桃園市龜山區文華國民小學
資通安全維護計畫

【版本沿革】

・本案名稱：資通安全維護計畫：

107 學年度 108.06.20(四)資通安全管理會議與校長同意後修正

(第 03 版、108 學年度起適用)

・本案名稱：資通安全管理系統實施原則：

104 學年度 105.05.16(一)校長同意後修正(第 02 版)

101 學年度 102.01.16(三)校務會議決議通過(第 01 版)

【實施依據】

108 年 01 月 16 日桃園市各級學校資通安全維護計畫

107 年 06 月 06 日立法院資通安全管理法

103 年 02 月 07 日 教育部國中小資通安全管理系統實施原則修訂(v02)

105 年 04 月 07 日 桃教資字第 1050024853 號函

102.01.16 校務會議決議通過(v01)

97 年 01 月 03 日 府教數字第 0970001689 號函

96 年 12 月 24 日 府教數字第 0960428732 號函

教育部 96 年 12 月 19 日 台電字第 0960196582 號函－

教育部所屬機關及各級公私立學校資通安全工作事項

立法院審議 96 年度中央政府總預算—通案附帶決議事項

中 華 民 國 108 年 06 月 26 日

桃園市龜山區文華國小資通安全維護計畫

(第 03 版、108 學年度起適用)

【目錄】

桃園市龜山區文華國小資通安全維護計畫

(第 03 版、108 學年度起適用)

註：有關文字標示，說明如下—

藍色字為新增部分。

黃色標框粗體為教職員重點閱讀。

紅色粗體字為參考表件。

一、目的、適用範圍與資通安全責任等級

1. 目的

本文件提供桃園市龜山區文華國小資通安全維護計畫與系統管理實施原則建議，以增進資訊作業之安全性，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）。

2. 適用範圍

桃園市文華國小內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

3. 資通安全責任等級

3.1 責任等級分級(根據桃園市各級學校資通安全維護計畫)

- C 級：維運自行或委外開發之資通系統者。
- D 級：自行辦理資通業務，未維運自行或委外開發之資通系統者。
- E 級：無資通系統且未提供資通服務。或，屬公務機關，且其全部資通業務由其上級或監督機關兼辦或代管。

3.2 本校目前責任等級為：C 級

- 本校於機房自建各項伺服器(Windows、Linux、Apple 等)供各項教學使用、行政處理與對外服務。
- 本校自建相關動態網站系統(LAMP:Linux,Apache,MySQL,PHP)供各項教學使用、行政處理與對外服務。

二、資通業務－核心與非核心系統

1. 核心業務資通系統列表

業務對象	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
全校	Windows AD 服務	全校教職員 Windows 登入	無法進行前述運作	1～2 小時
全校	SFS3 學務系統	學生成績輸入＆查核 行政填報、維修通報等	無法進行前述運作	1～4 小時
全校	NAS 網路硬碟	全校教職員校務資料交流	無法進行前述運作	1～4 小時

2. 非核心業務資通系統列表

業務對象	非核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
全校	教育公務單一認證	教育局各項線上服務登入用	無法進行前述運作	依上級規定

業務對象	非核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
	授權平台			(外部網站)
人事教學	人力資源網 2.0	教學、課務安排人力資源。	無法進行前述運作	依上級規定(外部網站)
教學	學校課程計畫網站	學校課程計畫上傳	無法進行前述運作	依上級規定(外部網站)
教學	桃園市國民教育輔導團-學校資料系統	教學相關資料查詢	無法進行前述運作	依上級規定(外部網站)
註冊	教育部國民及學前教育署國民中小學學生資源網	應就學而未就學通報	無法進行前述運作	依上級規定(外部網站)
註冊	桃園市國民小學課後照顧填報	課後照顧填報	無法進行前述運作	依上級規定(外部網站)
設備	教育部全國閱讀推動與圖書管理系統網	全校圖書建檔&查詢用	無法進行前述運作	依上級規定(外部網站)
輔導	教務部特殊教育通報網	辦理特殊教育業務	無法進行前述運作	依上級規定(外部網站)
輔導	學生轉銜輔導及服務通報系統	處理學生國中轉銜輔導	無法進行前述運作	依上級規定(外部網站)
事務	財產管理系統	全校設備財產管理	無法進行前述運作	依上級規定(外部網站)
出納	薪資管理系統	全校教職員工薪資管理	無法進行前述運作	依上級規定(外部網站)
文書	電子公文系統文書端	文書組長電子公文資料交換	無法進行前述運作	依上級規定(外部網站)
行政	電子公文系統承辦端	承辦人員電子公文處理	無法進行前述運作	依上級規定(外部網站)
主計	會計管理系統	全校預算管理	無法進行前述運作	依上級規定(外部網站)
生教	教育部校園安全暨災害防救通報處理中心	校園安全暨災害防救通報	無法進行前述運作	依上級規定(外部網站)
生教	藥物濫用學生個案輔導追蹤管理系統	藥物濫用學生個案輔導追蹤	無法進行前述運作	依上級規定(外部網站)
生教	教育部校園性侵害性騷擾及性霸凌事件回覆填報系統	校園性侵害性騷擾及性霸凌事件回覆填報	無法進行前述運作	依上級規定(外部網站)
生教	桃園市交通安全執行歷程網站	交通安全業務執行	無法進行前述運作	依上級規定(外部網站)
生教	桃園市志願服務整合資訊平台	國中生志願服務媒合管理	無法進行前述運作	依上級規定(外部網站)
全校	Apple MDM	校端 iPad 管理	無法進行前述運作	1～8 小時
全校	IES 智慧教學雲端	智慧教學班級名單、線上儲存	無法進行前述運作	1～8 小時
資訊	DNS 服務	DNS 解析	無法進行前述運作	1 天
資訊	學校網頁	對外資訊公告、成果展示等	無法進行前述運作	1 天

業務對象	非核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
資訊	數位資料展示中心	對外數位資料展示	無法進行前述運作	1 天
資訊	作文發表系統	供全校歷屆中高年級發表作文	無法進行前述運作	1 天
資訊	校內資訊競賽系統	供全校選手進行各項資訊競賽	無法進行前述運作	1 天
資訊	環景圖片展示系統	對外展示校園環景	無法進行前述運作	1 天

三、資通安全政策與目標

1. 資通安全政策

1.1 定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。

1.2 保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。

1.3 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。

1.4 針對辦理資通安全業務有功人員應進行獎勵。

2. 資通安全目標

2.1 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。

2.2 校長、主任與教職員於每年資通安全教育訓練應達 3 小時。(含線上課程)

2.3 適時因應法令與技術之變動，調整資通安全維護之內容，以確保其機密性、完整性及可用性。

2.4 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。

2.5 提升人員資安防護意識、防止發生中毒或入侵事件。

四、資通安全推動組織

1. 依據

1.1 立法院資通安全管理法－第 11 條

1.2 桃園市教育局各級學校資通安全維護計畫－第伍項

2. 資通安全管理首長(簡稱：資安長)

2.1 首長代表：校長(或校長指定適當人選)

2.2 推動項目：

- 資通安全管理政策及目標之核定及督導。
- 資通安全責任之分配及協調。
- 資通安全資源分配。
- 資通安全防護措施之監督。
- 資通安全事件之檢討及監督。
- 資通安全相關規章與程序、制度文件核定。
- 資通安全管理年度工作計畫之核定
- 資通安全相關工作事項督導及績效管理。

- 其他資通安全事項之核定。

3. 資通安全推動小組(簡稱：資安小組)

3.1 小組成員：資安長(校長或校長指定)、教務主任、各處室代表、資訊組長

3.2 推動項目：

(參考表件：SSH-ISAS-107-01-Q04_資通安全推動小組及分工表)

- 跨部門資通安全事項權責分工之協調。
- 應採用之資通安全技術、方法及程序之協調研議。
- 整體資通安全措施之協調研議。
- 資通安全計畫之協調研議。
- 其他重要資通安全事項之協調研議。

五、人力及經費配置

1. 人力及資源之配置

1.1 本校依資通安全責任等級分級辦法之規定，目前屬資通安全責任等級為 C 級(自建伺服器等網路服務者屬於該級別)，最低應設置資通安全人員 1 人，本校現有資通安全人員為資訊組長。

1.2 本校於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。

1.3 本校於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

1.4 本校之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

2. 經費之配置

2.1 資安小組規劃配置相關經費及資源時，應考量本校資通安全政策及目標，提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2.2 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資安小組提出，由資安小組視整體資通安全資源進行分配，並經資安長核定後，進行相關之建置。**（參考表件：SSH-ISAS-107-03_資通安全需求申請單）**

2.3 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

六、資通系統之盤點

1. 資通系統盤點方式

1.1 應每學年進行一次資通系統資產盤點。

1.2 依管理責任指定對應之資產管理人，並依資產屬性進行分類。

2. 資訊及資通系統資產項目：

2.1 資訊資產：以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。

2.2 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

2.3 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

2.4 支援服務資產：相關基礎設施級其他機關內部之支援服務，如電力、消防等。

2.5 人員資產：內部設備維運管理人員、主管、使用人員，以及委外廠商駐點人員等。

2.6 資料資產：以紙本形式儲存之資訊，如程序、清單、計畫、報告、指引手冊、政策、公文、作業紀錄、作業規範、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等等。

3. 資通系統資產清冊

3.1 每學年度應依盤點結果製作之。

（參考表件：SSH-ISAS-107-04-Q06,Q07_資通系統資產清冊暨風險評估表）

3.2 欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

3.3 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資產清冊。

4. 資通系統資產標籤

4.1 標示位置：標籤應標示於設備明顯處。

4.2 載明財產編號、保管人、廠牌、型號及作業系統等資訊。

七、資通安全風險評估

1. 資通安全風險評估

1.1 本校應每年針對資訊及資通系統資產進行風險評估。

（參考表件：SSH-ISAS-107-04-Q06,Q07_資通系統資產清冊暨風險評估表）

2. 資通安全風險之因應

2.1 選擇防護及控制措施時，亦應考量採行該項措施可能對資通安全風險之影響。

（參考表件：SSH-ISAS-107-05_風險類型暨風險對策參考表）

八、資通安全防護及控制措施(實施原則)

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，應僅限於經由市網中心之管控，以符合一致性與單一性之安全要求。
- 承上，學校與外界連線，應設置防火牆並設置相關規則，以抵制外界對學校的不當連線（包括對伺服器的防火牆設定與對校內網路資源存取的防火牆設定）。

- **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。
- 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、宿網等，以降低未經授權存取之風險。
- 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

- **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。
- 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，並經由校園無線路漫遊服務系統提供外校來賓使用。
  - 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。
  - 開放校外人士出入之公共空間可視需要提供民眾無線上網服務，其網段應與校園網路隔離，或委由網路服務業者提供。

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(電子郵件、網站主機)、教學系統主機(例如隨選視訊主機)等**(參考表件：SSH-ISAS-107-06_管制區域人員進出登記表)**。

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。
  - **裝置防惡意程式軟體**，以防止惡意程式肆虐。
  - **作業系統及軟體應定期更新**，以防範系統漏洞。
  - 建置個人電腦系統備份檔(如 Ghost、CloneZilla 所建置的系統映像檔等)，以利作業系統中毒致損毀無法修復時，可即時還原，並減少作業系統安裝的耗時。
- 電腦教室的電腦應：
  - 若已安裝還原系統（如軟體還原、還原卡或無硬碟系統），需設定為開機還原。
  - 因應特殊需求，可不安裝防毒軟體（需有還原系統），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。
- **學校內所有個人電腦所使用的軟體應有授權**。

- 新系統啟用前，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。
  (參考表件：SSH-ISAS-104-01-Q21,Q34_啟用與報廢紀錄單)

2.3 桌面淨空與螢幕淨空政策

- 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)及資料的儲存媒體(如USB隨身碟、磁碟片、光碟等)，妥善存放**。
- 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**。
- 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，如個人鑰匙、個人密碼以及螢幕保護。

2.4 資料備份

- 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。
- 每年應定期檢查備份資料之可用性與完整性。

2.5 操作員日誌（適用於主機機房）

- 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。
  （參考表件：SSH-ISAS-104-02-Q23_資訊工作日誌）
- 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

- 學校內共用的個人電腦（如：電腦教室電腦、教師休息室電腦等）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）。
- **禁止安裝與使用 P2P 軟體（如 Foxy、BT、eMule、迅雷等）**。

2.7 使用者註冊

- 人員報到或離退職應會辦電腦系統帳號管理人員，執行電腦系統的使用者註冊及註銷程序，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。
  （參考表件：SSH-ISAS-104-03-Q16_帳號申請單）

2.8 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。
  （參考表件：SSH-ISAS-104-04-Q17_系統特權帳號清單）

2.9 通行碼（密碼）之使用

- 管制使用者第一次登入系統時，必須立即更改預設通行碼（密碼），預設通行碼（密碼）應設定有效期限。
- **資訊系統與服務應避免使用共同帳號及通行碼（密碼）**。
- 由學校發佈通行碼（密碼—Password）制定與使用規則給使用者，內容應包含以下各項：
  （參考表件：SSH-ISAS-104-05-Q27_優質通行碼設定原則與使用原則）
- 使用者應該對其個人所持有通行碼（密碼）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。
- 建議使用者**應該定期更換通行碼，至少每學年應更換一次**。

2.10通報安全事件與處理

- 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。
- 資訊安全事件等級，由輕微至嚴重區分等級如下：
- 符合下列任一情形者，屬 0 級事件：
  (1)未確定事件或待確認工單:來自不同計畫所使用新型技術(A-SOC，miniSOC,…)所產生之工單，但其正確性有待確認。
  (2)其他單位所告知教育部所屬單位所發生未確定之資安事件。
  (3)教育部及區、縣網路中心檢舉信箱通告之資安事件。
- 符合下列任一情形者，屬 1 級事件：
  (1)非核心業務資料遭洩漏。
  (2)非核心業務系統或資料遭竄改。
  (3)非核心業務運作遭影響或短暫停頓。
- 符合下列任一情形者，屬 2 級事件：
  (1)非屬密級或敏感之核心業務資料遭洩漏。
  (2)核心業務系統或資料遭輕微竄改。
  (3)核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。
- 符合下列任一情形者，屬 3 級事件：
  (1)密級或敏感公務資料遭洩漏。
  (2)核心業務系統或資料遭嚴重竄改。
  (3)核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。
- 符合下列任一情形者，屬 4 級事件：
  (1)國家機密資料遭洩漏。

(2)國家重要資訊基礎建設系統或資料遭竄改。

(3)國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

- 本校**任何人於校內發現異常情況或疑似資安事件，應立即向資安業務承辦人通報**，資安業務承辦人應儘速進行處理並研判事件等級。
- 資安業務承辦人當發生研判事件等級 3（含）以上之事件，應立即通報資訊業務主管及校長，並以電話聯絡教育局(處)資訊安全管理單位，由校長儘快召集會議研商處理的方式。
  （參考表件：SSH-ISAS-104-06-Q39_資安事件通報程序）
- 當發生無法處理之資通安全事件，應通報教育局(處)資訊安全管理單位協助處理。
- 教育機構資安通報平台（網址：https://info.cert.tanet.edu.tw/），帳號為學校 OID：2.16.886.111.90030.90007.100011。
- 資安通報依情報來源分為「告知通報」與「自行通報」，若收到「告知通報」事件通知，由資安業務承辦人登入教育機構資安通報平台，完成通報及應變作業。
- 資安事件若為校內人員自行發現，由資安業務承辦人登入教育機構資安通報平台進行「自行通報」完成通報及應變作業。
- 資安事件須於發生後 1 小時內進行通報，0、1、2 級事件於事件發生後 72 小時內處理完成並結案(包括通報與應變)，3、4 級事件於事件發生後 36 小時內完成並結案。
- 如有收到教育機構資安通報平台「資安預警事件」通知，由資安業務承辦人登入教育機構資安通報平台，進行資安預警事件單處理作業。
- 相關通報應變流程請依照「教育機構資安通報應變手冊」規定辦理。

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。
- 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、亦禁止飲食**。
- 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。
- 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。
- 資訊設備主機機房及電腦教室應實施門禁管制。

3.2 溫濕度控制

- 重要的資訊設備（如：主機機房等）宜有溫濕度控制措施(溫度建議控制在 20℃~25℃，濕度建議控制在相對濕度 50%R.H.~70%R.H.)，以防止資訊設備意外損壞。機房內應有溫濕度顯示裝置，以觀察實際之溫濕度情況。

3.3 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。

- 資訊設備主機機房宜安裝一組大型不斷電系統（UPS），以利機房重要設備電源的統一管理，並有效延長斷電時系統管理人員的反應時間。

3.4 纜線安全

- 主機機房及電腦教室內線路應設置保護設施(如：高架地板、線槽、套管等)。

3.5 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。
  （參考表件：SSH-ISAS-104-01-Q21,Q34_啟用與報廢紀錄單）

3.6 財產攜出

- 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」。
  （參考表件：SSH-ISAS-104-07-Q35_設備進出紀錄表）
- **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**。
  （參考【設備進出紀錄表】，文件編號：SSHES-ISAS-A07）
- 相關財產之攜出應依教育部或學校既有之相關規定處理。

4. 可攜式電腦設備與媒體

4.1 公務用可攜式電腦設備(如：筆記型電腦、平板電腦、智慧型手機等)應設定保護機制，如設定通行碼、圖形辨識、臉孔辨識或指紋辨識等。

4.2 公務用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 公務用可攜式儲存媒體(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。

4.4 非公務用之個人可攜式電腦設備，原則上不得連接校園有線與無線網路(依據「桃園市各級學校資通安全維護計畫」玖-二-(一)-2)。

5. 人員安全

5.1 人員安全責任

- 非正式人員、約聘(僱)人員者，因業務需要，而接觸公務機密、個人權益及學校機敏資料者須填寫保密切結書。
  （參考表件：SSH-ISAS-107-02-Q38_資通安全保密同意書）

5.2 資訊安全教育與訓練

- 鼓勵資安業務承辦人參加資安管理系統相關教育訓練。
- 鼓勵所有教職員參與資訊安全教育訓練或宣導，以提昇資訊安全認知。
- **建議全校教職員全學年應參與資訊安全教育**相關訓練或宣導活動**（如晨會資安宣導、校內外研習或 K12 線上研習）**，以提升全校教職員資訊安全素養。
- 應將資訊安全教育納入學校電腦課程中。

6. 資訊業務委外管理

6.1 服務委外廠商合約之安全要求

- 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。
  （參考表件：SSH-ISAS-107-11-Q41_委外廠商查核項目表）
- 應要求委外廠商簽訂安全保密切結書。
  （參考表件：SSH-ISAS-107-09-Q41_委外廠商執行人員-保密切結書）
- 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。
  （參考表件：SSH-ISAS-107-10-Q41_委外廠商執行人員-保密同意書）

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。
（參考表件：SSH-ISAS-104-03-Q16_帳號申請單）

7. 資通安全教育訓練

7.1 對象與作法

- 實施對象：本校依資通安全責任等級分級屬Ｃ級，一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。
  (參考表件：SSH-ISAS-107-07-Q42_年度資通安全教育訓練計畫)
- 實施作法：利用各集會場合對全校師生口頭宣導(至少一學期一次)。
  (參考表件：SSH-ISAS-107-08-Q42_資通安全認知宣導簽到表)

7.2 教育訓練內容

- 教職員工部份
  - 各項相關法令有基礎之認知：資通安全管理法、智慧財產權與著作權法、個人資訊的資料保護及隱私、個人資料保護法及施行細則、刑法電腦犯罪專章。
  - 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
- 學生部分
  - 資訊安全倫理與素養
  - 智慧財產與著作權法

九、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本校所屬人員之平時考核或聘用，依據下列規定審酌辦理之：

1. 公務機關所屬人員資通安全事項獎懲辦法
2. 教育部公立高級中等以下學校教師成績考核辦法
3. 本校各項相關規定

十、資通安全維護計畫之實施與績效

1. 資通安全維護計畫之實施

為落實本安全維護計畫，使本校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，應與本校之資通安全政策、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。
(參考表件：SSH-ISAS-107-12-Q44_(D 級適用)資通安全維護計畫實施情形)

2. 資通安全維護計畫之持續精進及績效管理

2.1 資通安全推動小組應召開資通安全管理審查會議(每年至少一次)，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
（參考表件：SSH-ISAS-107-13-Q44_審查結果及改善報告）

2.2 管理審查議題應包含下列討論事項：

- 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。
- 資通安全維護計畫內容之適切性。
- 資通安全績效之回饋，包括：
  - 資通安全政策及目標之實施情形。
  - 人力及資源之配置之實施情形。
  - 資通安全防護及控制措施之實施情形。
  - 不符合項目及矯正措施。
- 風險評鑑結果及風險處理計畫執行進度。
- 資通安全事件之處理及改善情形。
- 利害關係人之回饋。
- 持續改善之機會。

2.3 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。
（參考表件：SSH-ISAS-107-14-Q44_改善績效追蹤報告）

3. 資通安全維護計畫實施情形之提出

依據資通安全管理法第 12 之規定，本校應向上級或監督機關(中央目的事業主管機關)，提出資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全計畫實施情形。

十一、相關參考與附件

1. 相關法令參考網址如下

1.1 立法院資通安全管理法
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030297

1.2 桃園市各級學校資通安全維護計畫
http://sun.sshes.tyc.edu.tw/xoops/modules/tadnews/page.php?nsn=8441

1.3 教育部公立高級中等以下學校教師成績考核辦法
https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=H0150002

1.4 智慧財產權

- 經濟部智慧財產局 http://www.tipo.gov.tw/
- 著作權法
  http://www.tipo.gov.tw/copyright/copyright_law/copyright_law_92.asp

1.5 個人資訊的資料保護及隱私

- 電腦處理個人資料保護法
  www.fpppc.gov.tw/bulletin/menu4-7/93year/pcinfo.doc

1.6 電子簽章法

- 電子簽章法
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm
- 電子簽章法施行細則
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05_p01.htm
- 核可憑證機構名單
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm

2. 表件編號說明

2.1 表件編號類別

- 修訂格式參考自：教育部公版的預設附件
  （依據 103 年 02 月 07 日－教育部國中小資通安全管理系統實施原則）
- 表件編號格式：SSH-ISAS-10X-XX-QXX_名稱
- 第 1 碼－SSH：本校英文校名縮寫(DNS 網址)
- 第 2 碼－ISAS：資訊安全管理系統之縮寫
- 第 3 碼－10X：新增該表件時的學年度別。
- 第 4 碼－XX：表件流水號(依附於學年度別)。
- 第 5 碼－QXX：該表件於 ISAS 系統的適用題次。
- 第 6 碼－名稱：該表件中文名稱。

2.2 表件名稱

- SSH-ISAS-104-01-Q21,Q34_啟用與報廢紀錄單
- SSH-ISAS-104-02-Q23_資訊工作日誌
- SSH-ISAS-104-03-Q16_帳號申請單
- SSH-ISAS-104-04-Q17_系統特權帳號清單
- SSH-ISAS-104-05-Q27_優質通行碼設定原則與使用原則
- SSH-ISAS-104-06-Q39_資安事件通報程序
- SSH-ISAS-104-07-Q35_設備進出紀錄表
- SSH-ISAS-107-01-Q04_資通安全推動小組及分工表
- SSH-ISAS-107-02-Q38_資通安全保密同意書
- SSH-ISAS-107-03_資通安全需求申請單
- SSH-ISAS-107-04-Q06,Q07_資通系統資產清冊暨風險評估表
- SSH-ISAS-107-05_風險類型暨風險對策參考表
- SSH-ISAS-107-06_管制區域人員進出登記表
- SSH-ISAS-107-07-Q42_年度資通安全教育訓練計畫
- SSH-ISAS-107-08-Q42_資通安全認知宣導簽到表
- SSH-ISAS-107-09-Q41_委外廠商執行人員-保密切結書
- SSH-ISAS-107-10-Q41_委外廠商執行人員-保密同意書
- SSH-ISAS-107-11-Q41_委外廠商查核項目表
- SSH-ISAS-107-12-Q44_(D 級適用)資通安全維護計畫實施情形

- SSH-ISAS-107-13-Q44_審查結果及改善報告
- SSH-ISAS-107-14-Q44_改善績效追蹤報告

十二、本實施原則經資安小組同意，校長核可後實施，修正時亦同。

承辦人　　教務主任　　校長

資訊組長 陳俊源　　代理教務主任 黃呈文　　文華國民小學 校長 葉俊泰