CHAPTER 11
CLOUD SERVICE

11.1 Cloud Security Overview

11.1.1 Data processed or stored by cloud service consumers in a cloud service may contain valuable, sensitive and personal information. Knowing only the security measures applied by the cloud service provider is not sufficient to protect this data.

11.1.2 Schools have to understand what data are being considered moving to the cloud, their risk tolerance, and the service and deployment models being chosen. IT Committee Members are advised to have an in-depth understanding of the issues and concerns for protecting their data in the cloud environment.

11.1.3 Appropriate security measures and controls should be deployed commensurate with the assessed risk level and the value of the data.

11.2 Cloud Service Security Consideration

11.2.1 Checklist on selecting a cloud service provider:

(a) Read carefully the terms of services, security and privacy policy.

(b) Check whether the service provider reserves rights to use, disclose or make public school information.

(c) Check whether the intellectual property rights of data schools own remain intact.

(d) Check whether the service provider retains rights to school information even if the school remove its data from the cloud.

(e) Understand whether they can move or transfer their data and the service to another provider, and whether export utilities are available and are easy to use.

(f) Check whether data can be permanently erased from the cloud, including any backup storage, when the school deletes this data or when the school ends the service.

(g) Select a service provider that ensures data confidentiality by:

- Using encryption, e.g. ~~s~~Secure ~~s~~Sockets ~~l~~Layer (SSL), to transmit data.

- Using encryption to protect stored data.

(h) Select a service provider that can explain clearly what security features are available, preferably supported by an independent information security management certification, e.g. ISO/IEC 27001.

(i) Select a service provider that provides a simple and clear reporting mechanism for service problems, security and privacy incidents.

(j) Select a service provider that provides regular service management reports and incident problem reports.

(k) Data protection and privacy legislation shall be observed. For protection of the privacy of individuals in relation to their personal data in Hong Kong, Personal Data (Privacy) Ordinance (PDPO) (Cap. 486), particularly the Data Protection Principle 4 (on security of personal data), should be observed.

(l) With increasing demand on a better cost-effective model, some outsourced data centres are located offshore. Data storing at or moving between the offshore data centres where information crossing borders may be subject to local legislations of the data centres, hence adoption of offshore outsourcing should be carefully considered.

11.2.2 On using cloud services, school should:

(a) Think twice when they want to store sensitive data in the cloud and assess the impact if this data is exposed.

(b) Consider the requirement of bandwidth of the Internet link and other resources for using the cloud applications and platforms, and make necessary implementation for enforcing the security and performance.

(c) Perform a regular backup of their 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 temporarily, e.g. network outage, or permanently.

(d) Keep operating systems, browsers and applications of their access device, including computers and mobile devices, up-to-date with the latest software versions and security patches. Furthermore, they should be cautious on browsing, especially not to click any links from untrusted sources.

(e) Delete access or change passwords immediately when there are staff changes.

(f) Use a strong authentication method, such as two-factor authentication, if available from the cloud service.

(g) Issue cloud application specific guidelines or reminders regularly to ensure that end-users of the cloud services are fully aware of the sensitivity of data and stay vigilant for possible security threats so that necessary actions can be taken during the data lifecycle, such as removing data stored in cloud when the data are unused.

(h) Remind users to:

- Use strong passwords for each account.
- Use different passwords for different accounts.
- Change passwords periodically.
- Turning off password saving in browsers and applications.
- Avoid keeping passwords in plain text on the device.

(i) Provide basic security awareness training for staff using the cloud service.

(j) Review and update the requirement of service level agreement with the service provider for enforcing the continuous support to schools.

(k) Understand and keep a record of what type of data is stored in the cloud.

(l) Use only trustworthy access devices to access cloud services. Avoid using public computers to process sensitive data in the cloud.

(m) Obtain service support contact information from the service provider and keep a list of telephone numbers for reporting computer security incidents.

(n) Work out alternatives when the cloud services or data is not available.