第四章
實體保安

4.1 實體保安的意義

4.1.1 實體保安是指保護硬件、電腦設備和其他資訊科技資產免受外來實體的威脅，例如未經授權的接達、偷竊或在運送到外面場地時遺失備份媒體。

4.2 學校的場地準備

4.2.1 由於大部分關鍵資訊科技設備一般放置在伺服器室內或電腦室內，因此伺服器室或電腦室的場地準備工作必須慎重進行。建議學校應：

(a) 評估學校場地的保安風險，以確保已推行足夠的保安控制措施以保護學校的數據。

(b) 在建立伺服器室或電腦室前，先評估實體環境的可行性：

- 選址及場地規劃
- 供電及電力需求
- 空氣調節及通風
- 防火、火警偵測及滅火
- 水患及水浸控制
- 實體出入控制

4.2.2 為加強保安及便於管理，建議學校為校內的不同區域設定不同的進入許可權。一般來說，學校可設定三個區域：

(a) 公共區:（例子：走廊）

- 開放予所有用戶使用，例如放置公用電腦資訊站的走廊。

(b) 防護區:（例子：學校辦公室、職員室和校長室）

- 開放予特定的用戶使用，例如只是教師及學校職員才可使用的教員室，及學生在教師陪同下才可使用的電腦室。

(c) 限制區:（例如：伺服器室)

- 僅開放予已獲授權的人士使用，例如伺服器室只供系統管理員使用。

4.2.3 不論學校劃分了多少個安全區，每個區域都必須採取適當的保安措施。例如，在圖書館及電腦室等防護區內，必須駐有負責人如圖書館管理員及教師等，以監察資訊科技設施的使用情況。

4.3 電腦硬件與軟件資產的保護

4.3.1 硬件清單：保存一份學校最新的電腦硬件設備清單，其中包括所有零件的詳細資料。清單內容應包括中央處理器（CPU）、隨機存取記憶體（RAM）、硬碟容量、顯示器尺寸等，並詳細列出相關指定的服務資訊，如保證書有效日期、序號、服務合約及服務聯絡人資料等。亦應制訂政策，以避免員工在未經許可下移除任何電腦設備。

4.3.2 軟件清單：保存一份最新的軟件清單。學校必須確保有足夠的軟件使用許可證，並提醒員工不可安裝自己的軟件。共享軟件在試用期完結前應移除。學校應注意 一些許可證會把許可證號碼以小標籤的形式顯示。無論如何，學校都要將它們保存在安全的地方。根據《版權條例》，學校有責任確保沒有使用非法軟件。

4.3.3 棄置電腦設備：在棄置任何硬件時，應移除已安裝的所有程式並刪除所有資料。

4.3.4 電腦設備實體保安：學校電腦設備的實體保護很重要。就像其他有價值的資產一樣，學校可考慮採用以下工具或方法來保護學校的電腦：

(a) 保護工作站／電腦室

- 使用保安鏈條鎖上電腦
- 自動關閉門
- 門窗鎖
- 房間之間的門可上鎖

- 保安門簾或百葉窗
- 警報器（確定每位員工都有自己的警報密碼）

(b) 伺服器及網絡設備的保護

- 存放伺服器和網絡裝置在上鎖的房間或櫃中
- 切斷沒有使用的網絡連結
- 伺服器室應配置專用電源及後備式不間斷電源供應器
- 推行火災及水災警報器系統。手提滅火器應放在電腦區域的當眼或適當位置，並貼上檢驗標籤及至少每年檢測一次
- 確保放置伺服器的地方有足夠的通風及冷氣
- 為所有公用設施安排定期維護及測試，例如空調設備、火警探測及防火系統和備用供電系統

(c) 流動裝置的保護

- 處理資訊科技設備，如流動裝置及抽取式媒體時，學校應備存一份獲授權設備清單，並定期進行盤點，以檢查這些設備的狀況。流動電腦在無人使用時，應放置於可上鎖的櫃中，如伺服器室內的筆記簿型電腦櫃及／或教員室內有關教師的辦公桌抽屜中。
- 管有流動裝置或抽取式媒體以作業務用途的人員，須保障有關裝置的安全。在沒有採取妥善保安措施的情況下，須避免裝置無人看管。

(d) 軟件、儲存及備份媒體

- 軟件程式及數據檔案的正本及備份本必須妥善保存。
- 學校應緊記定期備份以保護資料。
- 存放備份媒體在安全的地方，尤其是儲存敏感或關鍵資料的媒體。
- 學校應考慮將備份本離線及與正本分開存放，並與正本保持安全距離。

- 學校應妥善保管各種儲存媒體，如磁性、光學及快閃記憶設備。儲存了敏感數據的媒體應存放於上鎖的安全地方。

- 由於流動裝置及抽取式媒體體積細小及容易遺失或被竊，為盡量減低資料外泄的風險，應只使用具備適合保護保密資料的加密功能的裝置。

- 備份媒體的接達須只可通過獲授權人士按既定機制進行。未獲授權人士不得進入媒體儲存庫或儲存室。

4.3.5 應定期更新及覆檢獲授權進入伺服器室、電腦室、放置或儲存電腦設備及數據的其他關鍵操作地點的人員清單。

4.3.6 凡用作進入任何資訊系統及網絡的密碼匙、智能卡、密碼等，其實體安全應得到保障，或受到清晰明確及嚴格執行的保安程序所規管。獲授權人員應時刻監視所有進入伺服器室或電腦室的訪客，並須妥善保存訪客出入記錄作審核用途。