

Information Technology in Education Project

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.



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

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.

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.

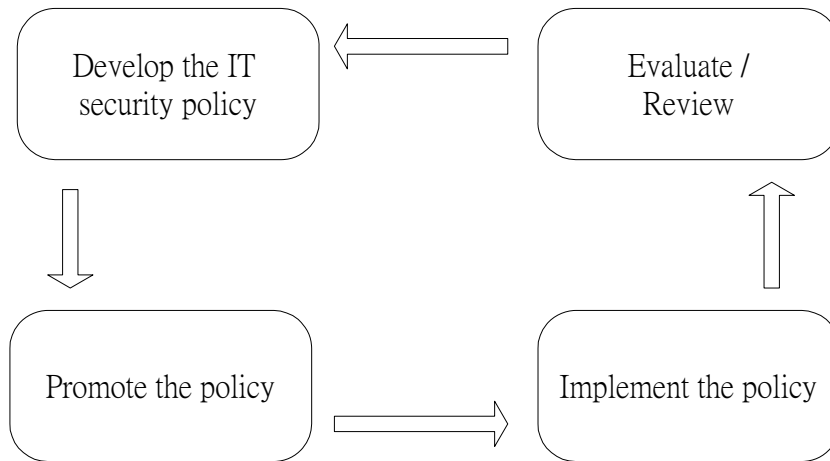
Evaluate and Review

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.



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:

[http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools \[Nov_05\].pdf](http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools_[Nov_05].pdf)

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	<ul style="list-style-type: none"> ● All computer equipment should be kept in a secure place with good physical security
Site Environment	<ul style="list-style-type: none"> ● The computer equipment should be kept in a place with good environmental condition.
Asset Management	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● The use of privileged accounts should be restricted and controlled. ● Users are responsible for all activities performed using their accounts.
Equipment Access Control	<ul style="list-style-type: none"> ● All computer equipment, such as servers, workstations and routers, should be password protected.
Password Management	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● Data backup should be carried out regularly. ● Backup and Recovery procedures should be well documented, tested and properly implemented.
System Failure Protection	<ul style="list-style-type: none"> ● All systems in school should have a recovery plan to prevent data loss.
Software Security Update	<ul style="list-style-type: none"> ● The software should be updated with security patches regularly, if applicable.
Virus Prevention	<ul style="list-style-type: none"> ● 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 conducive 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none">● 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/hkp-home/english/tcd/childsafte.htm>

* 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:

[http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools \[Nov_05\].pdf](http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools_[Nov_05].pdf)

Areas	Sample Policies
Security Audit	<ul style="list-style-type: none">● All systems should be audited and the report should be compiled periodically.● The use of audit program and the result of auditing should be classified, restricted and controlled.
Incident Handling	<ul style="list-style-type: none">● 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.

<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none"> <input type="checkbox"/> Secured areas in schools should be locked with limited access. <input type="checkbox"/> Physical access rights should be assigned to particular persons for secured areas (e.g. Server room). <input type="checkbox"/> Network equipment (e.g. switches and routers) should be locked for protection. <input type="checkbox"/> Mobile equipment (e.g. Notebook/Handheld computers) should never be left unattended. The mobile equipment should be locked after use. <input type="checkbox"/> Backup storage media should be kept in secured areas, which can be accessed by authorized persons only. <input type="checkbox"/> Property marking should be printed on all computer equipment. <input type="checkbox"/> The climate of server room should be kept in optimal condition for the equipment.
Access Control	<ul style="list-style-type: none"> <input type="checkbox"/> All users should be assigned with network accounts and passwords to access the network. <input type="checkbox"/> Network administrator account should be restricted only to designated persons. <input type="checkbox"/> User access rights on network should be assigned on a Need-to-Know basis. <input type="checkbox"/> BIOS passwords in all computer machines should be set and known by authorized persons. <input type="checkbox"/> All user passwords must be changed regularly.

Data Security	<ul style="list-style-type: none"> <input type="checkbox"/> Data should be classified with (e.g. public, private confidential) for different handling and disposal procedures. <input type="checkbox"/> Server(s) should be backed up regularly. <input type="checkbox"/> Server(s) should be connected to Uninterruptible Power Supply (UPS). <input type="checkbox"/> Security patches and updates for operating systems and Internet browsers should be checked and applied weekly/biweekly. <input type="checkbox"/> Anti-virus software should be installed in all servers and workstations. <input type="checkbox"/> The virus signature of the anti-virus software should be updated regularly.
Network and Communication Security	<ul style="list-style-type: none"> <input type="checkbox"/> All workstations in Learning & Teaching network should be barred from direct access to data and system in the SAMS network. <input type="checkbox"/> All dial-out and dial-in activities should be audited and controlled. <input type="checkbox"/> Use of remote access to school network should be made available to authorized users only. <input type="checkbox"/> All files downloaded from the Internet should be scanned with anti-virus software. <input type="checkbox"/> Internet gateway should be used to control the incoming and outgoing network traffic with the Internet. <input type="checkbox"/> 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	<ul style="list-style-type: none"> <input type="checkbox"/> The event logging function in server operating system should be enabled. Events about account, logon and system should be logged. <input type="checkbox"/> Logging function in the Internet gateway should be enabled. Information such as IP address, ports and service requested should be logged. <input type="checkbox"/> 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

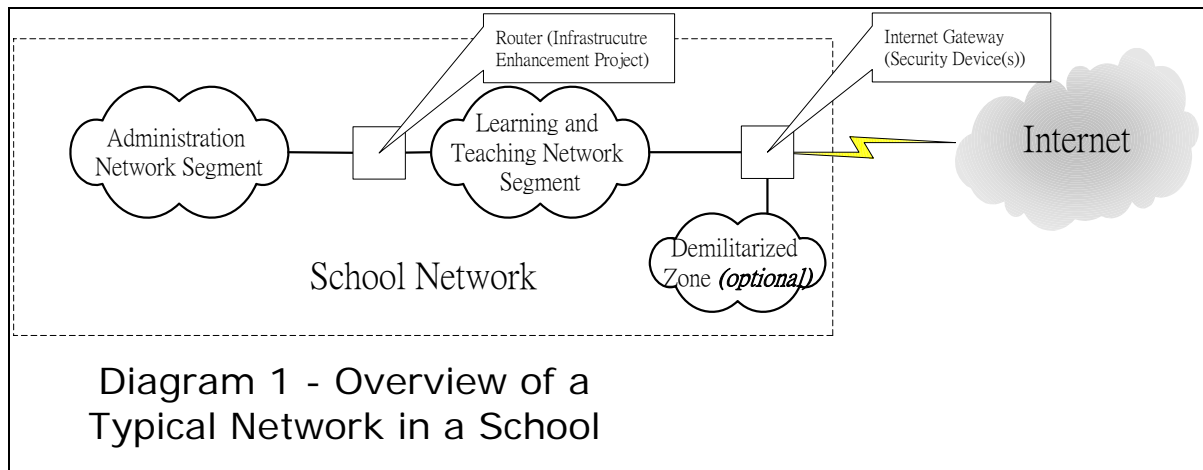
InfoSec web site, (<i>Information Security web site by HKSAR</i>)	http://www.infosec.gov.hk
Internet Security Handbook, <i>2nd ED</i> , HK University of Science and Technology:	http://www.hkcert.org/ish/internet.secur.v2.pdf
Computer Security for users of Small Computer Systems:	http://www.info.gov.hk/police/hkp-home/english/tcd/sms.htm

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.

1) Overview of the Network Segments

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



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)	<p>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.</p> <p>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.</p> <p>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.</p>

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)	<p>The L&T Network and DMZ are inter-connected at the Internet Gateway which is connected to the Internet.</p> <p>Typically, a school should have a <u>SINGLE</u> connection to the Internet, usually through the broadband service.</p> <p>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.</p> <p>For more information about the Internet Gateway, please refer to "<i>Understanding Internet Gateway</i>" in ITED web site:</p> <p>http://202.64.213.147/ited/Support_Service/TSS_Ref/Internet_Gateway.pdf</p>

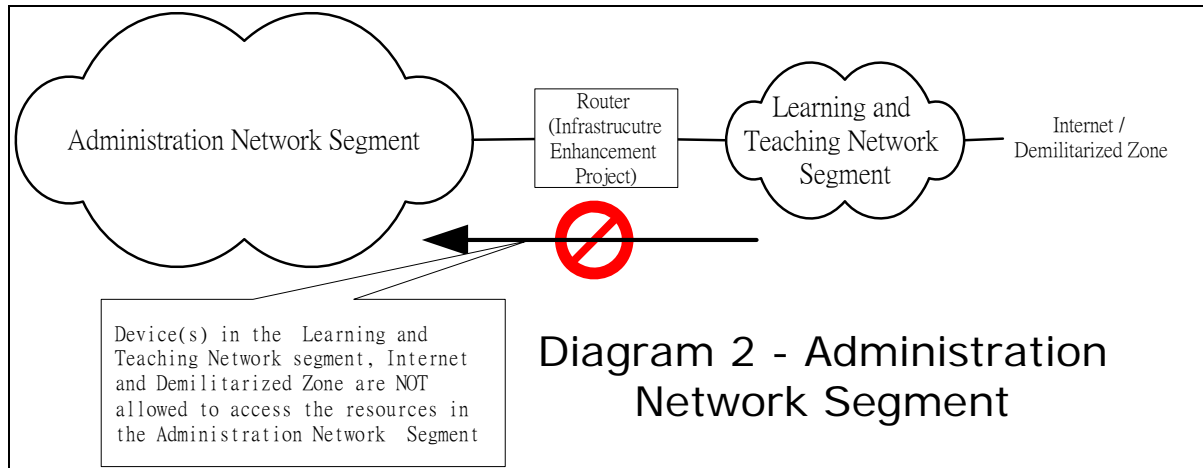
To ease security management tasks, other connections to external networks are normally prohibited unless the school has special requirements and proper security measures have been in-place (the security measures should align with the School IT Security Policy). For example, using Virtual Private Network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

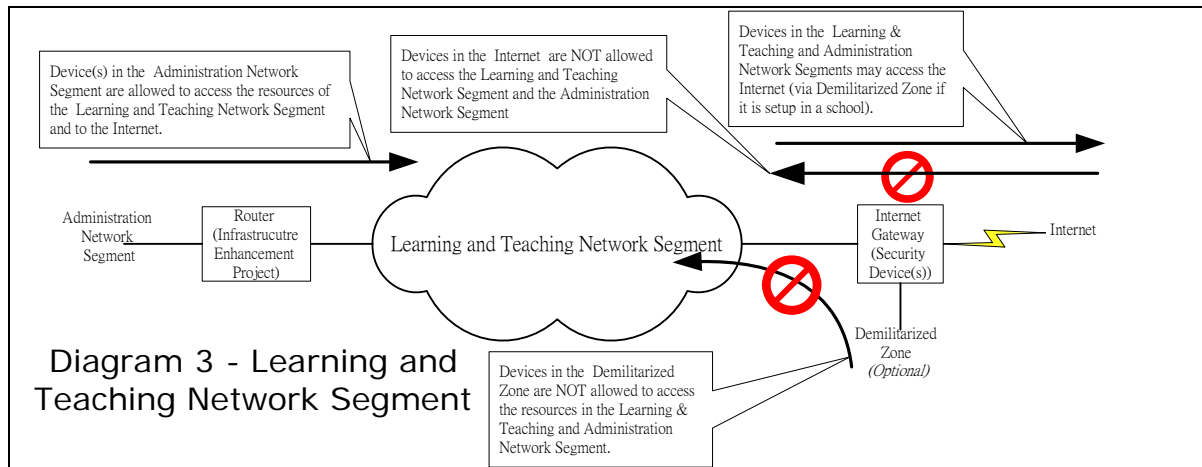


<p>Access to the sub-network</p>	<p>As this sub-network has a relatively higher security requirement, ONLY devices in the Admin sub-network itself are allowed to access its resources.</p> <p>No device such as workstation or server, either in L&T Network, DMZ or the Internet, is allowed to access the Admin Network by any means.</p> <p><i>Note: The only exception is the modem connection of CDS (Communication and Delivery System) for exchanging data between Education Manpower Bureau and school.</i></p>
<p>Connection point Devices involved</p>	<p>Router (IEP)</p>
<p>Examples of IT equipment in the sub-network</p>	<ul style="list-style-type: none"> ◆ 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. <p>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.</p>

For more information about the above area, please refer to "SAMS and ITed Network Integration Procedures" at:

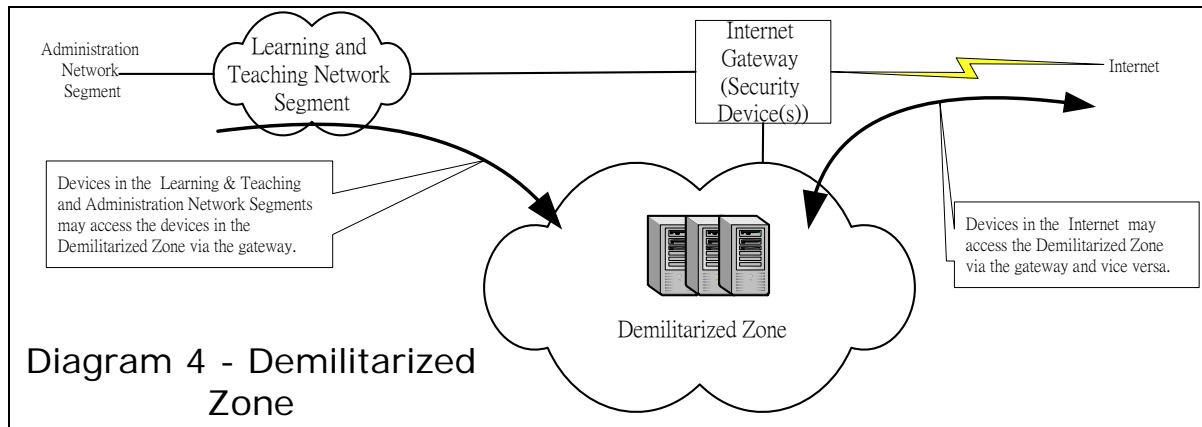
http://www.hkedcity.net/iworld/resource/index.phtml?iworld_id=105&file_id=11988

b) Learning & Teaching Network



<p>Access to this sub-network</p>	<p>The security requirement of a typical L&T Network is lower than that of the Admin Network.</p> <p>Devices in L&T Network and the Admin Network are allowed to access the resources in this sub-network.</p> <p>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.</p> <p><i>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.</i></p> <p><i>(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.</i></p>
<p>Connection point Devices involved</p>	<p>Internet Gateway and Router (IEP)</p>
<p>Examples of IT equipment in the network segment</p>	<p>IT equipment in</p> <ul style="list-style-type: none"> ◆ Classrooms; ◆ Multimedia Learning Centre (MMLC); ◆ Information Technology Learning Centre (ITLC); ◆ Computer Room; and ◆ Library and staff room.

c) Demilitarized Zone



<p>Access to the sub-network</p>	<p>The Demilitarized Zone is a special sub-network which sits between the school network and the Internet for hosting <u>public accessible server(s)</u> of a school, such as web server, mail server, proxy server and ftp server.</p> <p>Since this sub-network is public accessible, it can be accessed from both L&T network and Admin Network.</p> <p><i>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.</i></p> <p><i>(2) Access (or traffic) from the Internet to this network should be under control.</i></p>
<p>Connection point Devices involved</p>	<p>Internet Gateway</p> <p><i>Notes: (1) Internet Gateway can be a mix of Routers, Firewalls and Proxy Servers.</i></p> <p><i>(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).</i></p> <p><i>(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.</i></p>
<p>Examples of IT equipment in the sub-network</p>	<p>All application servers for public access such as web servers, mail servers and ftp servers.</p>