Information Security in Schools

Recommended Practice

Education Bureau
The Government of the HKSAR

Revised in Aug 2016

Table of Content

PART 1
ABOUT THIS DOCUMENT

1. Introduction

The Fourth Strategy on IT in Education was launched in 2015/16 school year. This document is written for schools’ reference in protecting their information and IT assets when implementing e-learning. Schools are responsible to take appropriate IT security measures to protect the IT systems and data of their schools. This document recommends common practices on IT security for reference by the schools. Schools may determine on their own requirements to adopt the practices where applicable to their own environment. The practices recommended in this document are by no means exhaustive. Schools may also make reference to other IT security measures, such as those listed in the "Additional Resources on IT Security" in Part 15 of this document, to protect their IT assets.

This document is prepared by the IT in Education Section of the Education Bureau. For enquiry, please contact the IT in Education Section on (852) 3698 3608 or by writing to the Chief Curriculum Development Officer, IT in Education Section, Education Infrastructure Division, Education Bureau Kowloon Tong Education Services Centre, Rm E420, 4/F, East Block, 19 Suffolk Road, Kowloon Tong, Kowloon.

The full text of this publication is available at the IT in Education Section website at http://www.edb.gov.hk/ited/.

PART 2
SECURITY MANAGEMENT

2. Information Security Objectives

2.1 When considering confidentiality of security, appropriate measures in IT systems should be implemented to protect the information, such as access control and data encryption.

2.2 When considering integrity of security, appropriate measures should be designed and implemented in IT systems.

2.3 When considering availability of security, the following items should be considered:

(a) Safeguard necessary resources and associated capability;

(b) Ensure the information must be highly available on a timely basis;

(c) Prevent unexpected loss or leakage;

(d) Achieve information security objects according to security level; and

(e) Identify any potential risks, and determine corresponding information security level.

3. Security Policy

3.1 Only authorised person is allowed to access, possess, modify, delete, copy and publish information stored in system.

3.2 When implementing monitoring measures, the following items should be considered:

(a) Define and implement preventive, detective, responsive and recovery measures for enforcing information security;

(b) Design and implement preventive measures to avoid the occurrence of an undesirable event;

(c) Design and implement detective measures to identify the occurrence of an undesirable event;

(d) Design and implement responsive measures to response to undesirable event (or incident);

(e) Design and implement recovery measures to restore the confidentiality, integrity and availability of information to their expected state;

(f) Designate authorised personnel to implement and review the related measures for verifying the eligibility of policy and explore any vulnerability regularly, and take immediate action if needs;

(g) Restore backup data and system for verification by authorised personnel; and

(h) Document the flow of incident escalation and history.

3.3 It is advised to design and implement the wired and wireless network with appropriate measures to enforce the confidentiality, integrity, and availability of network. It is useful to collaborate with service providers to ensure information security on wired and wireless network.

3.4 When considering safeguard from external systems, the following items should be considered:

(a) Design and apply security controls and policy to all boundaries between trusted and untrusted areas;

(b) Define and review security control and policy for entire system as a whole; and

(c) Adopt the appropriate security measures for their own IT environment.

4. Security Personnel

4.1 For segregation of duties, proper segregation of duties, in terms of technical, operational and managerial roles should be defined.

4.2 Organisation of stakeholders should be formed and identified to design, implement and maintain IT security in school network.

4.3 Roles and responsibilities should be design and assigned to stakeholder. Here is a suggested sample definition.

School Head

School Head is responsible for

(a) Directing and enforcing the development of security measures;

(b) Providing the necessary resources required for the measures to be implemented;

(c) Ensuring participation and support at all levels of management, administrative, technical and operational staff; and

(d) Aligning the security strategy with schools' objectives with regular review and update.

IT Head

IT Head is responsible for

(a) In-charge of entire campus IT environments, including design, strategic planning, and implementation, and is expected to have IT and Security knowledge;

(b) Leading the establishment, maintenance and implementation of IT security policies, standards, and procedures;

(c) Disseminating security alerts on impending and actual threats from the professional IT security institutions to responsible parties;

(d) Ensuring information security risk assessments and audits are performed as necessary;

(e) Initiating investigations and rectification in case of breach of security;

(f) Managing and handling incidents of IT security of the entire campus systems and networks;

(g) Granting authorisation and approval to concerned parties or person for management, and handling critical incidents;

(h) Defining and maintaining disaster recovery plan with regular verification;

(i) Providing management endorsement on the provision of resources for the incident handling process;

(j) Escalating and reporting information security incidents for central recording and necessary follow up actions; and

(k) Facilitating experience and information sharing within schools on information security incident handling and related matters.

IT Committee Members

IT Committee Members are responsible for

(a) Management of the information systems;

(b) Assisting IT Head in the implementation, administration, maintenance, operation;

(c) Managing and estimating resources in operation;

(d) Ensuring the implement of IT policies in school system and network;

(e) Evaluating and advising technologies, IT and security solutions to IT Heads; and

(f) Defining security requirement and policy with implementation plan for protection information security.

Technical Support Staff

Technical Support Staff are responsible for

(a) Daily operation and maintenance;

(b) Assisting IT Head in the implementation, administration, maintenance, operation;

(c) Monitoring to availability of system and services; and

(d) Handling fault case and escalate to concerned parties.

End User

End user should be the expected user who can use the services and data in the information system. And End user should be responsible for

(a) Knowing, understanding, following and applying all the possible and available security mechanisms to the maximum extent possible;

(b) Preventing leakage and unauthorised access to information under his/her custody;

(c) Safely keeping computing and storage devices, and protecting them from unauthorised access or malicious attack with his/her best effort; and

(d) Reporting any abnormal incident or fault case.

5. IT Security Functions

5.1 When considering physical and network security

(a) When defining user practice, the following items can be considered:

- Should not log on the school applications from public computers; and
- Should not leave their workstations and computer equipment unattended without sufficient physical access controls.

(b) When maintaining IT equipment, the following items can be considered:

- Keep IT equipment, including hardware and software in a safe place against unauthorised access;

- Enable password-enabled screen saver to prevent illegal system access attempt;
- Do not connect de-supported operating systems to school network;
- Do not connect to external network by means of dial-up modem, wireless interface or broadband link; and
- Enable encryption feature in the data transmission of wireless or mobile devices.

For further information, please refer to
http://www.infosec.gov.hk/english/yourself/handheld.html

5.2 When considering access control, the following items should be considered:

(a) Assign appropriated rights to individual users for accessing the associated resources;

(b) Define and assign access controls to data files, resources and other system rights;

(c) Prevent unauthorised access to system and/or network resources;

(d) Assign proper management of the accounts to corresponding staff;

(e) Review the usages of all kinds of personal/non-personal accounts annually;

(f) Inform and align with external parties who are engaged in school work with the equivalent information security requirements, policy and security responsibilities; and

(g) Promptly terminate any ceased account.

For further information, please refer to
http://www.infosec.gov.hk/english/yourself/account.html

5.3 When considering data security, security measures like provision of advanced hard disk sub-system and UPS could be considered for implementation. Recovery plan using backup and recovery process should be implemented. The following items should also be considered:

(a) Handling of data

- Release information and grant the access right based on a need-to-know basis;
- Develop proper "system backup and recovery" strategy for restoring

corrupted or accidentally deleted data;

- Define the steps and procedures to back up and recover all data with minimal human interaction; and
- Document, test and implement all backup and recovery procedures.

For further information, please refer to http://www.infosec.gov.hk/english/business/backup.html

(b) Virus, Patch and Software Management

- Apply latest security patches and regularly remove cache files or temporary files to protect data privacy;
- Install virus, malicious code detection measure with latest signatures and definition files in the computer of schools, and to perform virus scan including email, downloaded file, files in removable media or mobile device before use;
- Do not install P2P file sharing and unauthorised software in the computer of schools;
- Minimise the amount of data stored and avoid storing sensitive data;
- Encrypt sensitive data at all times during storage and transmission;
- Back up important data and test data recovery procedures where appropriate;
- Ensure all data have been completely erased before disposal or re-use of the mobile device; and
- Set up a remote data wiping feature, if available.

For further information, please refer to http://www.infosec.gov.hk/english/promotion/files/Script_DataEncryption.pdf

(c) Deploy firewall to control and safeguard the traffic among various inter-connected networks like LANs and WebSAMS.

5.4 When designing security Audit and Incident Handling, the following items should be considered:

(a) Enable activity logs for events and threats tracking;

(b) Periodic monitor and review activity logs of school systems and networks; and

(c) Define and publish procedure & contact to users for suspicious event escalation.

5.5 When designing security Awareness and Education, the following items should be considered:

(a) Educate end user the importance of security awareness; and

(b) Provide well-conceived and committed security training programs to users.

5.6 When considering striving for balance, it is advised to be aware that systems with few security controls are generally more vulnerable than those have made many. A balance can be strived between the need for adequate security versus the desire to stay within limited resources.

For further information, please refer to
http://www.infosec.gov.hk/english/main.html

PART 3

SECURITY INCIDENT HANDLING

6. In addition to deploying security protection, schools should respond to incidents and invoke proper procedures in case an information security incident occurs. It is recommended that a checklist for security incident handling should be prepared. An sample checklist is given below for reference.

	Item	Details	Status
1	Establish an IT Security Incident Response Team	• Include IT Head, IT Technical Staff and other related staff; and • Publish the security incident response procedure to all personnel involved.	
2	Escalation procedure	• All the security incidents should be addressed to the IT Security Incident Response Team upon such an incident is spotted.	
3	Security incident response procedure	• Mitigate the effects caused by security incident; and • Protect the information resources from future unauthorised access, use or damage.	
4	Reporting procedure	• Report on the incident and the ensuing investigation; • Summarizes findings regarding the Information Security Incident; and • Makes recommendations for improvement of related information security practices and controls. The Report will be distributed to the appropriate parties.	
5	Training and education	Please refer to the following for detailed information in • Security Incident Handling for Individuals http://www.infosec.gov.hk/english/yourself/security_3.html • Security Incident Handling Guidelines http://www.ogcio.gov.hk/en/information_security/policy_and_guidelines/doc/g54_pub.pdf	

PART 4

PHYSICAL SECURITY

7. Hardware and Software Asset Protection

7.1 All access media such as keys and access cards are advised physically secured and handled only by authorised persons.

7.2 Recommended practice to build server room protection is as follows:

(a) Install and use dedicate power supply circuit and UPS in server room;

(b) Keep temperature and humidity of server room at optimal level with 24-hour air conditioning;

(c) Enhance security by using heat and smoke detectors, motion detectors, alarm systems and fire extinguishing; and

(d) Regularly check to security facility to ensure their serviceability.

7.3 Network devices such as switches and hubs and servers are recommended to be secured in locked containers such as Floor-level Equipment Cabinet (FLEC) Protection to prevent theft and unauthorised access.

7.4 Surge protectors are recommended to protect the hardware equipment.

7.5 Recommended Practice to handle mobile devices is as follows:

(a) Do not leave unattended mobile computer equipment, such as notebook computers and projectors without proper security measures;

(b) Store the notebook computers that are not in use in lockable cabinets; and

(c) Safeguard the mobile devices on the network.

7.6 Recommended Practice to design storage media is as follows:

(a) Design and implement security measures to storage media such as backup tapes, floppy disks, CD-ROM discs and USB; and

(b) Locked media with sensitive data in secure areas.

7.7 Recommended Practice to handle Software Copies and Backup Tapes is as follows:

(a) Keep the original and backup copies of software programs and data files securely; and

(b) Maintain the backup copies in a separate location with a safe distance from the original copies.

7.8 When performing property marking and inventory taking, the following items should be considered:

(a) Perform property marking and inventory taking regularly to prevent and explore physical loss;

(b) Paint property marking to major hardware items;

(c) Record and maintain an IT equipment inventory list;

(d) Perform periodic checking on the items, including the system configuration, software media and licenses, network devices, data backup tapes, etc;

(e) Record the location as well as the status of the equipment such as "in use", "on loan", "repair", "discard", etc; and

(f) Use software asset management (SAM) tools for establishing software inventory list.

PART 5

ACCESS CONTROL

8. Access Control

8.1 When considering authentication and authorisation, the following items should be considered:

(a) Assign user name and password for authentication;

(b) Grant access right to user and group to access system and network resources;

(c) Prevent unauthorised access; and

(d) Manage for HKEdCity Accounts Authentication.

For further information, please refer to

http://www.hkedcity.net/emads/eng/frontpage.html

8.2 Recommended Practice to administrate user accounts is as follows:

(a) Identify and define possible users;

(b) Assign account with specific role, job level and privilege to users and groups; and

(c) Manage and monitor user account regularly.

E.g. teacher can perform account management for students.

8.3 Users should be responsible for handling their user accounts properly. They should keep their password secret.

For further information, please refer to

http://www.infosec.gov.hk/english/yourself/account.html

8.4 When performing user and access rights assignment, the following item should be considered:

(a) Assign appropriate privilege to user account in need-to-know basis;

(b) Do not assign unnecessary privileges to user;

(c) Review user rights periodically;

(d) Restrict log-on hours, if necessary;

(e) Require authentication for accessing certain resource, if necessary; and

(f) Enable screen saver.

PART 6

DATA SECURITY

9. Data Security

9.1 Some general data backup and recovery practices are provided below:

(a) Define and implement proper "system backup and recovery" strategy;

(b) Capable of restoring corrupted or being accidentally deleted data;

(c) Document the backup and recovery procedure;

(d) Minimal human operation is expected;

(e) Well documented, tested and properly implemented the backup and recovery procedures;

(f) Performed and monitored the data backup regularly;

(g) Verify and trial restore the backup files; and

(h) Keep and lock the backup media in a safe place.

9.2 It is advised to define data classification policy with corresponding data handling policy.

For example, having classification policy that “all files containing personal data should be classified as confidential”; and data handling policy specifying that “All confidential data should be encrypted in email and in removable media”.

9.3 It is advised to label the storage media with different data classification.

9.4 Recommended Practice to protect and dispose sensitive data is as follows:

(a) Enable encryption feature of servers;

(b) Enable password protection feature; and

(c) Securely erased all sensitive data from storage.

9.5 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. Under the Ordinance, data users might comply with the six internationally recognized data protection principles in the processing and use of personal data. For further information, please refer to http://www.pcpd.org.hk/english/data_privacy_law/6_data_protection_principles/principles.html

Personal Data (Privacy) Ordinance Related Information	Source
https://www.pcpd.org.hk/	Privacy Commissioner for Personal Data, Hong Kong
http://www.dutylawyer.org.hk/	Information of Personal Data (Privacy) Ordinance in the Duty Lawyer Service, HKSAR

9.6 When protecting data stored in mobile devices/applications, the followings general tips can be considered:

(a) When configuring a mobile device

- Turn off location services setting in a mobile device if it is not necessary to run location-based application;
- Do not jailbreak the mobile device (to override usage and/or access limitations); and
- Advise to review the recent vulnerabilities.

(b) When using a mobile device

- Protect an online user account that handles sensitive data with a strong authentication mechanism, such as two-factor authentication, if available;
- Do not leave a mobile device unattended, even for a moment;
- Do not process sensitive data in the mobile device unless with encryption feature on or secure end-to-end connection;
- Do not open or follow links in SMS/MMS or email from misleading URL, suspicious or un-trusted sources;
- Do not download or accept programs and content from unknown or un-trusted sources; and
- Be cautious when connecting to publicly available Wi-Fi hotspots, and

avoid access sensitive data unless with adequate security protection.

(c) When backup data in a mobile device

- Assess the security risks before synchronising data to cloud services and adopt adequate security measures, such as avoiding automatic backup/ synchronisation of sensitive data to cloud services;
- Turn on the encryption option in the backup/synchronisation software for storing the data in encrypted mode if available; and
- Make sure the backup copies are encrypted no matter stored in desktop PC or in removable media.

(d) When disposing your mobile device

- Completely clear all data and settings on your mobile device before disposal.

(e) At all time

- Keep the mobile devices in a secure place, especially when not in use;
- Stay alert on security vulnerability on mobile devices, and apply the latest patches and fixes when available;
- Do not install illegal or unauthorised software on the mobile device; and
- Do not allow wireless connections from unknown or un-trusted sources on your device.

9.7 Virus Definition Files

Regularly update and verify the latest anti-virus definition in all PC.

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.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

The following documents can be referred 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	
Guideline and Tips for virus prevention http://www.infosec.gov.hk/english/yourself/yourself.html	

9.8 Subscription to Security Alerts Mailing List

The mailing list from security agencies / software companies can be subscribed to practice safe computing in a proactive way. The subscription can be made for all responsible personnel, e.g. system administrators and support staff of the school network. Security alert can be found from the anti-virus software vendors (see the web sites below).

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

PART 7

APPLICATION SECURITY

10. Installation of Computer Software

10.1 Installation of computer software should be carried out by authorised person upon obtaining approval from responsible person. Computer software can only be installed if it does not lead to a compromise of existing security controls. All changes made to computer software should be fully documented and tested, and an audit trail of all installations and upgrades should be maintained.

10.2 Recommended security fixes for software vulnerabilities or bugs should be regularly applied to the school systems. Information of up to date alerts for software products can be obtained from https://www.hkcert.org/security-bulletin .

PART 8

NETWORK AND COMMUNICATION SECURITY

11. General Network Protection

11.1 It is suggested to limit connection to public networks to the hosts that do not store sensitive material and keep vital machines isolated.

11.2 Some general network protection guidelines are provided below:

(a) Keep network simple (i.e. minimise number of network interface points between "secured" network and "non-secured" network);

(b) Only allow authorised traffic to enter the "secured" network;

(c) Use multiple mechanisms to authenticate user (e.g. password system plus pre-registered IP/IPX network plus pre-registered terminal number);

(d) Manage the network with network management system; and

(e) Encrypt data with proven encryption algorithm before transmitting over the network.

12. Building a Secure Network

12.1 Recommended Practice to build a secure network is as follows:

(a) Plan for network security: address all security requirements and issues in selecting network and server and deployment including the management policy, technical training and outsourcing requirements;

(b) Design physical and environmental security: e.g. put critical assets such as network communication lines, servers, switches, firewalls and file servers in server room or a secured area;

(c) Use private IP addressing scheme for internal networks: to prevent internal network from access by external network;

(d) Design network security model by zoning i.e. segregation of network according to security requirements, e.g. the office network is totally isolated from the Internet, or the school servers and computers are located behind the firewall, or set up a demilitarized zone (DMZ) network. Unsecured or unmanaged systems are not advised to make connection to internal network;

(e) Configure firewalls and network routers: harden the firewall and router by limiting the administrative access to specified locations, closing unnecessary network services for incoming and outgoing traffic or using encrypted communication channel for administration;

(f) Configure servers: e.g. secure the server operating system by uninstalling unnecessary services and software, patch the system timely and disable unused accounts;

(g) Secure the application: by means of installing security patches, hardening the configuration of the applications or running the application with a least privilege account;

(h) Filter virus and malicious code: anti-virus software with up-to-date signature install in desktop and network servers to prevent the spread of virus / worm;

(i) Manage accounts and access privileges: e.g. access rights should be granted on an as-needed basis and should be reviewed regularly;

(j) Log security events and review regularly: Logging and auditing functions can be provided to record network connection, especially for unauthorised access attempt. The log can be reviewed regularly;

(k) Develop security management procedure: e.g. security log monitoring procedure, change management procedure or patch management procedure;

(l) Maintain good documentation of configuration and procedure; and

(m) Train the staff: training can be given to network/security administrator and supporting staff as well as users to ensure that they follow the security best practice and follow security policies.

13. Communication with the External Network

13.1 Remote Access

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

(b) Remote computers can be properly protected, by installation of personal firewall, anti-virus software and malicious code detection and repair measure; and

(c) To avoid information leakage, users can minimise storing information on remote or portable computers. Sensitive information is recommended not to be stored in privately-owned computer, mobile devices or removable media. When working in public areas, users should avoid working on sensitive documents to reduce the risk of exposing to unauthorised parties. Users should also avoid using public printers. If printing is necessary, the printout should be picked up quickly. Furthermore, users can protect the remote computers with password-enabled screen saver and never leave the computers unattended.

14. Virtual Private Network

14.1 Schools should evaluate compatibility with the existing network and consider implementing the following security advices for VPN set up:

(a) Authenticate with either one-time password authentication such as a token device or public/private key system with a strong passphrase;

(b) Disconnect automatically from school internal network after a pre-defined period of inactivity. The user must then logon again to reconnect to the network;

(c) Disallow dual (split) tunnelling. Only one network connection is allowed;

(d) Protect all computers or devices connected to school internal networks via VPN with personal firewall, latest security patches, anti-virus and malicious code detection and recovery software. All these security measures should be activated all the time and with the latest virus signatures and malicious code definitions;

(e) Provide logging and auditing functions to record network connection, especially for failed access attempt. The log should be reviewed regularly to identify any suspicious activities;

(f) Remind users with VPN privileges that they are accountable for the proper use of the account, ensuring that unauthorised users cannot use the account to access schools' internal networks;

(g) Educate LAN/system administrator, supporting staff as well as remote users to ensure that they follow the security best practices and policies during the implementation and usage of VPN; and

(h) Install gateway-level firewalls to control network traffic from VPN clients to authorised information systems or servers.

15. Wireless Network Protection

15.1 It is recommended to build the Wi-Fi network completely separated from schools' existing network with separate broadband line.

15.2 Schools' IT personnel needs to consider, understand, and eliminate the security issues and risks to school existing network when Wi-Fi network integrated or connected to schools' existing network.

15.3 A stronger wireless security protocol such as WPA (Wi-Fi Protected Access) or preferably WPA v2 (WPA2) should be considered, but by no means can such wireless security protocol be solely relied upon to protect data confidentiality and integrity as new weaknesses of these protocols might be discovered in the future. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal authenticates users for network access using a pre-shared password, while WPA2-Enterprise authenticates through a Remote Authentication Dial In User Service (RADIUS) authentication server. Although the setup for WPA2-Enterprise is more complicated, it is recommended because it provides additional security and offers better centralised control over access to the WLAN. WPA2-Personal is only recommended for small ad-hoc network such as guest WLAN for visitors. Virtual Private Network (VPN) can also be deployed on top of wireless network if sensitive data is to be communicated over wireless networks.

15.4 Adopt proper management controls to effectively protect wireless networks:

(a) Define a wireless security policy to address the usage of wireless networks and types of information that can be transmitted over wireless networks;

(b) Develop and securely keep a coverage map of the wireless network, including locations of respective access points and SSID information so as to avoid excessive coverage by the wireless signal;

(c) Search regularly for rogue or unauthorised wireless access points;

(d) Perform regular IT security risk assessments and audits to identify security vulnerabilities;

(e) Keep a good inventory of all devices with wireless interface. Once a device is reported missing, consider modifying the encryption keys and SSID;

(f) Implement strong physical security controls and user authentication for complementing physical security deficiencies of wireless devices; and

(g) Install access points far from a window or a door to prevent network tapping from publicly accessible area.

15.5 Adopt proper technical controls to effectively protect wireless networks:

(a) Change network default name at installation; SSID should not reflect the name of any school, system name or product name/model;

(b) Change product default access point configuration settings, which are considered unsecured most of the time for easy deployment;

(c) Disable all insecure and unused management protocols on access points and configure the required management protocols with least privilege;

(d) Ensure that all access points have strong, unique administration passwords and change the passwords regularly;

(e) Enable and configure security settings including SSID, encryption keys, Simple Network Management Protocol (SNMP) community strings;

(f) Deploy WPA2-Enterprise, or change encryption keys regularly if WPA2-Personal is used;

(g) Disable SSID broadcasting to prevent the access points from broadcasting the SSID so that only authorised users whose configured SSID matches that of the access point can connect to the network;

(h) Disable DHCP and assign static IP addresses to all wireless users to minimise the possibility of an unauthorised user obtaining a valid IP address;

(i) Use MAC address filtering for configuring access points so that they allow only clients with specific MAC addresses to access the network, or allow access to only a given set of MAC addresses;

(j) Do not directly connect wireless networks and wired networks. Install a firewall or router with access control lists (ACLs) between the access point and the schools' network to filter connections;

(k) Enable threshold parameters, such as inactivity timeouts;

(l) Activate logging features and redirect all log entries to a remote logging server if possible. The log records should be checked regularly;

(m) Install wireless intrusion detection system (WIDS) or wireless intrusion prevention system (WIPS) to monitor the wireless networks;

(n) Deploy VPN on top of wireless network for connection to internal network;

(o) Use client-side digital certificates for mobile devices with limited Wi-Fi defenses, so only authorised devices are allowed to access departmental network or resources;

(p) Segment the access point's coverage areas to balance the loading and minimise the probability/impact of Denial-of-Service (DoS) attack; and

(q) Erase all sensitive information, such as system configurations, pre-shared keys, digital certificates and passwords, on the devices upon disposal of wireless components.

15.6 Adopt proper End-user controls to effectively protect wireless networks:

(a) Install firewall on wireless clients (e.g. mobile devices);

(b) Turn off sharing or tethering at wireless clients;

(c) Don't attach the wireless clients to departmental network while it is connected to a third party wireless network;

(d) Connect to departmental network resources using VPN;

(e) Keep strict control of the wireless interface device (e.g. PCMCIA card and USB token for notebook computer) as access credentials such as SSID and/or encryption key are commonly stored on the card; and

(f) Only enable wireless connections when users need them; disable them when they are no longer in use.

16. Protection against Email Spam and Malicious code

16.1 Against Email Spam from system prospective

(a) Advise to install email spam filtering gateway to filter all spam emails from the Internet. Latest spamming lists / blacklists should be regularly updated;

(b) Audit logs should be kept at the email spam filtering gateway for regular review;

(c) Prevent email address harvesting from web sites;

(d) Stop third-party mail relay and open web proxy;

(e) Block by public and private DNS blacklists;

(f) Allow emails by whitelists; and

(g) Filter by sender email address, email subject or email content, or use heuristic content filtering.

16.2 Against Email Spam from End-user prospective

(a) Users are recommended to handle their email addresses with care, especially when filling out web registration forms, surveys and other online documents etc;

(b) Avoid publishing email address to unknown individuals and sources, especially as a link on a web site;

(c) Whenever feasible, users might use separate email addresses to avoid their school email addresses and/or mail systems to become a target of spam;

(d) Users should never mail-bomb spammers or perform vigilante actions;

(e) 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;

(f) 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; and

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

16.3 Prevent Malicious Code

(a) Schools are advised to establish anti-virus and malicious code detection and repair software has been installed and running. It is also advised to regularly update virus signature and malicious code definition; and

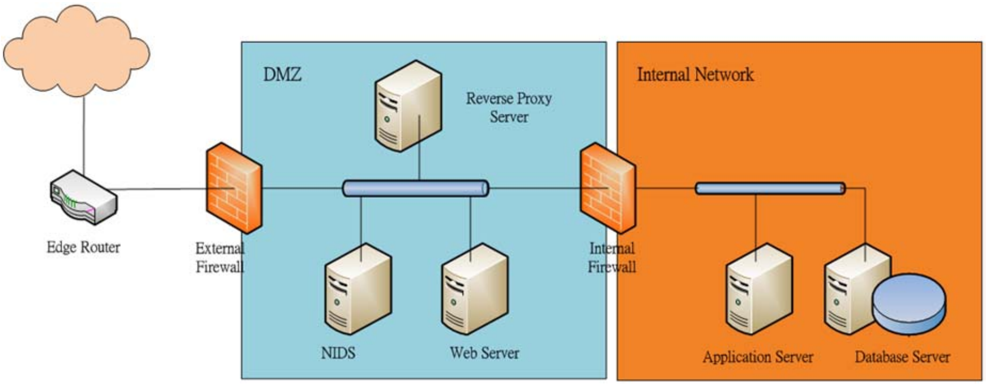
(b) Users should not forward any received hoax messages (i.e. untrue virus-related warnings/alerts started by malicious individuals) to avoid further spreading. Besides relying on technical controls stated above, users should take the responsibility to protect against computer virus and malicious code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

PART 9

WEB APPLICATION SECURITY

17. Adopt Web Application Security Architecture

17.1 Adopt the 3 tiers web application architecture. 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 can be confined within a Demilitarized Zone (DMZ). Sensitive servers are located in the internal network with additional protection. Two firewalls can 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 should be from different vendors.

Other systems such as Network intrusion detection system (NIDS) and reverse proxy server can 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 external users.

17.2 Schools are recommended to perform security risk assessment in order to determine the most appropriate security protection measures. Schools are advised to check their web servers to see if they are configured and running properly. The following guidelines can be observed in enhancing the security of the web servers:

(a) Configure web server securely according to the vendor's security guidelines;

(b) Run web server processes with appropriate privilege account;

(c) Avoid running the web server processes using privileged accounts (e.g. 'root', 'SYSTEM', 'Administrator');

(d) Apply latest security patches to the web server software;

(e) 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;

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

(g) Configure web server software to prevent leaking information like web server software version, internal IP address, directory structure, etc;

(h) Disable or remove unnecessary modules from the web server software;

(i) Identify application files on the web server and protect them with access control;

(j) When using SSL, backup the private key for the server certification and protect it against unauthorised access; and

For further information, please refer to
http://www.infosec.gov.hk/english/business/other_sywa.html

PART 10

SECURITY ISSUES OF MOBILE APPLICTIONS

18. Protecting Mobile Devices

18.1 When configuring mobile device:

(a) Enable a power-on password or other device password management tool if available;

(b) Configure the mobile device in the way that it locks automatically after some inactive time;

(c) Use mobile security software, such as anti-virus software on mobile device if available;

(d) Apply the latest patches and fixes for mobile operating system and related backup/synchronization software. Upgrade the software to the prevailing version where applicable;

(e) Scrutinize thoroughly all permission requests, for example those involving privileged access, when installing applications/services;

(f) Use encryption to lock sensitive data stored on the mobile device and removable media, if available;

(g) Set up a remote data wiping feature if available;

(h) Disable auto data synchronization to cloud services unless there are practical purposes;

(i) Turn off wireless connections such as Wi-Fi, Bluetooth and/or infrared connectivity when not in use;

(j) Turn off location services setting in mobile device if it is not necessary to run location-based application; and

(k) Do not jailbreak the mobile device (to override usage and/or access limitations);

18.2 Precautions of using mobile applications:

(a) Install only mobile applications from official application stores or trusted sources;

(b) Install mobile security software such as anti-malware software to protect both the device and data;

(c) Read the comments on the applications, the term and conditions as well as privacy policy, where available, before installing applications;

(d) Scrutinize thoroughly all permission requests, in particular of those involving privileged access, when installing/using mobile applications;

(e) Review if additional permission requests is necessary when updating applications;

(f) Enable security features provided by the mobile applications (e.g. password protection, secure connection, etc.) if available;

(g) Upgrade the operating system and mobile applications to the latest version;

(h) Do not download files from unknown sources, nor open or follow links from suspicious or un-trusted sources;

(i) Don’t forward any hoax messages to avoid further spreading when using instant messaging applications such as WhatsApp and WeChat;

(j) Regularly review mobile applications installed on the device and remove the applications whenever consider not necessary;

(k) Do not remove usage and access limitation controls of the device (e.g. jailbreak); and

(l) Turn off automatic connection feature for wireless services in mobile device such as Wi-Fi, Bluetooth, NFC, etc.

PART 11

COMPUTER VIRUS PROTECTION

19. Anti-Virus Software

19.1 Anti-virus software should be installed in all computer systems including servers and client computers. The virus monitoring and real time alert functions should be activated. This enable files to be scanned by anti-virus software before they are loaded and used.

19.2 Virus definition file of anti-virus software should be updated regularly.

20. Legal and Authorised Use of Software and Hardware

20.1 School computers and networks are only allowed installing software that comes from trustworthy sources and/or authorised agents. Illegal copies of software are regarded as the major source of viruses. The use of illegal software should be prohibited.

20.2 The use of unauthorised software and hardware should be avoided. A user's personal licensed software or his/her own personal computer is not advised to use in schools.

21. Prevention from Doubtful File Resources

21.1 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.

21.2 Data files from doubtful sources like USB and/or CD-ROM discs should also be checked and cleaned for virus before use.

PART 12

SECURITY REVIEW

22. Security Review Procedure

22.1 Security review is defined as a recursive process of evaluating security risks, which are related to the use of information technology. It shows the amount of work needs to be done in order to align and update the security enforcement. The review of a system includes the identification and analysis of:

(a) All assets and processes related to the system;

(b) Threats that can affect the confidentiality, integrity or availability of the system;

(c) System vulnerabilities and the associated threats;

(d) Potential impacts and risks from the threat activity;

(e) Protection requirements to mitigate the risks; and

(f) Selection of appropriate security measures and analysis of the risk relationships.

22.2 To obtain useful and more accurate review results, a complete inventory list and security requirements for a system should be made available as inputs to the identification and analysis activities. Interviews with relevant parties such as administrators, computer/network operators, or users can also provide additional information for the analysis. The analysis might also involve the use of automated tools depending on the review scope, requirements and methodology. After evaluation of all collected information, a list of observed risk findings will be reported. For each of the observed risks, appropriate security measures will be determined, implemented and deployed.

22.3 Due to the high demand of expert knowledge and experiences in analysing the collected information and justifying security measures, a security review should be performed by qualified security expert(s).

22.4 IT Security related staff should keep the security policy accessible to all staff, and should be viewed at any time. He/she is also responsible to educate and raise security awareness among staff.

PART 13

CLOUD SERVICE

23. Cloud computing security considerations

23.1 As security boundaries are extended from a school-managed environment to an external untrusted environment of the cloud. Some of the security considerations are:

(a) Feasibility to ensure the security of intellectual property and capital assets;

(b) Upgrade and evaluate the security capabilities to support cloud applications and services;

(c) Effectively manage confidential information and apply security policy; and

(d) Considerations for identity, entitlement, access management, and logging.

23.2 To simplify infrastructure and ease of management, schools are recommended to explore the feasibility of using cloud services (e.g. Microsoft Office 365 - O365 Education, Google Apps for Education - GAFE, etc) without maintaining and operating their own servers.

23.3 Schools should classify the sensitivity of data and consider the potential risk of using cloud services for storage or processing.

23.4 Schools' IT personnel should have regular review and evaluation on the security of cloud services.

23.5 Schools are advised to develop and perform risk assessment to ensure whether cloud computing is currently suitable to meet schools' requirements with an acceptable level of risk, including

(a) Integrity and availability of data;

(b) Availability of services or applications;

(c) Secure data and prevent unauthorized access; and

(d) Escalation and handling of security incident.

23.6 It is important to clarify and ensure the ownership of data when choosing service providers.

23.7 It is advised to evaluate and audit the service provider’s implementation, design, supporting technologies and policy on IT security.

23.8 It is recommended to define and apply data encryption technologies and key management to enforce data security, if necessary.

23.9 It is recommended to consider the identity and access management the service provider can support, e.g. two-factor authentication.

23.10 It is recommended to consider the choice of cloud deployment model with the level of security required. This can manage the risk of unauthorised access to data by a third party.

23.11 Tools of monitoring and management should be used to obtain high visibility of all systems regardless of whether these systems are located locally or in the cloud for integrity checking, compliance checking, security monitoring, access log and network management.

23.12 It is recommended to consider and evaluate the followings items with service provider’s service and handling

(a) Data backup and recovery plan;

(b) Disaster recovery plan;

(c) Data restoration for accidental deletion;

(d) Scalability for system expansion;

(e) Customer segregation for protecting unauthorised access;

(f) Incidents response plan and handling;

(g) Notification of security incident; and

(h) Training, documentation and support.

23.13 It is recommended to consider the requirement of bandwidth of the Internet link and other resources for using the cloud applications and platforms, and make necessary implementation for enforcing the security and performance.

23.14 It is recommended to review and update the requirement of service level agreement with service provider for enforcing the continuous support to schools.

PART 14

Wi-Fi SECURITY QUICK REFERENCE

24. Checklist

The checklist below serves to facilitate schools' consideration of IT security for Wi-Fi system. This acts as supplementary information on top of schools' current IT security policy and implementation. Schools are advised to append and amend the following items based on their actual environment.

Items	Security Consideration & Implementation
Client device access	□ MAC address Authentication □ AD Server Authentication □ Hong Kong Education City accounts Authentication □ Other ___________
Server access	□ Access control □ Zone protection □ Other ___________
External access to school internal resource	□ Number of accessible resources □ DNS record update □ Firewall configuration □ VPN connection □ Other ___________
Connection to other network segments	□ Internet □ Office LAN network □ Others __________
Bandwidth control per session/user	Choose one of the following options □ 10Mbps □ 20 Mbps □ 30Mbps □ Other __________ □ Unlimited

Items	Security Consideration & Implementation
Formation of Security Personnel	Define roles & responsibilities for □ School Head □ IT Head □ IT Committee Members □ Technical Support Staff □ End user
Data Security	□ Access rights management □ System & configuration backup and recovery □ Define steps and procedure for backup and recovery □ Document, test and implement all backup and recovery procedure
Security Policy	□ Preventive, detective, responsive and recovery measures for the occurrence of undesirable event □ User access rights & permission definition and assignment
Wireless security	□ Broadcast / hidden SSID □ Number of SSID □ Wireless security protocol WPA/WPA2/else □ Pre-shared key
Restriction to unsafe / unwanted Internet resources	□ Define unsafe/ unwanted Internet resources □ Implements access control / content filter on firewall or related network devices
Incident Handling	□ Define incident response team, escalation and reporting procedure
Resources & service monitoring	□ Resources (bandwidth, session, response time) monitoring by IT personnel regularly

25. Progress Update

PART	SECTION	Item	Plan & Design	Implement	Review & Update
2	2	Information Security Objectives	□	□	□
2	3	Security Policy	□	□	□
2	4	Security Personnel	□	□	□
2	5	IT Security Functions	□	□	□
3	6	Incident Handling	□	□	□
4	7	Hardware and Software Asset Protection	□	□	□
5	8	Access Control	□	□	□
6	9	Data Security	□	□	□
7	10	Application Security	□	□	□
8	11	Network Protection	□	□	□
8	12	Secure Network	□	□	□
8	13	Communication with External Network	□	□	□
8	14	Virtual Private Network	□	□	□
8	15	Wireless Network Protection	□	□	□
8	16	Protection against Email Spam and Malicious code	□	□	□
9	17	Web Application Security Architecture	□	□	□
10	18	Protecting Mobile Devices	□	□	□
11	19	Anti-Virus Software	□	□	□
11	20	Legal and Authorised Use of Software and Hardware	□	□	□
11	21	Prevention from Doubtful File Resources	□	□	□
12	22	Security Review Procedure	□	□	□
13	23	Cloud Computing Security	□	□	□

PART 15

ADDITIONAL RESOURCES ON IT SECURITY

The following documents are recommended to acquire further information on IT security:

Document Name and Link	Source
Cyber Security Information Portal http://www.cybersecurity.hk/en/index.php	Office of the Government Chief Information Officer (OGCIO)
InfoSec website http://www.infosec.gov.hk/english/useful/links_local.html	Office of the Government Chief Information Officer (OGCIO)
IT Security Policy and Guidelines http://www.ogcio.gov.hk/en/information_security/policy_and_guidelines/	Office of the Government Chief Information Officer (OGCIO)
Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) https://www.hkcert.org/home	Hong Kong Productivity Council

--- END ---