高雄市立楠梓特殊學校

資通安全維護計畫

機密等級：一般

承辦人簽章：教師兼圖資組長蔡宛玲

單位主管簽章：教師兼教務主任邱長森

校長(資安長)簽章：高雄市立楠梓特殊學校校長黃國書

中華民國 110 年 6 月 28 日

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。

貳、適用範圍

本計畫適用範圍涵蓋高雄市立楠梓特殊學校全校(含瑞平分校)，以下簡稱本校。

參、核心業務及重要性

一、 資通業務及重要性：

目前本校校內無核心資通系統。

二、 非核心業務及說明：

非核心業務及說明如下表:

非核心業務	非核心資通系統	業務失效影響說明	最大可容忍中斷時間
教務業務	由高雄市政府特教學籍管理系統（校務管理系統，向上集中）	影響學校部分教學業務運作	由上級管理單位訂之
學生事務業務			
輔導業務			
人事業務	行政院人事行政總處人事服務網	人事部份業務無法運作	由上級管理單位訂之
會計業務	地方教育發展基金會計資訊系統	會計部分業務無法運作	由上級管理單位訂之
總務業務	高雄市政府二代公文系統(機房向上集中)	收發公文部分業務無法運作	由上級管理單位訂之
資訊組業務	高雄市教育局資教中心校園網站(機房向上集中）	對外公告資訊無法運作	由上級管理單位訂之
出納組業務	薪資管理系統	出納部分業務無法運作	由上級管理單位訂之

事務組業務	採購相關業務系統 標案管理系統 財產管理系統	採購部分業務無法運作 標案管理業務無法運作 財產管理系統無法運作	由上級管理單位訂之

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. 建立資通安全風險管理機制，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。
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。
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。
4. 針對辦理資通安全業務有功人員應進行獎勵。
5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
6. 禁止多人共用單一資通系統帳號。
7. 校內同仁及外部廠商須簽屬相關資通安全保密切結與同意書。

二、資通安全目標

(一) 量化型目標

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. 校園電腦防毒軟體 100%啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
3. 每人每年接受三小時以上之一般資通安全教育訓練。

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

本校設置「資通安全推動小組」負責督導校內資訊安全相關事項，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業務人員代表成立資通安全推動小組，其任務包括：

1. 跨處室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分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：

(1) 資通安全政策及目標之研議。

(2) 訂定本校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年度工作計畫。

(4) 傳達資通安全政策與目標。

(5) 其他資通安全事項之規劃。

(6) 資訊及資通系統之盤點及風險評估。

(7) 資通安全相關規章與程序、制度之執行。

(8) 資料及資通系統之安全防護事項之執行。

(9) 資通安全事件之通報及應變機制之執行。

續運作計畫、稽核紀錄及歸檔之資訊等。

(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。

(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。

(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。

(5) 人員資產：校內各項資訊系統與設備使用人員清冊，以及委外廠商駐點人員清冊等。

(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。

二、機關資通安全責任等級分級

依據教育部臺教資(四)字第 1070202157 號函文，本校為公立高級中等以下學校，且配合資訊資源向上集中計畫，核心資訊系統均由上級或監督機關兼辦或代管，其資通安全責任等級為 D 級。

捌、資通安全風險評估

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，若配合資訊資源向上集中計畫，資訊系統由上級或監督機關兼辦或代管，則不需進行。

二、資通安全風險之因應

本校配合資訊資源向上集中計畫，核心資訊系統均由上級或監督機關兼辦或代管，不再另行訂定。

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

二、存取控制與加密機制管理

(一) 網路安全控管

1. 網路區域劃分如下：

(1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2) 內部區域網路 (Local Area Network, LAN) ：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3. 本校應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。若為向上集中管理，則由上級單位統一辦理更新與升級。

4. 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. 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。

6. 無線網路防護

(1) 機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2) 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工作站，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。

(三) 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。

2. 電腦機房之環境控制

(1) 電腦機房之空調、電力應建立備援措施。

(2) 電腦機房應安裝之安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全之危險。

3. 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。

(四) 資料備份

1. 重要資料及資通系統應進行資料備份，並執行異地存放。

2. 敏感或機密性資訊之備份應加密保護。

(五) 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。

(六) 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。

成果，並檢討執行情形。

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

銷毀履行委託契約而持有之資料。

3. 本校應定期或於知悉受託者發生可能影響受託業務之資通安全事件。

壹拾參、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 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. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立人員資通安全認知，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. 本校資通安全認知宣導及教育訓練之內容得包含：

(1) 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)。

(2) 資通安全法令規定。

(3) 資通安全作業內容。

(4) 資通安全技術訓練。

3. 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。

壹拾肆、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，及本校各相關規定辦理之。

壹拾伍、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，

2. 資通安全管理法施行細則

3. 資通安全責任等級分級辦法

4. 資通安全事件通報及應變辦法

5. 資通安全情資分享辦法

6. 公務機關所屬人員資通安全事項獎懲辦法

7. 資訊系統風險評鑑參考指引

8. 政府資訊作業委外安全參考指引

9. 無線網路安全參考指引

10. 網路架構規劃參考指引

11. 行政裝置資安防護參考指引

12. 政府行動化安全防護規劃報告

13. 安全軟體發展流程指引

14. 安全軟體設計指引

15. 安全軟體測試指引

16. 資訊作業委外安全參考指引

17. 本機關資通安全事件通報及應變程序

二、附件表單

1. 資通安全推動小組成員及分工表

2. 資通安全保密同意書

3. 資通安全需求申請單

4. 資訊及資通系統資產清冊

5. 風險評估表

6. 風險類型暨風險對策參考表

7. 資訊資產價值評定標準

8. 風險事件發生可能性評定標準

9. 管制區域人員進出登記表