CHAPTER 5
ACCESS CONTROL

5.1 Significance of Access Control

5.1.1 Users should always be granted access rights to school's information on a need-to-know basis. This is to avoid the security risks of unauthorised access to sensitive information, sabotage of information as well as breaking the law of the Personal Data (Privacy) Ordinance.

5.2 Requirements of Access Control

5.2.1 Schools are recommended to ensure that the least privilege principle is followed when assigning resources and privileges of information systems to users as well as technical support staff. This includes restrict a user's access (e.g. to data files, to IT services and facilities, or to computer equipment) or type of access (e.g. read, write, execute, delete) to the minimum necessary to perform his or her duties.

5.2.2 Information owners should determine appropriate access control rules, access rights and restrictions for specific user roles on their information. Access to information should not be allowed unless authorised by the relevant information owners. The rules should be reviewed from time to time and at least annually especially right before the start of a new school year where there usually has changes in people in subjects and functional committees.

5.2.3 Access to information systems containing classified or sensitive information should be restricted by means of logical access control. Logical access control refers to the controls to IT resources other than physical access control such as restricted access to the physical location of the system. In general, logical access control refers to four main elements: users/groups of users, resources, authentication and authorisation.

(a) Users / groups of users refer to those people who are registered and identified for accessing the IT resources.

(b) People will be granted with rights to access the system resources such as network, files, directories, programs and databases.

(c) Authentication is to prove the identity of a user. Usually, it is done based on three major factors, namely something you know (e.g. PIN or username / password), something you have (e.g. a token or a smart card) or something you are (e.g. biometrics characteristics such as fingerprint, facial characteristics, retina of eye and voice). A combination of two of these factors, often called two-factor authentication, can be applied to strengthen the authentication control.

(d) Upon user authentication, authorisation to access will be granted by mapping the user / group of users to the system resources.

5.3 User Access Management

5.3.1 Access rights to information should be granted on a need-to-know basis and should be clearly defined, documented and reviewed periodically.

5.3.2 For accounts or user access with privileged access rights such as administrator or system account, the following should be considered to restrict and control the use:

(a) Special privileges and data access rights associated with each system or application, and the users to whom they need to be allocated should be identified.

(b) Special privileges and data access rights should be granted to users based on the principle of least privilege and segregation of duties.

(c) Special privileges and data access rights should be granted to a user ID different from those used for regular business activities.

(d) Regular business activities should not be performed by privileged IDs.

(e) Specific procedures should be established to avoid the unauthorised use of default administration user IDs.

5.3.3 All user privileges and data access rights, including temporary and emergency access, should be revoked after a pre-defined period of inactivity.

5.3.4 User privileges and data access rights should be revoked when they are no longer required, e.g. upon a staff's termination of employment or change of employment. Documentation which identifies user privileges and data access rights should be updated to reflect the removal or adjustment of access rights. If the staff has known passwords for user IDs which will remain active, these passwords should be changed upon termination or change of their employment.

5.3.5 User privileges and data access rights may be granted on a group basis instead of individual basis, e.g. group access list. Schools should remove the departing staff from the corresponding group access lists as well as inform relevant parties not to share any information with the departing staff.

5.3.6 Individual accountability should be established so that the respective staff is responsible for his or her actions.

5.3.7 Shared or group user-IDs is not recommended.

5.3.8 Schools should educate users about the importance of information security and always remind them of security best practices.

5.4 User Responsibilities

5.4.1 Users should only use their user-IDs to perform authorised tasks and functions.

5.4.2 Passwords are not recommended to be shared or divulged unless there is a measure of determining user identification to enforce user accountability. If passwords need to be shared, schools should justify the usage of shared passwords against the security risks that a system may expose to. Also, the shared passwords should be reset immediately when no longer used and should be changed frequently if sharing is required on a regular basis to minimise the risk of security breaches.

5.4.3 Passwords should always be well protected. When held in storage, security controls such as access control and encryption should be applied to protect passwords and when transmitting over an un-trusted communication network. If password encryption is not implementable, schools should implement compensating controls such as changing the password more frequently.

5.5 System and Application Access Control

5.5.1 Schools should ensure that their information systems are implemented with appropriate authentication mechanisms and measures that are commensurate with their security requirements and the sensitivity of the information to be accessed.

5.5.2 Depending on the level of security control required, one simple way of authentication is to use password. Another way to perform authentication is to use two-factor authentication such as smart cards or tokens.

5.5.3 The following measures can help reduce the possibility of passwords being compromised by password guessing activity such as brute-force attack:

(a) Consecutive unsuccessful log-in trials should be controlled and the number of log-in trials, account lock-out duration and lock-out timer reset duration should be defined and enforced. This can be accomplished by disabling account upon a limited number of unsuccessful log-in attempts.

(b) The mechanism of increasing the time delay between each consecutive login attempt may also be considered to prevent password guessing activity.

(c) User access log analytic tools may be used together with central log server for maintaining the integrity of log records, monitoring user access activities, and facilitating incident investigation.

5.5.4 Schools should carefully define and document password policy for each category of accounts balancing the security requirements and operational efficiency. Some suggestions are as follows:

(a) The password policy should be enforced for all information systems.

(b) The password policy should at least include minimum password length, initial assignment, restricted words and format, password life cycle, and a good set of rules for password selection.

(c) Schools should use strong passwords (e.g. at least eight characters with mixed-case alphabetic characters, numerals and special characters), in combination with controls such as password history (e.g. eight passwords remembered), account lockout (e.g. after five invalid logon attempts) and regular password change (e.g. every 90 days).

5.5.5 All users are prohibited from capturing or otherwise obtaining passwords, decryption keys, or any other access control mechanism, which could permit unauthorised access.

5.5.6 All default passwords should be changed before any information system is put into operation. Also, all passwords should be promptly changed if they are suspected of/are being compromised.

5.6 Mobile Computing and Remote Access

5.6.1 Please refer to "Chapter 9 – Mobile Device and Mobile Application Protection" for details.