第七章
網絡及通訊保安

7.1 網絡保安全管理

7.1.1 以下是學校建立安全網絡的建議：

(a) 在設計網絡時加入保安的考慮：所有保安事項，例如管理政策，技術訓練和外判要求應該在設計網絡早期開始考慮。

(b) 為網絡和系統設計實體性和環境性保安措施：將重要的資產存放在上鎖的房間，包括網絡訊號線、交換器、路由器、防火牆和網路儲存（例如：網路儲存設備）。

(c) 使用私人的互聯網規約（IP）地址：學校應為內部網絡設立私人的互聯網規約地址以免被人從外間的網絡進入內部網絡。

(d) 用分區形式設計網絡保安模型：根據保安要求將網絡分區，例如學校內部網絡應與互聯網完全隔絕，而伺服器及電腦應置於防火牆後或設置非軍事區（DMZ）網絡。此外，不允許不安全或沒有管理的系統連接到內部網絡。

(e) 將網絡劃分為分隔的網域：學校可考慮將其網絡劃分為分隔的網域，可以按可信任的程度選擇網域（例如公眾可接達的網域、學生網域、教職員網域、伺服器網域），並可採用實體或邏輯（例如使用虛擬私有網絡（VPN））的方式分隔網域。此外每個網域的邊界應清晰界定。網域之間可容許互相接達，但應使用通訊閘（例如防火牆和路由器）在網域邊界作出控制，把網絡分隔為網域和容許通過通訊閘接達的準則，應根據對各網域保安要求的評估制訂。

(f) 設定防火牆和網絡路由器：設置合適的存取控制清單（ACL）以強化防火牆和路由器；只容許在特定地點進行網絡管理工作；關閉不必要的進出網絡服務或使用加密通道進行網絡管理工作。

(g) 推行入侵偵測策略：為偵測異常活動或潛在資訊保安事故，學校可考慮推行入侵偵測策略。在網絡安裝網絡入侵偵測系統（NIDS）或網絡入侵防禦系統（WAF）並具有最新的識別碼，以助偵測網絡是否遭到攻擊。學校應留意入侵偵測系統（IDS）及入侵防禦系統（IPS）的配置須調校識別碼及識別方式，以減少虛假警報。

(h) 妥善配置及管理資訊／通訊系統：學校須確保資訊／通訊系統已妥善配置及管理，包括關掉所有無須使用的服務和適當地設定保安配置。配置須定期覆檢，並在有需要時更新。

(i) 伺服器設定：移除不必要的服務和軟件、及時修補系統的漏洞和取消沒被使用的帳戶，以確保伺服器操作系統安全。

(j) 加強應用程式的保安：安裝保安修補程式及強化應用程式的設定。

(k) 過濾病毒和惡意代碼攻擊：學校應確保桌上電腦和伺服器已安裝和啟用抗惡意軟件和更新定義檔案，以防止惡意程式，如病毒、蠕蟲和木馬程式傳播。

(l) 正確處理帳戶和存取權：在有需要時才開啟及每年檢閱存取權。

(m) 記錄和定期檢閱保安事宜：應提供記錄及審計功能以記錄網絡的連接情況，尤其是未經授權的接達。此外，也應定期檢閱這些記錄。

(n) 建立保安管理的程序：如保安事件記錄監測程序，變更管理程序或修補程式管理程序。

(o) 建立一個安全桌面的標準模式：設計一個安全的工作站設定，並將它作為學校內部標準，亦可以將這模式的映像複製到學校電腦的桌面。此外，學校應建立備份和復原策略。

(p) 妥善儲存文件記錄：建議學校妥善備存設定及程序文件，並備存最新的系統或網絡資料，特別是網絡圖、內部網址和配置，顯示最新的網絡環境，以有效推行保安控制措施。這些資料須適當地分類及穩妥地儲存。

(q) 提供培訓：學校應為技術支援人員及用戶提供培訓，以確保他們可以遵從保安良好作業模式和保安政策。

7.1.2 遠程接達

(a) 遠程接達是指在沒有直接連接網絡的遠程地點使用網絡資源。

(b) 不建議學校使用遠程接達軟件直接連接至內部伺服器或用戶的工作站。這樣使用遠程接達軟件相當於為攻擊者開啓了資訊系統的後門，讓他們能夠避開防火牆／路由器的保護。

(c) 為維護學校基礎設施和資訊資產的保安，學校應制訂政策，建議用戶如何安全地進行遠程工作。如必須使用遠程接達軟件，應採取設有記錄功能的適當保安控制措施。為防止在未獲授權的情況下被接達，應開啓遠程接達軟件的閒置超時控制功能。學校亦應提供安全的渠道（例如虛擬私有網絡連線），讓用戶連接至內部網絡。對於利用虛擬私有網絡連線以遠程接達方式連接至內部網絡的情況，則建議使用雙重認證。

(d) 學校應清晰界定哪些用戶會獲得遠程接達權限，以及他們會得到甚麼類型的服務。學校應只讓獲授權用戶在適當認證及記錄下，獲得網絡的遠程接達。

(e) 用戶應妥善保護遠程電腦，例如安裝個人防火牆、抗惡意程式軟件及惡意軟件偵測及修復措施。所有這些保安功能任何時候均應處於啓動狀態，並具有最新的惡意軟件識別碼及定義。此外，亦須為這些遠程電腦安裝最新的保安修補程式。在這些遠程電腦連接至學校內部網絡前，應為系統進行全面掃描，以偵測任何惡意軟件。

(f) 為避免學校資料外泄，用戶應盡量避免在遠程或便攜式電腦上儲存保密資料。保密資料不應儲存在私人擁有的電腦、流動裝置或抽取式媒體內。

(g) 在公共場所工作時，用戶應避免處理敏感文件，以減低把資料外泄予未獲授權人士的風險。用戶亦應避免使用公共打印機。如需打印，應迅速取回打印文件。此外，用戶應使用已設密碼的屏幕保護程式，以保護遠程電腦，並切勿讓電腦無人看管。

7.1.3 虛擬私有網絡

(a) 設立虛擬私有網絡是建立安全通訊渠道的可行方法，可讓在辦公室以外地點工作的人員使用。在推行虛擬私有網絡前，學校應評估虛擬私有網絡與現行網絡是否兼容，並考慮執行下述虛擬私有網絡保安建議：

- 使用權標等一次性密碼認證機制，如以較複雜密碼組成的公開／私人密碼匙系統認證。
- 如在一段指定的時間內沒有操作，應自動終止與學校網絡的連接。用戶須重新登入才能與網絡連接。
- 禁止使用雙重（分隔）隧道技術。只允許單一網絡連接。
- 保護所有透過虛擬私有網絡與學校網絡連接的電腦或裝置，如使用個人防火牆、最新保安修補程式、抗惡意軟件偵測與修復軟件。所有這些保安措施應經常處於啓動狀態，且具有最新的惡意軟件識別碼及定義。
- 透過記錄及審計功能以記錄網絡連接情況，尤其是記錄未能接達的情況。此外，亦應定期覆檢記錄，以識別任何可疑的活動。
- 提醒擁有虛擬私有網絡使用權限的用戶，他們有責任適當地使用帳戶。
- 培訓教師、支援人員及遠程用戶，以確保他們在建立及使用虛擬私有網絡時遵守保安良好作業模式及政策。
- 安裝防火牆於通訊閘，以控制從虛擬私有網絡客戶至獲授權資訊系統或伺服器之間的網絡通訊。

7.2 構建無線網絡的安全考慮

7.2.1 無線局部區域網絡（WLAN）通常被視為不可信任的網絡，如無適當的保安控制措施，不應用於傳遞保密／敏感／個人資料。

7.2.2 學校應意識到與無線網絡安全相關的風險，例如：

(a) 無線信號的特點是有關信號普遍在無線局部區域網絡的覆蓋範圍內的空間傳輸，並可穿越建築物的牆壁及窗戶。因此，除非已採取保安措施保護無線傳遞不被「竊聽」，否則會帶來任何人也可截取及閱讀這些信號的潛在保安風險。

(b) 懷有惡意的人士可通過無線連接，並有可能避開防火牆，在未獲授權的情況下接達學校內部網絡及發動攻擊。

(c) 電腦惡意軟件可破壞無線裝置內的數據，繼而入侵有線網絡。

(d) 懷有惡意的人士可利用未獲授權設備（例如客戶裝置及無線接駁點），暗中接達或竄改資料。

(e) 未經加密（或採用較弱的加密技術）的保密資料在無線裝置之間傳遞時或會被截取及外泄。

(f) 拒絕服務攻擊（DoS）可能會針對無線連接或裝置發動。

(g) 可能有虛假的無線接駁點被建立，以獲取無線局部區域網絡內傳送的資料。

(h) 802.11 標準的保安機制在設計上的瑕疵也引發了一連串被動和主動攻擊，導致無線傳輸的資訊被竊聽及遭竄改。

7.2.3 學校部署無線網絡的建議：

(a) 留意 WiFi 標準的發展：自從 802.11 標準推出並不斷加以改良，數據傳輸率、訊號範圍和無線網絡的保安都得以加強。因此，當採購新設備或獲取新的無線網絡服務時，最好時常留意新標準的發展。在採購新設備時，應考慮以較安全的無線保安規約如 WPA／AES 或 WPA2／AES 作保護。由於日後可能在這些規約中發現新的保安漏洞，故不能只依賴這些保安規約作為確保資料保密性和完整性的唯一措施。

(b) 在設計無線網絡前，須了解學校無線方案的運作及功能要求，因為這些要求可能會影響應採取的網絡保安措施。例如容許非註冊用戶接達系統，在設計階段便應考慮相關的保安良好作業模式。

(c) 學校應制訂一套穩建的無線保安政策，以處理使用無線網絡的問題及釐定可傳送的資料種類。該政策應描述一個制訂安裝、保護、管理和使用程序的架構，以及訂立保安與運作指引、標準和各員工的職責。

(d) 進行保安風險評估及審計以識別保安漏洞：保安風險評估及審計是檢查無線網絡安全程度的重要方法，用以確定所需的修正措施，維持可接受的保安水平。這些方法有助於識別無線網絡的漏洞，例如使用預設或易猜的密碼和簡單網絡管理規約（SNMP）的社群字串的無線接駁點，或是否已啟動加密功能。然而，保安風險評估只能揭示資訊系統於某一段時間的部分風險，故在無線網絡運作後，應定期進行風險評估及審計。

(e) 進行實地調查：基於射頻（RF）的性質，無線網絡訊號一般不會受樓宇阻隔。無線訊號的覆蓋範圍過大，可能會對網絡構成重大威脅如「停車場」攻擊（“Parking Lot” attack）。因此，在網絡規劃階段中，應充份了解無線網絡的覆蓋範圍要求並進行實地調查，以便確定：

- 採用適當的技術。
- 須避免、刪除或處理的障礙。
- 應採用的覆蓋模式。
- 需要的容量。

7.2.4 建議學校將 WiFi 網絡與學校現有網絡完全分開，並使用獨立的寬頻線路，以減低保安風險。基於無線技術的特質，無線網絡比較難以受樓宇阻隔，故一般被視為不可靠的網絡。連接網絡時，良好作業模式是有線和無線網絡不應直接連接在一起。防火牆的安裝通常用於分隔和控制不同網絡的通訊。例如有線網絡的地址解析協定（ARP）廣播封包不應傳送至無線網絡，否則惡意用戶便可揭露內部信息，如這些廣播的以太網媒體接達控制（MAC）地址。

7.2.5 當加入或連接 WiFi 網絡至學校現有網絡時，學校資訊科技的負責人員須評估和了解相關的保安事宜，避免學校現有網絡出現風險。建議將 WiFi 網絡連接至有固網的學校，採用「縱深防禦」方式有線網絡的保安設計，一直廣泛採用「縱深防禦」的概念，這原理亦適用於無線網絡。經採取多重保安措施後，無線網絡遭成功入侵的風險將大幅減少。如一項措施受襲，尚有多重保安措施可保護網絡。分隔無線與有線網絡數據段、使用強化的裝置及用戶認證方法、依據位址及規約作出網絡過濾，以及對無線與有線網絡進行監視和入侵偵測，均屬多重防禦的措施。

7.3 無線局部區域網絡的保安控制措施

7.3.1 保護無線局部區域網絡的管理控制措施

(a) 就無線局部區域網絡的使用及可經無線局部區域網絡傳遞的資料類別，制訂無線保安政策。

(b) 制訂及妥善保存無線局部區域網絡的覆蓋圖，涵蓋相關無線接駁點的位置及服務設定識別碼（SSID）資料，避免無線信號的覆蓋範圍過大。

(c) 確保硬件及軟件得到妥善修補及更新。

(d) 定期搜尋虛假或未獲授權的無線接駁點。

(e) 定期進行資訊科技保安風險評估及審計，以找出保安漏洞。

(f) 妥善保存所有配置無線界面的裝置的記錄。某裝置一旦遺失，應考慮更改密碼匙及服務設定識別碼。

(g) 推行嚴格的實體保安控制措施及鑑定用戶身分，以彌補無線裝置實體保安的不足。

(h) 在遠離門窗的位置安裝無線接駁點，以防止網絡在可公開進入的地方被竊聽。

(i) 建議學校限制訪客專用的 WiFi 網絡連接到學校的內部網絡。

7.3.2 保護無線局部區域網絡的技術控制措施

(a) 在安裝時更改網絡預設名稱。服務設定識別碼不應包含任何學校的名稱、系統名稱或產品名稱／型號。

(b) 更改產品預設的無線接駁點配置設定。為方便設置，有關預設配置設定在大部分情況下視為不安全。

(c) 關閉無線接駁點上所有不安全及未使用的管理規約，並以最小權限配置所需的管理規約。

(d) 確保所有無線接駁點均有嚴謹而獨立的管理密碼，並定期更改密碼。

(e) 開啓及配置保安設定，包括服務設定識別碼、密碼匙、簡單網絡管理規約的社群字串。

(f) 採用「WPA2-Enterprise」如使用「WPA2-Personal」，則應定期更改密碼匙。

(g) 關閉服務設定識別碼廣播功能，以免無線接駁點廣播服務設定識別碼，以便只有配置與無線接駁點服務設定識別碼相符的獲授權用戶才可與網絡連接。

(h) 關閉動態主機配置協議伺服器（DHCP），並向所有無線用戶指派固定的互聯網規約地址，從而將未獲授權用戶取得有效互聯網規約地址的機會減至最低。

(i) 配置無線接駁點時使用媒體接達控制地址過濾功能，使只有具特定媒體接達控制地址的客戶才可接達網絡，或只容許接達一系列設定的媒體接達控制地址。

(j) 啓動記錄功能，並在可行的情況下把所有記錄轉移至遠程記錄伺服器。有關記錄應定期檢查。

(k) 安裝無線網絡入侵偵測系統（WIDS）或無線網絡入侵防禦系統（WIPS），以監察無線局部區域網絡。

(l) 在無線局部區域網絡之上設置虛擬私有網絡，以連接學校內部網絡。

(m) 把無線接駁點的覆蓋區域分段，以平衡網絡負荷及減低受到拒絕服務攻擊的可能性／影響。

(n) 棄置無線組件時，刪除有關裝置所載的所有敏感資料，例如系統配置、共享密碼匙、數碼證書和密碼。

(o) 關掉無線接駁點的通用即插即用（uPnP）功能，以防止惡意軟件通過連接的裝置繞過防火牆。

7.3.3 保護無線局部區域網絡的終端用戶控制措施

(a) 在無線客戶端（例如流動裝置）安裝防火牆及啟用抗惡意軟件作保護。

(b) 關掉無線客戶端的共用或網絡共享功能。

(c) 已連接第三方無線局部區域網絡的無線客戶端不得同時連接學校網絡。

(d) 嚴格控制無線界面裝置（例如通用串列匯流排（USB）無線網卡），因為接達憑證（例如服務設定識別碼及／或密碼匙）通常儲存在該裝置。

(e) 只在用戶需要時才開啓無線連接，不需要時則關閉。

(f) 替裝置上的敏感／個人資料加密。

(g) 使用公共無線服務時刪除個人「慣用網絡」。

(h) 不要同時啟動無線及有線網絡界面卡。

7.4 郵件通訊閘保安和電子郵件處理

7.4.1 保護郵件伺服器

(a) 郵件伺服器應由防火牆系統作掩護，防火牆系統可以限制對郵件伺服器的接達，並提供各種保安保護措施。適當配置防火牆或路由器，以攔截不必要的通訊（例如由某個已知濫發電郵者的互聯網規約地址所發出的通訊）進入郵件伺服器或通訊閘。

(b) 應採用抗惡意軟件防護，過濾帶有惡意軟件附件的進出電郵。

(c) 電郵系統不應披露內部網絡或系統的名稱或互聯網規約地址。應適當配置電郵系統，以避免透過電郵的標題洩露內部系統或配置的資料。

(d) 使用可靠服務供應商的電子郵件系統。

7.4.2 以下列出保護學校免受電郵轟炸、濫發電郵及電郵仿冒的提示：

(a) 移除不用的電郵伺服器程式，例如 Sendmail。

(b) 確保郵件通訊閘使用最新的版本。

(c) 開啟記錄功能，以記錄仿冒電郵訊息的來源和標題。使用入侵偵測及防禦系統（IDPS）來偵測任何可疑的活動，例如某寄件人所寄入／寄出的電郵突然大量增加的情況等，以協助偵測／防禦電郵轟炸。

(d) 適當配置防火牆和路由器，只容許符合簡單郵遞傳送規約（SMTP）的外來連接連結到指定的郵件通訊閘或伺服器，並集中記錄和控制通訊。

(e) 應堵截來自未獲授權或不存在的地址使用郵件轉遞，例如郵件伺服器應只容許一些指定內部的互聯網規約地址，或已獲授權內部用戶使用郵件轉遞，而並非供外部用戶使用。

(f) 應適當地配置電郵伺服器程式或郵件通訊閘軟件所配備的過濾無效訊息功能，以清除一些未獲授權網域所發出的垃圾郵件或無效的訊息。

(g) 限定每個電子郵件的大小上限，或在特定時段內可傳送郵件數量的上限，以避免因電郵泛濫而耗盡網絡資源或磁碟容量。

(h) 定期更新濫發電郵者名單。

(i) 設置電郵濫發的阻截系統，藉以過濾不需要的電郵。此電郵濫發阻截系統可發揮郵件通訊閘的功能，按照多項標準（例如電郵標題、內容、電郵濫發黑名單、電郵濫發白名單、反向域名系統查詢、發件人政策框架及郵件域名密鑰識別郵件資料）在電郵進入電郵伺服器之前，篩除濫發電郵。

7.4.3 學校可以採取多種方法來減少收到濫發電郵的數量。這些方法包括保護學校的電郵地址，為僱員的工作站和電郵伺服器安裝過濾軟件及採用具體的保安措施。以下是一些提示：

(a) 學校應訂立和實施一個明確的資訊保安政策，並教育員工不要回覆濫發電郵。

(b) 學校應規定員工禁止使用公司電郵地址發送個人訊息，參與新聞群組或聊天室。

(c) 如果需要在學校網站上公佈電郵地址，學校可考慮以一種濫發電郵者難以直接獲取的書寫方式，例如，把電郵地址 "info@xyz.com.hk" 改寫成 "info[at]xyz.com.hk"。另外，可以附加一項聲明，如「請勿濫發電郵」，表明學校不希望接收任何非應邀電郵。

(d) 如學校自設電郵伺服器，需安裝伺服器級別的電郵過濾軟件。過濾軟件可於電子郵件送達用户前作出篩查。

(e) 如果學校使用的是網上電郵服務，這些服務供應商可能會提供一些反濫發電郵的設定。為了減少錯誤地過濾了非濫發電郵的風險，學校可考慮在過濾系統中增設一個資料夾，保存被攔截的電郵，以便在刪除這些電郵前進行檢查。

(f) 採用良好的保安措施，例如加強學校的電郵伺服器及網絡伺服器保護措施，以防被駭客入侵和被第三者利用來發送濫發電郵。

7.4.4 濫發電郵者會收集用戶電郵地址，並驗證它們是否有效，然後開始發送電郵。所以，為了減少接收濫發電郵的可能性，用戶必須保護他們的電郵地址／帳戶及電腦。以下是一些提示：

(a) 不建議用戶輕易透露個人資料，包括電郵地址，亦不要在公開網站、聯絡人目錄、會員目錄或聊天室披露個人的電郵地址。

(b) 建議用戶若情況許可，盡量使用不同的電郵地址作不同用途。

(c) 不建議用戶使用字典裏簡單的字和通用的姓名作為電郵地址。

(d) 用戶不要被濫發電郵者最常用的「你還記得我嗎？」此類標題所誤導。

(e) 當打開電郵及電郵附件時，用戶應小心，尤其是收到陌生人的電子郵件。

(f) 建議用戶刪除來歷不明或可疑電郵。

(g) 用戶應檢查電郵程式或網上電郵服務的外發電郵資料夾或寄件匣，留意是否有非由自己發出的外發電郵。如果有這樣的訊息時，用户的電腦可能已被駭客入侵，或被濫發電郵者用來發送電郵。用戶應立即中斷網路連線，並立即啟動防毒軟件或間諜防護程式掃描你的電腦（請確保該軟件已安裝最新的病毒識別碼）。

7.4.5 慎防電郵騙案

(a) 未經收件人同意的電子郵件，除了對收件人造成滋擾外，也可能含有行騙及欺詐的成分。如果跟從郵件裏的指令，可能會使你的電腦感染病毒，身份資料被盜竊，甚至是金錢上損失。這樣的欺騙訊息稱為「詐騙電郵」。

(b) 香港警務處提供建議來避開這些欺詐性的電郵所設的陷阱。有關詳情請瀏覽：https://www.police.gov.hk/ppp_tc/04_crime_matters/ccb/fst.php?msg_id=cct_16