第九章
流動裝置與流動應用程式防護

9.1 流動裝置保安考慮

9.1.1 隨著科技日新月異，流動裝置的運算能力與日俱增。部分學校開始推行學生「自攜裝置」政策，以進一步發揮使用流動電腦裝置進行學習的優勢。流動裝置一方面有許多明顯的好處，同時也帶來需要解決的保安問題。

9.1.2 流動裝置和流動應用程式的保安威脅來自不同方面，因為流動裝置的特性一般令它們比其他客戶端裝置（例如辦公室內的工作台）面對更多保安的威脅，所以流動裝置經常需要額外的保護。流動裝置的主要威脅可以來自裝置本身、網絡（例如流動通訊網絡、互聯網）及應用程式（例如流動應用程式、流動網絡應用程式）。以下是一些流動技術的相關保安風險：

(a) 流動裝置比其他裝置更容易遺失或被盜，令資料外泄的風險增加。

(b) 使用保安控制不足的流動裝置配件，如相機及麥克風，以及不恰當的錄影、錄音及攝影都可能導致保安問題。另外，若流動裝置未有得到適當的保護，未獲授權人士便有可能獲取裝置內的敏感錄影、錄音或照片。

(c) 使用不可靠的流動裝置，尤其是私人擁有的裝置，可能有保安風險。

(d) 使用不可信的網絡，如外部 WiFi 及流動電話網絡以連接互聯網會令敏感資料有機會外泄。

(e) 使用不安全的通訊技術，例如藍牙和近距離無線通訊（NFC）作數據連接，都有其保安風險。若敏感資料於通訊媒介中遭攔截，則會導致保安事故。

(f) 使用不可信的應用程式，會帶來明顯的保安風險，尤其在不設保安限制或其他制約的流動裝置平台及流動應用程式商店所發佈的由第三方開發的應用程式。

(g) 流動應用程式易受來自不可信來源的惡意程式的入侵，這種情況在其他類型裝置較不常見。例如現時流動電話和平板電腦中因有內置相機而常用的二維碼。這樣會導致針對性攻擊，例如在目標用戶聚集的地方放置惡意二維碼。

(h) 已啟用定位服務的流動裝置會較有機會成為被攻擊的目標，因為這會令潛在攻擊者更易知道使用者及流動裝置的位置，然後將位置資料結合其他來源的資訊，從而發動如魚叉式仿冒詐騙的攻擊。

9.2 流動裝置的資訊保安政策

9.2.1 學校應制定流動裝置保安政策，以列明流動裝置存取的操作和保安要求。

9.2.2 學校須制訂正式的使用政策及程序，並針對使用流動資訊處理及通訊設施的風險採取適當的保安措施。

9.2.3 有關的使用政策及程序應訂明實體保護、接達控制、加密技術、備份和抗惡意軟件等方面的要求。此外，亦應訂定把流動設施連接至網絡的規則和建議，以及在公眾場所使用這些設施的指引。

9.2.4 獲批准的流動裝置種類及其審批機制應符合運作及保安要求。

9.2.5 資訊科技負責人應向用戶傳遞合理使用政策及保安提示，提醒用戶採用良好保安作業模式。同時，亦需取得用戶的確認，表明已收到有關合理使用政策、保安提示以及狀態良好的流動裝置。該確認可以是已簽署的協議或電郵。

9.2.6 應備存已獲學校審批的桌上應用程式或流動裝置應用程式清單。這些應用程序應根據其實際需要和信任級別定義。

9.2.7 用戶培訓是加強用戶保安意識的重要一環。學校應從流動裝置用戶角度理解保安要求，從而將人為錯誤減至最低。應為流動裝置用戶提供培訓，讓他們對流動裝置保安要求、保安政策及保安威脅有一定程度的認識。

9.3 流動裝置的數據通訊及儲存保安

9.3.1 用戶連接公共的 WiFi 熱點時應要謹慎及避免存取敏感資料。

9.3.2 不建議用戶在流動裝置上處理敏感資料，除非使用具有加密功能的或安全的端到端連接。

9.3.3 學校應在重用或棄置流動裝置前，確保所有資料已徹底刪除。

9.3.4 用戶應開啟備份／同步軟件的加密選項。

9.3.5 建議用戶安裝流動保安程式（如防禦惡意軟件），以保護裝置和資料的安全。

9.3.6 用戶應把流動裝置放置在安全的地方，尤其是在不使用時。

9.4 用戶及流動裝置認證保安

9.4.1 學校應為流動裝置備存庫存記錄，包括裝置使用者資料及已安裝的應用程式。

9.4.2 學校應為流動裝置設置登入要求條件，例如啟用開機密碼功能，並根據學校的保安要求，執行密碼長度及複雜性要求，以及設定流動裝置在閑置一段時間後自動鎖上。

9.4.3 用戶不應在流動裝置上儲存電郵、網絡登入等密碼，亦應停用自動儲存密碼功能。

9.5 流動應用程式的保安

9.5.1 建議學校按可行性安裝保安控制工具，例如流動裝置管理、數據遺失防護、個人防火牆軟件及抗惡意軟件，並為流動裝置進行保安強化處理，將已強化的裝置交付用戶。

9.5.2 用戶應定時更新系統及裝置上的應用程式，確保操作系統和已安裝的應用程式的保安功能已經開啟，並已安裝最新的病毒及惡意程式的識別碼及定義。

9.5.3 用戶應只限從官方商店下載可信任的應用程式，或安裝獲學校批准及提供的應用程式。不要從不明或不可信的來源下載程式，亦不要在流動裝置上安裝非法或未獲授權的軟件。

9.5.4 用戶不應嘗試使用未經授權的工具為流動裝置越獄／破解根權限或損害流動裝置操作系統。

9.6 流動裝置管理方案

9.6.1 流動裝置管理（MDM）方案對流動裝置（如流動電話及平板電腦）的政策、庫存、保安及服務各方面提供管理功能。學校可根據校本資訊科技保安政策執行技術性措施，透過流動裝置管理方案技術統一設定所有流動裝置。

9.6.2 流動裝置管理（MDM）軟件可用於控制流動裝置的使用地域，並為裝置設定配置檔及施行安全群組政策。

9.6.3 流動裝置管理方案技術功能包括：

(a) 透過實體、虛擬，或應用程式容器，提供一個隔離的環境處理數據。

(b) 當流動裝置遺失或被盜時，遙距清除裝置內的數據。

(c) 重覆登入失敗後清除裝置內的數據。

(d) 按配置設定採用及配置流動裝置。

(e) 執行保安控制，如在使用無線網絡傳送資料時使用虛擬私人網絡為資料加密。

(f) 為數據接達提供詳細的審計追蹤。

(g) 監察異常活動。

(h) 控制安裝及移除流動應用程式。