桃園市立楊梅國民中學
資通安全維護計畫

承辦人簽章：

單位主管簽章：

校長(資安長)簽章：

中華民國 108 年 6 月 2 日

目　　錄

壹、依據及目的

依據資通安全管理法第 10 條及施行細則第 6 條訂定資通安全維護計畫,作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。

貳、適用範圍

本計畫適用範圍涵蓋桃園市立楊梅國民中學 (以下簡稱本校)。

參、資通業務及重要性

一、 非核心業務及說明：

本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
學校官網	可能使民眾無法查詢本校公告資訊	12 小時
公文電子交換系統	電子公文無法即時送達機關，影響機關行政效率	12 小時
公文整合資訊系統	影響機關行政效率	12 小時
薪資系統	影響機關行政效率	24 小時
排課系統	影響機關行政效率	24 小時
調代課系統	影響機關行政效率	24 小時
出納管理系統	影響機關行政效率	24 小時

肆、資通安全政策及目標

一、資通安全政策

為使本校業務順利運作，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），特制訂本政策如下，以供全體同仁共同遵循：

1. 應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。
2. 針對辦理資通安全業務有功人員應進行獎勵。
3. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
4. 禁止多人共用單一資通系統帳號。
5. 不得私接網路。
6. 安裝市府規定之防毒系統。
7. 配合政策使用市府網域帳號登出入電腦及系統。

二、資通安全目標

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. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
3. 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。
4. 提升人員資安防護意識、防止發生中毒或入侵事件。

三、資通安全政策及目標之核定程序

資通安全政策由本校教務處簽陳資通安全管理代表核定。

四、資通安全政策及目標之宣導

1. 本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向所有人員進行宣導，並檢視執行成效。
2. 本校應每年進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於內部會議中檢討其適切性。

伍、資通安全推動組織

一、資通安全管理代表

依本法第 11 條之規定，本校訂定校長為資通安全管理代表，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定及督導。

2. 資通安全責任之分配及協調。

3. 資通安全資源分配。

4. 資通安全防護措施之監督。

5. 資通安全事件之檢討及監督。

6. 資通安全相關規章與程序、制度文件核定。

7. 資通安全管理年度工作計畫之核定

8. 資通安全相關工作事項督導及績效管理。

9. 其他資通安全事項之核定。

二、資通安全推動小組

(一) 組織

為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理,由資通安全管理代表召集各主管/副主管以上之人員代表組成立資通安全推動小組，其任務包括：

1. 跨部門資通安全事項權責分工之協調。

2. 應採用之資通安全技術、方法及程序之協調研議。

3. 整體資通安全措施之協調研議。

4. 資通安全計畫之協調研議。

5. 其他重要資通安全事項之協調研議。

(二) 分工及職掌本校之資通安全推動小組依下列分工進行責任分組，並依資通安全管理代表指示負責下列事項，本校資通安全推動小組人員名單及職掌應列冊，並適時更新之：

1. 資通安全推動小組，其工作內容得參考下列事項：

(1) 資通安全政策及目標之研議。

(2) 訂定機關資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。

(3) 依據資通安全目標擬定機關年度工作計畫。

(4) 傳達機關資通安全政策與目標。

(5) 資料及資通系統之安全防護事項之執行。

(6) 資通安全事件之通報及應變機制之執行。

(7) 資訊及資通系統之盤點及風險評估。

(8) 其他資通安全事項之規劃。

陸、人力及經費配置

一、人力及資源之配置

1. 本校依資通安全責任等級分級辦法之規定，屬資通安全責任等級D級，最低應設置設置一名正式人員兼辦資通安全業務負責，本校現有資通安全人員名單及職掌應列冊，並適時更新。

2. 本校之承辦單位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。本校之相關單位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。

3. 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。

二、經費之配置

1. 資通安全推動小組於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2. 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通安全推動小組提出，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全管理代表核定後，進行相關之建置。

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。

柒、資訊及資通系統之盤點

一、機關資通安全責任等級分級

本校因自行辦理資通業務，未維運自行或委外開發之資通系統者，為資通安全等級分類 D 級機關。

捌、資通安全風險評估

(C 級機關資通訊設備及系統、D 級機關資通訊設備(如電腦、網路設備))

一、資通安全風險評估

本校應每年針對資訊及資通系統資產進行風險評估。

二、資通安全風險之因應

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。

玖、資通安全防護及控制措施

本校依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及資通系統之防護基準，採行相關之防護及控制措施如下:

一、存取控制與加密機制管理

(一) 網路安全控管

1. 本機關應定期檢視防火牆政策是否適當，並由上級單位統一辦理更新與升級。

2. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

3. 有關網路安全控管主要由本府資訊中心統籌辦理，網路使用均依規定填具申請書。

4. 本校內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

5. 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與電腦，應安裝防毒軟體，並定期更新病毒碼。

(二) 資通系統權限管理

1. 資通系統應設置通行碼管理，通行碼之要求需滿足：

(1) 通行碼長度 8 碼以上。

(2) 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。

(3) 使用者每 90 天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

二、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校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。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

3. 使用者不得私自使用已知或有嫌疑惡意之網站。

4. 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。

5. 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。

(二) 確保實體與環境安全措施

1. 電腦機房之門禁管理

(1) 電腦機房應進行實體隔離。

(2) 機關人員或來訪人員應申請及授權後方可進入電腦機房，管理者並應定期檢視授權人員之名單。

(3) 人員及設備進出應留存記錄。

(4) 電腦機房之空調、電力應建立備援措施。

2. 辦公室區域之實體與環境安全措施

(1) 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。

(2) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(三) 資料備份

1. 重要資料及資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求。

2. 敏感或機密性資訊之備份應加密保護。

(四) 媒體防護措施

1. 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。

2. 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。

(五) 電腦使用之安全管理

1. 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。

2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

3. 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。

4. 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。

5. 下班時應關閉電腦及螢幕電源。

6. 如發現資安問題，應主動循機關之通報程序通報。

(六) 行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。

2. 機敏會議或場所不得攜帶未經許可之行動設備進入

三、資通安全防護設備

應安裝防毒軟體，持續使用並適時進行軟、硬體之必要更新或升

級。

壹拾、資通安全事件通報、應變及演練

為即時掌控資通安全事件，並有效降低其所造成之損害，本校應訂定資通安全事件通報、應變及演練，依本校資通安全事件通報應變程序辦理。

壹拾壹、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、可接受之風險及本校之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

二、資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資通安全推動小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 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。

壹拾貳、資通安全教育訓練

一、資通安全教育訓練要求

本校依資通安全責任等級分級屬 D 或 E 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。

二、資通安全教育訓練辦理方式

1. 每年參加中央機關、桃園市政府辦理之資通安全教育訓練或利用數位學習以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。
2. 員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。
3. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾參、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，依據公務機關所屬人員資通

安全事項獎懲辦法審酌辦理。

壹拾肆、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、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。

二、資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動小組應 (每年至少一次)召開內部會議，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。

2. 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。

壹拾伍、資通安全維護計畫實施情形之提出

本校依據資通安全管理法第 12 之規定，應向上級或監督機關，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。