高雄市立楠梓特殊學校資訊安全管理系統實施要點

96 年 5 月 30 日教育部國中、小學資通安全管理系統實施原則
101 年 8 月 29 日高雄市立楠梓特殊學校校務會議通過
104 年 8 月 28 日高雄市立楠梓特殊學校校務會議通過

一、 依據

96 年 5 月 30 日教育部國中、小學資通安全管理系統實施原則。
104 年 7 月 13 日教育部與所屬機關（構）及學校資通安全責任等級分級作業規定。

二、 實施要點

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由高雄市教育網路中心之管控，以符合一致性與單一性之安全要求。

1.2 網路安全管理服務委外廠商合約之安全要求

- 委外開發或維護廠商必須簽訂安全保密切結書[文件編號 A-1、A-6]。

2. 系統安全

2.1 職責區隔

- 學校行政電腦依個別應用系統之需要，設置專屬電腦，由各行政人員自行負責保管。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學校內的個人電腦應：
  - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理
  - 定期（至少每季）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞
  - 電腦教室若已安裝還原系統（需設定為開機還原），為因應教學特殊需求，可不安裝防毒軟體，但各種系統更新、漏洞修補程式（如 Windows Update）至少每學期更新一次。
- 學校內個人電腦所使用的軟體應有授權。
- 行政用電腦設定開機密碼及螢幕保護程式，以防資料不慎外洩。

2.3 資料備份

- 學校各系統管理人員需針對學校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作。

2.4 資訊存取限制

- 學校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。
  - 安裝還原系統，並設定系統碟為開機還原。
  - 禁止安裝 P2P 軟體。

2.5 特權管理

- 學校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，應予以文件化記錄備查，記錄表[文件編號：A-7]由系統或檔案保管人保管。

2.6 通報安全事件與處理

- 資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。
- 學校應建立資訊安全事件通報程序[文件編號 A-3]以及安全事件通報單[文件編號 A-4]；通報程序應包括學校內部通報，以及學校與高雄市教育網路中心的通報。
- 當學校內部無法處理之資通安全事件，應通報高雄市教育網路中心。
- 所訂出資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者瞭解。

3. 實體安全

3.1 設備安置及保護

- 學校重要的資訊設備（如主機機房）應置於設有空調空間。
- 學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食。
- 學校資訊設備主機機房、電腦教室區域內的電源線插頭應有接地的連結、或有避雷針等裝置，避免如雷擊事件所造成損害情況。
- 學校資訊設備主機機房、電腦教室區域，應至少於入出口處加裝門鎖或其他同等裝置。

3.2 電源供應

- 學校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置 UPS、電源保護措施，以免斷電或過負載而造成損失。

3.3 纜線安全

- 學校資訊設備主機機房、電腦教室區域內應避免明佈線。

3.4 設備與儲存媒體之安全報廢或再使用

- 所有包括儲存媒體的設備項目，在報廢前，應先確保已將任何敏感資料和授權軟體刪除或覆寫。

3.5 設備維護

- 應與設備廠商建立維護合約。
- 廠商進入安全區域需由學校人員陪同或簽訂安全保密切結書[文件編號 A-1、A-6]。

3.6 財產攜出

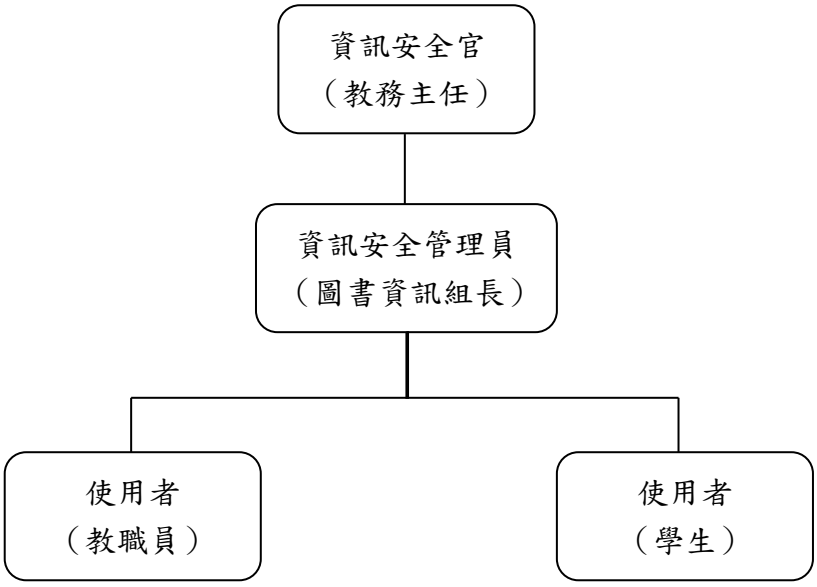
- 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。
- 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。
- 相關財產之攜出應依教育部或學校既有之相關規定處理。

3.7 桌面淨空與螢幕淨空政策

- 結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感特性的資料（例如公文、學籍資料等）及資料的儲存媒體（如 USB 隨身碟、磁碟片、光碟等），妥善存放。
- 學校提供教職員工或學生使用的個人電腦應設定保護裝置，如密碼以及螢幕保護[文件編號 A-2]。

4. 人員安全

4.1 組織架構簡圖



資訊安全組織成員表詳如[文件編號 A-6]

4.2 資訊安全教育與訓練

- 使學校(或委託)系統管理人員有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序。

- 學校鼓勵或安排資訊組長/老師/系統管理人員、以及所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。若全學年參與資訊安全教育相關訓練或宣導活動時數為零者，且無正當理由，得限制其使用校內資訊設備，以維護全校資訊安全。
- 將資訊安全教育納入學校電腦課程中。

5. 應對以下各項相關法令有基礎之認知

5.1 智慧財產權

- 經濟部智慧財產局 http://www.tipo.gov.tw/
- 著作權相關法規
  http://www.tipo.gov.tw/ch/Download_DownloadPage.aspx?path=2173&Language=1&UID=9&ClsID=35&ClsTwoID=71&ClsThreeID=0
- 著作權法
  http://www.tipo.gov.tw/ch/AllInOne_Show.aspx?path=1362&guid=a71977ea-6478-4e37-a46a-15497ba7c275&lang=zh-tw

5.2 個人資訊的資料保護及隱私

- 電腦處理個人資料保護法
  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=I0050021

5.3 電子簽章法

- 電子簽章法
  http://law.moj.gov.tw/LawClass/LawContent.aspx?PCODE=J0080037
- 電子簽章法施行細則
  http://law.moj.gov.tw/Scripts/newsdetail.asp?no=1J0080039
- 核可憑證機構名單
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm