CHAPTER 4
PHYSICAL SECURITY

4.1 Meaning of Physical Security

4.1.1 Physical security refers to the protection of hardware, computer equipment, and other IT assets from external physical threats, such as unauthorised access, theft, or loss of backup media during transportation to external sites.

4.2 Site Preparation in School

4.2.1 As most of the critical IT equipment are normally housed in server room or computer room, careful site preparation of the server room or computer room is important. Schools are recommended to:

(a) Assess the security risks in the school site to ensure that sufficient security controls are in place to protect the school's data.

(b) Evaluate the physical feasibility of the environment including the following aspects before building a server room or computer room:

- Site selection and accommodation planning
- Power supply and electrical requirement
- Air conditioning and ventilation
- Fire protection, detection and suppression
- Water leakage and flood control
- Physical entry control

4.2.2 For better security and easier management, schools are recommended to define different access permissions for different zones within a school. Generally three different zones could be defined:

(a) Public zone: (Example: Hallway)

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

(b) Protected zone: (Example: School Office, Staff and Principal Room)

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

(c) Restricted zone: (Example: Server Room)

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

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

4.3 Computer Hardware and Software Assets Protection

4.3.1 Hardware inventory: Keep an updated inventory list of your school's computer hardware facilities including details of all component items. The inventory should include information like CPU, RAM, hard disk capacity, monitor size, etc. It is also useful to specify related service information like warranty expiry dates, serial numbers, service contracts and contacts, etc. A policy should also be established to prevent staff from removing any computer equipment without prior approval.

4.3.2 Software inventory: Keep an updated software inventory list. Schools must ensure that enough licences have been acquired for the software and remind staff not to install their own software. Shareware should be removed before the evaluation period expires. Schools should pay attention to the fact that some licences appear in the form of a licence number on a small label. In any case, schools must store them in a safe location. In accordance with the Copyright Ordinance, it is school's responsibility to make sure no illegal unlicensed software is used.

4.3.3 Disposal of computer equipment: Uninstall all programs and erase all data, if applicable, before disposing any piece of hardware.

4.3.4 Physical security of computer equipment: Physical protection of schools' computer equipment is important. Like any other valuable asset, schools could consider using the following tools or methods to protect computer equipment physically:

(a) Workstation / Computer Room Protection:

- Lock computers with security chains
- Self-closing doors
- Window and door locks
- Lockable internal doors between rooms
- Security curtains or window shutters
- Alarms (ensure that each employee has his/her own unique alarm code)

(b) Server and Network Device Protection

- Keep your servers and network devices in a locked room or cabinet
- Disconnect any unused network connections
- Dedicated power supply circuit and uninterruptible power supply (UPS) should be made available for the server room
- Implement fire and flooding alarming systems. Hand-held fire extinguishers should be in strategic locations in the computer area, tagged for inspection and inspected at least annually
- Make sure there is enough ventilation and air conditioning for your servers
- Arrange regular maintenance and testing for all service utilities such as air conditioning equipment, fire prevention and detection systems and standby power supplies

(c) Mobile Device Protection

- For IT equipment such as mobile devices and removable media, schools should keep an authorised equipment list and periodically perform inventory check for the status of such IT equipment. When mobile devices are not in use, they must be placed inside lockable cabinets (e.g. the notebook cabinet in server room, and/or the desk cabinet of the corresponding teacher in staff rooms).

- Staff in possession of mobile device or removable media for any purposes shall safeguard the equipment in his/her possession, and shall not leave the equipment unattended without proper security measures.

(d) Software Copies, Storage and Backup Media

- The original and backup copies of software programmes and data files should be kept secured.
- Schools are reminded to protect their data by making backups regularly.
- Store the backup media in a secure and safe location especially for media containing sensitive or mission-critical information.
- Schools should consider keeping the backup copies offline and in a separate location with a safe distance from the original copies.
- Schools should define security measures for handling various storage media such as magnetic, optical, and flash memory devices. Storage media with sensitive data should be locked in secure areas.
- It is risky to store data to mobile device and removable media as they are small and can be easily lost or stolen. To minimise the risk of data leakage, only devices with encryption feature suitable to protect classified data should be used.
- Access to the backup media should only be done via authorised persons according to the established mechanism. Unauthorised access to the media library or storage room should not be allowed.

4.3.5 A list of persons who are authorised to gain access to server rooms, computer rooms or other areas supporting critical activities, where computer equipment and data are located or stored, should be kept up-to-date and be reviewed periodically.

4.3.6 All access keys, cards, passwords, etc. for entry to any of the information systems and networks should be physically secured or subject to well-defined and strictly enforced security procedures. All visitors to server rooms or computer rooms should be monitored at all times by authorised staff. A visitor access record should be properly maintained for audit purpose.