Information Security in Schools—Recommended Practice (January 2019)

IT in Education Section
Education Bureau
15 January 2019
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.
Information Security in Schools – Recommended Practice (January 2019)

## Major Updates

### 2016 Version

- PART 1 ABOUT THIS DOCUMENT
- PART 2 SECURITY MANAGEMENT
- PART 3 SECURITY INCIDENT HANDLING
- PART 4 PHYSICAL SECURITY
- PART 5 ACCESS CONTROL
- PART 6 DATA SECURITY
- PART 7 APPLICATION SECURITY
- PART 8 NETWORK AND COMMUNICATION SECURITY
- PART 9 WEB APPLICATION SECURITY
- PART 10 SECURITY ISSUES OF MOBILE APPLICATIONS
- PART 11 COMPUTER VIRUS PROTECTION
- PART 12 SECURITY REVIEW
- PART 13 CLOUD SERVICE
- PART 14 WI-FI SECURITY QUICK REFERENCE
- PART 15 ADDITIONAL RESOURCES ON IT SECURITY

### 2019 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 & 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
Major Updates – Chapter 8
Network and Communication Security

2016 Version

- General Network Protection
- Building a Secure Network
- Communication with External Network
  - Remote Access
- Virtual Private Network
- Wireless Network Protection
  - Management Control
  - Technical Control
  - End-user Control
- Protection against Email Spam and Malicious code
  - System Prospective
  - End-user Prospective
  - Prevent Malicious Code (Merge to Chapter 11)

2019 Version

- Network Security Management (Revised)
  - Recommendations for schools on building a secure network
  - Remote Access
  - Virtual Private Network
- Wireless Network Build Up Security Concerns (New)
  - Security Risks
  - Recommendations for schools on wireless network deployment
  - Network Mode (Separate / Integrate)
- Security Controls to Protect WLAN (Revised)
  - Management Control
  - Technical Control
  - End-user Control
- Mail Gateway Security and Email Handling
  - Mail Server Protection (Revised)
  - Tips for protecting schools from email bombing, spamming and spoofing (New)
  - Reduce the amount of incoming spam (Revised)
  - Protection against Email Scam (New)
Major Updates – Chapter 8
Network and Communication Security

• Security concerns on the communication with the external network and access privilege.
• Protection against the system and end-user strengthened.
• Email Bombing, Spamming & Spoofing and Email Scam.
• Security concerns on the network modes (Separate / Integrate) adopted by schools.
Separate or Integrate?

• It is recommended to build the WiFi network completely separated from schools’ existing network with separate broadband line to reduce security risk.

• 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.
IT Security Measures to address the Security Concerns on Integrating the Networks

• For schools adopting the integration mode of WiFi 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
Major Updates – Chapter 9
Website & Web Application Security

2016 Version

WEB APPLICATION SECURITY
  • Adopt Web Application Security Architecture
    • Architecture
    • Web Server Security

2019 Version

WEBSITE & WEB APPLICATION SECURITY
  • Website & Web Application Security Architecture
  • Web Server Security (Revised)
  • Web Server Monitoring and Incident Handling (New)
  • Web Application Security (New)
  • Keep Your School’s Website Safe (New)
  • Secure Website with HTTPS Protocol (New)
  • Anti-DDoS Protection (New)
Major Updates – Chapter 9  
Website & Web Application Security

• Important of web server security such as account management, web server application management, ports management, patch management, security monitoring, backup.

• Web application security and data protection.

• HTTPS issue.

• How to prevent DDoS / Botnet attack.

• For better security incidents handling, schools are recommended to:
  • Follow the security incident handling procedure to handle the security incident until it is mitigated; and
  • Report the case to Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and Hong Kong Police Force (HKPF).
# Major Updates – Chapter 10
## Mobile Device and Mobile Application Protection

<table>
<thead>
<tr>
<th>2016 Version</th>
<th>2019 Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY ISSUES OF MOBILE APPLICATIONS</td>
<td>MOBILE DEVICE AND MOBILE APPLICATION PROTECTION (New)</td>
</tr>
<tr>
<td>• Protecting Mobile Devices</td>
<td>• Security Concerns of Mobile Devices</td>
</tr>
<tr>
<td>• Configuration Mobile Device</td>
<td>• Information Security Policy for Mobile Devices</td>
</tr>
<tr>
<td>• Precautions of Using Mobile Applications</td>
<td>• Data Communication and Storage for Mobile Devices</td>
</tr>
<tr>
<td></td>
<td>• User and Device Authentication for Mobile Devices</td>
</tr>
<tr>
<td></td>
<td>• Security Control for Mobile Device Application</td>
</tr>
<tr>
<td></td>
<td>• Mobile Device Management (MDM) Solution</td>
</tr>
</tbody>
</table>
Major Updates – Chapter 10
Mobile Device and Mobile Application Protection

• Schools should establish a mobile device security policy to specify the operation and security requirements for mobile devices access.

• A formal usage policy and procedures should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

• Schools are recommended to install security control tools such as MDM, anti-malware software.
## Major Updates – Chapter 11
### Malware Protection

<table>
<thead>
<tr>
<th>2016 Version</th>
<th>2019 Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMPUTER VIRUS PROTECTION</strong></td>
<td><strong>MALWARE PROTECTION (New)</strong></td>
</tr>
<tr>
<td>- Anti-Virus Software</td>
<td>- Protection against Malware by Schools</td>
</tr>
<tr>
<td>- Legal and Authorised Use of Software and Hardware</td>
<td>- Protection against Malware by Users</td>
</tr>
<tr>
<td>- Prevention from Doubtful File Resources</td>
<td>- Malware Incident Handling and Recovery</td>
</tr>
<tr>
<td></td>
<td>- Protection against Ransomware</td>
</tr>
<tr>
<td></td>
<td>- Ransomware Incident Handling and Recovery</td>
</tr>
</tbody>
</table>
Major Updates – Chapter 11
Malware Protection

• Malware can cause different level of security risks to computer assets, such as disrupt computer operations, gather sensitive information, etc.

• Schools are advised to adopt the precaution measures against ransomware.

• Ransomware Incident Handling:
  a) **Disconnect** the network cable of the computer to avoid affecting network drives and other computers.
  b) **Power off** the computer to stop the ransomware encrypting more files.
  c) **Jot down** what have been accessed (such as programs, files, emails and websites) before discovering the issue.
  d) **Report** to the HKCERT and HKPF the criminal offence if necessary.
  e) **Recover** the data from backup to a clean computing device.
<table>
<thead>
<tr>
<th>2016 Version</th>
<th>2019 Version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CLOUD SERVICE</strong></td>
<td><strong>CLOUD SERVICE (New)</strong></td>
</tr>
<tr>
<td>• Cloud computing security considerations</td>
<td>• Cloud Security Overview</td>
</tr>
<tr>
<td></td>
<td>• Cloud Service Security Consideration</td>
</tr>
<tr>
<td></td>
<td>• Checklist on selecting cloud service provider</td>
</tr>
<tr>
<td></td>
<td>• On using cloud services</td>
</tr>
</tbody>
</table>
Updates – Chapter 13
Cloud Service

• A checklist on selecting cloud service provider was provided to schools for reference.
• Using encryption to protect stored data.
• Think twice when you want to store sensitive data in the cloud and assess the impact if the data concerned is exposed.
• Perform a regular backup of the data stored in the cloud service and maintain a local backup copy of important data so that this data can still be available when the service provider is out of service.
Security Tips

• TSS or IT Head should harden the firewall regularly including update firmware, review policy and check event log.

• Cyber attack are become more advance and unpredictable. Schools are recommended to deploy security device with the latest technology to secure the school’s network.

• Many schools were infected ransomware by opening attachments in suspicious email. Schools are recommended to purchase the latest anti-malware software with signature to filter the malicious attachment.

• There were security vulnerability in WPA2, schools are recommended to deploy network device with WPA3 when upgrading the Wi-Fi network.

• Apply latest approved security patches to any software (especially the operating system) and avoid using the end of supported components.
Related Promotion and Support by EDB

- Information Security in Schools webpage
- Email Message on IT Security Alert
- Information Security in Schools – Recommended Practice
- Co-organise with professional bodies to provide IT security related seminars
- Promote IT security related events / activities through school circular memorandum
- Grants
Overview of Various ITE Grants

**Recurrent**

**Composite IT Grant (CITG)**

- $202,679 – 697,086 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 $307,200
- 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
Information Literacy

https://www.edb.gov.hk/il/eng

Information Literacy for Hong Kong Students

Introduction

Information technology (IT) is a powerful tool to unleash the learning capability of students. With the advancement of technology and its application through innovative pedagogies in all KLAS, students’ capability in information literacy (IL), self-directed learning and other 21st century skills such as creativity, problem solving skills, collaboration skills and computational thinking skills are enhanced. Strategies on IT in Education are formulated at various stages to enable students to learn and excel through realizing the potential of IT in enhancing interactive learning and teaching experiences.

As an important competency, IT helps students identify the need for information, locate, evaluate, extract, organise and present information; create new ideas; cope with the dynamics in our information world; use information ethically, as well as refrain from immoral practices such as cyber bullying and infringing intellectual property rights. IL could be developed through the application of the generic skills (see Section 2.3.1 and Appendix 1 of this booklet) in the context of handling information in different media in our information world. This also involves various knowledge contexts and has close linkage with the KLAS.

Schools can make reference to the “Information Literacy for Hong Kong Students” for suggestions on how to develop students’ knowledge, skills and attitudes to use information and information technology ethically and effectively as responsible citizens and lifelong learners. Incorporation of IL in the whole-school curriculum will provide authentic contexts for students to apply the skills and benefit their learning in relevant KLAS.
Promote IT security related events / activities through school circular memorandum


EDBCM No.164/2018 Cyber Security Campaign – Smart Devices Security

https://www.cybersecuritycampaign.com.hk/
Thank you