Information Technology in Education Project

IT Security

In Schools

Education Infrastructure Division
Education Bureau
The Government of the HKSAR

www.edb.gov.hk/ited/

revised in May 2007

Table of Contents

1   Why IT Security is Important to Your School?

At present, most schools in the Hong Kong should have already installed their local area network (LAN) such as School Administration and Management Systems (SAMS), Teaching and Learning School Network, and for some schools the Multimedia Learning Center (MMLC).

To enable better teaching and learning as well as broader information access, most schools have acquired Internet access services and some even have hosted their school Web pages at their Internet Service Provider (ISP). Some schools are also implemented new information technology (IT) projects like school intranet system to let teachers and students have interactive communications and collaboration.

It is envisaged that the operation of schools will be adversely affected if their IT facilities do not function properly or data cannot be accessed.

About This Document

This document provides the basic IT security knowledge and concepts which would be applicable to the school environment. It generally describes the purposes or objectives that should be considered in defining IT security policy for schools, and the key concerns in each of the IT security control areas.

This document serves to help schools to define their own IT security policy and standards to suit their own situation.

This document is written for all school IT users including school IT management, technical staff as well as end-users. IT management, such as school heads, IT co-ordinators, school IT committee members, may find the information in this document useful in defining their high level IT security policy. The technical staff, such as LAN administrators and other technical support personnel, may base on this document to work out detailed IT security guidelines and standards to suit their own environment. Some information in this document may be useful for reference by the end users of students, teachers, and other staff or even parents who will access the IT facilities, with an aim to arouse their awareness on safe use of IT facilities.

There are many potential causes of damage to computer systems which may be natural or human by nature. Such kinds of causes are usually called **threats**. For example:

■ **Natural Threats**

Catastrophic (e.g. fire and floods) and environmental threats (e.g. extreme temperature and humidity).

■ **Human Threats**

There are two kinds of human threats and they are:

Intentional

Hacking (e.g. unauthorized access of network resources), spoofing (e.g. impersonate other users to access network resources), theft and willful destruction.

Unintentional

Equipment and power failure, human errors (e.g. unprotected password) and mis-managed systems (e.g. mis-configured equipment and unpatched software).

Unfortunately, if threats occur, they may induce risk of **losses** to schools.

Nowadays, more and more IT facilities are integrating into school networks, including teaching materials, students' homework, valuable information and data files which are stored in school systems. In order to protect them against threats and to reduce the risk of losses, it is important for schools to:

■ Arouse systems and networks' users, including students, teachers, school head, school staff and sometimes parents of the students to have awareness of IT security so that they can properly use IT facilities in schools; and

■ Define a set of policies and procedures for users to protect the computer systems, data, information, as well as hardware and software assets in schools.

To facilitate schools achieving these goals, the chapters later in this document aim to:

■ Provide information about **security basics**; and

■ Indicate appropriate levels of **security measures** in different **IT security controls** in school environment.

2   Security Basics

IT security can be considered as "the state of being free from unacceptable risk in relation to IT". It covers **technical, operational and managerial issues**. For example, in addition to the proper configuration and administration of systems, workstations and servers, proper IT security also depends on the faithful observance of related policies and procedures, physical access controls as well as audit functions.

2.1   IT Security Objectives

In previous chapter we mentioned that it is important for your school to effectively reduce the risk of losses to protect your school IT facilities against threats. In order to do so, it is advisable for you to adopt the following three **IT security objectives**:

- Protection of sensitive information from unauthorized disclosure (i.e. **Confidentiality**);

- Accuracy, completeness, consistency and timeliness of data (i.e. **Integrity**); and

- Safeguarding of necessary resources and associated capability (i.e. **Availability**).

Though the three security objectives are all necessary, depending on your school's circumstances and requirements, the emphasis of each security objective may vary among schools. The sections below provide detailed description on these three objectives.

2.1.1   Confidentiality

When information is read or copied by unauthorized persons, it is considered as loss of confidentiality, such as a student makes a copy of the examination paper (soft-copy), from his/her school server without any authorization or permission from the teachers.

You should assure that users could only access the information that they are authorized to. Your systems may therefore require appropriate settings such as access control or even data encryption (i.e. translation of data into a secret code) to protect the data.

2.1.2   Integrity

When data are modified in unexpected ways, for example, a clerk amends a student's ID number wrongly in SAMS, or a character in a data file is altered due to disk failure, it would be considered as loss of data integrity.

You should ensure the accuracy, completeness and validity of data that no unauthorized change can be made, either accidentally or maliciously.

2.1.3   Availability

Information must be available on a timely basis wherever it is needed to meet your school requirements or to avoid substantial losses.

For example, if power failure unexpectedly occurs and the server(s) of Teaching and Learning School Network is set up without an uninterruptible power supply (UPS), the server(s) will not be properly shut down and cannot be resumed normally. This eventually makes the systems unstable/unavailable. Users like students and teachers will then be unable to use their systems or access the information. Uninterrupted access to information and system resources is a fundamental need of a network system. You should ensure that your school systems and networks provide full and normal functionality.

2.2   IT Security Controls

So now you know the importance and objectives of IT security. While your school systems and networks may provide sorts of security features and options, you need to review your security needs and make appropriate security decisions and settings.

To achieve your school's IT security objectives and requirements, you should take appropriate levels of **security measures** on different **IT security controls**. Some of the common IT security controls include:

- Physical Security

- Access Control

- Data Security

- Network and Communication Security

- Security Audit and Incident Handling

- User Awareness and Education

Brief description on these security controls is introduced in the following sections. Details of security measures on each of these IT security controls are provided in later chapters in this document.

2.2.1   Physical Security

Physical security is the first line of security defense. It prevents direct access and/or intruders from circumventing IT security.

The IT equipment in your school, such as servers, workstations, backup tapes, recovery diskettes, original software packages etc. should be kept in

a safe place against unauthorized access. In addition, you should define the school areas that are having different levels of physical security requirements.

2.2.2   Access Control

Different users on different systems should have different rights on using the associated resources. Access controls are defined for and assigned to specific data files, resources and other system rights. Proper access control prevents unauthorized access to system and/or network resources.

2.2.3   Data Security

The data in your school systems and networks are valuable asset. Therefore, with respect to the levels of security required, it is necessary to classify data into different classes and protect your systems against loss of data with corresponding measures. Some of the potential causes of data loss include:

- Destructive viruses
- Hard disk subsystem failure
- Power failure
- Software failure
- Accidental or malicious use of deletion or modification commands
- Natural disasters

2.2.4   Network and Communication Security

There are many systems and LANs such as SAMS, Teaching and Learning School Network and/or MMLC at your school. Schools may have different security requirements on them. As there is a need to connect them together, the communication between these LANs should be carefully managed.

Apart from the security within LANs in schools, careful planning is also required for communications to other networks like remote and Internet accesses to prevent possible outside intruders. School users accessing to these external networks or services should also be properly administered and monitored.

2.2.5   Security Audit and Incident Handling

Security logging can trace and detect the occurrence of threats. Periodic monitoring and review of your school systems and networks can give early alarm for IT security incidents.

Moreover, having security controls in place cannot completely avoid the occurrence of threats. You should therefore prepare for security incidents and assure all users know whom to call when suspicious problem occurs.

2.2.6   User Awareness and Education

User education is the most important factor for successful implementation of IT security in schools. All precautions will become ineffective if user awareness is not aroused.

Through well-conceived and committed security training programs, users will be better prepared to avoid problems in the first place.

2.2.7   Other Security Concerns

In addition to the above security controls, there may be some other security concerns unique in your school. When planning IT security, you need to take all these concerns into account.

An example of these is **systems and applications security**. There may be various types of desktop and network operating systems (e.g. Microsoft Windows NT/2000/XP, Apple iMac, Linux, etc.) and custom-made applications installed in your school. They usually provide sorts of security utilities for ease of configuration. While on the other hand, they require special attention for proper association and cooperation.

Your system administrators are therefore required to carefully manage all these systems and applications, with compliance to other security controls and measures adopted in your school.

2.3   Striving for Balance

Before going into details we would like to stress that no IT system or network is ever totally fortified. Adopting security measures merely wants to reduce the risk of losses against threats.

Though no IT system is 100% secure, you should be aware that systems with few security controls are generally more vulnerable than those have made many. You should therefore strive for a balance between the need for adequate security versus the desire to stay within limited resources.

2.4   More Information

You may refer to the following documents to acquire more information on IT security:

Document Name and Link	Source
■ 與兒童上網安全相關的網址 **(Useful Sites Relating to Internet Access Safety for Children)** http://www.edb.gov.hk/FileManager/TC/Content_2342/4a.htm	The Government of HKSAR (HKSARG) - Education and Manpower Bureau (EMB)
■ **IT Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G3) ■ http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/	HKSARG - The Office of the Government Chief Information Officer (OGCIO)
■ **Internet Gateway Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G50) ■ http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/	HKSARG - OGCIO
■ **Legal Aspects of Computer Crimes and Information Systems Security in Hong Kong**	City University of Hong Kong

3   Physical Security

Physical security refers to the protection of sites, the IT equipment and the assets in the sites. It serves as the first line of defense to prevent unauthorized use of and access to the hardware, software and information by keeping them in physically secured areas.

Physical security is fundamental to all security controls. Different areas in your school are generally having different levels of physical security requirements. You should therefore define different access permissions for different zones in your school areas (i.e. **security zone assignment**).

Moreover, hardware, software and data storage media such as servers, workstations, backup tapes, recovery diskettes, original software packages etc. should be stored in a safe place against unauthorized access.

3.1   Security Zone Assignment

For better security and easier management, you should define different access permissions for different zones within a school. Generally three different zones can be defined:

- **Public zone**

   Open to all users, such as corridors where kiosk computers are located.

- **Protected zone**

   Open to specific users, for example, staff rooms for teachers and school staff, and computer rooms for students accompanied with teachers.

- **Restricted zone**

   Open to authorized persons only, for example, server room(s) for system administrators only.

No matter how many security zones your school assigned, appropriate security measures should be adopted. For example, for protected zones like library and computer rooms, responsible persons like librarians and teachers should be present to monitor the use of IT facilities.

Examples

School A has major IT equipment such as servers and network switches storing in the server room. The system administrator of School A

---

therefore assigns the server room as Restricted Zone, in which only authorized persons are allowed to access. The system administrator also locks up its door and windows when the server room is unattended.

Besides, other persons such as visitors or engineers from service contractors who wish to enter the Restricted Zone should be accompanied by system administrator(s). Their accesses should be properly registered in a logbook.

3.2   Hardware and Software Asset Protection

Limit the access to critical system components to a small number of individuals would be crucial in protecting your school. Below are some examples of security measures for protecting your school's hardware and software assets.

3.2.1   Access Media

All access media such as keys and access cards should be physically secured and handled only by authorized persons.

3.2.2   Server Room Protection

Since the equipment in the server room, including the servers, network devices and other major IT equipment are usually required to operate round-the-clock, dedicated power supply circuit and UPS should be made available for the server room.

Moreover, in order to keep the temperature and humidity at optimal level, the air conditioner(s) in the server room also has to operate on 24-hour-a-day basis.

Furthermore, you should consider installing other security measures such as heat and smoke detectors, motion detectors, alarm systems and fire extinguishing equipment to further enhance the security. These items should be regularly checked to ensure their serviceability.

3.2.3   Floor-level Equipment Cabinet (FLEC) Protection

Network devices such as switches and hubs should be secured in locked containers such as FLEC to prevent theft and unauthorized access.

3.2.4   Power Damage Prevention

You may consider using surge protectors to protect the hardware equipment, including servers, workstations, printers and scanners.

3.2.5   Mobile Devices

Mobile computer equipment, such as notebook computers and projectors, should not be left unattended without proper security measures. For example, when notebook computers are not in use, they must be placed inside lockable cabinets (e.g. the notebook cabinet in server room, and/or the desk cabinet of the corresponding teacher in staff rooms).

On the other hand, when mobile devices are in use, they should be safeguarded by responsible persons.

3.2.6   Storage Media

You should define security measures for handling various storage media such as backup tapes, floppy disks and CD-ROM discs. Media with sensitive data should be locked in secure areas.

3.2.7   Software Copies and Backup Tapes

The original and backup copies of software programs and data files should be kept secured. You should consider keeping the backup copies in a separate location with a safe distance from the original copies. This could minimize the possibility of total loss of the copies from damages arising from a disaster at your school site.

3.2.8   Property Marking and Inventory Taking

Property marking and inventory taking are important measures to prevent physical loss. Property marking should be properly painted to all major hardware items such as system units, monitors, notebook computers, printers, scanners, projectors, removable storage devices etc.

On the other hand, you should use a log book to record and maintain an IT equipment inventory list and perform periodic checking on the items, including the system configuration, software media and licenses, network devices, data backup tapes, etc. The logbook should also record the location as well as the status of the equipment such as "in use", "on loan", "repair", "discard", etc. If there are missing parts and/or difference you should investigate immediately.

For establishing software inventory list, you may consider using software asset management (SAM) tools for the ease of information collection.

More Information

For more information about physical security, see the following:

Document Name and Link	Source
■ **IT Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G3) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/	HKSARG - OGCIO
■ **Internet Gateway Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G50) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/	HKSARG - OGCIO

4   Access Control

Different users would have different rights on using the network resources. Access controls are measures defined for and assigned to specific data files, network resources like printers as well as other system access rights like log-on hours.

Proper access control prevents the unauthorized access of system and network resources. In controlling the access, authentication and authorization are usually adopted:

- **Authentication**

  Authentication (sometimes it is simply called "user log-on") is the process of identifying a user, usually based on a user name and password.

- **Authorization**

  Authorization is the process of granting user right to access system and network resources like printers and the data files in your school servers. Special care should be taken in protecting the password and access right assignment to prevent unauthorized access.

Users must have their own identities, or **user accounts**, in order to access the resources in your school systems and networks. According to their roles in your school, different users may have different access rights. Therefore different rules may need to be set for different groups of users and computers.

The following sections would provide more information on user accounts administration and their related security options.

4.1   User Accounts Administration

There are various users in your school systems and networks, including students, teachers, school head, school staff and system administrators. In some schools, it may include external service contractors and parents of the students. These users usually have their respective user accounts specific to their role, services required, or job level.

Examples

Teachers should have separate authorities from students when accessing computer information. On the other hand, administrators of a school network like Teaching and Learning School Network have special privilege

---

over other users in order to perform system administration and network management.

For easy user administration and security settings, you should therefore identify the similarities among users and create roles associated with the groupings. Commonly there are two main classes of user accounts: **general** and **special** user accounts.

4.1.1   General User Accounts

Each user may be provided with his/her own identity, or a user account, to access the school systems and/or networks. A user account at least consists of a user name and a password.

Generally there are two types of user accounts in schools. They are **network** and **local user accounts**. Network user accounts are used for logging on to a network in order to access the network-wide resources, while local user accounts are used for logging on to a local computer and accessing the resources associated with that local computer only.

Examples

School A uses Microsoft Windows 2000 systems for her Teaching and Learning School Network. Windows 2000 domain user accounts (i.e. network user accounts) are used for the users to access the network-wide resources while Windows 2000 local user accounts are used for the users of standalone computers.

In addition to different types of user accounts, user accounts can also be classified as personal user accounts or shared user accounts.

■   **Personal User Accounts**

For personal user accounts, each of the users may have a unique identity in the system so that he/she can have the flexibility of personalizing his/her own user and data settings.

Moreover, since each user has an individual identity, security permission of system resources can be customized for each user. Furthermore, user activities on the system can thus be **traceable** and accountable to the corresponding person.

Pros

-   Security settings can be customized to an individual

- User activities can be traceable to the corresponding person

Cons

- Massive personal user accounts may increase workload for user accounts administration

- **Shared User Accounts**

    For shared user accounts, a group of users will have the same identity in accessing the system. For example, when students are attending a computer course, they may use a shared account so that all user and data settings as well as security permission defined for that shared account can be applied to all students.

    However, you should note that activities performed using shared user accounts are difficult to trace. If shared user accounts are necessary, such accounts should only be granted with the **minimum privileges** that are sufficient for the account holders to carry out their work.

    Pros

    - The use of shared user accounts may simplify user administration

    Cons

    - Security settings are difficult to be customized to an individual

    - User activities are difficult to trace to the corresponding person

---

Examples

School A has kiosk computers in corridors for casual use. For easy operation a single shared user account is created for logging on to these kiosk computers. As these kiosk computers would be used and shared by many users, it will be hard to trace the activities of that shared user account. School A therefore decides to assign that shared user account with minimum access rights.

4.1.2   Special User Accounts

Another class of accounts is the functional user account, or sometimes called a "special user account". Special user accounts are those accounts that are created to support some particular functions as opposed to a general user account issued to an individual person for normal daily operation.

__Examples__

__Default User Accounts - Administrators and Power Users__

In Microsoft Windows 2000 or NT 4.0 systems the default "Administrator" user account as well as the user accounts in the "Administrators" and "Power Users" groups are examples of the special user accounts. It is critical to manage these accounts explicitly because they have a superset of privileges __by default__.

__Default User Accounts - Guests__

In Microsoft Windows 2000 or NT 4.0 there are some special user accounts like the default "Guest" user account and the "Guests" group. They require special configuration on security settings. Depending on your school requirements and for better security control sometimes these guest accounts should be disabled.

__Teachers who are also acting as System Administrator__

In your school some teachers would act as system administrator. They should be given two user accounts for different purposes: a personal user account for teaching purpose while a special user account with administrative privilege for system administration.

For better security control, teachers concerned should use the two accounts accordingly. For example, when performing teaching duties such as preparing teaching materials or surfing the Internet for non-administrative purpose, they should use their non-privileged personal user account.

On the other hand, for testing and/or troubleshooting purposes, it is common to change users' security options in an attempt to test or solve a particular function or problem. In each case it is important for schools to review the security configuration of user accounts that have established deviations.

__Examples__

__User Accounts for External Parties / Temporary Purposes__

School A requires an external service contractor to help install and configure a new system to her Teaching and Learning School Network. The system administrator of the Teaching and Learning School Network creates a temporary user account with advanced privileges for the engineer of the service contractor. He disables it immediately after creation.

> *Whenever the engineer comes to the school the system administrator will activate the engineer's user account so that the engineer can perform system installation and configuration under the administrator's monitoring. And each time after the engineer properly completed the task and left the school, the system administrator will disable the user account of the engineer again to prevent unauthorized log-on and access.*
>
> *After all tasks are completed by the engineer and the service is accepted by School A, the system administrator will remove that temporary engineer user account from the Teaching and Learning School Network.*

4.2   User Security Options

Password and access right should be properly handled and assigned to each user account. Depending on your school's requirements, some user accounts may require more system or application specific security settings.

4.2.1   Password Handling

You should let your users know that they are responsible for the activities carried out through their user accounts. They should keep their password secret. Otherwise someone may use their user account to access or even destroy the data/documents in the school systems and networks on behalf of themselves.

Below are examples of best practices for password handling.

> ### *Examples*
>
> *Keep Passwords Secret*
>
> *You should remind your users never to disclose their passwords to others and keep the passwords on hard copies. On the other hand, system administrators should ensure that passwords are well protected or encrypted when either held in storage or transmitted over networks.*
>
> *Use Hard-to-Guess Passwords (i.e. Strong Passwords)*
>
> *All passwords should not be in the form of dictionary words. Besides, personal identification information such as user's name should also be prohibited. You should advise users to choose passwords containing a considerable number of characters, such as eight characters with a combination of alphabetic, numbers and special characters.*

Prevent Default Passwords

Users are required to change their default passwords upon first log-on. In addition, system administrators are required to change the preset passwords that are built into the software (e.g. the preset password of "Administrator" for user account created for Microsoft Windows 2000/NT 4.0).

Set Expiry for Passwords

System administrators should consider assigning a password expiry period to every account of a networking system in order to force the users to change their passwords regularly, for instance, every 60-day.

Restrict Failed Log-on

System administrators should restrict the number of failed log-on to all accounts in order to prevent password guessing from intruders. For instance, after five consecutive failed log-ons, the specified account would be locked to prevent further password guessing.

Protect BIOS Passwords

In addition to the password for logging on to the computer system or network, each computer machine itself has a BIOS supervisor and power-on password as the first-level hardware protection.

System administrators may request contractors to preset and activate the BIOS passwords for all computer machines. Details of the passwords should only be disclosed to authorized persons in your school.

Moreover, system administrators may consider requiring users to input BIOS power-on password in order to use that computer machine.

4.2.2   User and Access Rights Assignment

You should ensure that user rights are assigned on a need-to-know basis. You should avoid assigning unnecessary privileges to users, i.e. users should only be given rights to resources they need to do their jobs.

Below are some examples of best practices for user and access rights assignment.

__Examples__

Assign Appropriate Rights

System administrators should properly administer their systems and assign appropriate rights to their users for accessing system and network resources. For instance, students should not be able to access the teachers' home directory or print documents to the printers in administration office.

Revise User Rights

User rights should be reviewed periodically. System administrators should remove unnecessary rights and delete obsolete user accounts as soon as possible.

Restrict Log-on Hours

User log-on to school systems and networks should only be enabled when necessary. For instance, you may consider setting the log-on hour for most users between 7:00 a.m. and 7:00 p.m. in normal school days.

Require Authentication for All Computers

In addition to physical security, all your school systems, including servers, networked and/or standalone workstations and notebook computers, should require the key-in of the user name and password for gaining access. Moreover, the users have to log off when they are not using the systems. Besides, user name should be cleared in the log-on dialog box.

Enable Screen Saver Protection

System administrators should consider enforcing password-protected screen savers to all computers. It is intended to automatically prevent access to the computers without any activity after a pre-defined period of time, for instance, 10 minutes.

4.3   More Information

For more information about access control, see the following:

Document Name and Link	Source
■ **IT Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref.	HKSARG - OGCIO

	G3) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/	
■	**Internet Gateway Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G50) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/	HKSARG - OGCIO

5   Data Security

The data within your school systems and networks may be the most valuable asset. In establishing the physical security measures and user access framework, you should also pay attention to the protection of data.

In general, data security requires data files to be properly created, labeled, stored and backed up. The data should also be protected from virus attack.

The following sections are intended to provide you some examples to prevent data loss in school environment.

5.1   Data Classification

In your school systems and networks, data should be classified according to their sensitive levels. Appropriate access privileges of the different data classes should then be assigned to different users according to their needs.

In general data can be classified into three basic classes:

- **Public Data**

    Public data are intended for all users, for example, school announcement.

- **Private Data**

    Private data are intended for the owner of data only, for example, data files storing in a user's home directory.

- **Restricted Data**

    Restricted data are intended for a pre-defined groups or persons only, for example, examination paper.

Examples

School A decides to classify the data stored in the servers into three classes. For instance:

- *"Public" data like school calendar, school-bus timetable, activity schedule, etc. for all users' to have read-only access privilege;*

- *"Private" data like files/documents stored in home directory of each user which could be modified by the owner only; and*

> - *"Restricted" data like examination papers which are encrypted and only the corresponding subject-teachers are permitted to access.*

However, you should note that the above data classification is for your reference only and may not be suitable to all school environments. You may be required to define more or less data classes. For instance, some schools may find that data like staff appraisal reports require stronger data security, e.g. storing the data in floppy disks only and locking them in a safe place.

Anyway, no matter how many data classes are defined in your school environment, you should protect the data from any attempt on unauthorized access and handle the data properly as described in the sections below.

5.2   Data Handling

Data security protects your school systems and networks against loss of data. Potential causes of data loss may include computer viruses, power/hard disk subsystem/software failure, accidental or malicious use of deletion or modification commands, natural disasters, etc.

Computer virus intrusion would corrupt or even destroy data. You should install and configure anti-virus software in order to protect your data from viruses. We would provide detailed information on virus protection in later sections of this chapter.

On the other hand, data loss and network downtime caused by damage of storage media and power failure can be prevented by security measures like provision of advanced harddisk sub-system and UPS respectively. Lastly, in case of data loss or corruption for any reason, you may recover the data by means of backup and recovery process.

5.2.1   Data Storage in Servers

The servers of your school networks are considered as the heart of your system. The data stored in the servers which are critical to all network users should be properly protected. Therefore you should consider using advanced technology to improve resistance to disk fault (e.g. Redundant Array of Independent Disks 5 (RAID-5) hard disk sub-system) and availability of services (e.g. UPS).

5.2.2   Data Backup and Recovery

You should develop a proper "system backup and recovery" strategy that corrupted or accidentally deleted data can be restored from a proper data backup.

The strategy should define the steps and procedures to back up and recover all critical data. The procedure should be fully automatic with minimal human interaction. Besides, all backup and recovery procedures should be well documented, tested and properly implemented.

You should **assign a person** (e.g. technical support services engineer / system administrator) **to be responsible for data backup and recovery**. Data backup should be performed and monitored at regular intervals. Periodically, it is advised to perform a trial restoration to verify that files could be properly backed up.

Moreover, as mentioned in "Physical Security" chapter, you should keep the backup media (e.g. backup tapes) in a safe place. For example, after each time of data backup (usually automatically takes place at mid-night), instead of keeping the backup media inside the server room, the technical support services engineer removes the backup media from the backup device as soon as possible (usually the next early morning) and then hands the backup media to the responsible teaching staff/system administrator or even the school head for placing them in a locked cabinet.

You may also consider keeping the backup media "off-site", i.e. with a safe distance from the original copies. This could minimize the possibility of total loss of the copies from damages arising from a disaster at your school site.

You may refer to "Windows 2000 Technical Guidelines for School Network Implementation" for detailed information on data backup and recovery as well as tape-rotation scheme at:

[appendix]

5.2.3 Storage Media Labeling and Storing

You should label the storage media such as backup tapes, floppy disks and CD-ROM discs according to the different data classes. And as mentioned in previous sections, you should place storage media in their corresponding data class areas.

5.2.4 Sensitive Data Protection and Disposal

You may consider enhancing the security level of sensitive data by encryption (e.g. the Encrypting File System (EFS), a data encryption feature in Microsoft Windows 2000).

In addition, you may consider enabling password protection feature available in some application software (e.g. programs of Microsoft Office suite) for protecting documents containing sensitive data.

Besides, you should clear all sensitive data completely from the storage media prior to disposal or destruction of them.

5.2.5   Principles of Protection of Personal Data

The Personal Data (Privacy) Ordinance applies to data users, i.e. persons who collect, hold, process and use the personal data, of public and private organizations including government departments. Under the Ordinance, data users must comply with the six internationally recognized data protection principles in the processing and use of personal data. For details about these principles, please check the following URL: http://www.pcpd.org.hk/english/ordinance/section_76.html.

Principle 4 relates to the security of personal data, where a data user must take appropriate safeguards for the protection of personal data. Following the Principle, schools have to protect against unauthorized or accidental access, erasure, processing or other use of personal data. Schools must also consider the protection of

- the personal data that you hold;

- data that you process; and

- data that you transmit.

Personal Data (Privacy) Ordinance Related Information	Source
http://www.pcpd.org.hk/.	Office of the Privacy Commissioner for Personal Data, Hong Kong
http://www.privacy.com.hk/	Privacy of Personal Data in Hong Kong
https://www.pcpd.org.hk/	PERSONAL DATA (PRIVACY) ORDINANCE
http://www.dutylawyer.org.hk/	Information of Personal Data (Privacy) Ordinance in The Duty Lawyer Service of HKSAR

5.3   Computer Virus Protection

Computer viruses are programs written specifically to cause damage or do mischief to other programs or to information. Like real viruses, these programs can replicate themselves and propagate to other computers. It may affect the normal operation of your school systems and networks by corrupting or even destroying the data within.

There are many kinds of computer viruses. They are classified according to their residence, way of propagation and damage to computers. For instance, boot sector virus residents in the boot part of storage and loads to computer memory for infection.

Below are some examples of best practices for protecting your data from computer viruses.

5.3.1   Anti-Virus Software

You should install memory-resident anti-virus software in all school computer systems including servers and client workstations (desktop and notebook computers). The virus monitoring and real time alert functions should be activated. This could enable software and data files in your school systems to be scanned with the anti-virus software before they are loaded and used.

You should also update the virus definition file of your anti-virus software regularly. More details will be discussed later in this chapter.

5.3.2   Legal and Authorized Use of Software and Hardware

Your school computers and networks should only run software that comes from trustworthy sources and/or authorized agents only. Illegal copies of software are regarded as the major source of viruses. The use of illegal software should be prohibited.

In addition to illegal software, the use of unauthorized software and hardware should also be avoided. A user's personal licensed software or even his/her own personal computer (e.g. a teacher's personal notebook computer) should not be used in school without prior approval from school's authority.

Moreover, you should ensure these personal software and hardware are licensed and virus-free before installing or attaching them to your school systems and networks.

5.3.3   Prevention from Doubtful File Resources

Nowadays communication via electronic mails (e-mails) is very common. With the use of Web browsers (e.g. Microsoft Internet Explorer and Netscape Navigator for Web-mail) and/or e-mail readers (e.g. Microsoft Outlook), students and teachers can easily "talk" to any one in the Internet. They may exchange data files, i.e. e-mail attachments, via e-mails.

Besides, users may use the computer systems in your school to access the World Wide Web (WWW) and sometimes download software programs for trial (e.g. freeware/shareware from the Internet).

You should be aware that e-mail attachments and software programs from the Internet, especially from doubtful origins with filename extension of ".exe", ".com" and ".vbs", are considered as the most common source of viruses. These documents and software programs should be checked and cleaned for virus before use.

Furthermore, data files from doubtful origins like floppy disks and/or CD-ROM discs should also be checked and cleaned for virus before use.

5.3.4   User Education and Incident Handling

Users must not intentionally write, generate, copy, propagate, execute or introduce computer viruses.   However, it is likely that users may unwittingly introduce a virus into your school systems by downloading files and/or receiving e-mails from the Internet, or by copying files from their home PC.   Therefore one of the best ways to keep your systems safe from viruses is by educating users.

You should educate users about viruses and let them realize how much damage a virus can inflict.   You should request users to report immediately if a virus is found.   In addition, they should stop using the computer and/or disconnect it from the network when it is suspected to be infected by a virus.   You should manage to defect the virus as soon as possible.

More information on handling virus infection will be discussed in "Security Audit and Incident Handling" chapter.

5.4   Software Configuration and Change Control

You should practice **proactive security** for your systems and networks. For example:

5.4.1   Disabling or Removing all Unnecessary Services and Components

"Full" or even "Typical" installation of Microsoft Windows 2000 and/or NT Server / Professional / Workstation as well as the installation of some applications like Microsoft FrontPage may automatically trigger the installation of Microsoft Internet Information Service/Server (IIS) and other Internet-related services like FTP, SMTP, NNTP, Internet Printing, Indexing Service, etc.

It is noted that in many situations schools do not need these services/components indeed.   However, neglected configuration of these services/components will usually cause security exploits.   Therefore, if the service/ component is neither functional nor necessary on your systems, you are encouraged to disable or remove them.

5.4.2   Using Administrative Tools

Some Microsoft Windows 2000/NT 4.0 built-in functions and administrative tools, such as mandatory roaming profiles, "User Manager for Domains", "System Policy Editor", Group Policies, etc. are useful for security

configurations and desktop management. System administrators may utilize these tools to customize user accounts and settings (i.e. user profiles), and restrict users to change any system setting.

For example, system administrators can use these tools to standardize the desktop user interface (e.g. "Start" menu, desktop icons, wallpaper, screen-saver, etc.) for all or groups of their users.

In addition, these tools can also facilitate system administrators restricting users to change any desktop settings, system files and applications. For instance, they can remove access to the "Display" and "System" Control Panel applet for students to prevent them from changing the system configuration and network settings of the computers.

5.4.3 Applying Recommended Security Fixes

You are reminded that no software is infallible. You should keep an eye on the latest news about IT security and apply the recommended security fixes to your school systems, if any.

5.4.3.1 Virus Definition Files

You should regularly visit the Web sites of your anti-virus software and check any virus alerts or new virus definition files. Additionally, you should regularly update the virus definition files in all computers. For instance, **at least once a week**.

The following Web sites are some of the organizations and anti-virus companies providing up-to-date virus information and alerts:

Virus Alerts	Source
http://www.hkcert.org/valert/valert.html	Hong Kong Computer Emergency Response Team Coordination Center (HKCERT/CC)
http://www.cert.org/current/current_activity.html#virus	CERT/CC
http://www.f-secure.com/virus-info/	F-Secure Corporation
http://www.mcafee.com/anti-virus/	McAfee.com Corporation
http://www.symantec.com/avcenter/	Symantec Corporation
http://www.antivirus.com/vinfo/	Trend Micro, Incorporated

5.4.3.2 Software Patches

You should be aware that there may be bugs and security holes in the software installed in your school systems and networks. Therefore you

should regularly visit the Web sites of the software vendors as well as some security agencies to observe for any up-to-date security alerts.

The following Web sites are some of the organizations and software companies providing up-to-date security alerts:

Security Bulletins	Source
http://www.hkcert.org/salert/salert.html	HKCERT/CC
http://www.microsoft.com/security/default.aspx	Microsoft Corporation

If new security fixes or system patches are released then you should carefully read the related information and consider installing these fixes and patches to your systems.

For example, **Web browsers** like Microsoft Internet Explorer and Netscape Navigator, **e-mail readers** like Microsoft Outlook, **Web servers** like Microsoft Information Internet Server and **operating systems** like Microsoft Windows 2000/NT 4.0 are some common software you need to pay special attention.

Microsoft provides some security checker programs for assessing system security and advising the necessity of software patch, if any. The followings are some examples. You may find them useful for your school systems.

Add-on Tools for Security Checking	Source
■ **Microsoft Baseline Security Analyzer (MBSA)** It is an on-line Web application that checks Windows 2000 and XP systems and generates a report of security settings and recommendations for improvement. http://www.microsoft.com/technet/security/tools/mbsahome.mspx ■ **Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool** It is a command-line tool that school system administrators can use to centrally assess a computer or group of computers for the presence or absence of security patches of Windows 2000/NT, Internet Information Server 4/5, Internet Explorer 5.01 or later, etc. ■ http://support.microsoft.com/kb/821379	Microsoft Corporation

5.4.3.3 Subscription to Security Alerts Mailing List

To practice safe computing in a proactive way, you are encouraged to subscribe the mailing list from security agencies / software companies.

The subscription should be made for all responsible personnel, e.g. system administrators and support staff of Teaching and Learning School Network.

You may also subscribe security alert from your anti-virus software company (see the Web sites above).

Subscription to Security Alerts	Source
https://www.hkcert.org/	HKCERT/CC

5.5   More Information

For more information about data security, see the followings:

Document Name and Link	Source
■ **IT Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G3) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/index.htm	HKSARG - OGCIO
■ **Internet Gateway Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G50) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/index.htm	HKSARG - OGCIO

In addition, you may refer to the following documents in order to acquire more information about computer virus protection:

Document Name and Link	Source
■ **Types of Computer Virus** http://www.infosec.gov.hk/english/virus/types.html	HKSARG
■ **Virus Hoax** (Hoax is false virus alert, often in the form of e-mail) http://www.infosec.gov.hk/english/virus/types_om.html	HKSARG
■ **Guideline and Tips for virus prevention** http://www.infosec.gov.hk/tc_chi/yourself/yourself.html	HKSARG

6   Network and Communication Security

Remotely accessing your school systems and networks as well as resources in the Internet are useful and helpful to your school. However, one of the drawbacks is that your school is vulnerable to the outside attacks.

Other than the connection between your school and external networks, there are also many LANs such as Teaching and Learning School Network, MMLC and WebSAMS which are inter-connected within your school. In accordance with your school circumstances you may have different security requirements on some of these LANs.

In this connection, you should carefully manage the communication between **external networks** and your school, as well as among different components **within the LAN** in your school. Appropriate security measures are required to safeguard and control the communications between them.

6.1   Communication between Your School & External Networks

There are tremendous resources on **the Internet** and most schools had already connected to this "Information Super Highway" via different types of communication channel such as traditional telephone line with modem, leased line or broadband connection.

In addition, in some schools users may be allowed to **remotely access** their school systems and networks from external locations. For example, in some urgent cases your system administrators may be required to remotely administer your Teaching and Learning School Network with their PC at home at night.

You should implement appropriate security measures in order to protect your school from possible outside attacks. Moreover, your should educate your users on the use of these external networks and monitor their accesses.

6.1.1   Remote Access

Typically there are two types of remote access in school environment. They are:

■   **Dial-in Access**

With the use of dial-up equipment (e.g. a telephone line and a computer with modem), users at remote site (e.g. at home) could dial-in to their school networks and work as if they were directly connected in LAN environment.

■   **Dial-out Access**

With the use of dial-up equipment (e.g. a telephone line and a computer with modem), users at school site can dial-out to other computer networks (e.g. the Internet).

6.1.1.1 Dial-in Control

Dial-in access to your school networks should only be provided to authorized person(s).   A central dial-in server (e.g. a Windows 2003/2000/NT server with Remote Access Services (RAS) installed) should be installed to support dial-in access.

You should also adopt appropriate security measures in your system such as callback function and audit logging. The audit logs should be reviewed periodically to check if there is any intrusion attempt.

6.1.1.2 Dial-out Control

Users should not be allowed to use the dial-out functionality on networked desktop or notebook computers. If dial-out access is required, the access should be carried out via a central dial-out server (e.g. a Windows 2003/2000/NT RAS or a single IP sharer with multiple telephone lines for Internet access) with regular auditing. If central dial-out server is not available, dial-out access should be carried out in standalone computers or isolated systems.

In addition, the dial-out equipment should be closely controlled and monitored.

6.1.1.3 Other Considerations

You should not use the same dial-up equipment for both dial-in and dial-out purposes. Dial-in and dial-out activities can be monitored and traced much easier if their equipment is separated. And all modems should be powered off when not in use.

6.1.2   Internet Access

Your school may already have connection to the Internet via telephone dial-up, leased line or broadband connections for the access of Internet resources and/or establishment of your school Web site.

However, it is impossible to guarantee that malicious hackers would not attack your school networks via your Internet connection. Besides, it is also difficult to know what sort of content your school users will access using Internet search engines.

Therefore, no matter which type of Internet connection your school is using, you should adopt appropriate security measures.

You should connect your school network/server to the Internet via a central **Internet gateway** with adequate security measures like Internet services and Web sites **filtering**. In addition, all related settings as well as the **audit** logs generated should be reviewed regularly.

You are advised to consult your service contractor(s) in planning/designing the Internet security for your school.

6.1.2.1 Internet Gateway

In general an Internet gateway is a combination of hardware and software that acts as a bridge to link up a private network and the Internet, and protects the private network from unwanted intrusions.

It acts as a gatekeeper that controls traffic between the private network and the Internet based on the user-defined security criteria called **rule-set**. It intercepts any internal Internet request, executes that request, and then sends the information back to the internal users. If an outside hacker attempts to hack the private network, the Internet gateway will intercept the request and deny the hacker's access.

For example, a school Internet gateway can act as a middleman between your Teaching and Learning School Network (i.e. the private network) and the Internet to control the data traffic between them. All data entering or leaving the Teaching and Learning School Network pass through Internet gateway, which examines each data and blocks those that do not meet your defined rule-set.
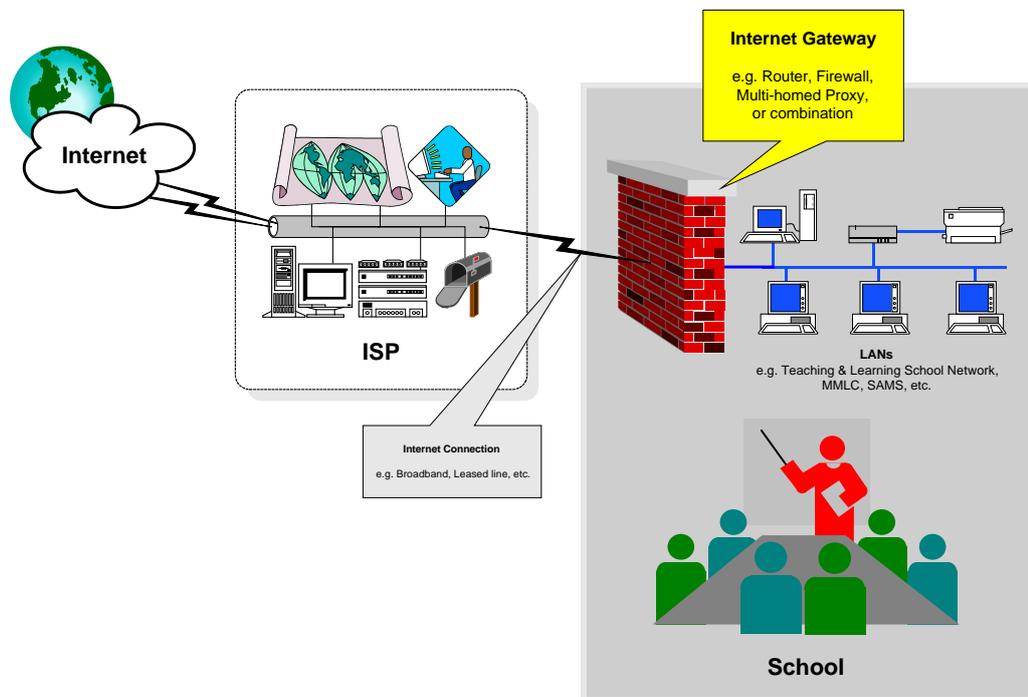
Types of Internet Gateway

A school Internet gateway can be implemented in many ways. Some schools may simply choose to use a **router** as their school Internet gateway, while some may use a **firewall system**, a **multi-homed proxy system** or a combination of them in order to strengthen the security protection.

The following provides description on various types of Internet gateways:

■ **A Router**

A typical hardware-based router device can act as a simple Internet gateway at a relatively low cost. At a very minimum, two interfaces are required: one is for connecting your local school networks while the other is for connecting to the Internet.

In fact, the router on loan from an ISP can act as the Internet gateway itself. However, you may find it difficult to configure sophisticated data filtering (i.e. rule-set) through a router. Moreover, some ISPs may not allow you to change the configuration under the service agreement.

■ **A Firewall System**

A firewall system can be implemented in a "black box" hardware device, or through software installation on top of a computer.

There are several types of firewall techniques, such as packet filtering (e.g. IP addresses) and application filtering (or called protocol filtering) (e.g. "FTP" and "Telnet"). You could define rule-set in order to precisely filter and control the packets and applications between your school and the Internet.

For example, you may use a firewall and configure appropriate rule-set to prevent students from accessing a specific set of Web sites (for instance, pornographic and violent Web sites), or to disable services like "Telnet" and "ICQ" so that remote access and ICQ communication to the your school are not allowed.

■ **A Multi-homed Proxy System**

Generally a multi-homed proxy system is an isolated proxy system (a low-end server or a workstation with adequate resources can be used) with **two network interface cards**, sits between and connects your school and the Internet.

Similar to a firewall system, it can filter and control the packets and applications based on the user-defined rule-set. However, sometimes only limited rule-set can be configured with a multi-homed proxy system.

Notes

In general, a proxy system is a server that sits between a client application (e.g. a Web browser) and a real server (e.g. a Web server). For example, a school proxy system intercepts the requests from the Web browser of a student computer and on behalf of the student computer it then forwards the requests to Web servers outside the school.

A proxy system usually has two main purposes:

- *Improve Web access performance (Web caching): instead of forwarding the Web requests to (outside) Web servers, the proxy system simply returns Web pages/contents that are already fetched (cached) for previous requests/users.*

- *Filter requests: that is the multi-homed proxy system mentioned in this section.*

A sophisticated proxy system can serve these two services simultaneously, for example, the proxy server software under the standard provision of the IT in Education project (e.g. Microsoft Proxy Server and Netscape Proxy Server). However, you should note that in addition to the proxy server software, client software installation and configuration are usually required.

Which Type of Internet Gateway is Most Secure?

There is no absolute answer for this question. Depending on your school circumstances and security requirements, each of the above mentioned items, or combination of them can be used as an Internet gateway for your school.

The following table briefly compares routers, firewalls and multi-homed proxy systems when they are used as an Internet gateway:

Type	Pros	Cons	Remarks
A router	Low cost (free-loaned from ISP).	Sophisticated configuration cannot be easily done.	Some schools may find that a router alone may not be sufficient enough for Internet protection.
A firewall system	Extensive filtering rule-set can be configured.	Technical skills required. Relatively expensive.	Though a firewall system may incur addition costs, some schools choose to deploy it for better Internet protection. Available in a "black box" device, or a computer with a firewall

			software on top.
A multi-homed proxy system	Can also be used for content caching.	Technical skills required.	A proxy system with single interface (i.e. one network interface card) which is usually used for content caching cannot be used as an Internet gateway. Though a multi-homed proxy system may serve as the security solution for many schools, it does not include all the features that high-end firewall packages provide. Generally a computer with a proxy software on top is required. However, a multi-homed proxy system should not be installed on Windows 2000 or NT domain controllers (DC).

Cost

In the past an advanced firewall software system may cost tens of thousands of Hong Kong dollars, not to mention the cost of its dedicated hardware. But in recent years firewalls are getting much cheaper and popular. Many hardware manufacturers and software developers are able to produce inexpensive but sophisticated small office/home office (SOHO) firewalls for small businesses as well as personal, home or school systems.

Hardware -vs- Software Internet Gateway

In practice, many manufacturers or developers use two or more of the above techniques together to build an Internet gateway. Some of them are so-called "all-in-one" hardware Internet gateway / sharing / firewall / proxy device that can serve as a "black box" to link up your school network/server and the Internet, while some of them are software-based and need a computer to run with. Additionally some of the software are freeware (limited functions) while some are required to pay (full features).

The following comparison table briefly discusses key benefits of both the hardware and software Internet gateways:

Internet Gateway	Benefits
■ **Hardware**	Multiple services. Vendors often bundle different services (e.g. router, firewall, proxy, switch/hub, DHCP server (for IP address assignment and management), etc.) within one device. Easy-to-install. Plug the device into a school LAN and with little server configuration the device will be up and running. No additional server machine (or high-end workstation) as well as its peripherals are required. Easy-to-use. Web-based interface for software

	configuration. The device can usually be updated by a software download from the vendor Web site.
■ **Software**	Total control. Software Internet gateways offer total control that a great variety of options can be configured.

User-level control.   Software Internet gateways can usually retrieve user accounts and security settings from the network (e.g. Windows 2000/NT 4.0) that in-depth user-level control is allowed.

Better audit logging and reporting.   Software Internet gateways usually come with comprehensive audit functions.   These help system administrators to monitor the data traffic coming into and out of the school network, streamline network efficiency and analyze the logs if they suspect a security incident.

Better integration.   Some software Internet gateways can be integrated with products from other vendors onto single (or multiple) server machine.   This collaborative approach will usually make a network more secure than a single hardware device solution. |

__Examples__

School A's network has a broadband connection to the Internet.   School A also hosts many valuable educational resources at the school Web site inside the school server.   It is expected that students and teachers at home as well as many outside visitors will visit the Web site frequently, School A decides to install a firewall "black box" to safeguard their school systems and networks.

*A **firewall** complements with the **router** on loan from the ISP as well as the school **proxy system** could provide a better security and Web access solution to School A.*

6.1.2.2 Filtering

As we mentioned before, appropriate filtering should be adopted for safer Internet access.   There are several kinds of filtering services such as **Internet applications/protocols filtering**, **Web sites filtering** as well as **Web contents filtering**.

No matter what kind of filtering services your school plans to have, you should ensure to implement the following policy -- grant users only those access they need to perform their tasks.

Internet Applications/Protocols Filtering

Firewall and multi-homed proxy systems can control and filter the Internet services   and   protocols   communicating   between   your   school   and   the

Internet, including protocols like "HTTP" for Web access, "POP" and "SMTP" for e-mail, "FTP" for files transfer, "Telnet" for remote log-on, "NNTP" for news discussion, "ICQ" for instant messaging, etc.

You may allow only senior students (for instance, Primary 4 to 6 in primary schools) streaming multimedia contents from the Internet, allow all users in your school accessing World Wide Web pages, disallow all users using workstations in your school chatting to anyone outside your school via ICQ.

Web Sites Filtering

In general Web sites filtering can be done in one of the followings or both:

- **By the Firewall / Multi-homed Proxy System at School**

    A firewall or a multi-homed proxy system at your school can oversee users' Internet use and block access to inappropriate sites. It does this by comparing the user's request in their Web browsers with the school's pre-defined list of rated sites configured in the firewall or multi-homed proxy system.

- **By ISP**

    Many ISPs in Hong Kong provide Web sites filtering service customized for education-sector at no additional charge. Some of them would even offer services to review and maintain their filtering list daily.

    When acquiring or evaluating ISPs' proposal for Internet services you should take such service into account in order to filter inappropriate sites.

The followings are some characteristics of these two filtering services:

By	Characteristics
■ **The Firewall / multi-homed proxy system at schools**	Filtering list is unique to the school and can be customized (added, modified and deleted) easily and quickly. Greater manageability and flexibility for change and configuration. Additional administration workload is required for filtering list maintenance. Cost for the system deployment and maintenance.
■ **ISP**	Acts as a central, admirable filtering list for education-sector. Schools can provide and suggest ISP with addition, modification or deletion to the filtering list. Filtering list maintenance depends on the ISP's performance and management. Administration work is off-loaded to ISP.

	Usually a free service by ISP.

Web Contents Filtering

Some Web browsers like Microsoft Internet Explorer support ratings standards such as Platform for Internet Content Selection (PICS) which is ratified by the World Wide Web Consortium (W3C). These ratings standards let you choose different levels of allowable language, nudity, sex, and violence of Web contents.

You could therefore set appropriate ratings level to the Web browser(s) of your school computers so that whenever users visiting Web sites with inappropriate contents their access can be blocked.

You should regularly review and maintain the ratings level to suit your school's preference. However, such de-centralized settings to each computer may cause additional administrative work.

Administration and Management

To enable easy administration, some firewall and multi-homed proxy systems utilize the user accounts of your school systems to define which students, teachers or groups can use the services that your school plans to.

For example, you may select the users or groups from your Microsoft Windows 2000 and/or NT 4.0 Teaching and Learning School Network and centrally administer the users with corresponding Internet application and/or Web site filtering settings in the firewall / multi-homed proxy system.

Besides, in most cases you are also required to conduct software installation and/or Web browser settings at students and teachers' computers (e.g. set the proxy server address). You may use administrative tools like Microsoft Internet Explorer Administrator's Kit (IEAK, for Microsoft Internet Explorer only) to simplify the settings and ease the installation.

6.1.2.3 Logging and Audit

Audit logs are important for security incident handling. You should enable the audit function of your Internet gateway for tracking the services and accesses passing through it.

Successful and/or failed events can be logged to track malicious activities and security violation. Information like time, day, user, application protocol, TCP/IP port number as well as source and destination domain names and IP addresses etc. can all be logged.

You should also regularly review the audit log in order to strengthen the Internet security. More information will be discussed in "Security Audit and Incident Handling" chapter.

6.1.2.4 User Education

There are tremendous useful resources on the Internet that your school users would likely want to access and use for teaching and learning purposes. However, Internet access also raises issues about where your users, especially the students, go as they move away from the classroom.

We will discuss more information about the proper use of the Internet in "User Awareness and Education" chapter.

6.2 LANs within Your School

There are many systems and LANs such as SAMS, Teaching and Learning School Network and/or MMLC at your school. If your school has different security requirement on each of them and there is a need to connect them altogether, then the communication between these LANs should be carefully managed.

6.2.1 LANs of Same Security Level

It is easy to manage LANs with same security requirements. For instance, a network switch or hub can be used to simply connect these LANs together. Data traffic between these LANs can be directly transmitted from one another via the network switch or hub.

Examples

Background

School A has MMLC and Teaching and Learning School Network (workstations are mainly located in the computer room) and these two LANs are implemented with Microsoft Windows 2000. In addition there is an Internet connection in the Teaching and Learning School Network.

Needs

For better resources utilization, users of MMLC require to access the Internet via the connection in Teaching and Learning School Network.

Solution

Since these two LANs are of same security level at School A, the system administrator decides to connect these two networks to the network backbone switch for direct data exchange and communication.
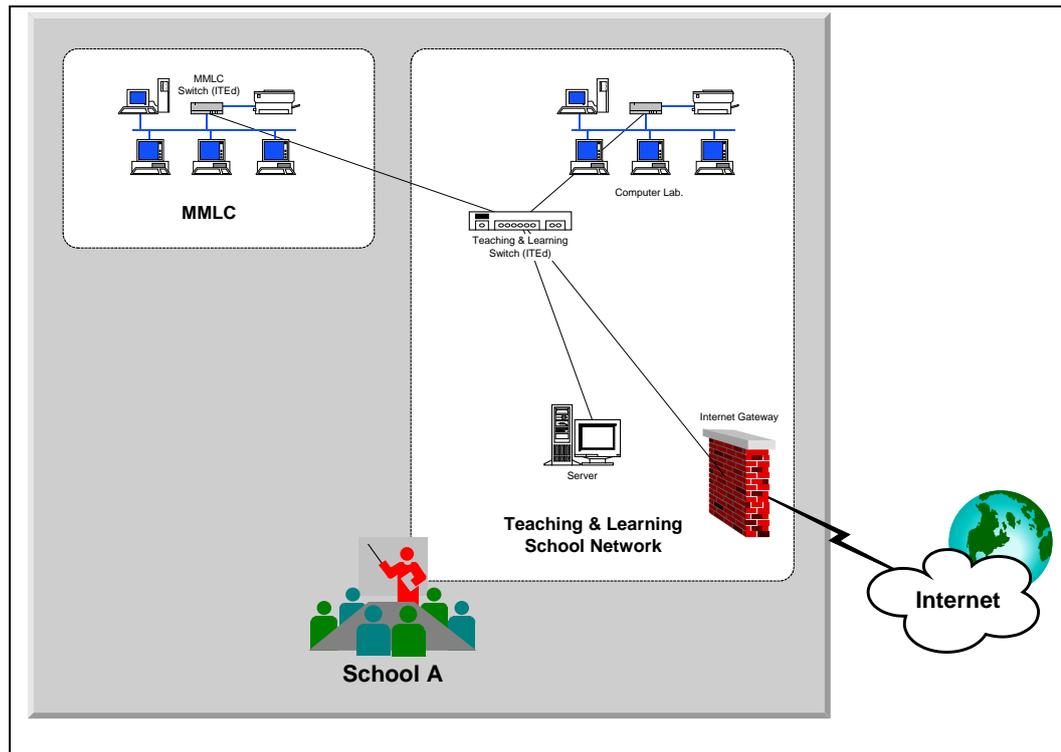
6.2.2   LANs of Different Security Levels

However, for LANs with different security requirements, **there must be something to do** before connecting them together.

For instance, depending your school circumstances, security measures like access control devices (ACD) (e.g. a router, a routing switch, a firewall system, or combination of them) that play like the Internet gateway we discussed in earlier sections can control and safeguard the data traffic between these LANs.

In addition, some other methods may also serve to control the data exchange and communication between those LANs of different security levels, such as configuring appropriate security settings to the computer systems used in those LANs (e.g. trust-relationship establishment in Microsoft Windows 2000 or NT domains).

You are advised to consult your service contractor(s) when planning to connect and manage LANs of different security levels.

__Examples__

__Background__

In addition to MMLC and Teaching and Learning School Network, the same School A in previous example has another LANs -- SAMS. SAMS Windows 2000 version, which runs on Microsoft Windows 2000 Professional (client computers) and NT 4.0 Server (server machine), aims at storing and

---

processing sensitive administrative data that unauthorized access to SAMS must be strictly prohibited. Thus SAMS was originally isolated from other LANs of the school.

Needs

For better resources sharing and utilization, users of SAMS require accessing WWW pages via the Internet connection as well as the data files in Teaching and Learning School Network. Therefore there is a need for School A to connect SAMS and Teaching and Learning School Network together.

However, since these LANs are of different security levels, an ACD must sit between them in order to control the data exchange and communication accordingly.

The ACD must fulfill School A's requirements that users' requests initiated from SAMS to Teaching and Learning School Network (e.g. WWW pages and file access) are allowable, while requests initiated from Teaching and Learning School Network (and other connected LANs of same security level) to SAMS must be forbidden.

Solution

*There are several security measures can serve as the ACD. After consulting service contractors, analyzing related SAMS and ITEd network integration documents (see Notes below), and considering the school's unique circumstances, the system administrator decides to use a **router** as the ACD.*
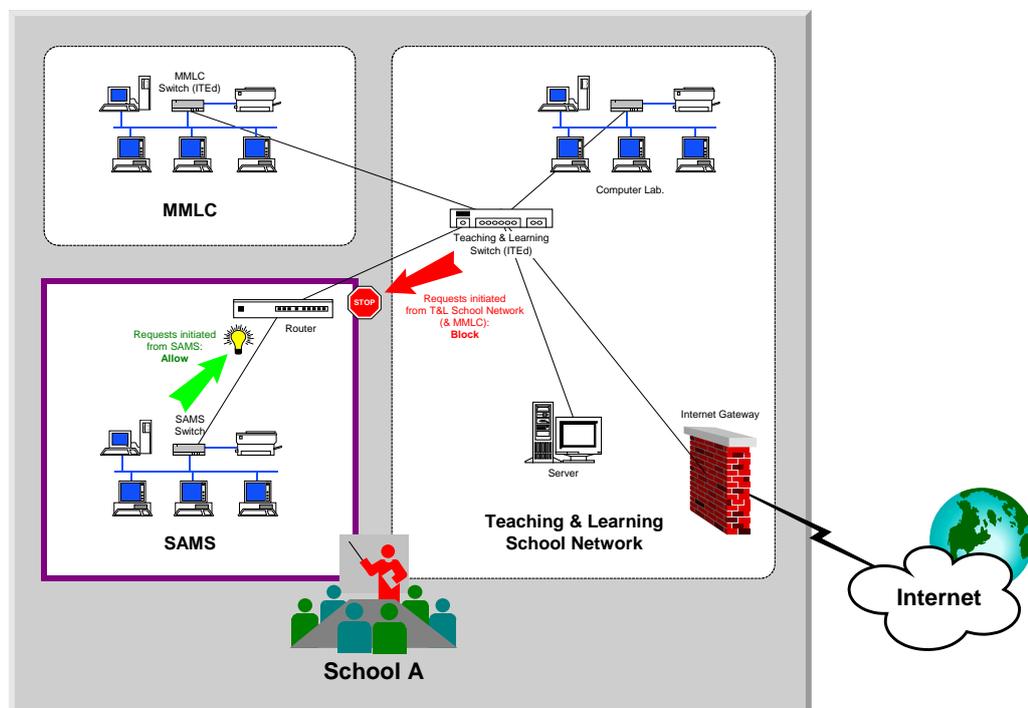
In addition to some pre-requisite network re-configuration work, the designated contractor configures appropriate rule-set to the router and

applies proper security settings to the systems used in these LANs (i.e. trust-relationship establishment and access control settings in Windows 2000 and NT in this example).

After several tests, School A finds the result can fully address the school's needs. The system administrator then trains the users on its related operational procedures. Now SAMS users can access files as well as WWW pages via the Internet connection in Teaching and Learning School Network, while no user from Teaching and Learning School Network (and MMLC) can access SAMS.

Notes

This example only illustrates high-level description on security measures and arrangement for connecting SAMS and ITEd networks. More information about SAMS can be found in EMB SAMS web site:

http://www.edb.gov.hk/index.aspx?nodeID=2238&langno=1

6.3   Protection against Email Spam and Malicious code

6.3.1   Email Spam

An email spam refers to bulk, unsolicited emails sending to many recipients who do not want to receive them, such as advertisement. An email spam also increases network loading and thus wastes network bandwidth.

Schools should consider installing email spam filtering gateway to filter all spam emails from the Internet. Latest spamming lists / blacklists should be regularly updated. Audit logs should be kept at the email spam filtering gateway for future reference. In addition, the following security countermeasures can be used to prevent spam email:

- Prevent email address harvesting from web sites

- Stop third-party mail relay and open 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

__Notes__

School users should observe the following common practices against spam email:

- *Users are reminded to handle their email addresses with care, especially when filling out web registration forms, surveys and other online documents etc.*

- *Avoid publishing email address to unknown individuals and sources, especially as a link on a web site;*

- *Whenever feasible, users may use separate email addresses to avoid their school email addresses and/or mail systems to become a target of spam;*

- *Users should never mailbomb spammers or perform vigilante actions;*

- *Users should not reply to spam, as this would only result in the generation of non-delivery messages or allow the spammers to obtain a validated email address for future spamming;*

- *Users can also control spam by using email filtering tools in email software that allow users to block or screen out spam by defining some simple filtering rules;*

- *Users can file a formal complaint according to the established procedure of the respective ISP for its necessary follow up.*

6.3.2   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 unauthorized access to the system, popping up unwanted screens, and doing things that user does not intend to do.

Examples of malicious code 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.

Traditionally, malicious codes are spread via two main channels:

(a) data transmitted through network, or

(b) external storage media (e.g. CD-RW, storage card or floppy diskettes).

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.

To prevent from computer virus and malicious code attacks, schools should ensure anti-virus and malicious code detection and repair software has been installed and running. Schools should also regularly update virus signature and malicious code definition.

On the other hand, school users should beware of their IT usage behavior. Users should not forward any received hoax messages (i.e. untrue virus-related warnings/alerts started by malicious individuals) to avoid further spreading. Besides relying on technical controls stated above, users should take the responsibility to protect against computer virus and malicious code attacks.

6.4   Web Application Security

Web application provides convenience and efficiency. However, 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.

Because of the complexity of web technologies, conducting a detailed security analysis is not easy and straightforward. The following sections describe some best practices for Schools' information only.

6.4.1   Web Application Security Architecture

Typical web application architecture contains 3 tiers. The architecture separates 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.
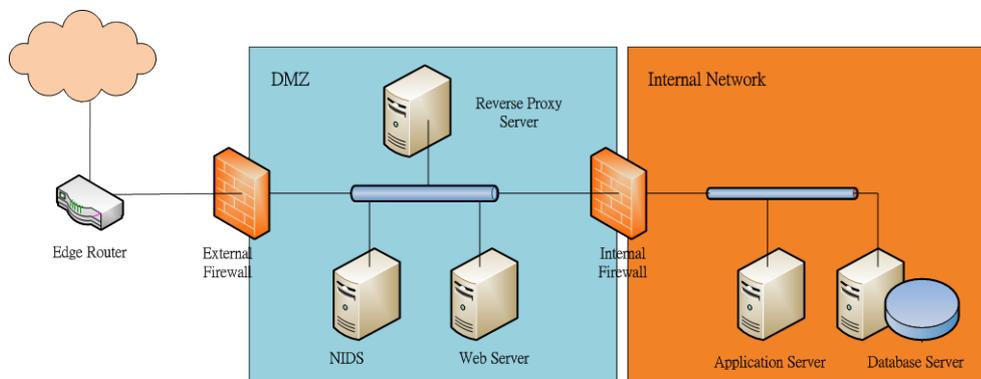
The external facing web server should be confined within a Demilitarized Zone (DMZ). Sensitive servers are located in the internal network with additional protection. Two firewalls should be installed, e.g. the external firewall can be a web application firewall while the internal firewall can be a network layer stateful inspection firewall. They shall be from different vendors.

Other system such as Network intrusion detection system (NIDS) and reverse proxy server should be installed in the DMZ; they are to detect attacks and to act as a single point to provide all web applications to the users respectively.

For web application servers which only serve internal users and have no connection to external network, Schools can consider implementing fewer security protection measures such as implementing just one layer of firewall to segregate the web server from internal users.

Schools are recommended to perform security risk assessment in order to determine the most appropriate security protection measures. It is also noted that Schools shall check their Web servers to see if they are configured and running properly. See web server security in the listed box below:

Note

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;*

- *Install host-based intrusion detection system (HIDS) in web servers storing or processing sensitive information to monitor suspicious activities or unauthorized creation / deletion / modification of files. Alerts and reports from the HIDS should be actively reviewed to identify security attacks at the earliest possible moment;*

- *Configure web server software to prevent leaking information like web server software version, internal IP address, directory structure, etc;*

- *Disable or remove unnecessary modules from the web server software;*

> - *Identify application files on the web sever and protect them with access control;*
>
> - *When using SSL, backup the private key for the server certification and protect it against unauthorized access.*

6.4.2   Web Application Development Process

If the web application is developed by Schools themselves or it is subcontracted to other vendors, the security controls of web application should be analyzed and defined during early stage of the software development with the following considerations:

- Ensure that security requirements are well defined for the web applications;

- Perform IT security risk assessment for critical systems during design and implementation stages;

- 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.

The software development team should follow a set of web application secure coding practices that can help withstand common web application security vulnerabilities.

Please read chapters 10.7.4 of "IT Security Policy and Guidelines (Ref. G3)" as stored in the following URL for information about web application secure coding.

http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/index.htm

6.5   More Information

For more information about network and communication security, see the following:

Document Name and Link	Source
■ **IT Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G3)	HKSARG - OGCIO

http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/index.htm	
■ **Internet Gateway Security Guidelines** (OGCIO Documents on IT Security Policy and Guidelines Ref. G50) http://www.ogcio.gov.hk/en/infrastructure/methodology/security_policy/index.htm	HKSARG - OGCIO

7   Security Audit and Incident Handling

You should periodically monitor and review all defined security controls at your school. Such audit activities are intended to ensure that all associated security measures are properly implemented to prevent any security threats.

However, as we mentioned earlier, even all security controls and measures are well implemented, no IT system or network is 100% secure. Therefore you should prepare yourself for handling security incidents before they actually occur. Moreover you are also required to assure that every user in your school knows whom to contact when he/she suspects the occurrence of problem(s).

7.1   Security Audit

Security logging can trace and detect the occurrence of threats. And depending on the extensiveness of the logging, the detected event could be traceable throughout your systems and networks.

For instance, when an intruder breaks into your Teaching and Learning School Network, the log should indicate who was logged on to the system at the time, the sensitive files that had been failed accesses, programs that had been attempted executions, etc. The log should also indicate sensitive files and programs that were successfully accessed in this time period. Your system administrators can then audit the log to uncover the unauthorized actions and follow up the incident.

In addition, you should ensure that only authorized individuals have access to the audit logs. Regular security audits are important and required since the audit logs together with other supporting information are crucial for recording, tracing and handling security incidents.

Examples

School A uses Windows 2000 as the network operating system for the Teaching and Learning School Network. The system administrator utilizes the built-in auditing function of Windows 2000 since it is capable of tracking successful and/or failed events of malicious activities and security violation.

After considering the school environment, the system administrator decides to perform the followings:

- *Audit failed attempts on "account log-on" and "object access" events*

- *Audit all system, application and security errors*

> *The system administrator regularly uses the associated auditing tools to review the entries generated. For instance, he audits the logs to see whether there are excessive failed log-on attempts as well as events related to denied access to sensitive files.*

7.2   Incident Handling Procedures

In case a security threat unfortunately occurs to your school then you have to handle it properly.

Some of the common security incidents occur in school environment are as follows:

Common IT Security Incidents	Examples
■ **Virus infection**	Receiving e-mails with virus; using files from unknown source, etc.
■ **Issues related to user accounts and passwords**	Users forget their password; accounts lock-up due to excessive failed log-ons, etc.
■ **Damage / loss of hardware, software, data and information**	Breakdown of computers; harddisk failure; loss of software media; accidental deletion of data files, etc.
■ **Misuse of systems and networks**	Unauthorized software installation; malicious configuration changes; excessive print jobs to network printers, etc.
■ **Network intrusion**	Hacking from the Internet; network attacks from internal users, etc.

However, you should note that different incidents require different handling procedures. In any cases you should assure that every user in your school should know whom to call when they suspect a security incident, and should know how to preserve their files, etc.

And you should perform a follow-up analysis after the incident to review any security controls to be improved. In some cases, disciplinary actions may be required.

The followings are examples of procedures for handling IT security incidents of virus infection and network intrusion. While they may not be suitable for all schools and in all cases, in addition to the references linked in next section, they may be helpful for you to handle IT security incidents, if any.

7.2.1   Example - Handling Virus Infection

The following are some general guidelines and procedures for handling virus infection.   You should of course read the user's manual of your anti-virus software to learn more.

Handling Virus Infection

```
┌─────────────────────────────────────────────────┐
│   Step 0  -  Install & Activate Anti-Virus Software │
└─────────────────────────────────────────────────┘
                         ⇩
┌─────────────────────────────────────────────────┐
│   Step 1  -  Isolate the Infected System(s)         │
└─────────────────────────────────────────────────┘
                         ⇩
┌─────────────────────────────────────────────────┐
│   Step 2  -  Notify the Right People & Get Help     │
└─────────────────────────────────────────────────┘
                         ⇩
┌─────────────────────────────────────────────────┐
│   Step 3  -  Try to Kill the Virus & Repair the System(s) │
└─────────────────────────────────────────────────┘
                         ⇩
┌─────────────────────────────────────────────────┐
│   Step 4  -  Inoculate the Infected System(s)       │
└─────────────────────────────────────────────────┘
                         ⇩
┌─────────────────────────────────────────────────┐
│   Step 5  -  Get Back in Business & Review          │
└─────────────────────────────────────────────────┘
```
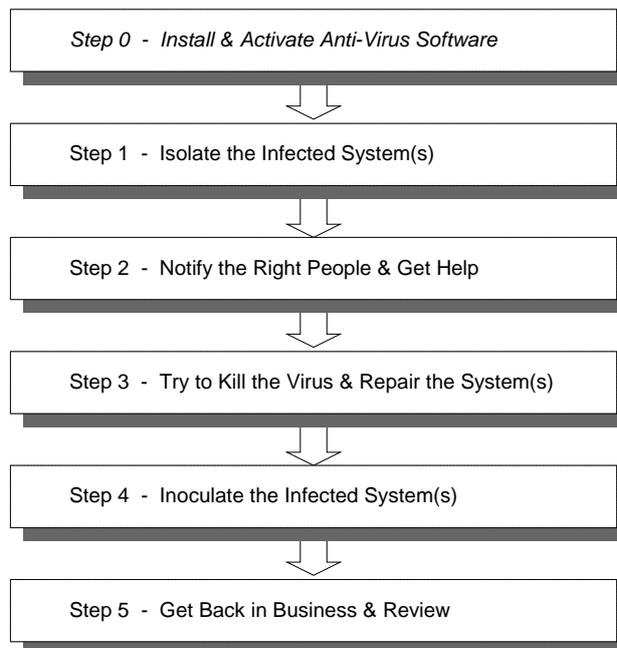
■ *Step 0*   *Install and Activate Anti-Virus Software*

As we mentioned in earlier chapter, all computer systems including workstations and servers should be installed with anti-virus software. Anti-virus software should be activated each time the computer systems start up. Such arrangement is important and acts as a pre-requisite to avoid, inspect and clean computer viruses.

■ **Step 1   Isolate the Infected System(s)**

When the anti-virus software detects a virus or virus-like activity in your system(s), it displays a message, or called virus alert, on your screen.   These alerts indicate that your system(s) is possibly infected with virus.

You are suggested to concentrate on handling the incident and stop processing any other programs and tasks.   Since there are some viruses that will destroy data in the harddisk if the system is rebooted, you should not power off or reboot the infected system(s) immediately.

If the infected system(s) is connected to your school networks then you should isolate it as soon as possible.   For example, you may

disconnect it by unplugging the network cable.

■   **Step 2   Notify the Right People and Get Help**

It is important to immediately notify the **right people** and ask for help. In general, system administrators and/or the technical support services engineer at your school could help handle virus infection incidents. You may also consider seeking advice from security experts, if necessary.

■   **Step 3   Try to Kill the Virus and Repair the System(s)**

You should follow instructions and procedures prompted by anti-virus software, and carefully determine what options/actions you should take.

If you are not sure what option to select, you should immediately get help from technical personnel. For instance, your system administrators or technical support services engineer.

You may be given a "Repair" (or the like) option. "Repair" is always the best choice since it can eliminate the virus and repair the infected file/item.

However, depending on the type and power of the virus infected, the updates of your anti-virus software as well as the configuration of your system, your anti-virus software sometimes may not be able to kill the virus and repair your file/system. In these situations you should carefully think what action you should correctly take. Sometimes you may need to repair your system by restoring files from backup.

And again, you should get help from technical personnel if you are not sure what option to select.

■   **Step 4   Inoculate the Infected System(s)**

You should inoculate and improve the system's defenses by installing the appropriate software like applying latest anti-virus definition and system/application patches.

Moreover, you should monitor closely to determine whether the system can resume its tasks and any viruses exist.

■   **Step 5   Get Back in Business and Review**

After the incident has been fully handled and the infected system(s) are restored to a normal mode of operation, a follow-up analysis should be performed. All involved parties should meet and discuss actions that were taken and the lessons learned.

All existing procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the

appropriate personnel. You should ensure all related security controls and measures are properly implemented.

The last section of this chapter provides some links to security agencies and software vendors. You are recommended to periodically visit these sites for acquiring up-to-dated virus alerts information.

7.2.2   Example - Handling Network Intrusion

The followings are some general guidelines and procedures for handling network intrusion.   Perhaps you may find some of the steps are a little bit serious in your school environment, however, they are worth for you to take a look and use them as a basis reference.

Handling Network Intrusion

| Step 1 - Remain Calm |
| Step 2 - Take Good Notes |
| Step 3 - Notify the Right People & Get Help |
| Step 4 - Enforce a "Need-to-Know" Policy |
| Step 5 - Use "Out-of-Band" Communication |
| Step 6 - Contain the Problem |
| Step 7 - Make Backups |
| Step 8 - Get Rid of the Problem |
| Step 9 - Get Back in Business & Review |
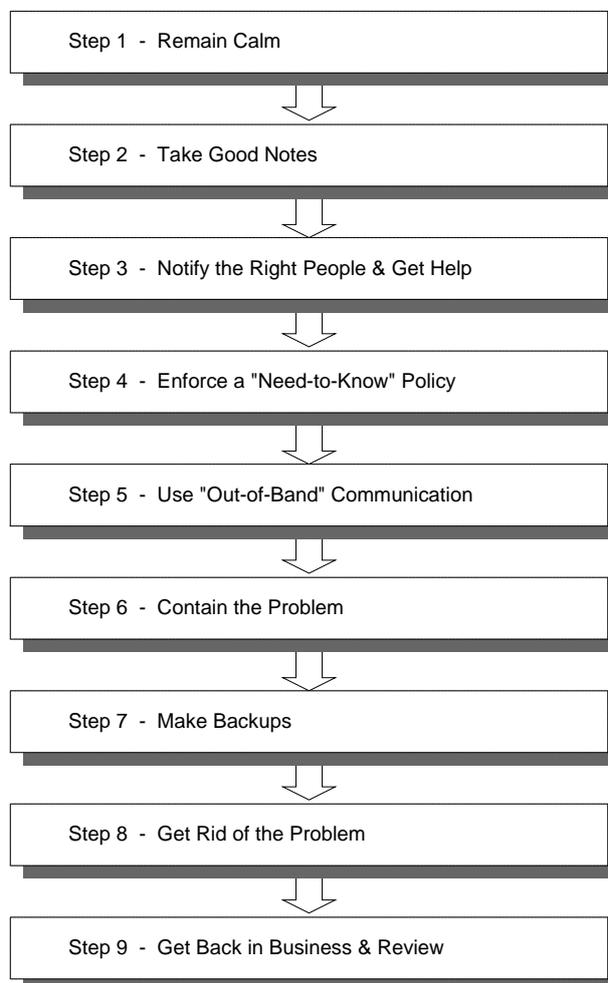
■   **Step 1   Remain Calm**

Since intruders have probably been in the compromised system for days or possibly even weeks, another few hours won't make any difference. You should remain calm, review and consider following the steps below.

■   **Step 2   Take Good Notes**

You should take organized and complete notes during the incident. The notes should record (i) dates and times when incident-related events were discovered or occurred, (ii) the information of systems, programs or networks that have been affected, and (iii) all conversations including the persons talked with, the dates and times and the contents such as instructions. These notes and observations are crucial to clear communication and event recall, and may serve as evidence if the case ends up in court!

■   **Step 3   Notify the Right People and Get Help**

It is important to immediately notify the **right people** and ask for help. You should inform people with a **"need-to-know"** basis about the incident. Providing incorrect information to the wrong people can have undesirable side effects. You should also consider seeking advice from external security experts, if necessary. In addition, you may assign a coworker to help coordinate the process and take notes.

■   **Step 4   Enforce a "Need-to-Know" Policy**

You should tell the details of the incident to the minimum number of people as far as possible. Computer security incidents can easily be mis-diagnosed early on. You should keep quiet and avoid speculation except when it is required to do. Furthermore, you should beware of suspicious requests for information. Incident specific information, such as account involved, programs or system names, are not to be provided to any callers claiming to be a security officer from another site.

■   **Step 5   Use "Out-of-Band" Communication**

You should avoid using the compromising system for incident handling discussions. You should contact through telephones and faxes instead. Since the intruders may possibly have full access to the compromised system and possibly other systems (e.g. e-mail system) at your site, they can read the mail messages and intercept the network traffic. If it absolutely needs to use a computer to communicate, consider using an isolated system with security measure, like a notebook computer with all incident handling mails encrypted.

■   **Step 6   Contain the Problem**

You should take the necessary steps to keep the problem from getting worse. Usually that means removing the compromised system from the network, though your school management may decide to keep the connections open in an effort to catch an intruder.

The following are some of the actions which may be required to be performed to contain the problem:

- If the source of the attacks can be identified, lock the suspicious persons and network connections out of the system

- Consider disconnecting the compromised system from the outside world (e.g. the Internet) and any remaining networks; especially isolating the affected system from sensitive data and mission-critical systems

- Consider disabling remote log-on services like "rlogin" or "telnet" sessions

- Consider disabling program remote execution services like "rexec"

- Consider killing all suspicious active processes

- Assure only authorized persons are granted with administrative privilege

■ **Step 7   Make Backups**

You should make backups of file system as well as system information. System state including network connections, temporary files and other volatile data sources (like data in RAM) should be dumped to files and then backed up with the file system. You should also make multiple full backups of files (if possible using at least two different methods) and the backups should be carefully labeled.

■ **Step 8   Get Rid of the Problem**

You should identify what went wrong. This is not an easy or quick task--it is required to determine which vulnerability had made the intruders to gain access. Some common security incidents are virus/worm infection and hacker/cracker intrusion.

The following are some of the actions which may be required to be performed to determine the problem:

- Scan the system with the most up-to-date anti-virus program

- Check the integrity of system binaries

- Check all audit trails, including system, application as well as security logs

After determining the cause of the incident and checking the most up-to-date and clean backups, you should reload the system from the most up-to-date clean backups to a safe and normal operation with minimal user impact.

Afterwards you should inoculate and improve the system's defenses by installing the appropriate software with the latest patches and disabling any unnecessary services. You should also delete the user accounts that are no longer required and consider requesting users to reset their password.

Moreover, you should monitor closely to determine whether the system can resume its tasks and any security holes exist.

Lastly, remember to preserve all evidence before eradicating the event, and perform a vulnerability analysis on the other systems in your systems and networks. Failure to eradicate the vulnerability network-wide will almost certainly lead to more break-ins.

- **Step 9   Get Back in Business and Review**

    After the incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up analysis should be performed. All involved parties should meet and discuss what were taken and learned.

    All existing procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the appropriate personnel. You should ensure all defined security controls and measures are properly implemented.

7.3   More Information

For more information about security audit and incident handling, see the following:

Document Name and Link	Source
■ **Security Incident Handling for Company** http://www.infosec.gov.hk/	HKSARG
■ **Site Security Handbook - Sep. 1997** (Request for Comments (RFCs) No. 2196) http://www.ietf.org/rfc/rfc2196.txt	The Internet Engineering Task Force (IETF)
■ **Incident Handling Procedures** (Template) http://www.sans.org/resources/policies/	System Administration, Networking, and Security (SANS) Institute

8 User Awareness and Education

There may be cases that schools concentrate on protecting their IT assets solely with proper hardware and software installation and configuration. On the other hand they may overlook the importance of well user operation and training.

We, however, would like to stress that education to users on security awareness would be more important than any security controls mentioned in previous chapters.

8.1 Education is the Most Important!

All precautions designed on hardware and software will be ineffective if they are not executed properly by their users.

Data security mentioned in earlier chapter does not only imply securing something in electronic form but also securing information to be viewable and accessible by authorized persons. You can make use a software utility to encrypt a data file and store the encrypted file on your server with proper access permission. However, you are also reminded not only protect your valuable information in electronic form, but also in printed format.

Therefore, in addition to the security measures for systems and networks that we mentioned in previous chapters, it is even more important to raise users' awareness and educate users about IT security.

8.2 Protection to Both Computers and Users

Security measures such as gate-door and alarm system of server room, property markings on hardware, log-on passwords, anti-virus software, Internet gateway, etc. are all intended for the protection of your school's IT assets like hardware, software, data and information.

You should, however, note that well planned user education on IT security does not only protect the IT assets but also the **users themselves**.

8.2.1 Example - Users' Safety on the Internet

Let us take the use of Internet as an example. Nowadays access to the Internet is getting simple and popular. Students and teachers can easily access the materials on the Internet at their home or in many public facilities like youth centers and libraries.

Anyone in the world, including students, teachers, you and us, can publish materials on the World Wide Web. However, no one can fully control what

content is available on WWW -- it is up to individuals to make sure that they behave in a way that is safe and appropriate.

The Internet world is made up of a wide array of people. Most are decent and respectful, but some may be rude, offensive, insulting, or even mean and exploitative. While your users can get a lot of benefits from being online, but they, particularly students, can also be targets of crime and exploitation.

8.2.2   Risks on the Internet

Several risks exist on the Internet. For example, your users may be exposed to inappropriate material that is sexual, hateful, or violent in nature. They may also be encouraged to participate in activities that are dangerous or illegal.

Students are particularly at risk because they are more likely to participate in online discussions (e.g. chat rooms, ICQ) regarding companionship. They might provide information or arrange an encounter that could risk their safety. For instance, misconduct persons might use e-mail, bulletin boards, or chat rooms to gain a young student's confidence and then arrange a face-to-face meeting.

8.2.3   Education and Guidance

You should educate your users on the use of the Internet as well as other systems. You should stay in touch with what they are doing so that their IT experiences in both "Cyberspace", their school or even their home are happy, healthy and productive.

8.3   Best Practices

When users are given a new system you should teach them the best practices on (i) how to use the system, and (ii) how to stay secure. Many security controls and measures we discussed in this document require user education and participation. Some examples are listed below:

- Access and storage media protection

- Password handling

- Virus protection

- Legal and authorized use of software and hardware

- Software change control

- Prevention from unknown file resources

- Code of behavior on computer use

- Code of ethics on Internet use

- Incident awareness and handling

You should note that the above are just some examples. Your school may have different or more topics on user education. Some useful and helpful guidelines are linked in the last section of this chapter for your further reference. These guidelines mainly provide advice on securing computers and keeping users safe on the Internet.

You are encouraged to read through these guidelines and determine which security measures are suitable and required at your school environment. Afterwards you should include them in your user education plan and regard the processes below when conducting user education.

8.3.1 Ways for Education

There are several ways to educate users and raise their awareness about IT security. For example, in the beginning of a school year teachers can educate their students during computer studies lessons.

Teachers and school staff can acquire IT security knowledge by attending IT training programs and/or learn it bit-by-bit from day-to-day tasks. They are also encouraged to share their experiences in their staff meeting.

In addition, you can also remind users about IT security during some school events like morning assembly.

8.3.2 Obligation and Responsibility

You should stress the importance of IT security, state out all related rules and code of ethics, and educate your users to properly and responsibly use the systems and networks at your school. In addition, you should also consider having an acceptable user policy (AUP) for your users.

A school AUP is a document specifying what a user can and cannot do while using the school's IT facilities. Some schools may choose to contain things like liability disclaimers, lists of actions or behavior that will result in security violation, etc.

You may refer to the samples below to formulate an AUP of your school. You may also consider having all your users read and signed on it before they use the IT facilities at your school.

Document Name and Link	Source
■ 資訊科技用戶守則 **Information Technology Acceptable User Policy** http://www.hkcampus.net/ser_zone/info/rule.html	Hong Kong Cyber Campus

■ **Acceptable Use Statement** (Template) http://www.sans.org/resources/policies/	SANS Institute

8.3.3   Promotion and Supervision

It is required to promote and remind users about the importance of IT security in your school.

For ease of information access you may consider AUP as public data and publicize them in public zones, such as display the AUP on notice boards of corridors, library and computer laboratories, and/or paste it on your school's Web page, if any.

And you should remember that regardless of the education of IT security and the promise of good behavior, supervision is equally important. Teachers' supervision and guidance of computer use in library and computer laboratories are always required and essential.

8.4   More Information

The following links provide you more information on user education in IT security. Some of them can be used as reference materials for basic user training.

Document Name and Link	Source
■ 青少年資訊保安認知簡介 **Web-based Training on Information Security** http://www.info.gov.hk/digital21/chi/ecommerce/pki/wbt/flash/ITSecuWBT.html	HKSARG - Digital 21
■ **How to Keep your Child Safe on the Internet** http://www.info.gov.hk/police/	HKSARG - Hong Kong Police (Crime Prevention Bureau)
■ **Users of Small Computer Systems** http://www.info.gov.hk/police/	HKSARG - Hong Kong Police (Crime Prevention Bureau)
■ **Using the Internet and Technology in the Classroom** http://www.ehhs.cmich.edu/~tvantine/edint.html	Teacher's Tips

Furthermore, some organizations as well as government bureaux and departments from time to time would organize IT security seminars or training programs for students and teachers. You are encouraged to visit their Web sites and search for information or application of such events.

Home Page

- **Education Bureau - IT in Education (ITEd)**

  http://www.edb.gov.hk/ited

- **HkeducationCITY.net**

  http://www.hkedcity.net/

- **Office of the Privacy Commissioner for Personal Data (PCO)**

  http://www.pco.org.hk/

- **Digital 21 - Information Security Awareness Seminars for Secondary School Students**

  http://www.info.gov.hk/digital21/chi/pastevents/isas_sss.html

9   IT Security Policy

After reading previous chapters you should perceive fundamental knowledge on IT security. In order to let all your systems, networks, users and management comply with the planned/adopted security measures, you should consider establishing an **IT security policy**.

9.1   What is an IT Security Policy?

An IT security policy is a set of written policies and procedures for the documentation of security measures adopted in each security control.

For example, under physical security, you may write down the security zones of your school as well as the guidelines on mobile devices, access and storage media protection.

Besides, you may also record down the guidelines for password handling, virus protection, appropriate use and safeguards of Internet access, the contact information for incidents, as well as code of practice in the use of systems and networks in other security controls.

9.1.1   Formulation

No single IT security policy is applicable to all schools. You should read through the information provided in this document, determine the security requirements with respect to your school's unique environment, and then decide and write down appropriate levels of security measures in each security control.

You may refer to the documents linked in last section of this chapter and formulate the IT security policy for your school.

9.1.2   Systems Matching

Your school systems and networks should be configured to reflect the policies you established.

If a policy states that user passwords must be changed every 60 days, then your system administrator(s) should configure your school systems to match. Users should then follow this policy, and any exceptions should be identified.

As mentioned before, you can make use of some built-in administrative tools (e.g. mandatory roaming profiles, "User Manager for Domains", "System Policy Editor", Group Policy, etc. for Microsoft Windows NT 4.0 and/or Windows 2000 systems) as well as add-on utilities (e.g. Internet Explorer Administrator's Kit, security advisor/checker) to ease the security settings.

In some cases you may find that setting security policies to match the objectives of your school systems is difficult. To make the policies effective you should strike a balance between being overly cautious on the one hand and lax on the other.

9.1.3   Education and Promotion

All your users, including students, teachers, school staff, system administrators and management, should be educated to comply with school's policies and procedures.

In addition, the policy document should be easily accessible. You should consider posting the printed document on notice boards of corridors, computer laboratories and classrooms with IT facilities, and storing the soft-copy in public area of your school Web site and/or file servers.

Although generally you may find that security procedures will reduce the flexibility of user operations and increase the management work, it is crucial to have a school IT security policy in place.

9.1.4   Audit and Review

Auditing of compliance of IT security policy must be performed periodically. Moreover, you should review the policies and procedures periodically to tally with changes in school's requirements, as well as adapt to changes in environment and technology.

9.2   More Information

More information about IT security policy can be found in the following documents. You may refer to these documents and make use the relevant parts to formulate an IT Security Policy of your school.

Document Name and Link	Source
■ **Standards and Guidelines for Strategic Systems**	Murdoch University (Australia)
■ **Standards and Guidelines for Desktop Computers**	
■ **A Short Primer for Developing Security Policies** http://www.sans.org/resources/policies/Policy_Primer.pdf	SANS

10   Conclusion

IT security is important to your school. As the use of IT in schools is getting extensive and complicated, in order to secure the IT facilities at your school, you and your users should bear the **three security objectives** in mind when planning, designing, deploying and using the school systems and networks.

In addition, there are **six common security controls** in school environment. You have to adopt appropriate levels of security measures in these controls and address any other security concerns in your unique circumstances.

Moreover, IT security concerns technical, operational and management issues. Making it part of your school culture is crucial. You should consider establishing an **IT security policy** to document the measures adopted in each security control and let all users comply with the policies.

Managing IT Security

in Schools

Quality Education Division
Education and Manpower Bureau
The Government of the HKSAR

www.emb.gov.hk/ited/

Nov 2005

For enquiry on this document, please direct to the Information Technology in Education Section, Education and Manpower Bureau at (852) 3123 8228 or write to the Principal Inspector, Information Technology in Education Section, Quality Education Division, Shop 28-37, UG/F, Phase I, Waterside Plaza, 38 Wing Shun St., Tsuen Wan, N.T.

The full text of this publication is available at the Information Technology in Education website at http://www.emb.gov.hk/ited/

Introduction

Today, Information Technology (IT) has been widely used in schools in learning and teaching as well as administrative activities. However, the extensive use of IT has brought and increased the risk of accidental or deliberate actions that cause damage to schools.

The hardware and software components in schools, which represent considerable monetary and time investment, should be protected. Besides, various kinds of data in the computer systems, which may have taken a lot of time and effort to produce, should also be protected. Schools should pay special attention on IT security in order to protect such valuable assets in schools.

Why do schools need IT security program?

A security program helps an organization to manage the risks to their business. Many schools nowadays have communication pathways that extend beyond the physical boundaries of the school premises. It used for schools to have physical security measures in place to protect the school premises. The same principle should be used to justify the implementation of a school IT security program in today's environment. Many schools or organizations will implement an IT security program only following an actual loss or incident. However, the costs associated with the incidents sometimes may extend beyond the monetary loss.

Schools become Hacking Centre

According to the information provided by the Internet Services Providers (ISPs), hacking activities had been detected in the web sites of 3Com Corporation, NASA Ames Research Center and Rope Internet Services in the summer of 2002, which were found to be initiated from some servers in schools of Hong Kong. The schools concerned did not notice the hacking activities in their servers until they were told by their Internet Service Providers.

Here are some possible consequences, which may be derived from the absence of IT security program in schools:

- Loss of data privacy (e.g. leakage of personal information or sensitive data)

- Operation disruption (e.g. teaching and learning activities can be disrupted when the computer network is down)

- Loss of assets (e.g. lost of school/personal data, hardware or software items/licenses)

- Legal problem (e.g. the hacked school servers might be used by the hacker as a tool of committing computer crime)

- Damage of school's Reputation/Image (e.g. the school web site may be defaced by hackers)

Basic IT Security Concepts

IT security aims to protect schools from threats. In general, IT security comprises three basic concepts: **Confidentiality, Integrity** and **Availability.**

Confidentiality	**:**	To protect data/information privacy. To prevent unauthorized disclosure.
Integrity	**:**	To safeguard the accuracy and reliability of data and system. To prevent unauthorized modification.
Availability	**:**	To maintain reliability and timely access of system/service to users. To prevent disruption of system/service.

All the objectives of IT security should be built around these concepts. It is important to note that implementing IT security is not just a technical issue but a management issue as well. Support from the school management is crucial to its success.

Concerns for IT Security

For implementing IT security in schools, the management may need to consider the following:

Management Support

IT Security program should be initiated and supported by the management. Without management direction and support, the coverage of the IT security program would be limited and ineffective.

Public Services to be offered

Nowadays, schools are using the Internet to enhance communication with the public. However, schools should note that the more public services (e.g. web site, FTP sites, e-mail and remote access) offered, the more security measures should be set up along side the services. Without revisiting the IT security measures, adding more public services will make the school more vulnerable. Schools should be careful in implementing public IT services with potential security risks in mind.

IT Security Requirements

Computer networks connected to the Internet will always be exposed to a certain degree of risk. The function of IT security is to minimize that risk. However, security requirements vary according to a collection of technical and usage factors and ultimately it should be the school's management decision. ***Risk analysis*** may be helpful in understanding one's security requirements. In general, schools have more IT services and equipment would have more security requirements. However, schools should be aware that there should be an appropriate balance between freedom of access to increase/enhance school's activity and the security to prevent

loss of data and resources. Schools may refer to the Appendix of this document for better understanding on the technical aspects of their IT environment.

IT Security Policy

IT security policy is a documented list of management instructions that describe in detail the proper use and management of computing resources with the objective to protect these resources. To have a school-based "IT Security Policy" is just the first step in implementing meaningful IT security in schools. An appropriate dissemination process must be in place so that all IT users, including staff and students, are well aware of the policy and should take ownership to follow the Rules/Guidelines to ensure the Confidentiality, Integrity, and Availability of computer assets. In addition, the effective IT security policy are constantly re-evaluated and measured against in order to gauge their success.

IT Security Roles Assignment

As mentioned earlier, security program should start with the school management. In setting up IT security policy, implementing security program, and reviewing IT security policy, it is important to have the support from the management to overcome the possible obstacles and difficulties, such as user complaint, privacy infringement, and resource allocation.

The School IT team should be responsible for managing and implementing the school IT security policy. Management roles and implementation roles should be defined as one of the terms of reference of the School IT Team.

The management roles include the responsibilities for the formulation and maintenance of the IT security policy.

The implementation roles include the implementation of the IT security policy and ensure that all units/departments within school are in line with the school security strategy and each individual has the responsibility for implementing a school wide program in their specified areas.

School IT Team

In general, school IT team is composed of three to seven members, including:

Chairman: the school head or a senior teacher.

IT Teacher: the IT coordinator, computer subject panel head, computer/IT teacher or a teacher with good IT knowledge.

Team members: teachers from different panels.

Schools are suggested to form a taskforce under the School IT Team to look after the IT security matters in schools. Members of the taskforce should include senior management as well as the technical support personnel.

Risks Analysis

Before drafting the IT security policy, a thorough risk analysis should be conducted for identifying security requirements.   Here are the steps for risk analysis:

1.   Identify Assets to be protected

The assets could be data, systems, hardware, software or even the image of schools. In short, everything that is essential for school operation or related to data privacy must be protected.   As the importance of different assets may vary in different schools, assets identification is school specific.

2.   Identify Threats and Vulnerabilities

Vulnerability is the weakness in the school's IT environment.   It may be caused by problems in software/hardware or faulty procedure/management.   Examples of vulnerabilities are software bugs, unmanaged services, or weak password management.   Vulnerability should be identified in risk analysis.

Threat is the potential danger to the IT assets.   After asset identification, the threats to these assets have to be discovered.   Threats will jeopardize the Confidentiality, Integrity, and Availability of the identified assets.   Examples of common threats are:

Environment: Fire, flooding, power failure, extreme temperature.

Deliberate: Hacking (hackers, insiders), virus, theft, use pirated software

Accidental: Human errors, communication link errors

Schools may prioritize the threats and identify which threats are critical or tolerable in schools.

3.   Assess Risks

Risk is the probability that a threat will exploit a vulnerability resulting in loss to the schools.   For instance, if there were high burglary rate in the district where school is located, the risk of theft of computer equipment would be rated higher.   Risk is also highly related to the vulnerabilities in schools.   For example, if the door of the school server room was not locked when nobody was there, such vulnerability would easily lead to a burglary.   The following table of asset, threat and vulnerability may help in assessing risks:

Asset	Threat	Vulnerability
Data	Unauthorized Dial-in Access	Unrestricted use of modem
All facilities	Fire	Lack of fire detection device
Server	Power Failure	No Uninterruptible Power Supply (UPS) is used

After schools have recognized the risks that they are facing, they may proceed to draft the IT security policy.

Security Roles Assignment   ⟹   Risk Analysis   ⟹   Security Policy Drafting

Steps in formulating IT Security Policy

Since IT security policy will affect all users in schools, it is generally better for schools to consult different groups, such as the school management, teachers, administrative staff, or even students during the formulation of the IT security policy.

In general, the following are the steps for formulating IT security policy:

(1)   Develop the IT Security Policy

(2)   Promote the policy

(3)   Implement the policy operation

(4)   Evaluate and review

Develop the IT Security Policy

After risk analysis, school can start drafting the school IT security policy.   Security requirements have to be determined which may vary from school to school.   Members of the School IT Team should work in collaboration with the users to collect their views in drafting the policy.   It is recommended that the policy has to be:

■   *Implementable and enforceable*: it should be realistic to be carried out

■   *Concise and easy to understand*: users should be able to understand

■   *Balance protection with productivity*: too strict security measures may hinder the productivity of users

For the content of the IT security policy, the following can be included:

■   Reasons of the policy

■   Policies, rules, guidelines and procedures in different areas

■   Incident handling procedures and responsible person/party

■   Usage and responsibility definition for different users groups (e.g. students, teachers, supporting staff and management)

■   Violations handling and enforcement

<div style="border: 2px solid; padding: 20px; background-color: #e0e0e0;">

Policies, Rules/Guidelines and Procedures

IT security policy provides the vision for IT security. To realize the vision, lower level rules, guidelines and procedures are needed for execution.

Policies: Broad and high level terms to cover many subjects in a general fashion

Rules: Compulsory statements to provide standard procedures to be carried out across the schools

Guidelines: Recommended actions to deal with the gray areas where rules do not apply

Procedures: Low level and detailed step-by-step actions. Procedures provide steps for implementing the statements in the policies, rules and guidelines.

</div>

Promote the Policy

The success of implementing school IT security policy depends on and is assured by the user's awareness and their willingness to comply. In addition to the introduction of the IT security policy, awareness training is also important. Training could be provided to different kinds of users such as students, teachers, administrative staff and technical staff. The rules, guidelines and procedures should be published and delivered to the appropriate user groups. Users should understand their IT security responsibilities. A culture of security awareness must be built into any deployment plan and a persistent maintenance program put into place to ensure continual awareness.

Implement the Policy

This would be the longest stage in the life cycle of an IT security program. School IT security policy will only be effective when all the users know their IT security responsibilities, and the policies/rules/guidelines have to be executed. Ongoing management and monitoring of the security controls implemented must be accounted and budgeted for. The day-to-day configuration and maintenance of the security controls and the IT facilities have to be monitored by responsible groups for the compliance with the IT security policy. Violation of the policy should be reported and handled.
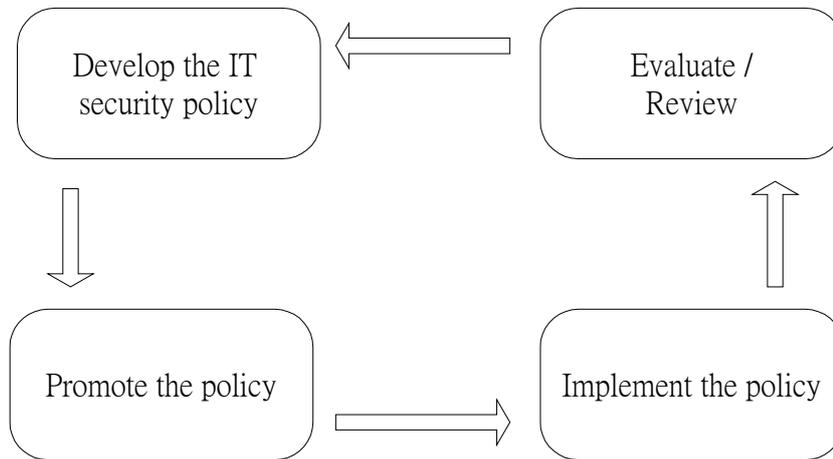
Evaluate and Review

Schools should periodically monitor the conformance of the defined IT security policy. Such audit activities are intended to ensure that the IT security policy and all the associated measures are properly implemented.

However, security threats are continually evolving. Security Audit may eventually result in a review exercise so that some improper or inefficient policies may require

enhancement or updating. The results of audit should be documented and reviewed by the School IT Team.

Drafting and implementing the IT security policy is just only part of an IT security program. An effective IT security program itself is not event driven; it should be treated with a life cycle approach. IT Security policy will only be effective if continuous risk reviews start the life cycle over again with management support.

```
┌─────────────────┐        ┌─────────────────┐
│  Develop the IT │  ⟸     │   Evaluate /    │
│ security policy │        │     Review      │
└─────────────────┘        └─────────────────┘
         ⇓                          ⇑
┌─────────────────┐        ┌─────────────────┐
│ Promote the     │   ⟹    │ Implement the   │
│ policy          │        │ policy          │
└─────────────────┘        └─────────────────┘
```

Life Cycle IT Security Program

Areas in IT Security Policy

The IT security policy could be one document; or it could be comprised of several specific policy documents. Though there is no one single standard way in drafting the school IT security policy, schools may consider including the following five areas in its own IT security policy:

- ■ Physical Security;

- ■ Access Control;

- ■ Data Security;

- ■ Network and Communication Security; and

- ■ Security Audit and Incident Handling.

> For more information about the above areas, please refer to the paper "*IT Security in Schools*" in the ITED web site:
>
> Examples of IT security policy can be referred from those of Murdoch University (key in 'security policy' in keyword search of the site): *http://www.murdoch.edu.au*

Physical Security

Physical security refers to the protection of IT equipment and assets in the school. The formulated IT security policy should exhibit detailed measures to protect the above against disasters and theft. Physical access control can work as the first line defense to prevent unauthorized person to access the network directly. Also, asset management is one of the main concerns in physical security. When developing the physical security policy, schools may consider the following areas:

Areas	Sample Policies
Physical Access Control	● All computer equipment should be kept in a secure place with good physical security
Site Environment	● The computer equipment should be kept in a place with good environmental condition.
Asset Management	● The inventory record on hardware, software and license should be well documented and kept in secure area. ● The inventory record should be audited periodically.
Equipment protection	● All IT equipment such as Server, Workstation, Network Equipment and Mobile Device should be well protected from different form of threats.

Server Backup Media Protection	● Server backup media should be stored remote from the server system and be protected.

Suggested Rules/Guidelines for Physical Security

● Only authorized persons should be allowed to enter the Server room.

● The air conditioner(s) of the server room(s) should always be turned on to keep the temperature and humidity in optimal condition for the equipment.

● Network equipment (e.g. switches and routers) should always be locked in the Floor Level Equipment Cabinet (FLEC) to prevent theft or vandalism.

● Mobile equipment such as Notebook or Handheld computers should be under lock and key when the equipment is left unattended.

● Backup storage media (e.g. tape or CD) for server should be under lock and key in room xxx (a designated room in the school premises) and be accessed by authorized person(s) only.

● All computer equipment should have property marking with school and/or former ED/EMB logo and wordings.

Access Control

Users have different privileges to access the resources in a network. Hence, user log-in control and assignment of user network rights are major areas of access control. In developing the access control policy, schools may need to consider the following areas:

Areas	Sample Policies
Network Access Control	● The use of privileged accounts should be restricted and controlled. ● Users are responsible for all activities performed using their accounts.
Equipment Access Control	● All computer equipment, such as servers, workstations and routers, should be password protected.
Password Management	● All passwords should NOT be shared amongst users. ● All passwords should be changed periodically.

> **Suggested Rules/Guidelines for Access Control**
>
> - In accessing the network resources, each user should have his/her own network account with password for identification.
>
> - The use of administrator account should be restricted only to the following designated persons: Mr. XX, Ms. XXX and Mr. XXXXX *(N.B: normally the they are ITC, TSS in the school)*
>
> - The user access right should be assigned on a Need-to-Know basis. No extra right should be assigned beyond the normal operation of the specific users.
>
> - BIOS passwords in all computer machines should be set to prevent disruption of the BIOS configuration.
>
> - The user passwords must be changed once every 3 months.

Data Security

Data in the school systems and networks are valuable asset.   Special attention should be given in protecting the data. It would be a good practice to classify data into different security levels which would have different handling procedures.   School could define data security policy into the following areas:

Areas	Sample Policies
Data Classification	- All data should be classified according to the sensitivity of the data. - Different classes of data should be handled with different procedures.
Data Backup and Recovery	- Data backup should be carried out regularly. - Backup and Recovery procedures should be well documented, tested and properly implemented.
System Failure Protection	All systems in school should have a recovery plan to prevent data loss.
Software Security Update	The software should be updated with security patches regularly, if applicable.
Virus Prevention	All systems in schools should be installed with anti-virus software.

Suggested Rules/Guidelines for Data Security

- Only data which is classified as public can be accessed and disposed without special procedures.

- All data in server(s) should be backed up daily.

- Uninterruptible Power Supply (UPS) system should be used in servers to protect data loss from power surge or failure.

- Security patches and updates for operating systems and Internet browsers should be checked and applied weekly/biweekly.

- All servers and workstations should be installed with anti-virus software.

- The virus signature of the anti-virus software should be updated weekly.

Network and Communication Security

Within the school premises, the computer network system may itself contain several different sub-networks, such as Multimedia Learning Centre (MMLC) network, SAMS network, and Learning & Teaching network. These sub-networks may have different security levels. (Details of the school network segments and the security characteristics are depicted in Appendix.) When these sub-networks are connected, security measures should be taken to deal with the differences in security level amongst these sub-networks. These measures should be included in the school IT security policy.

Apart from the communication within the school network, school networks that are connected to the Internet posted extra vulnerabilities and risks. While it is convenient and conductive to student-teacher communication, students and/or teachers may need to remote access the school network after school hours. Such remote access to the school network imposes one of the greatest risks to schools. Hence, schools are advised to consider the following related issues.

Areas	Sample Policies
Internal Network Boundary Management	• Sub-networks with different security levels should never be connected without control. • Rules should be defined for the traffic between different sub-networks.
Remote Access Management	• The use of remote access should be restricted, unless there is a genuine need. • Security measures should be taken to prevent unauthorized remote access to the system and the data.

Internet Security	• All traffic in and out the Internet should go through the Internet gateway. • The e-mail security should be scrutinized to prevent virus and different forms of hacking.

Suggested Rules/Guidelines for Network and Communication Security

- All workstations in Learning & Teaching network should be barred from direct access to data and system in the SAMS network.

- All dial-out and dial-in activities should be audited and controlled.

- Remote access to school network should only be available to authorized users.

- All files downloaded from the Internet should be scanned with anti-virus software.

Internet Security

School network usually connects with the Internet. Students and teachers may access the Internet for information retrieval, communication or even web publishing. To enforce school IT security, it is necessary to develop Internet security policy. Here are some areas which should be considered for Internet security:

◆   E-Mail Security

◆   Uploading/Downloading Security

◆   Internet Gateway Policy

◆   Acceptable Use Policy*

Internet gateway should be deployed at the connection to the Internet. It is a must for schools to offer public services on the Internet (e.g. school web page, webmail). Security policy for the Internet gateway should specify:

1. Types of traffic which are accepted and denied

2. Filtering measures, e.g. protocols filtering, web services filtering and web contents filtering,

3. Logging and monitoring mechanism

Apart from setting rules and procedures, *user education* is the most important. Training/Awareness on the Internet safety to students can protect their personal safety and prevent them from committing computer crime. For example, students should not release their personal information to strangers on the Internet.

"How to keep you child safe on the Internet"

http://www.info.gov.hk/police/

* Acceptable Use Policy for Internet

In some foreign countries, schools may request the parents to sign an **Acceptable Use Policy** (AUP) for their children to use Internet in school. The policy mainly deals with issues related to the following:

- Inappropriate materials/language

- Privacy

- Intellectual property violations

- Forgery

- Hacking activities

Schools may consider taking AUP as a reference for controlling the use of Internet. However, schools should understand more on AUP before limiting users to access the Internet or establishing policy to minimize the risk of controversy and litigation. An example of acceptable user policy can be referred from:

http://www.hkcampus.net/ser_zone/info/rule.html

Security Audit and Incident Handling

Security Audit

As mentioned earlier, school IT security program should take a life cycle approach. Schools should develop audit policy to ensure that the defined IT security policy is followed by the School IT Team as well as school users. As mentioned, result from the security audit is also a means that lead to a review and/or enhancement of the school IT policy.

Incident Handling

Security incidents are inevitable. Schools have to cater for the occurrence of security incidents with appropriate handling procedures. Remedial steps have to be taken to respond to or recover from the security incident.

Some of the common security incidents which may occur in the school environment are:

- Virus infection (e.g. email attachment infection)

- User management (e.g. staff leaving/joining the school)

- Damage / loss of assets (e.g. theft or lost of hardware)

- Misuse of systems and networks (e.g. wrong server configuration)

- Network intrusion (e.g. hacking from hackers or insiders)

Different incidents would require different handling procedures. Schools are suggested to define incident handling procedures for at least each of the above mentioned security incidents. Schools should assure that every user should know what to do and whom to report to when they spot or suspect a security incident. The handling procedures should be covered in the IT security policy. In general, it may include the following steps:

- Identification   (Find out the problem)

- Containment   (Limit the extent of the problem)

- Escalation   (Report to the right person if necessary)

- Eradication   (Get rid of the problem)

- Recovery   (Recover to normal operation)

- Record Keeping   (Log the problem)

- Incident Follow-Up   (To improve the performance in similar situations)

For detail examples of incident handling, please refer to the paper "*IT security for Schools*" in ITED web site:

Areas	Sample Policies
Security Audit	• All systems should be audited and the report should be complied periodically. • The use of audit program and the result of auditing should be classified, restricted and controlled.
Incident Handling	• All incident handling mechanisms and procedures should be defined and delivered to administrator(s) and users. • All administrator(s) and users should be well versed with the appropriate incident handling procedures and follow them accordingly.

■ **Suggested Rules/Guidelines for Security Audit and Incident Handling**

• The event logging function in server operating system should be enabled. Events about account, logon and system should be logged.

• Logging function in the Internet gateway should be enabled. Information such as IP address, ports and service requested should be logged.

• The system event logs and supporting information should be retained for the proof and tracing of security incidents.

Summary of IT security policy in schools

Below is the abstract of the major areas of concern that have been mentioned. **Schools should note that the summary is NEVER a complete checklist.** Different schools would have different security requirements, resources available and campus environment. Security policies in one school may be a reference and be not applicable to another schools. For example, some schools do not have separate server rooms; the servers are placed in the staff room. Hence, the suggested rules about server room security may not be appropriate for them. Besides, some schools do not have expert IT human resources, hence the configuration and maintenance of a firewall may impose extra burden to their workload. Teachers can have a glimpse of these areas when preparing the IT security policy.

Areas	Abstract
Physical Security	❑ Secured areas in schools should be locked with limited access. ❑ Physical access rights should be assigned to particular persons for secured areas (e.g. Server room). ❑ Network equipment (e.g. switches and routers) should be locked for protection. ❑ Mobile equipment (e.g. Notebook/Handheld computers) should never be left unattended. The mobile equipment should be locked after use. ❑ Backup storage media should be kept in secured areas, which can be accessed by authorized persons only. ❑ Property marking should be printed on all computer equipment. ❑ The climate of server room should be kept in optimal condition for the equipment.
Access Control	❑ All users should be assigned with network accounts and passwords to access the network. ❑ Network administrator account should be restricted only to designated persons. ❑ User access rights on network should be assigned on a Need-to-Know basis. ❑ BIOS passwords in all computer machines should be set and known by authorized persons. ❑ All user passwords must be changed regularly.

Data Security	❑ Data should be classified with (e.g. public, private confidential) for different handling and disposal procedures.
	❑ Server(s) should be backed up regularly.
	❑ Server(s) should be connected to Uninterruptible Power Supply (UPS).
	❑ Security patches and updates for operating systems and Internet browsers should be checked and applied weekly/biweekly.
	❑ Anti-virus software should be installed in all servers and workstations.
	❑ The virus signature of the anti-virus software should be updated regularly.
Network and Communication Security	❑ All workstations in Learning & Teaching network should be barred from direct access to data and system in the SAMS network.
	❑ All dial-out and dial-in activities should be audited and controlled.
	❑ Use of remote access to school network should be made available to authorized users only.
	❑ All files downloaded from the Internet should be scanned with anti-virus software.
	❑ Internet gateway should be used to control the incoming and outgoing network traffic with the Internet.
	❑ For schools who are hosting their public services (e.g. web sites) on the Internet, extra security setting should be adopted in the Internet gateway setup (e.g. DMZ)
Security Audit and Incident Handling	❑ The event logging function in server operating system should be enabled. Events about account, logon and system should be logged.
	❑ Logging function in the Internet gateway should be enabled. Information such as IP address, ports and service requested should be logged.
	❑ The system event logs and supporting information should be retained for the proof and tracing of security incidents.

Schools should strike the balance for the IT services offered, resources available, security requirements and user satisfaction. It is very important that in preparing the IT security policy, schools would understand more on the risks and their specific IT security requirements and reach the balance. For instance, if schools do not have the

expertise and resources for firewall acquisition and maintenance, hosting their web sites to the Internet services providers would be a more cost effective way, while at the same time giving up the flexibility of web site maintenance.

Schools have their specific IT security requirements. The requirements have to be spelled out and defined by schools themselves. Schools are reminded that IT security policy should always be tallied with the IT security requirements.

Final Remark

There are many areas to be catered for in managing IT security in schools. Without IT security policies, appropriate implementation and reviewing procedures, the IT environment of school could easily get into trouble resulting in loss of computer asset or out of service. Schools are advised to immediately start formulating, making reference to the areas suggested in this paper as a start, their own School IT Security Policy.

For example, a school may begin by performing an **assessment** of its current IT environment and referencing its documentation, rules and regulations. For areas that the school has already catered for, e.g. TSS routine support task schedule, it should perform the necessary evaluation, enhancement and refinement; and then adapt them into the School IT Security Policy. The school could then proceed to include the details of the remaining areas in the School IT Security Policy.

Based on School IT Security Policy, the school should evaluate aspect(s) that require improvements. It may prioritize these aspects and prepare a **schedule** for actions to be taken for improvements. After such planning activities, the school can **implement** the planned actions according to the schedule.

Lastly, developing and maintaining the School IT Security Policy is a continuous process. Continuous assessment, periodic and routine **evaluation** of the School IT Security Policy is necessary to ensure that the policy is feasible, practical, and enforceable, and at the same time can protect the school network, both internally and externally.

Reference material on Internet

InfoSec web site, *(Information Security web site by HKSAR)*	http://www.infosec.gov.hk
Internet Security Handbook, *2nd ED, HK University of Science and Technology:*	http://www.hkcert.org/
Computer Security for users of Small Computer Systems:	http://www.info.gov.hk/police/

Appendix - Overview of a typical School Network

A typical school network is composed of sub-networks each with their own security requirements. This part aims at providing an overview of these sub-networks and their related security considerations.

I) Overview of the Network Segments

A typical computer network in a school is shown in Diagram 1.

Diagram 1 - Overview of a Typical Network in a School
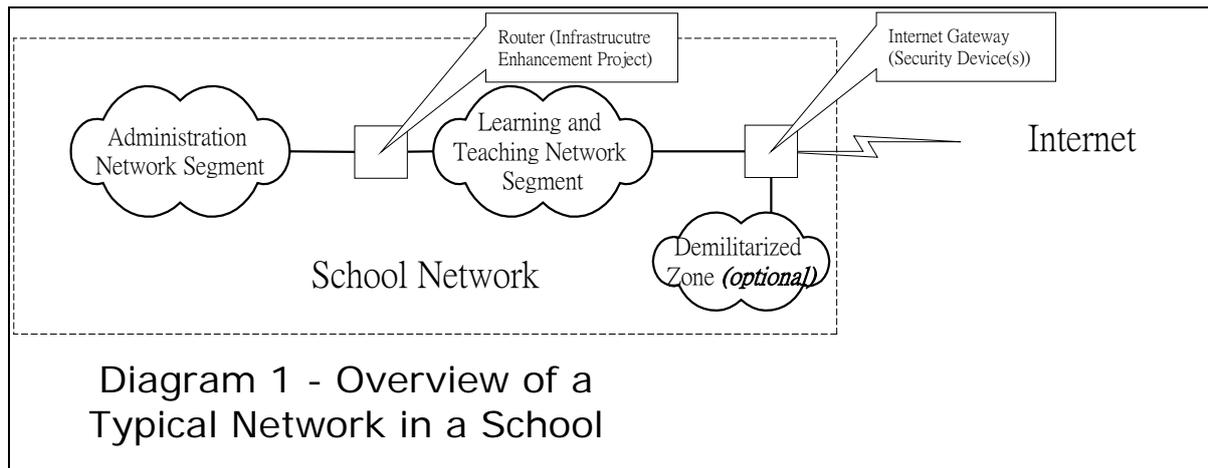
It comprises three major sub-networks:

Administration Network Segment	This sub-network **(Admin Network)** contains <u>SENSITIVE</u> information such as student examination marks and personal data, etc. Information of the SAMS system and other administration information of the school are stored in this sub-network.
Learning and Teaching Network Segment;	This sub-network **(L&T Network)** comprises learning & teaching materials such as lecture notes and presentation files, assignments and other content which are specifically for a school's own use. Such material is typically <u>NOT SENSITIVE</u>.
Demilitarized Zone **(*optional*)**	This sub-network **(DMZ)** comprises information and IT equipment for <u>public access</u>. Information typically found in this segment includes school web pages and files for download through the Internet. This network segment is <u>optional</u>. If a school does NOT have facilities for public access then it is NOT necessary for school to setup a DMZ. On the other hand, a school <u>MUST</u> setup its own Demilitarized Zone if it needs to host information/data in its public accessible equipment.

The major sub-networks are inter-connected at two connection points with the whole school network being connected to the Internet.

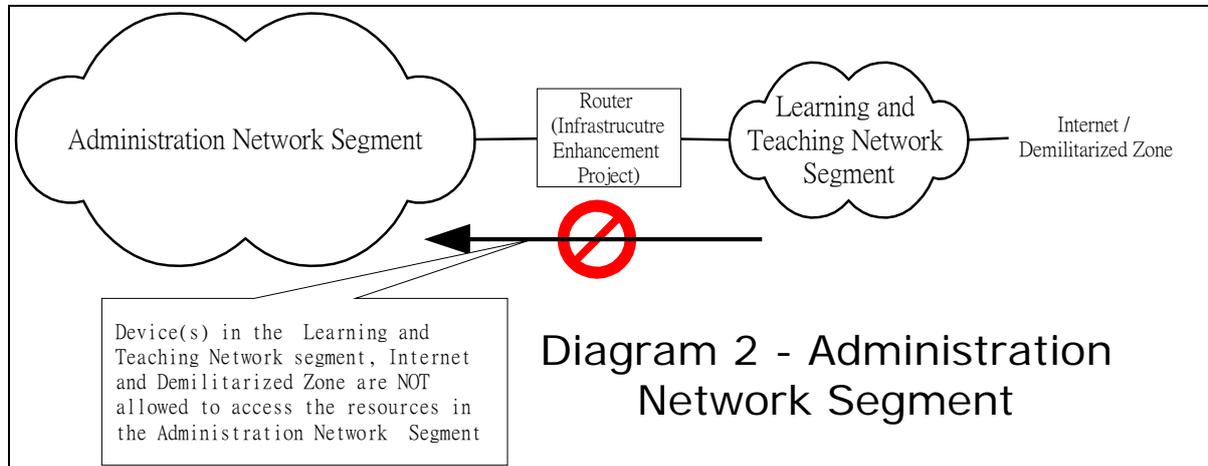| Router (Infrastructure Enhancement Project)	The **Admin Network** and **L&T Network** are inter-connected via a <u>SINGLE CONNECTION</u> by a **router** provided by the Infrastructure Enhancement Project **(IEP)** (see diagram 1)
Internet Gateway (Security Devices)	The **L&T Network** and **DMZ** are inter-connected at the Internet Gateway which is connected to the Internet. Typically, a school should have a <u>SINGLE</u> connection to the Internet, usually through the broadband service. Schools should note that all its equipment especially the security devices at the Internet Gateway, routers and servers in the Demilitarized Zone have to be properly configured and maintained in order to satisfy its IT security requirements. For example, routine check on the firewall logs should be performed by Technical Support Service (TSS) colleague once every week. If necessary, firewall rule sets would be tuned accordingly. For more information about the Internet Gateway, please refer to "*Understanding Internet Gateway*" in ITED web site:

To ease security management tasks, other connections to external networks are normally prohibited unless the school has special requirements and proper security measures have been in-place (the security measures should align with the School IT Security Policy). For example, using Virtual Private Network (VPN) connections to support student and/or teachers remote access.

However, the number of such connections must be kept at the minimum and they must be well managed and monitored. Otherwise these connections may become "backdoors" for malicious access to the school network.

II) Security Characteristics of the Sub-Networks

The following sections briefly describe the security characteristics of the three major sub-networks in a typical school.

a) Administration Network
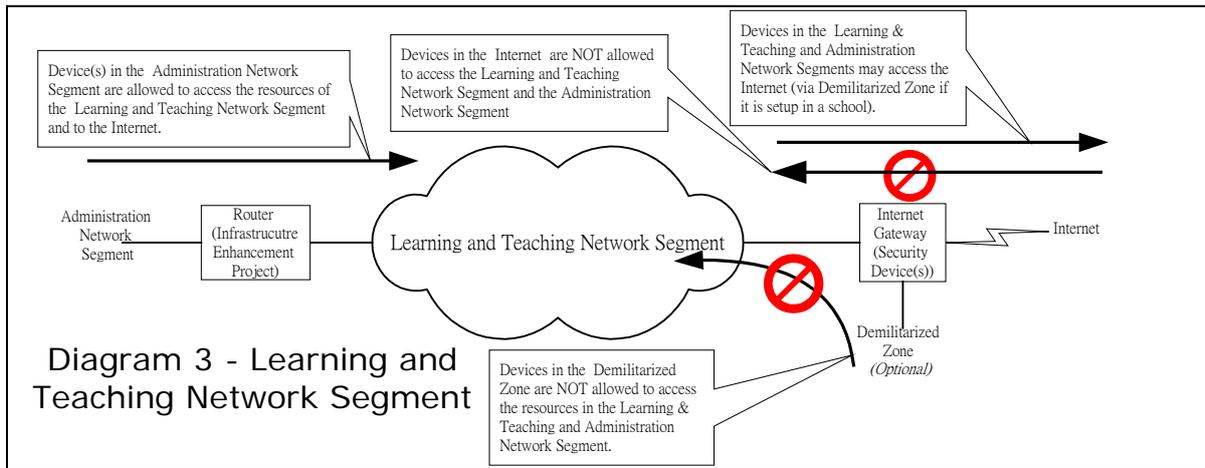

Diagram 2 - Administration Network Segment

Access to the sub-network	As this sub-network has a relatively higher security requirement, ONLY devices in the Admin sub-network itself are allowed to access its resources. No device such as workstation or server, either in L&T Network, DMZ or the Internet, is allowed to access the Admin Network by any means. *Note: The only exception is the modem connection of CDS (Communication and Delivery System) for exchanging data between Education Manpower Bureau and school.*
Connection point Devices involved	Router (IEP)
Examples of IT equipment in the sub-network	♦ IT Equipment provided by the SAMS project ♦ **Designated** workstations provided by the ITEd project that are located in staff room which can access the SAMS system. The devices in this sub-network should be located in staff room(s) or in other specific confined areas such as the general office to which access is restricted to authorized persons only.

For more information about the above area, please refer to "SAMS and ITEd Network Integration Procedures" at:
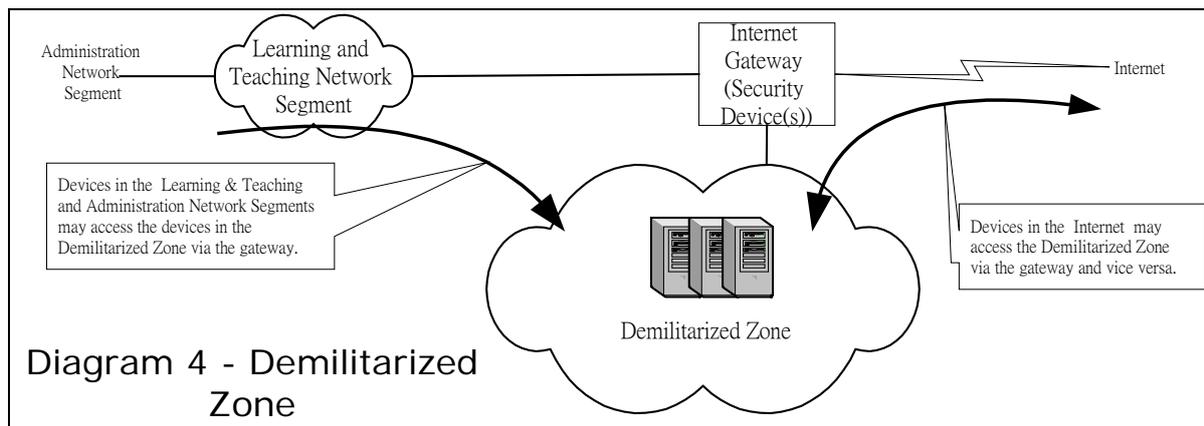
http://www.hkedcity.net/iworld/resource/index.phtml?iworld_id=105&file_id=11988

b) Learning & Teaching Network

Device(s) in the Administration Network Segment are allowed to access the resources of the Learning and Teaching Network Segment and to the Internet.

Devices in the Internet are NOT allowed to access the Learning and Teaching Network Segment and the Administration Network Segment

Devices in the Learning & Teaching and Administration Network Segments may access the Internet (via Demilitarized Zone if it is setup in a school).

Administration Network Segment

Router (Infrastrucutre Enhancement Project)

Learning and Teaching Network Segment

Internet Gateway (Security Device(s))

Internet

Demilitarized Zone *(Optional)*

Diagram 3 - Learning and Teaching Network Segment

Devices in the Demilitarized Zone are NOT allowed to access the resources in the Learning & Teaching and Administration Network Segment.

Access to this sub-network	The security requirement of a typical L&T Network is lower than that of the Admin Network. Devices in L&T Network and the Admin Network are allowed to access the resources in this sub-network. Access from either the Internet or DMZ is usually prohibited unless there is special arrangement, such as, access to a database server from a web server, or VPN connection. Schools are advised to discuss with the market practitioners to identify the most suitable solution for such special requirements. *Notes: (1) Virtual Private Network (VPN) is a special traffic (channel) that allows communication of the L&T network with a student and/or teacher remote access through data encryption.* *(2) In case that some internal host like database server requested to be access by a web server in the DMZ, the Internet Gateway must be configured to allow communication (or channel) between these two hosts only.*
Connection point Devices involved	Internet Gateway and Router (IEP)
Examples of IT equipment in the network segment	IT equipment in ♦ Classrooms; ♦ Multimedia Learning Centre (MMLC); ♦ Information Technology Learning Centre (ITLC); ♦ Computer Room; and ♦ Library and staff room.

c) Demilitarized Zone

Diagram 4 - Demilitarized Zone

Access to the sub-network	The Demilitarized Zone is a special sub-network which sits between the school network and the Internet for hosting public accessible server(s) of a school, such as web server, mail server, proxy server and ftp server.
	Since this sub-network is public accessible, it can be accessed from both L&T network and Admin Network.
	Note: (1) For example, a proxy server is placed inside this sub-network. Workstations in the L&T network and Admin network would access the Internet via this proxy server.
	(2) Access (or traffic) from the Internet to this network should be under control.
Connection point Devices involved	Internet Gateway
	Notes: (1) Internet Gateway can be a mix of Routers, Firewalls and Proxy Servers.
	(2) The Internet Gateway should be installed onto a dedicated machine. Other applications such as ftp server, web server, file server, email server and domain controllers… etc. should be installed in separate server(s).
	(3) The router provided by most Internet Service Providers is solely for Internet connection purpose. It should not be considered as part of the Internet Gateway.
Examples of IT equipment in the sub-network	All application servers for public access such as web servers, mail servers and ftp servers.