第十一章
雲端服務

11.1 雲端平台保安概述

11.1.1 雲端服務用戶透過雲端平台處理或儲存的數據，可能包含有價值、敏感和牽涉個人的資訊。用戶要保護這些資料，單靠雲端服務供應商所採取的保安措施並不足夠。

11.1.2 學校需要考慮何種數據會被轉移至雲端平台，學校可承受的風險，以及選擇的服務和部署模式。資訊科技委員會需要深入了解在雲端平台上保護其數據所遇到的困難和考慮。

11.1.3 應就評估得出的風險水平及數據價值，部署適當的保安控制及措施。

11.2 雲端平台服務保安考慮

11.2.1 選擇雲端服務供應商的備忘事項：

(a) 閱讀服務供應商的服務條款、保安及私隱政策。

(b) 查核服務供應商是否保留權利以使用、披露或公開用戶所擁有的資料。

(c) 查核用戶能否保留所擁有資料的知識產權。

(d) 查核即使資料從雲端平台上被刪除後，服務供應商會否保留使用該些數據的權利。

(e) 了解用戶能否按本身意願把數據及服務轉移至另一服務供應商，以及是否有容易使用的資料匯出功能供用戶使用。

(f) 從雲端平台上刪除資料或停止使用該服務時，應檢查這些資料（包括任何儲存備份資料）是否可被永久刪除。

(g) 選擇能透過以下途徑確保用戶資料得以保密的服務供應商：

- 使用加密功能（例如保密插口層（SSL））以傳送資料。
- 使用加密功能以保護儲存的資料。

(h) 選擇能清楚說明提供哪些保安功能的服務供應商，以有獨立資訊保安管理認證（例如 ISO/IEC 27001）者為佳。

(i) 選擇設有簡單清晰通報機制的服務供應商，以供通報服務問題、保安事故和侵犯私隱事宜。

(j) 選擇能定期提交服務管理報告及保安事故報告的服務供應商。

(k) 須遵守資料保護和私隱法規。為保障個人私隱而又位於香港境內的個人資料，須遵守《個人資料（私隱）條例》（第 486 章），特別是保障資料第四原則（個人資料的保安）。

(l) 為追求更高成本效益，有些外判數據中心會設置於海外。跨境儲存於海外數據中心，或與海外數據中心作轉移的數據，因跨境的原因，此類數據中心可能受到當地法例規管，因此需要小心考慮採用海外外判服務。

11.2.2 關於使用雲端服務，學校應：

(a) 審慎考慮是否必需把敏感資料儲存於雲端平台上，並評估這些資料一旦被披露所造成的影響。

(b) 考慮網絡連結的頻寬要求，以及使用雲端應用和平台的其他資源，作出所需措施以加強保安及表現。

(c) 定期為儲存在雲端服務中的資料備份，以及為重要資料進行備份至學校的儲存裝置。即使服務供應商暫時（例如網絡發生故障）或永久不能提供服務，有關資料仍可供使用。

(d) 定期為電腦及流動裝置的操作系統、瀏覽器和電腦應用程式進行更新和安裝最新的保安修補程式。此外學校用戶瀏覽互聯網時應小心，特別不要點擊來歷不明的連結。

(e) 在出現人事變動時，即時刪除有關用戶帳戶或更改密碼。

(f) 如雲端服務有提供的話，應使用嚴謹的認證方式，例如雙重認證。

(g) 應定期發出針對個別雲端應用系統的指引或通知，以確保雲端服務終端用戶留意數據的敏感程度，並對潛在的保安威脅保持警覺，讓使用戶能就數據的生命周期採取適當行動，例如在雲端系統刪除不再使用的數據。

(h) 提醒使用者：

- 帳戶應使用難以被猜中的密碼。
- 不同的帳戶應使用不同的密碼。
- 定期更改密碼。
- 關閉瀏覽器和應用程式的密碼儲存功能。
- 避免以純文字方式把密碼儲存於裝置上。

(i) 為使用雲端服務的員工提供基本保安認知培訓。

(j) 與服務提供者一起評估及更新服務水平協議的要求，以加強對學校的持續支援。

(k) 了解並記錄儲存於雲端平台上資料的種類。

(l) 只使用可信靠的存取裝置接達雲端服務。切勿使用公用電腦處理雲端平台上的敏感資料。

(m) 向服務供應商索取有關服務支援的聯絡資料，並保存可以用作通報電腦保安事故的電話號碼清單。

(n) 制訂替代方案，以應對雲端服務停用或資料不能被讀取的情況。