7
11.4.4 Server 11-7
11.4.5 Workstation 11-8
11.4.6 Hoax Virus Warning 11-9
11.5 COMMUNICATE OVER UN-TRUSTED NETWORK 11-10
11.5.1 Dial-in Access 11-10
11.5.2 Wireless Network 11-11
11.6 VIRTUAL PRIVATE NETWORK SECURITY 11-12
11.7 BROWSER SECURITY 11-13
11.8 MOBILE COMPUTING DEVICE SECURITY 11-13
11.9 ADDITIONAL REFERENCES 11-15

12. SECURITY RISK ASSESSMENT & AUDITING 12-1

12.1 OVERVIEW 12-1
12.2 ADDITIONAL REFERENCES 12-1

13. SECURITY INCIDENT MANAGEMENT 13-1

13.1 OVERVIEW 13-1
13.2 ADDITIONAL REFERENCES 13-1

14. SECURITY POLICY CONSIDERATIONS 14-1

14.1 WHAT A SECURITY POLICY IS 14-1
14.2 TOOLS TO IMPLEMENT SECURITY POLICY 14-2
14.3 HOW TO DEVELOP A SECURITY POLICY 14-2
14.3.1 Organisation Of Security Policy Group 14-3
14.3.2 Planning 14-6
14.3.3 Determination Of Security Requirements 14-7
14.3.4 Construct A Security Policy Framework 14-10
14.3.5 Evaluate And Periodic Review 14-11
14.4 HOW TO GET SECURITY POLICY IMPLEMENTED 14-12
14.4.1 Security Awareness & Training 14-12
14.4.2 Enforcement And Redress 14-12
14.4.3 On-going Involvement of All Parties 14-13
14.5 ADDITIONAL REFERENCES 14-13

15. ADDITIONAL RESOURCES 15-1

APPENDIX

A SAMPLE IT SECURITY END USER INSTRUCTIONS A-1
B EXTRACTS FROM SECURITY REGULATIONS B-1
C EXTRACTS FROM PERSONAL DATA (PRIVACY) ORDINANCE C-1

The Office of the Government Chief Information Officer

SECURITY RISK ASSESSMENT & AUDIT GUIDELINES

[G51]

Version : 2.1

Jul 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

1. PURPOSE 1-1

2. SCOPE 2-1

2.1 IT SECURITY DOCUMENT OVERVIEW 2-2

3. REFERENCE 3-1

4. DEFINITIONS AND CONVENTIONS 4-1

4.1 Definitions 4-1
4.2 Conventions 4-1

5. OVERVIEW OF IT SECURITY MANAGEMENT 5-1

5.1 Overview of IT Security Management 5-1
5.2 Security Risk Assessment Vs Security Audit 5-2
5.2.1 What A Security Risk Assessment Is 5-2
5.2.2 What A Security Audit Is 5-3

6. SECURITY RISK ASSESSMENT 6-1

6.1 Benefits of Security Risk Assessment 6-1
6.2 Security Risk Assessment STEPS 6-1
6.2.1 Planning 6-1
6.2.1.1 Project Scope and Objectives 6-2
6.2.1.2 Background Information 6-2
6.2.1.3 Constraints 6-2
6.2.1.4 Roles and Responsibilities of Different Parties 6-2
6.2.1.5 Approach & Methodology 6-3
6.2.1.6 Project Size & Schedule 6-3
6.2.2 Information Gathering 6-3
6.2.2.1 Information To Be Gathered 6-3
6.2.2.2 Information Collection Methods 6-4
6.2.3 Risk Analysis 6-4
6.2.3.1 Asset Identification & Valuation 6-5
6.2.3.2 Threat Analysis 6-5
6.2.3.3 Vulnerability Analysis 6-6
6.2.3.4 Assets/Threats/Vulnerabilities Mapping 6-7
6.2.3.5 Impact & Likelihood Assessment 6-7
6.2.3.6 Risk Results Analysis 6-8
6.2.4 Identifying & Selecting Safeguards 6-10
6.2.4.1 Common Types of Safeguards 6-10
6.2.4.2 Major Steps of Identifying & Selecting Safeguards 6-11
6.2.5 Monitoring & Implementation 6-12
6.3 common security RISK assessment tasks 6-12
6.4 Deliverables 6-13

7. SECURITY AUDIT 7-1

7.1 AUDIT FREQUENCY & TIMING 7-1

7.1.1 Audit Frequency 7-1
7.1.2 Audit Timing 7-1
7.2 Auditing Methods 7-2
7.2.1 General Control Review 7-2
7.2.2 System Review 7-2
7.2.3 Penetration Testing 7-3
7.3 Auditing Tools 7-3
7.4 Auditing Steps 7-4
7.4.1 Defining Audit Scope & Objectives 7-5
7.4.1.1 Audit Scope 7-5
7.4.1.2 Audit Objectives 7-6
7.4.2 Planning 7-6
7.4.3 Collecting Audit Data 7-7
7.4.4 Performing Audit Tests 7-7
7.4.5 Reporting for Audit Results 7-8
7.4.6 Protecting Audit Data & Tools 7-8
7.4.7 Making Enhancements & Follow-up 7-8

8. SERVICE PREREQUISITES & COMMON ACTIVITIES 8-1

8.1 ASSUMPTIONS & LIMITATIONS 8-1
8.2 Client Responsibilities 8-1
8.3 Service Prerequisites 8-1
8.4 Responsibilities of Security AUDITORS 8-2
8.5 EXAMPLES OF COMMON ACTIVITIES 8-2

9. SECURITY RISK ASSESSMENT & AUDIT FOLLOW-UP 9-1

9.1 Importance of Follow-up 9-1
9.2 Effective & Qualified Recommendations 9-1
9.3 Commitment 9-2
9.3.1 Security Auditors 9-2
9.3.2 Staff 9-2
9.3.3 Management 9-2
9.4 Monitoring and Follow-up 9-2
9.4.1 Set Up Monitoring & Follow-up System 9-3
9.4.2 Identify Recommendations & Develop Follow-up Plans 9-3
9.4.3 Perform Active Monitoring & Reporting 9-3
9.4.3.1 Progress & Status of Actions 9-3
9.4.3.2 Follow-Up Actions 9-3

APPENDIX

A - SAMPLE LIST OF QUESTIONS FOR SECURITY RISK ASSESSMENT A-1
B - SAMPLE CONTENTS OF DELIVERABLES B-1
C - DIFFERENT TYPES OF SECURITY AUDIT C-1
D - SAMPLE AUDIT CHECKLIST D-1

The Office of the Government Chief Information Officer

INFORMATION SECURITY INCIDENT HANDLING GUIDELINES

[G54]

Version: 2.2

Sep 2004
The Government of the Hong Kong Special Administrative Region

TABLE OF CONTENTS

1 PURPOSE 1-1

2 SCOPE 2-1

2.1 IT SECURITY DOCUMENT OVERVIEW 2-2

3 REFERENCES 3-1

4 DEFINITIONS AND CONVENTIONS 4-1

4.1 DEFINITIONS 4-1
4.2 CONVENTIONS 4-1

5 INTRODUCTION TO SECURITY INCIDENT HANDLING 5-1

5.1 SECURITY INCIDENT HANDLING IN INFORMATION SECURITY MANAGEMENT 5-1
5.2 WHAT IS SECURITY INCIDENT HANDLING 5-1
5.2.1 Information Security Incident 5-1
5.2.2 Security Incident Handling 5-2
5.3 IMPORTANCE OF SECURITY INCIDENT HANDLING 5-3

6 ORGANISATION FRAMEWORK FOR INFORMATION SECURITY INCIDENT HANDLING IN THE GOVERNMENT 6-1

6.1 HONG KONG COMPUTER EMERGENCY RESPONSE TEAM COORDINATION CENTRE 6-2
6.2 GOVERNMENT INFORMATION SECURITY INCIDENT RESPONSE OFFICE 6-2
6.2.1 Functions of GIRO 6-3
6.2.2 GIRO Formation 6-3
6.3 INFORMATION SECURITY INCIDENT RESPONSE TEAM (ISIRT) 6-4
6.3.1 Functions of the ISIRT 6-4
6.3.2 ISIRT Formation 6-4
6.3.3 Roles of the ISIRT 6-5
6.3.3.1 Commander 6-5
6.3.3.2 Incident Response Manager 6-5
6.3.3.3 Information Officer 6-6
6.4 DEPARTMENTAL IT SYSTEM 6-6
6.4.1 Departmental IT System Manager 6-7

7 OVERVIEW OF STEPS IN SECURITY INCIDENT HANDLING 7-1

8 PLANNING AND PREPARATION 8-1

8.1 SECURITY INCIDENT HANDLING PLAN 8-1
8.1.1 Scope 8-1
8.1.2 Goals and Priorities 8-1
8.1.3 Roles and Responsibilities 8-2
8.1.4 Constraints 8-2
8.2 REPORTING PROCEDURE 8-2
8.3 ESCALATION PROCEDURE 8-3
8.4 SECURITY INCIDENT RESPONSE PROCEDURE 8-3
8.5 TRAINING AND EDUCATION 8-4
8.6 INCIDENT MONITORING MEASURE 8-4

9 RESPONSE TO SECURITY INCIDENT 9-1

9.1 IDENTIFICATION OF INCIDENT 9-2

9.1.1 Determine if an incident occurs 9-2
9.1.2 Perform preliminary assessment 9-3
9.1.3 Log the incident 9-3
9.1.4 Obtain system snapshot 9-4
9.2 ESCALATION 9-4
9.3 CONTAINMENT 9-5
9.3.1 Operation Status of the Compromised System 9-5
9.4 ERADICATION 9-6
9.4.1 Possible Actions for Incident Eradication 9-6
9.5 RECOVERY 9-7

10 AFTERMATH 10-1

10.1 POST-INCIDENT ANALYSIS 10-1
10.2 POST-INCIDENT REPORT 10-2
10.3 SECURITY ASSESSMENT 10-2
10.4 REVIEW EXISTING PROTECTION 10-2
10.5 INVESTIGATION AND PROSECUTION 10-3

APPENDIX

A CHECKLIST FOR INCIDENT HANDLING PREPARATION
A.1 SAMPLE CHECKLIST FOR INCIDENT HANDLING PREPARATION

B REPORTING MECHANISM
B.1 SUGGESTIONS ON REPORTING MECHANISM
B.2 PRELIMINARY INFORMATION SECURITY INCIDENT REPORTING FORM
B.3 POST-INCIDENT REPORT

C ESCALATION PROCEDURE
C.1 PARTIES TO BE NOTIFIED
C.2 CONTACT LIST
C.3 SAMPLE ESCALATION PROCEDURE

D IDENTIFICATION OF INCIDENT
D.1 TYPICAL INDICATION OF SECURITY INCIDENTS
D.2 INFORMATION COLLECTED FOR IDENTIFICATION
D.3 TYPES OF INCIDENTS
D.4 FACTORS AFFECTING THE SCOPE AND IMPACT OF INCIDENT

E SECURITY INCIDENT ESCALATION WORKFLOW

F DEPARTMENTAL IT SECURITY CONTACTS CHANGE FORM

REGULATIONS
OF THE
GOVERNMENT OF THE
HONG KONG SPECIAL
ADMINISTRATIVE REGION

VOLUME 5

SECURITY REGULATIONS

1998

(updated September 2004)

CHAPTER I

GENERAL

Disclosure of Classified Information to persons outside the Government Service

131. Classified information should be passed to non-Government organisations or individuals, e.g. members of boards or committees, consultants etc. only on a "need to know" basis, subject to Regulation 111 above.

132. Departments providing classified information to such persons must ensure that arrangements for its protection comply as far as possible with the standards adopted throughout Government.

CHAPTER IX

INFORMATION SYSTEMS

General

350. In this chapter-

(a) "Information System" means an electronic system that processes data electronically through the use of information technology, including computer systems, servers, workstations, terminals, storage media, communication devices and network resources;

(b) "Hard drive" means a hard drive that is, designed or intended to be used permanently, installed inside of the computer casing during use;

(c) "Key" means a numeric code that is used in respect of classified information for-

(i) authentication;
(ii) decryption; or
(iii) generation of a digital signature;

(d) logical access control and the encryption method and procedures must comply with requirements specified from time to time by Office of the Government Chief Information Officer (OGCIO). Logical access control includes access controls other than physical access control. Note, however, that physical access control may also involve the use of digital means, e.g. use of smart cards and biometrics. Requirements for physical access control are specified by the Government Security Officer of the Security Bureau.

Storage, Processing, Transmission – TOP SECRET/SECRET

351. TOP SECRET/ SECRET information must be encrypted during storage and transmission.

352. TOP SECRET/SECRET information must be stored –

(a) on removable media kept in compliance with Regulations 194 and 195 when not attended or when not in use;

(b) on the hard drive of a portable computer or stand-alone personal computer if the computer is attended or is in a physically secure environment approved by the Government Security Officer;

(c) on the local hard drive of a networked personal computer if the computer is connected to an isolated LAN approved by the Government Security Officer subject to the technical endorsement of OGCIO; or

(d) on the hard drive of a server computer on an isolated LAN approved by the Government Security Officer subject to the technical endorsement of OGCIO and located in a room compliant with Level 3 Security.

353. Shared access to a computer referred to in Regulation 352(b)-(c) is prohibited except among persons who are authorised to see all of the information stored on the computer.

354. Shared access to a computer referred to in Regulation 352(b)-(d) is prohibited unless all activity in relation to the TOP SECRET/SECRET information is tracked by audit trail and logical access control software.

355. Access to an Information System on which, or through which TOP SECRET/SECRET information may be accessed must be restricted by means of logical access control.

356. TOP SECRET/SECRET information may only be processed on an Information System that complies with the requirements of Regulations 352(b)-(d), 354 and 355.

357. TOP SECRET/SECRET information must not be transmitted from a computer referred to in Regulation 352(b), or outside of the isolated LAN approved under Regulation 352(c) or (d).

Storage, Processing, Transmission – CONFIDENTIAL

358. Stored CONFIDENTIAL information must be encrypted.

359. CONFIDENTIAL information must be stored –

(a) on removable media kept in compliance with Regulation 196 when not attended, or when not in use;

(b) on the hard drive of a portable computer or stand-alone personal computer if the computer is attended, or is in a physically secure environment approved by the Government Security Officer;

(c) on the local hard drive of a networked personal computer if the computer is attended, or is in a physically secure environment; or

(d) on the hard drive of a server computer if the computer is in a room compliant with Level 2 Security, or in a location that the Government Security Officer considers provides an equivalent or satisfactory level of physical security.

360. Shared access to a computer referred to in Regulation 359(b)-(c) is prohibited except among persons who are authorised to see all of the information stored on the computer.

361. Shared access to a computer referred to in Regulation 359(b)-(d) is prohibited unless all activity in relation to the CONFIDENTIAL information is tracked by audit trail and logical access control software.

362. Access to a computer on which or through which CONFIDENTIAL information may be accessed must be restricted by means of logical access control.

363. CONFIDENTIAL information may only be processed on an Information System that complies with the requirements of Regulations 359(b)-(d), 361 and 362.

364. CONFIDENTIAL information must be encrypted when transmitted over an un-trusted communication network – e.g. general purpose local area networks, networks that use leased or public telecommunication lines, or wireless networks.

365. CONFIDENTIAL information, when transmitted by electronic mail, may only be transmitted on an Information System approved by the Government Security Officer subject to the technical endorsement of OGCIO.

Storage, Processing, Transmission - RESTRICTED

366. RESTRICTED information must be stored–

(a) on removable media kept in compliance with Regulation 197 when not attended or when not in use; or

(b) on the hard drive of a portable computer, stand-alone personal computer, networked personal computer or server computer if the computer is attended or is in a locked room or cabinet.

367. RESTRICTED information may only be processed on an Information System that complies with the requirements of Regulation 366(b).

368. RESTRICTED information must be encrypted when transmitted over an un-trusted communication network – e.g. general purpose local area networks, networks that use leased or public telecommunication lines, or wireless networks.

369. RESTRICTED information, when transmitted by electronic mail, may only be transmitted on an Information System approved by the Government Security Officer subject to the technical endorsement of OGCIO.

Cryptographic Key Management

370. A key has the same classification as the classified information in respect of which it is used.

371. For keys that are used for the processing of information classified CONFIDENTIAL or above, they must be stored separately from the corresponding encrypted information.

372. A key must be safeguarded at all times -

(a) keys stored on Information Systems must be properly controlled and protected;

(b) for keys issued to individual officers (e.g. keys stored on smartcards, floppy disks, etc.), the respective officers are personally responsible for the keys' safe custody and must take all necessary precautions to prevent them from being stolen or copied. If such a key has been left unattended and there is reason to believe that an unauthorised person has access to it, it will be assumed that the key has been compromised. The facts must be reported to the Departmental IT Security Officer who will arrange for the immediate replacement of the key and advise the Government Security Officer. Officers are personally responsible for any costs arising from the loss, damage or possible compromise of keys in their custody.

Classification Reminder

373. Users given access to classified information on Information Systems should be alerted of the type(s) of classified information they are accessing or going to access.

374. The Subject field of a classified electronic mail document must include the classification category of the document.

375. Removable media on which classified information is stored must have clearly legible identification and conspicuous classification markings on labels fixed firmly to them and on their protective containers.

376. Removable media on which a key is stored, and is not used for backup purposes, need not have its classification marked on a fixed label.

Destruction of Classified Information

377. All classified information shall be completely cleared from media before disposal, or re-use. Any method that only temporarily erases the classified information or allows alternative means of recovery must not be used.

378. If the classified information cannot be completely cleared, the media unit must be physically destroyed in a manner that prevents recovery of the classified information.

Physical Security

379. Access to every office, computer room or work area where an Information System containing classified information is located, shall be physically restricted.

380. The display screen of a personal computer, workstation or dumb terminal on which classified information can be viewed shall be carefully positioned so that unauthorised persons cannot readily view it.

Breaches of Security

381. In addition to the breaches of security specified in Chapter VIII, breaches of security relating to Information Systems may be divided into –

(a) Losses - when Information Systems that process or store classified information are missing or there is reason to believe that an Information System has been compromised, or destroyed without authorisation; and

(b) Unavailability - when classified information is not accessible when needed or is accessible with undue delay, as a result of unauthorised activities.

382. Breaches of security on Information Systems should be investigated initially by the Bureau or Department with the objectives as stated in Regulation 331.

383. Following are examples of breaches of security on Information Systems –

(a) the unauthorised access of classified information that is on an Information System;

(b) an Information System key or authentication device is left unattended in a location which might permit access to the key or authentication device by an unauthorised person;

(c) the tampering of classified information during transmission;

(d) the loss or apparent loss, temporary or permanent, of a notebook computer or any removable media such as compact disks or floppy diskettes that contain classified information.

384 – 400.