資料文件
2006 年 5 月 4 日

立法會保安事務委員會
有關資訊保安的指引

目的

應保安事務委員會的要求，本文件載列政府當局就資訊保安方面的指引。指引的有關內容，適用於與資訊科技有關的合約。

指引

2. 由前資訊科技署、政府資訊科技總監辦公室和保安局所發出的有關指引如下—

(a) 資訊科技署通告第 1/96 號的《微型電腦及局部區域網絡保安指引》，載於**附件 A**（只備英文版）；

(b) 政府資訊科技總監辦公室發出的《基準資訊科技保安政策》，其目錄載於**附件 B**；

(c) 政府資訊科技總監辦公室發出的《資訊科技保安指引》，其目錄載於**附件 C**；

(d) 政府資訊科技總監辦公室發出的《保安風險評估及審計指引》，其目錄載於**附件 D**；

(e) 政府資訊科技總監辦公室發出的《資訊保安事故處理指引》，其目錄載於**附件 E**；及

（由於以上(b)至(e)項提及的指引頁數眾多，我們沒有附上指引的全文。指引的全文可於 www.infosec.gov.hk/english/itpro/guidelines.htm（英文版）及 www.infosec.gov.hk/chinese/itpro/guidelines.htm（中文版）瀏覽。）

(f) 保安局發出的《保安規則》，其較相關的摘錄載於**附件F**。

3. 議員亦可參考資訊科技及廣播事務委員會於2006年3月17日的會議討論的文件，文件的題目為"資訊保安"，編號為CB(1)1097/05-06(01)。

保安局
政府資訊科技總監辦公室
2006年4月

附件 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

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.

政府資訊科技總監辦公室

基準資訊科技保安政策

[S17]

第2.3版

二零零四年十一月
香港特別行政區政府

目錄

政府資訊科技總監辦公室

資訊科技保安指引

[G3]

第 4.3 版

二零零四年十一月
香港特別行政區政府

目錄

附錄

政府資訊科技總監辦公室

保安風險評估及審計指引

[G51]

第 2.1 版

二零零四年七月
香港特別行政區政府

目錄

政府資訊科技總監辦公室

資訊保安事故處理指引

[G54]

第 2.2 版

二零零四年九月
香港特別行政區政府

目錄

附錄

香港特別行政區政府規例

第五冊
保安規例

一九九八年
(二零零四年九月修訂)

第一章

總則

向非政府人士披露機密資料

131. 機密資料必須根據"需要知道"的原則，才可交給非政府機構或個人，例如委員會或小組委員會委員、顧問等，但須符合上文第111條的規定。

132. 負責將機密資料交給該等人士的部門，必須確保資料的保密安排盡可能符合政府所採取的一貫標準。

第九章

資訊系統

通則

350. 就本章而言—

(a) “資訊系統”指運用資訊科技以電子方式處理數據的電子系統，包括電腦系統、伺服器、工作站、終端機、儲存媒體、通訊設備及網絡資源；

(b) “硬盤驅動器”指使用時裝設於電腦機箱內部，專為長遠使用而設計的硬盤驅動器；

(c) “密碼匙”指關乎機密資料作下列用途的數字代碼：

(i) 認證；

(ii)解密；或

(iii) 產生數碼簽署；

(d) 邏輯接達控制以及加密方法和程序必須符合政府資訊科技總監辦公室不時作出的規定。邏輯接達控制包括實體接達控制以外的接達控制，但實體接達控制亦可能涉及使用數碼設備，例如聰明卡和人體測定方法。有關實體接達控制的規定則由保安局政府保安事務主任訂明。

儲存、處理和傳送絕對機密/高度機密資料

351. 絕對機密/高度機密資料在儲存和傳送時必須加密。

352. 絕對機密/高度機密資料必須按照以下規定妥為儲存：

(a) 該等資料可儲存於可抽離媒體內，而當該媒體在沒有人員看管或使用時，必須按照規例第 194 和 195 條所述方式存放；

(b) 該等資料可儲存於手提電腦或獨立個人電腦的硬盤驅動器，而該電腦必須有人員看管或放置於經政府保安事務主任核准的保安妥善的環境中；

(c) 該等資料可儲存於已聯網個人電腦的本機硬盤驅動器，而該電腦必須接駁至經政府資訊科技總監辦公室技術審核及政府保安事務主任核准的獨立局部區域網絡；或

(d) 該等資料可儲存於獨立局部區域網絡的伺服器電腦的硬盤驅動器。該網絡必須是經政府資訊科技總監辦公室技術審核及政府保安事務主任核准的，及該伺服器電腦必須放置於符合第三級保安標準的房間內。

353. 規例第 352(b)及(c)條所指的電腦，不得供超過一人共同接達，除非該等人士已獲授權查閱該電腦儲存的所有資料。

354. 規例第 352(b)至(d)條所指的電腦，不得供超過一人共同接達，除非涉及**絕對機密/高度機密**資料的所有活動均可透過稽核蹤迹及邏輯接達控制軟件追查。

355. 必須透過邏輯接達控制，限制任何人透過接達資訊系統從而接達或藉以接達**絕對機密/高度機密**資料。

356. **絕對機密/高度機密**資料只可在符合規例第 352(b)至(d)、354 及 355 條規定的資訊系統上處理。

357. **絕對機密/高度機密**資料不得由規例第 352(b)條所指的電腦傳送，或傳送至根據規例第 352(c)或(d)條獲得核准的獨立局部區域網絡以外的地點。

儲存、處理和傳送機密資料

358. 機密資料儲存時必須加密。

359. 機密資料必須按照以下規定妥為儲存：

(a) 該等資料可儲存於可抽離媒體內，而當該媒體在沒有人員看管或使用時，必須按照規例第 196 條所述方式存放；

(b) 該等資料可儲存於手提電腦或獨立個人電腦的硬盤驅動器，而該電腦必須有人員看管或放置於經政府保安事務主任核准的保安妥善的環境中；

(c) 該等資料可儲存於已聯網個人電腦的本機硬盤驅動器，而該電腦必須有人員看管或放置於保安妥善的環境中；或

(d) 該等資料可儲存於伺服器電腦的硬盤驅動器，而該伺服器電腦必須放置於符合第二級保安標準的房間內，或政府保安事務主任認為能達致相同或滿意保安標準的地方。

360. 規例第 359(b)及(c)條所指的電腦，不得供超過一人共同接達，除非該等人士已獲授權查閱該電腦儲存的所有資料。

361. 規例第 359(b)至(d)條所指的電腦，不得供超過一人共同接達，除非涉及機密資料的所有活動均可透過稽核蹤迹及邏輯接達控制軟件追查。

362. 必須透過邏輯接達控制，限制任何人透過接達電腦從而接達或藉以接達機密資料。

363. 機密資料只可在符合規例第 359(b)至(d)、361 及 362 條規定的資訊系統上處理。

364. 透過不可靠通訊網絡(例如一般用途的局部區域網絡、使用租賃或公眾電訊線路的網絡或無線網絡)傳送的機密資料，必須經過加密處理。

365. 以電郵方式傳送的機密資料，只可透過經政府資訊科技總監辦公室技術審核及政府保安事務主任核准的資訊系統傳送。

儲存、處理和傳送限閱資料

366. 限閱資料必須按照以下規定妥為儲存：

(a) 該等資料可儲存於可抽離媒體內，而當該媒體在沒有人員看管或使用時，必須按照規例第 197 條所述方式存放；

(b) 該等資料可儲存於手提電腦、獨立個人電腦、已聯網個人電腦或伺服器電腦的硬盤驅動器，而該電腦必須有人員看管或放置於已鎖上的房間或櫃內。

367. 限閱資料只可在符合規例第 366(b)條規定的資訊系統上處理。

368. 透過不可靠通訊網絡(例如一般用途的局部區域網絡、使用租賃或公眾電訊線路的網絡或無線網絡)傳送的限閱資料，必須經過加密處理。

369. 以電郵方式傳送的限閱資料，只可透過經政府資訊科技總監辦公室技術審核及政府保安事務主任核准的資訊系統傳送。

管理密碼匙

370. 密碼匙與該匙所用於的機密資料的機密類別相同。

371. 用作處理機密或以上資料的密碼匙必須與所處理的資料分開貯存。

372. 密碼匙必須經常妥為保管 -

(a) 貯存在資訊系統內的密碼匙必須給予妥善的管制和保護;

(b) 發給個別人員的密碼匙（例如儲在聰明咭、磁碟等），有關人員須對密碼匙的妥善保管負上個人責任，並須採取一切預防措施防止密碼匙遭盜取或複製。如果密碼匙曾經無人員看管，且有理由相信曾有未獲授權的人接達，則應假設該密碼匙已經遭外洩。遇此情況，有關人員必須向部門資訊科技保安事務主任報告，並由他即時安排更換密碼匙和知會政府保安事務主任。如果密碼匙被遺失、受損或可能遭外洩，則有關人員須自行承擔由此引起的一切開支。

機密類別提示

373. 資訊系統的使用者在使用資訊系統內提供的機密資料時，須獲得提示所使用資料的機密類別。

374.機密電郵文件的主題欄必須包括該文件的機密類別。

375. 存有機密資料的可抽離媒體和盛載媒體的保護盒必須穩固地貼上標籤，展示清晰可讀的識別記號和顯而易見的機密類別標記。

376.存有密碼匙的可抽離媒體，若不是用作備份用途時，則毋須貼上附有機密類別標記的標籤。

銷毀機密資料

377. 在棄置或再用媒體前，必須把媒體內的所有機密資料徹底清除。有關人員不得使用只可暫時清除機密資料或可讓資料以其他途徑還原的方法。

378.如無法徹底清除媒體內的機密資料，則須把媒體的實體摧毀至內存的機密資料無法還原的地步。

實體保安

379. 存有機密資料的資訊系統所在的每間辦公室、電腦房或工作間，必須嚴禁閒人進入。

380. 展示機密資料的個人電腦、工作站或簡易終端機的顯示屏必須小心擺放，以免遭未獲授權的人輕易看到資料。

違反保安規定

381. 除了第八章所指的違反保安規定情況外，涉及資訊系統的違反保安規定情況還可分為下列兩類：

(a) 遺失—用以處理或儲存機密資料的資訊系統遺失或有理由相信資訊系統在未經授權下已遭入侵或破壞；以及

(b) 無法使用—因未獲授權的活動而引致在需要接達機密資料時未能接達或接達時受到阻延。

382. 違反資訊系統保安規定的個案，應由局或部門根據規例第 331 條訂明的方針展開初步調查。

383. 以下列舉一些違反資訊系統保安規定的例子：

(a) 未獲授權而接達資訊系統的機密資料；

(b) 任由資訊系統密碼匙或認證裝置無人員看管，且放於可能被未獲授權的人接達的地方；

(c) 機密資料於傳送時受到干擾；

(d) 暫時或永久遺失或表面遺失存有機密資料的筆記簿型電腦或任何可抽離媒體，例如光碟或軟磁碟。

384. – 400.