Information Security in Schools – Recommended Practice

• Since 2002, the EDB has been providing recommended practice on IT security to assist schools in formulating IT security policies and promoting related good practices.

• The EDB updates the document from time to time (last updated version issued in January 2019).

• Under the principle of school-based management, schools are responsible for taking appropriate IT security measures to protect the IT systems and data of their schools, and they may determine their own requirements to adopt the practice where applicable to their own environment and operational needs.

• Schools could adopt different technical solutions.
School satisfaction of current IT security situation

Suggested improvement by schools:
(a) Network security e.g. firewall setting and update
(b) Cloud backup
(c) Data privacy
(d) Teachers and students consciousness on IT security
(e) Technical support on IT security

89.2% 10.8%

Source: ITE Annual Survey 2018/19 School Year
Security Threats in Schools

Ransomware 71%
Virus Infection 11%
Cyber Attack (e.g. hacking / DDoS / Port Scanning etc.) 9%
Website Defacement 5%
Phishing Email & Spam Email 4%

Source: ITE Annual Survey 2018/19 School Year
Information Security in Schools – Recommended Practice (September 2019)


TABLE OF CONTENT

CHAPTER 1    ABOUT THIS DOCUMENT
CHAPTER 2    SECURITY MANAGEMENT
CHAPTER 3    SECURITY INCIDENT HANDLING
CHAPTER 4    PHYSICAL SECURITY
CHAPTER 5    ACCESS CONTROL
CHAPTER 6    DATA SECURITY
CHAPTER 7    NETWORK AND COMMUNICATION SECURITY
CHAPTER 8    WEBSITE AND WEB APPLICATION SECURITY
CHAPTER 9    MOBILE DEVICE AND MOBILE APPLICATION PROTECTION
CHAPTER 10   MALWARE PROTECTION
CHAPTER 11   CLOUD SERVICE
CHAPTER 12   RESOURCES OF REFERENCE ON IT SECURITY

This document is written for schools' reference in protecting their information and IT assets when implementing e-learning. Schools are responsible for taking 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 and adopt the practices 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 Chapter 12 “Resources of Reference on IT Security” of this document, to protect their IT assets.
Major Updates

2019 January Version

CHAPTER 1 ABOUT THIS DOCUMENT
CHAPTER 2 SECURITY MANAGEMENT
CHAPTER 3 SECURITY INCIDENT HANDLING
CHAPTER 4 PHYSICAL SECURITY
CHAPTER 5 ACCESS CONTROL
CHAPTER 6 DATA SECURITY
CHAPTER 7 APPLICATION SECURITY
CHAPTER 8 NETWORK AND COMMUNICATION SECURITY
CHAPTER 9 WEBSITE AND WEB APPLICATION SECURITY
CHAPTER 10 MOBILE DEVICE AND MOBILE APPLICATION PROTECTION
CHAPTER 11 MALWARE PROTECTION
CHAPTER 12 SECURITY REVIEW
CHAPTER 13 CLOUD SERVICE
CHAPTER 14 ADDITIONAL RESOURCES ON IT SECURITY

2019 September Version

CHAPTER 1 ABOUT THIS DOCUMENT
CHAPTER 2 SECURITY MANAGEMENT (Updated)
CHAPTER 3 SECURITY INCIDENT HANDLING (Updated)
CHAPTER 4 PHYSICAL SECURITY (Updated)
CHAPTER 5 ACCESS CONTROL (Updated)
CHAPTER 6 DATA SECURITY (Updated)
CHAPTER 7 NETWORK AND COMMUNICATION SECURITY
CHAPTER 8 WEBSITE AND WEB APPLICATION SECURITY
CHAPTER 9 MOBILE DEVICE AND MOBILE APPLICATION PROTECTION
CHAPTER 10 MALWARE PROTECTION
CHAPTER 11 CLOUD SERVICE
CHAPTER 12 ADDITIONAL RESOURCES ON IT SECURITY

*Those chapters/items highlighted in green are with substantial revisions.
Major Updates – Chapter 2
SECURITY MANAGEMENT

2019 January Version
- Information Security Objectives
- Security Policy
- Security Personnel
- IT Security Functions

2019 September Version
- Introduction to Information Security
- Security Management Cycle
- Assessing Security Risks
- Implementing and Maintaining a Secure Framework
  - Set up and Implement a Security Policy
  - Set up and Implement Management and Administrative Processes
  - Select and Implement Technological Measures
- Monitoring and Recording
- Reviewing and Improving
  - Security assessment
  - Security audit
Major Updates – Chapter 2
SECURITY MANAGEMENT

• Introduction to Information Security
• Security Management Cycle
• Assessing Security Risks
• Implementing and Maintaining a Secure Framework
• Monitoring and Recording
• Reviewing and Improving
Major Updates – Chapter 3
SECURITY INCIDENT HANDLING

2019 January Version
• Checklist
  ➢ Establish an IT Security Incident Response Team
  ➢ Escalation procedure
  ➢ Security incident response procedure
  ➢ Reporting procedure
  ➢ Training and education

2019 September Version
• What is an Information Security Incident?
• Objectives of Security Incident Handling
• Steps for Security Incident Handling
• Training and Education
Major Updates – Chapter 3
SECURITY INCIDENT HANDLING

• What is an information security incident?
• Objectives of Security Incident Handling
• Steps for Security Incident Handling
• Training and Education
  ➢ School-based policy and guidelines
  ➢ EDB professional training programmes / seminars
    e.g. Training programmes by ITE Section
  ➢ EDB website / email notifications
    e.g. Information Security in Schools by ITE Section
    https://www.edb.gov.hk/ited/i-security
  ➢ HKCERT news / notifications / alerts
  ➢ Security reports
Major Updates – Chapter 4
PHYSICAL SECURITY

2019 January Version

• Hardware and Software Asset Protection
  ➢ **Recommended practices for server room protection**
  ➢ **Recommended practices to secure mobile devices**
  ➢ **Recommended practices to handle software copies and backup device / media**
  ➢ **Recommended practices for performing property marking and inventory taking**

2019 September Version

• **Meaning of Physical Security**
• **Site Preparation in School**
• **Computer Hardware and Software Assets Protection**
  ➢ **Workstation / Computer Room Protection**
  ➢ **Server and Network Device Protection**
  ➢ **Mobile Device Protection**
  ➢ **Software Copies, Storage and Backup Media**
Major Updates – Chapter 4
PHYSICAL SECURITY

• Meaning of Physical Security
• Site Preparation in School
• Computer Hardware and Software Assets Protection
## Major Updates – Chapter 5
### ACCESS CONTROL

**2019 January Version**

- Access Control
  - Recommended practices for the authentication and authorisation to prevent unauthorised access
  - Recommended practices or administration of user accounts including (Third Party)
  - Recommended practices for performing user and access rights assignment

**2019 September Version**

- Significance of Access Control
- Requirements of Access Control
- User Access Management
- User Responsibilities
- System and Application Access Control
- Mobile Computing and Remote Access
Major Updates – Chapter 5
ACCESS CONTROL

• Significance of Access Control
• Requirements of Access Control
• User Access Management
• User Responsibilities
• System and Application Access Control
• Mobile Computing and Remote Access
## Major Updates – Chapter 6
### DATA SECURITY

<table>
<thead>
<tr>
<th>2019 January Version</th>
<th>2019 September Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Security</td>
<td>• Information Classification</td>
</tr>
<tr>
<td>• Some general data backup and recovery practices</td>
<td>• Cryptography</td>
</tr>
<tr>
<td>• Recommended practices for protecting sensitive data</td>
<td>• Backup</td>
</tr>
<tr>
<td>• Disposing old computer equipment or media containing non-volatile data</td>
<td>• Personal Data (Privacy)</td>
</tr>
<tr>
<td>• Personal Data (Privacy) Ordinance</td>
<td>• Information Erasure</td>
</tr>
<tr>
<td></td>
<td>• Promotion of Security Awareness of the Data Security Requirements</td>
</tr>
</tbody>
</table>
Major Updates – Chapter 6
DATA SECURITY

• Information Classification
• Cryptography
• Backup
• Personal Data (Privacy)
• Information Erasure
• Promotion of Security Awareness of the Data Security Requirements
Some Security Tips

• Schools should incorporate security management in the school policy.
• Schools are recommended to develop school-based security policy and assign roles and responsibilities to stakeholders. Also, the security policy should be reviewed annually.
• Schools should define school-based security incident handling procedures and disseminate to all stakeholders.
• Schools should provide training and sharing on the latest security trends to all stakeholders.
• Schools should disable the port 3389 (RDP) to prevent unauthorised attack.
• There are security vulnerability in WPA2, schools are recommended to deploy network device with WPA3 when upgrading the Wi-Fi network.
For schools adopting the Integration Mode of WiFi networks

• It is recommended to build the WiFi network completely separated from schools’ existing network with separate broadband line to reduce security risk in the coming WiFi services contract renewal exercise.

• Due to the nature of wireless technology, wireless networks are relatively hard to contain within a building and it is generally considered to be an un-trusted network.

• As a best practice, wireless networks and wired networks should not be directly connected to each other.

(Please refer to Section 7.2.4 of Chapter 7 for details)
IT Security Measures to address the Security Concerns on Integrating the Networks

• Schools’ IT personnel needs to assess, understand and eliminate the security issues and risks to school existing network when the WiFi network is integrated or connected to schools’ existing network.

• Schools adopting the integration mode of WiFi networks are recommended to apply the “Defence-in-Depth” approach.

• Possible measures that can be employed to build multiple layers of defense:
  - Separation of wireless and wired network segments
  - Use of strong device and user authentication methods
  - Application of network filtering based on addresses and protocols
  - Deployment of intrusion detection systems on the wireless and wired networks

(Please refer to Section 7.2.5 of Chapter 7 for details)
Related Promotion and Support by EDB

• Webpage of Information Security in Schools
  https://www.edb.gov.hk/ited/i-security

• Email Message on IT Security Alert

• Information Security in Schools – Recommended Practice

• Co-organise with professional bodies and schools to provide IT security related seminars / workshops (6 events planned for 2019/20 s.y. and this seminar will also be rerun)

• Promote IT security related events / activities through school circular memorandum

• Professional development programmes (PDP) in Information Literacy
  https://www.edb.gov.hk/il/eng

• Grants
Overview of Various ITE Grants

Recurrent

Composite IT Grant (CITG)
-$209,367 – 720,089$ dependent on school type and size
Operational needs for e-learning, such as -
- IT-related consumables
- Digital resource materials
- Technical Support Staff (TSS)
- Maintenance of IT facilities, etc.

Funding for ITE4
-$70,000$ on average
- WiFi services fee
- Maintenance/replacement of mobile devices

ITSSG
- Flat rate of $317,338
- Recruitment of TSS through contract or services procurement

One-off

ITE4 ($100,000$ on average)
- Mobile devices

Extra One-off IT Grant ($200,000$ on average)
- Mobile devices
- Recruitment of TSS
- E-resource/platform
Promote IT security related events / activities through school circular memorandum


Thank you