Policies and Framework for Privacy and Information Security in School

25 September 2019
Information Security Management System

- Based on ISO 27001
  - (US : NIST)

- Describe “organised approach” – whole school

- Based on Risk Management

- Address Confidentiality, Integrity and Availability

- Anchor on:
  - People, Process, IT System

ISMS Key Issues

- Risk Management
- Information Security Policy
  - Roles and Responsibilities
  - Controls, Technical Implementation
  - Guidelines, Procedures
Information Security Management Cycle

- Security Policy
- Roles and Responsibilities
- Security Controls

## Risk Assessment – School Example

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Data</td>
<td>Accounting</td>
<td>Network / WiFi</td>
</tr>
<tr>
<td>Teacher / HR Data</td>
<td>Payroll</td>
<td>School email system</td>
</tr>
<tr>
<td>Exam papers</td>
<td>Exam Grades / Assessment Data</td>
<td>Admin / Learning Systems</td>
</tr>
</tbody>
</table>
## Risk Registry

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Data</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Payroll Data</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Exam papers</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Attendance Record</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Description</td>
<td>Storage</td>
<td>Processing and I/O</td>
<td>Transmission</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Student Data</td>
<td>eClass server, WebSAMS, Cloud Storage Backup, USB, Paper Document</td>
<td>Excel, Server, Paper Form Filling</td>
<td>School network, public network, Email, File sharing, Paper mails</td>
</tr>
<tr>
<td>Exam papers</td>
<td>Teacher Personal Storage School Server</td>
<td>MS Office Other editing tools Grading Tools</td>
<td>LAN only, Paper distribution</td>
</tr>
</tbody>
</table>
Related Legislations

- Theft and damage of property (digital assets)
- Personal data protection
- Copyright / IP rights
- Software Asset Management
- Digital marketing and unsolicited electronic messages
- Electronic Transactions Ordinance
- Safety in the use of Display Screen Equipment
Policies, Standards, Guidelines, Procedures

Policies
- Principles, intentions, directional
- Clearly defines AUTHORITIES, ROLES and RESPONSIBILITIES

Standards
- Compliance – data centre, encryption

Guidelines
- More detail description to guide operation

Procedures
- Detailed step-by-step instructions that should be followed
Roles and Responsibilities

Information Security in Schools - Recommended Practice (Sept 2019)
Chapter 2 Security Management

2.4.3 Set up and Implement Management and Administrative Processes

(a)(i) Assign roles and responsibilities

- School Management
- IT Head
- IT Committee Members
- Technical Support Staff

Details:
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **Incorporated Management Committee (IMC)** | • Approve policies  
• Delegate authority to Principals  
• Risk Management  
• Crisis Management |
| **IT Committee under IMC**    | • Delegated with the above duties by the Council |
| **School Supervisor**        | • Execution and Monitoring of the above |
| **School Principal**         | • Implement IS policy  
• Resource (budget, manpower) provision  
• Overall responsibilities covering IT and non-IT |
| **IT Head (Information Security Officer)** | • Overall responsibility of IT related issues  
• Implement the IT infrastructure and procedures accordingly  
• Formulate IT guidelines and procedures |
| **IT technical staff**       | • Carry out duties according to guidelines and procedures |
| **Teachers with IT related duties** (sensitive data, privileged accounts) | • Understanding the guidelines and procedures related to their special duties |
| **Teacher Users**            | • Follow the guidelines and procedures  
• Comply with legal requirements  
• Comply with teacher code of conducts |
| **Student Users**            | • Understand AUP  
• Comply with school requirements for students (conduct, discipline)  
• Comply with legal requirements |
IMC and Principal

➢ Conduct Risk Assessment
➢ Develop IS Policies
➢ Assign Roles and Responsibilities
➢ Monitoring and Review
FOR IT HEAD - Infrastructure and Systems Related

- **Network** Security – private network, remote access
- **Server** security – patch and upgrades, rights management
- **Classifying** sensitive data (personal data, mailbox, exam papers etc.)
- Managing **file** storage, backup and cloud services, IT **Assets** (keys)
- Security in IT Procurement and Service Contracts, **third party services**
- Managing Technical **Support Staff** – security training, procedures, monitoring
- Reviewing system statistics and **logs**
- Managing privileged / **admin accounts**
- Managing staff / student **accounts**

| Use school provided accounts instead of personal accounts (cloud account) | ✓ |
| ✓ | Use school provided email instead of personal emails |
| ✓ |
| ✓ | Automatic removal of rights after staff / student leaving |
| ✓ |
| ✓ | Not using real name with third party systems |
Personal Data Handling

- Collection – PICS / Consent Form
- Minimum data – no unnecessary HKID, address, phone in student list, email, reports etc.
- Encryption – in storage, processing and transmission
  - Especially: USB, email, Excel
- Hash Key – Integrity of data
- Transfer to third parties (e.g. publishers)
### Third Party Data Transfer Checklist

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement with third parties on purpose and usage of personal data</td>
<td>✓</td>
</tr>
<tr>
<td>Clear authority on who can transfer data</td>
<td>✓</td>
</tr>
<tr>
<td>Encryption in storage and transmission</td>
<td>✓</td>
</tr>
<tr>
<td>Hash Key to protect integrity and reduce liability</td>
<td>✓</td>
</tr>
<tr>
<td>Contractual rights to request removing data upon request</td>
<td>✓</td>
</tr>
<tr>
<td>Clear record of who transferred the data</td>
<td>✓</td>
</tr>
<tr>
<td>Choose what data fields to be transferred</td>
<td>✓</td>
</tr>
<tr>
<td>Clear record what data has been transferred</td>
<td>✓</td>
</tr>
<tr>
<td>Secure transfer system (not email, WhatsApp etc)</td>
<td>✓</td>
</tr>
</tbody>
</table>
Transfer of Student Data

Publisher A

Publisher B

Publisher C

School X

School Y

Secure??
EdData

Publisher A
Publisher B
Publisher C

HKEdCity

Student Data

School X
School Y

Request
Authorise
Request
Authorise
Request

Secure transfer

www.hkedcity.net
Assign Product

Product Information

Student Scope

- Whole School
  - P1
  - S1
  - S2
  - S3
  - S4
  - S5
  - S6

Current Requested Scope

Whole School

Clear all  Restore to default
<table>
<thead>
<tr>
<th>Task</th>
<th>Responsible Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signing of Agreement, that clearly states</td>
<td></td>
</tr>
<tr>
<td>1) The purpose and usage of personal data</td>
<td></td>
</tr>
<tr>
<td>2) The contractual rights to request for data removal (Revoke Function)</td>
<td></td>
</tr>
<tr>
<td>Clear authority on who can transfer data</td>
<td></td>
</tr>
<tr>
<td>Choose what data needs to be accessed</td>
<td></td>
</tr>
<tr>
<td>Choose to approve what data to be accessed</td>
<td></td>
</tr>
<tr>
<td>Provide a safe data transfer platform, including</td>
<td></td>
</tr>
<tr>
<td>1) Encryption in storage and transmission</td>
<td></td>
</tr>
<tr>
<td>2) Hash Key to protect integrity</td>
<td></td>
</tr>
<tr>
<td>Provide a comprehensive and clear data transfer logs, listing out the data access details</td>
<td></td>
</tr>
<tr>
<td>Check publishers' / providers' data access details from the data transfer logs</td>
<td></td>
</tr>
</tbody>
</table>
Technical Framework to Strengthen Privacy & Security

More info: https://www.hkedcity.net/eddata/