CHAPTER 2
SECURITY MANAGEMENT

2.1 Information Security Objectives

2.1.1 Information is an asset to schools. Information Security refers to the protection of these assets in order to achieve confidentiality, integrity and availability.

2.1.2 When considering confidentiality of information, appropriate measures in IT systems should be implemented to protect the information from being disclosed to unauthorised parties.

2.1.3 When considering integrity of information, appropriate measures in IT systems should be implemented to protect information from being changed by unauthorised parties.

2.1.4 When considering availability of information, appropriate measures in IT systems should be implemented to ensure the availability of information to authorised parties only when requested. 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 objectives according to security levels.
   (e) Identify any potential risks, and determine corresponding information security level.

2.2 Security Policy

2.2.1 Only authorised person is allowed to access, possess, view, modify, delete, copy and publish information stored in the systems.

2.2.2 When implementing security measures, the following practices are recommended:
   (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 respond to an undesirable event.
(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 vulnerabilities regularly, and take immediate action, if necessary.

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

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

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

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

(a) Design and apply security controls and policies to all boundaries between trusted and untrusted areas.

(b) Define and review security controls and policies for entire system as a whole.

(c) Adopt appropriate security measures for school’s IT environment.

2.3 Security Personnel

2.3.1 Proper segregation of duties, in terms of technical, operational and managerial roles should be defined.

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

2.3.3 Roles and responsibilities should be designed and assigned to stakeholders. Suggested roles and responsibilities of school personnel are as follows:

(a) **School Head** is responsible for:

   - Directing and enforcing the development of security measures.
   - Providing the necessary resources required for the measures to be implemented.
   - Ensuring participation and support at all levels of management, administrative, technical and operational staff.
   - Aligning the security strategies with schools’ objectives with regular review and update.
(b) **IT Head** is responsible for:

- Incharge of the entire campus IT environments, including design, strategic planning, and implementation, and is expected to have IT and security knowledge.
- Leading the establishment, maintenance and implementation of IT security policies, standards, and procedures.
- Disseminating security alerts on impending and actual threats from the professional IT security institutions to responsible parties.
- Ensuring information security risk assessments and audits are performed as necessary.
- Initiating investigations and rectification in case of breach of security.
- Managing and handling incidents of IT security of the entire campus systems and networks.
- Granting authorisation and approval to concerned parties or persons for management and handling critical incidents.
- Defining and maintaining disaster recovery plan with regular verification.
- Providing management endorsement on the provision of resources for the incident handling process.
- Reporting information security incidents for central recording and necessary follow up actions.
- Facilitating experience and information sharing within the school on information security incident handling and related matters.

(c) **IT Committee Members** are responsible for:

- Management of the information systems.
- Assisting IT Head in the implementation, administration, maintenance and operation.
- Managing and estimating resources in operation.
- Ensuring the implementation of IT policies in school systems and networks.
- Evaluating and advising on technologies, IT and security solutions to IT Heads.
- Defining security requirements and policies with implementation plan for information security.
• Collecting views from colleagues on their feedback to the policy.

(d) **Technical Support Staff** are responsible for:

• Daily operation and maintenance.
• Assisting IT Head in the implementation, administration, maintenance and operation.
• Performing monitoring to ensure the availability of system and services.
• Handling fault cases and escalating them to concerned parties.

(e) **End Users** (including teachers, students and staff) can use the services and data in the information system. An end user should be responsible for:

• Knowing, understanding, following and applying security mechanisms.
• Preventing leakage and unauthorised access to information.
• Safely keeping computing and storage devices, and protecting them from unauthorised access or malicious attack.
• Reporting any abnormal incident or fault case.

### 2.4 IT Security Functions

#### 2.4.1 Recommended practices for user:

(a) Should not log on the school applications from public computers and avoid handling personal or sensitive information when using public WiFi. Furthermore, clear all history, cookies, temporary files, data files, account names and passwords from the public computer once finished.

(b) Should not leave their workstations and computer equipment unattended.

#### 2.4.2 Recommended practices for maintaining IT equipment:

(a) Keep IT equipment, including hardware and software in a safe place against unauthorised access.

(b) Enable password-enabled screen saver to prevent illegal system access attempts.

(c) Do not use de-supported operating systems.

(d) Do not directly connect IT equipment to external networks by means of dial-up modem, wireless interface or broadband link.

(e) Enable encryption feature in the data transmission of wireless or mobile devices.
2.4.3 Recommended practices for access control:

(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 systems 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 information security requirements, policies and security responsibilities.
(g) Promptly terminate any ceased account.

2.4.4 For data security, implementation of measures like provision of advanced hard disk sub-system and UPS could be considered. Recovery plan using backup and recovery process should be implemented. The related recommended practices are as follows:

(a) Handling of data
   - Grant the access right based on a need-to-know basis.
   - Develop proper “system backup and recovery” strategies for restoring corrupted or accidentally deleted data.
   - Define the steps and procedures to backup and recover all data with minimal human interaction.
   - Document, test and implement all backup and recovery procedures.

(b) Anti-malware, Security Patches and Software Management
   - Apply the latest security patches and regularly remove cache files and temporary files to protect data privacy.
   - Install anti-malware detection measures with latest definition files in the computers of the school and perform virus scan including emails, downloaded files, files in removable media or mobile devices before use.
   - Do not install point-to-point (P2P) file sharing and unauthorised software in the computer of schools.
   - Avoid storing unnecessary 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.
• Set up a remote data wiping feature, if available.
(c) Deploy firewall to control and safeguard the traffic among various inter-connected networks like LANs and WebSAMS.

2.4.5 Recommended practices for security audit and incident handling:
(a) Enable activity logs for events and threats tracking.
(b) Periodically monitor and review activity logs of school systems and networks.
(c) Define and publish procedures and contact points to users for suspicious event escalation.

2.4.6 Recommended practices for implementing security awareness education:
(a) Educate end users the importance of security awareness.
(b) Provide well-conceived and committed security education programmes to users.

2.4.7 Schools should be aware of the fact that systems with few security controls are generally more vulnerable than those with many. A balance can be strived between the need for security versus the desire to stay within available resources.