臺北市文山區實踐國民小學資通安全管理規範

一、 目的

（一）制定校內教職員工於校內使用電腦及上網之管理準則以保護校內重要資料與學生、家長個人資料之安全。

（二）提升校內教職員工對資訊安全的重視。

二、 依據

（一）依據臺北市政府教育局 105 年 3 月 3 日函，教育部「全國中小學資訊安全線上稽核系統推廣實施計畫」辦理。

（二）依據電腦處理個人資料保護法，公務機關保有個人資料檔案者，應指定專人依相關法令辦理安全維護事項。

三、 適用範圍

本校校內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

四、 實施規定

1 網路安全

1.1 網路控制措施

1.1.1 與外界連線，應僅限於經由臺北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。

1.1.2 應禁止以私人架設網路（如：電話線、2G 或 3G 網路等）連結機房內之主機電腦或網路設備。

1.1.3 宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、電腦教室等，以降低未經授權存取之風險。

1.1.4 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之來源 IP 及網路連線埠(Port)，以確保安全。

1.2 無線網路存取

1.2.1 應禁止使用者私自將無線網路存取設備介接至校園網路;若有介接之必要應經權責管理人員同意並設定帳號通行碼或加密金鑰以防未經許可之盜用。

1.2.2 校園內應提供無線網路存取服務，並採取適當安全管控措施：

- 專供行政使用之無線網路熱點建議設定加密金鑰防護，並避免使用開放之無線網路存取重要資訊系統及處理敏感性資料。
- 於教學區域、會議室等場所佈建之無線網路熱點應具有使用者身分認證機制，並經由校園無線網路服務系統提供外校來

實使用。

- 專供師生教學活動使用之無線網路熱點,若採用其他管理方式確有不便時,應採取限定開放時間及限制開放區域等管理措施，減少遭受不當利用之機會。

2 系統安全

2.1 設備區隔

- 伺服器主機可依個別應用系統之需要，設置專屬主機，以避免未經授權之存取，例如網路服務主機(資訊交流平台、網站主機)、教學系統主機(例如隨選視訊主機)等。
- 學校的行政系統主機（例如財務、人事、會計、公文系統等）電腦，由各個縣（市）教育網路中心或教育局等單位統籌管理。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

2.2.1 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。
- 作業系統及軟體應定期更新，以防範系統漏洞。

2.2.2 個人電腦所使用的軟體應有授權。

2.2.3 新伺服器系統啟用前，應執行相關程序(如：確認適合該作業系統之掃毒工具、預設通行碼更新、系統更新等，並記錄於啟用與報廢紀錄單)，以防範可能隱藏的病毒或後門程式。

2.3 桌面淨空與螢幕淨空政策

2.3.1 個人電腦辦公桌面應避免存放機敏性文件，結束工作時，應將其所經辦或使用具有機密或敏感特性的資料(如公文、學籍資料等）妥善存放。

2.3.2 當個人電腦或終端機不使用時,應使用鍵盤鎖或其他控管措施保護個人電腦及終端機安全個人電腦應設定螢幕保護機制。

2.4 資料備份

2.4.1 系統管理人員需針對學校重要電腦系統及資料（如:系統檔案、網站、資料庫等）應每週至少進行一次備份工作；建議使用設備執行異地備份或使用光碟、隨身碟或外接式硬碟執行異地存放。

2.4.2 每年應定期檢查備份資料之可用性與完整性。

2.5 資訊工作日誌

2.5.1 系統管理人員需針對重要電腦系統進行檢查、維護、更新等動作時，應針對這些活動填寫日誌予以紀錄，作為未來需要時之查核。

2.5.2 系統管理人員應至少每季執行一次校時。

2.6 資訊存取限制

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(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)。

2.7 使用者註冊

校內電腦系統使用的使用者需向資訊組註冊帳號密碼,離職應立即註銷,透過該註冊及註銷程序來控制使用者資訊服務的存取,該作業應包括以下內容:

- 使用唯一的使用者帳號。
- 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
- 保存一份包含所有帳號註冊的記錄。
- 使用者調職或離職後,應移除其帳號的存取權限。
- 每學期應檢查使用者帳號,以確保帳號的有效性。

2.8 特權管理

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。

2.9 通行碼(Password)之使用

2.9.1 管制使用者第一次登入系統時,必須立即更改預設通行碼,預設通行碼應設定有效期限。

2.9.2 資訊系統與服務應避免使用共用帳號及通行碼。

2.9.3 由學校發佈通行碼制定與使用規則給使用者,內容應包含以下各項:

- 使用者應該對其個人所持有通行碼盡保密責任。
- 要求使用者的通行碼設定,應該包含英文字及數字,長度為8碼(含)以上。

2.10 通報安全事件與處理

2.10.1 資訊安全事件包括:系統被入侵、對外攻擊、針對性攻擊、散播惡意程式、中繼站、電子郵件社交工程攻擊、垃圾郵件、命令或控制伺服器、殭屍電腦、惡意網頁、惡意留言、網頁置換、釣魚網頁、個資外洩等。

2.10.2 學校應建立資訊安全事件通報程序;通報程序應包括學校內部通報,以及學校與市網中心通報。

2.10.3 當學校內部無法處理資安事件時,應通報市網中心。

3 實體安全

3.1 設備安置及保護

3.1.1 主機機房及電腦教室宜設置偵煙、偵熱或滅火設備(氣體式滅火器),並禁止擺放易燃物或飲食。

3.1.2 主機機房及電腦教室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。

3.1.3　主機機房及電腦教室應實施門禁管制。

3.2　電源供應

重要的資訊設備（如：主機機房等）應有適當的電力保護設施，例如設置UPS、電源保護措施(如：穩壓器、接地等)，以免斷電或過負載而造成損失，並設置緊急照明設備以作為停電照明之用。

3.3　纜線安全

主機機房及電腦教室內線路應考量設置保護設施(如:高架地板、線槽、套管等)。

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,在報廢前應填寫「啟用與報廢紀錄單」,確認已將任何敏感資料和授權軟體刪除或覆寫。

3.5　財產攜出

3.5.1　禁止資訊設備在未經授權之情況下攜離所屬區域,若需將設備攜出，應遵守財產管理相關規定並填寫「設備進出紀錄表」。

3.5.2　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。

4　可攜式電腦設備與媒體

4.1　校內可攜式電腦設備(如：筆記型電腦、平板電腦等)應設定保護機制。

4.2　校內可攜式電腦設備應執行安全相關程序（如：掃毒、預設通行碼更新、系統更新等)，以防範可能隱藏的病毒或後門程式。

4.3　校內可攜式儲存媒體(如：隨身碟、光碟、磁帶等)應依儲存資料的機敏性實施安全控管措施，如檔案加密儲存或將該儲存媒體存放於上鎖儲櫃或安全處所。

5　人員安全

5.1　人員安全責任

5.1.1　應將資訊安全納入教職員手冊說明中,強化工作上之資訊安全意識。

5.1.2　制定「臺北市文山區實踐國民小學個人電腦使用注意事項」，於校內網站上公告，列入新進員工教育訓練。

5.2　資訊安全教育與訓練

5.2.1　鼓勵校內資安業務承辦人參加資安管理系統相關教育訓練。

5.2.2　鼓勵校內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。

6　資訊業務委外管理

6.1　服務委外廠商合約之安全要求

6.1.1　在資訊業務委外合約中,應訂定委外廠商的資訊安全責任及保密規定。

6.1.2　應要求委外廠商簽訂安全保密切結書。

6.1.3 委外廠商人員到校服務時，應請其簽署委外廠商人員保密切結書。

6.2 委外廠商服務異動或終止時，應中止或刪除其系統上的帳號與權限。

7 應對以下各項相關法令有基礎之認知

7.1 智慧財產權

著作權法

7.2 個人資訊的資料保護及隱私

個人資料保護法及施行細則

7.3 刑法電腦犯罪專章

8 本計畫陳校長核准後實施，如有未盡事宜修正亦同。

承辦人　　教務主任　　校長