臺北市立文山特殊教育學校資通安全注意事項

適用對象：機關全體同仁

壹、 資通業務權限管理(含主機)

一、本機關之資通業務應設置通行碼管理，通行碼之要求需滿足：

(一)、通行碼長度8碼以上。

(二)、通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(三)、使用者每三個月(90天)應更換一次通行碼。

二、使用者辦理資通業務前應經授權，並使用唯一之使用者帳號，除有特殊營運或作業必要經核准並紀錄外，不得共用帳號。

貳、 特權帳號之存取管理

一、 資通設備之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

二、 資通設備之特權帳號不得共用。

三、 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者帳號。

四、 資通設備之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

五、 資通設備之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

參、 加密管理(例如：文書、人事、事務採購及學生個資)

一、 本機關之機密資訊於儲存或傳輸時應進行加密。

二、 本機關之加密保護措施應遵守下列規定：

(一) 應落實使用者更新加密裝置。

(二) 應避免留存解密資訊。

(三) 一旦加密資訊具遭破解跡象，應立即更改之。

肆、 作業與通訊安全管理

一、 防範惡意軟體之控制措施

（一） 本機關之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

A. 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

B. 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

C. 確實執行網頁惡意軟體掃描。

（二） 管理者並應每年定期針對管理之設備進行軟體清查。

（三） 使用者不得私自使用已知或有嫌疑惡意之網站。

（四） 使用者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

伍、 電子郵件安全管理

一、 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

二、 原則不得電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

三、 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

四、 使用者應確保電子郵件傳送時之傳遞正確性。

陸、 辦公室區域之實體與環境安全措施

一、 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

二、 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

三、 機密性及敏感性資訊，不使用或下班時應該上鎖。

四、 機密資訊或處理機密資訊之資通業務應避免存放或設置於公眾可接觸之場域。

五、 顯示存放機密資訊或具處理機密資訊之資通業務地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

六、 資訊或資通業務相關設備，未經管理人授權，不得被帶離辦公室。

柒、 資料備份

一、重要資料應進行定期資料備份。

二、敏感或機密性資訊之備份應加密保護。

捌、 媒體防護措施

一、 使用隨身碟或磁片等存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

二、 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

三、 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

四、 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

玖、 電腦使用之安全管理

一、 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。

二、 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

三、 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

四、 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

五、 下班時應關閉電腦及螢幕電源。

六、 如發現資安問題，應主動循機關之通報程序通報。

壹拾、支援資訊作業的相關設施

如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入，及減少敏感性資訊遭破解或洩漏之風險。

壹拾壹、 行動設備之安全管理

一、機密資料不得由未經許可之行動設備存取、處理或傳送。

二、機敏會議或場所不得攜帶未經許可之行動設備進入。

壹拾貳、 資通安全事件通報

在機關內使用之資通訊設備有被不當使用、資料遭不明竄改、刪除或中毒之情事等，請通報設備資訊組進行處理。

壹拾參、 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

壹拾肆、 資通安全維護計畫之實施

為落實本安全維護計畫，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時(例如：委外施作案件涉及使用機關資通訊設備時)，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。