澎湖縣沙港國民小學

資通安全維護計畫

機密等級：一般

承辦人簽章：

單位主管簽章：

資安長(校長)簽章：

簽章日期：115.08.01

壹、依據及目的

本計畫依據下列法規訂定：

資通安全管理法第13條（第20條第2項及第21條第1項規定）及資通安全管理法施行細則第9條。

貳、適用範圍

本計畫適用範圍涵蓋本校澎湖縣沙港國民中/小學(以下簡稱本校)。

參、核心業務及重要性

一、核心業務及重要性：

本機關之核心業務、核心資通系統及重要性如下表，並針對全部核心資通系統訂定營運持續計畫，定期辦理業務持續運作演練：：

核心業務	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(MTPD)	復原時間目標（RTO）	復原點目標（RPO）
教務業務	學務管理系統（向上集中） 學生資源網（向上集中）	■為本機關依組織法執掌，足認為重要者	違反法遵義務： 依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	由上級管理單位訂之	由上級管理單位訂之	由上級管理單位訂之
學生事務	學務管理系統（向上集中）	■為本機關依組織法執掌，足認為重要者	違反法遵義務： 依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。	由上級管理單位訂之	由上級管理單位訂之	由上級管理單位訂之
總務業務		■為本機關依組織法執掌，足認為重要者	可能使本校部分業務中斷			
輔導業務	教育部相關系統（向上集中） 學務管理系統（向上集中）	■為本機關依組織法執掌，足認為重要者	可能使本校部分業務中斷	由上級管理單位訂之	由上級管理單位訂之	由上級管理單位訂之

各欄位定義：

1.核心業務：請參考資通安全管理法施行細則第10條之規定列示。

2.核心資通系統：請列出支持核心業務運作必要之系統（無可免）。

3.重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4.最大可容忍中斷時間單位以小時計。

二、非核心業務及說明：

本校之非核心業務及說明如下表：

非核心業務	資通系統	業務失效影響說明	最大可容忍中斷時間(MTPD)	復原時間目標(RTO)	復原點目標(RPO)
校園相關資訊	學校網站（向上集中）	可能造成家長、民眾無法瀏覽	由上級管理單位訂之	由上級管理單位訂之	由上級管理單位訂之
個人電腦安全防護	防毒軟體	未安裝容易造成校園電腦中毒	24小時	24小時	24小時
網路管理	防火牆 無線 AP （向上集中）	可能使本校對外連線中斷	由上級管理單位訂之	由上級管理單位訂之	由上級管理單位訂之
公文交換	公文系統	電子公文無法即時送達機關，影響機關行政效率	由上級管理單位訂之	由上級管理單位訂之	由上級管理單位訂之

各欄位定義：

1.業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)

2.業務失效影響說明：說明該業務失效時之影響。

3.最大可容忍中斷時間單位以小時計。

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），特制定本政策如下，以供全體同仁共同遵循：

(一)應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。

(二)應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。

(三)應強固核心資通系統之韌性，確保機關業務持續營運。

(四)應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本機關同仁之資通安全意識，本機關同仁亦應確實參與訓練。

(五)針對辦理資通安全業務有功人員應進行獎勵。

(六)勿開啟來路不明或無法明確辨識寄件人之電子郵件。

(七)禁止多人共用單一資通系統帳號。

(八)校內同仁及外部廠商須簽屬相關資通安全保密切結/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.電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於5%及2%。

（二）質化型目標：

1.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。

2.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。

3.提升人員資安防護意識、有效偵測與預防外部攻擊等……。

三、資通安全政策及目標之核定程序

資通安全政策由本校簽陳資通安全長核定。

四、資通安全政策及目標之宣導

本機關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、電子郵件、個人電腦螢幕保護程式等方式，向機關內所有人員進行宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資安政策及目標每年定期於資通安全管理審查會議中檢討其適切性。

伍、資通安全推動組織

一、資通安全長

依本法第12條（公務機關）、第23條規定（特定非公務機關）之規定，本校擇請校長/林宗彥兼任本校資通安全長，負責督導機關資通安全相關事項，其任務包括：

（一）資通安全管理政策及目標之核定、核轉及督導。

（二）資通安全責任之分配及協調。

（三）資通安全資源分配。

（四）資通安全防護措施之監督。

（五）資通安全事件之檢討及監督。

（六）資通安全相關規章與程序、制度文件核定。

（七）資通安全管理年度工作計畫之核定。

（八）資通安全相關工作事項督導及績效管理。

（九）其他資通安全事項之核定。

二、資通安全推動小組

(一)組織

為推動本機關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，由資通安全長召集本校相關主管及承辦人員代表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，並依資通安全長之指示負責下列事項，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：

A.風險管理及法律遵循：負責資產盤點管理作業，包含資訊資產清冊之維護等。

B.法律遵循：負責規劃及辦理資通安全管理適法性之識別、相關爭訟（議）案件之協調處理，並配合司法單位調查之進行，提供必要資源等。

C.推動、執行及危機應變：

1.負責執行資通安全管理法中各項措施及管制。

2.規劃教育訓練及相關宣導事項之辦理，承辦人員需參加本縣教網中心辦理之相關教育訓練。

3.建立資通安全維護計畫等。

4.推動資通安全業務，彙整實施成果等。

5.執行資通安全危機應變處理、事件通報及相關演練活動等。

D、稽核：負責執行資通安全稽核作業，包含稽核計畫之撰寫、稽核發現之改善追蹤等。

陸、專職(責)人力及經費配置

一、專職(責)人力及資源之配置

(一)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，最低應設置資通安全專職人員1人，並應將資通安全人員名單及其職掌列冊及適時更新。

(二)本校之承辦人員於辦理資通安全業務時，應強化資安人員之培訓，挹注資源以提升其資通安全管理或防護技術能力。本校辦理資通安全業務時，如資通安全人力或經驗不足，得洽請澎湖縣教育網路中心或相關專業機關（構）/人員，提供顧問諮詢服務。

(三)資安專職人員之培養，依據資通安全責任等級分級辦法之規定辦理。

(四)本校之首長，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

(一)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。

(二)校內如有資通安全相關設備之需求，可向上級機關提出相關申請，由上級機關審核申請需求及相關資源來決議。

(三)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、資訊及資通系統盤點

本機關每年辦理資通系統及資訊資產盤點，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，分別為資訊資產、軟體資產、實體資產、支援服務資產等。

(一)資通系統及資訊資產項目如下：

1.人員類：內部人員、外部人員（含委外人員）等。

2.資訊類：作業文件（含系統文件）、合約、電子資料紀錄（含系統紀錄）、稽核紀錄及歸檔之資訊等。

3.軟體類：作業系統、系統軟體、應用系統、套裝軟體、資安軟體等。

4.硬體類：個人電腦（含筆記型、平板電腦）、伺服器、其他硬體、網路設備、可攜式儲存媒體（有資料/無資料）、電腦保護設施、物聯網裝置等。

5.建築與保護類：辦公區域、資訊機房、檔案室區域、倉庫/庫房、建築保護設施等。

6.服務類：內外部服務、委外服務、雲端服務等。

7.支援服務類：相關基礎設施及其他機關內部之支援服務，如電力、消防等。

(二)本校每年度應依資訊及資通系統盤點結果 ，製作「資通系統及資訊資產清冊」 ，欄位應包含：資產名稱、資產類別、擁有者、管理者、使用者、存放位置、資產說明、機密性、完整性、可用性、可律遵循性、資產價值等級。

(三)本校依前揭盤點結果，倘發現機關有下載、安裝或使用危害國家資通安全產品（含大、香港或澳門廠牌資通訊產品）時，應確認下列事項：

1.自114年12月1日資通安全管理法修正施行後，凡下載、安裝或使用之產品，應依規定向主管機關申請專案核准使用；未經主管機關核定

之產品，應即刻移除、解除安裝或停止使用。倘因使用未經核定之產品，致有影響機關資通安全之虞，本機關得依資通安全管理法第28條規定，對相關人員予以懲戒或懲處。

2.機關現存之危害國家資通安全產品（含軟體、硬體及服務），應依「危害國家資通安全產品審查辦法」第7條規定，採取相關必要之管控措施 。

(四)網路設備、桌上型電腦、筆記型電腦等之硬體類資產，應將可供識別之資產清冊資訊以適當方式或財產標籤標示於硬體外觀（如：財產編號、財產名稱、財產別名、購買日期、年限、保管單位等），以供區別。

(五)為確保使用物聯網（IoT）裝置安全，避免不當使用，遭受蓄意資料竊取、遺失或惡意程式入侵等資通安全事件發生，每年度應盤點 IoT 裝置，並針對網路印表機、門禁設備、網路攝影機、無線網路基地台/無線路由器、環控系統、網路儲存伺服器（NAS）等進行資安檢核。

(六)校內各單位管理之資通系統或資訊資產如有異動，應即時通知總務處及網管更新資產清冊。

二、機關資通安全責任等級分級

依資通安全責任等級分級辦法第7條規定，本機關為資通安全責任等級D級機關。

捌、資通安全風險管理

一、資通安全風險評估

(一)本機關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)執行風險評估時應參考國家資通安全研究院頒布之最新「資通系統風險評鑑參考指引」，並依其中之「詳細風險評鑑」進行風險評估之工作。

二、核心資通系統及最大可容忍中斷時間

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核心資通系統之防護基準，採行相關之防護及控制措施如下:

一、管理面

(一)實施資通系統分級及防護基準。

(二)配置資通安全專職人員。

(三)系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

二、使用及技術面

(一)本校同仁使用資訊及資通系統前應經其管理人授權。

(二)本校同仁離職前，應依規定之程序歸還或移交相關設備或資訊。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

(三)非本校同仁不得使用本校之資訊及資通系統。

(四)建置並維護資通安全監測管理機制，並實施政府組態基準。

(五)完成啟用並維護資通安全防護措施（包括防毒軟體、網路防火牆)，同時應定期進行軟、硬體之必要更新或升級。

(六)電子資料安全管理措施 。

三、認知與訓練

(一)依據資安法規及D級機關應辦事項，定期辦理資通安全教育訓練。

(二)確保人員於進用、任職及職務終止等各階段均了解其資通安全責任，並進行相關教育訓練以降低因人為因素所造成的安全風險。

四、存取控制與加密機制管理

依教育網路中心相關程序辦理，以確保資通作業其所運用之系統與資料的存取權限及存取密碼，經適當的授權及控管，以防止不當存取：

(一)IP 造冊：對於校內所有 IP 位址，對應其使用者或資訊設備來進行登記造冊，務必確實記錄。

(二)校內所有人員應依規定之方式存取網路服務，不得於校內任何場所私裝電腦、無線基地台及通訊等相關設備。

(三)機密資料原則不得透過無線網路及設備存取、處理或傳送。

(四)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。

(五)本校之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，且複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

2.使用者每180天應更換一次通行碼。

(六)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。

(七)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

(八)本校之機密資訊(含個資)於儲存或傳輸時應進行加密。

(九)使用者不得私自使用已知或有嫌疑惡意之網站。

五、資料備份

(一)重要資料應定期進行資料備份，並執行異地存放。

(二)本校應定期確認資料備份之有效性，且敏感或機密性資訊之備份應加密保護。

(三)資料備份禁止共用單一帳號雲端硬碟進行備份，且應注意個人權限。

六、校園 OpenID 安全管理(含電子郵件安全管理)

(一)本校人員到職後應經網管向本縣教網中心申請 OpenID 教育單一登入體系帳號，即可使用各項雲端服務及電子郵件帳號，並應於人員離職後向教育

網路中心申請刪除帳號之使用。

(二)定期進行 OpenID 帳號清查，令使用者需定期依本法修改通行碼。

(三)原則不得透由電子郵件傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

(四)使用者不得利用電子郵件服務從事侵害他人權益或違法之行為。

(五)使用者應確保電子郵件傳送時之傳遞正確性。

七、實體與環境安全管理

(一)電腦機房之門禁管理

1.電腦機房及相關設備，應進行實體隔離。

2.確保機房及辦公區域之實體環境安全，並保護相關資產之安全。

3.校內人員應隨時注意身分不明或可疑人員。

(二)電腦機房環境控制

1.應安裝之安全偵測及防護措施，如熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備等系統，以減少環境不安全引發之危險。

2.各項安全設備應定期執行檢查、維修。

(三)辦公室區域之實體與環境安全措施

1.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.文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

3.機密性及敏感性資訊，不使用或下班時應該上鎖。

4.機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

5.顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

6.資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

八、電腦及媒體防護安全管理措施

(一)使用隨身碟(含隨身硬碟)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。

(二)資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

(三)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，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(四)電腦、業務系統，若超過十五分鐘不使用時，應設置自動登出或啟動螢幕保護功能。

(五)禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

(六)如發現資安問題，應主動循機關之通報程序通報。

(七)相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

九、即時通訊軟體之安全管理

(一)使用即時通訊軟體傳遞機關內部公務訊息，其內容不得涉及機密資料(含個資)。但有業務需求者，應使用經專責機關鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。

(二)使用於傳遞公務訊息之即時通訊軟體宜考量下列安全性需求：

1.用戶端應有身分識別及認證機制。

2.訊息於傳輸過程應有安全加密機制。

壹拾、資通安全事件通報、應變及演練相關機制

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、應變及演練相關機制，詳資通安全事件通報應變程序。

壹拾壹、資通安全情資之評估及因應機制

因本校為D級資安機關，配合教育部向上集中計畫，相關資安情資之獲取，主要由上級機關教網中心管理及處理，次要再依教網中心通知之情資內容，視其對本校之影響，決定最適當之因應方式並留下文件化紀錄，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

(一)資通安全相關之訊息情資及入侵攻擊情資，由上級機關教網中心統一進行評估、分析。

(二)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、國民身分證、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及入侵攻擊情資

由上級機關教網中心統一進行評估、分析及處理。並依教網中心之要求或規範，進行校內因應、管理、修正及保護作業。

(二)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、資通系統或服務委外辦理之管理措施

本校依資通安全責任等級分級辦法第7條D級機關法規，並配合教育部向上集中之規範，不得自行辦理資通系統之建置、維運或委外。

壹拾叁、資通安全教育訓練

一、資通安全教育訓練要求

(一)本校依資通安全責任等級分級屬D級，資通安全專職人員每人每二年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。

（二）本校之一般使用者與主管，每人每年接受三小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式。

(一)校內應於每學年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全教育訓練計畫，以建立校內全體同仁資通安全認知，提升機關資通安全水準，並應保存相關之資通安全教育訓練紀錄。相關專責人員則需參加上級機關辦理之相關教育訓練。

(二)本校資通安全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、作業內容及技術訓練。

3.資訊安全及倫理宣導。

4.電腦處理個人資料保護法相關法規及作業原則。

(三)校內人員報到時，應使其充分瞭解本校資通安全相關規範及重要性，並簽訂相關同意書(含個資法授權同意書、資安法保密同意書)。

(四)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。

壹拾肆、所屬人員辦理業務涉及資通安全事項之考核機制

本機關所屬人員辦理業務涉及資通安全事項，依資通安全管理法第18條第1項及第28條第1項規定，績效優良者，應予獎勵；未依該法規定辦理者，應按其情節輕重，依相關規定予以懲戒或懲處。

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，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一)稽核機制之實施

1.資通安全推動小組配合教網中心之規範及要求，依教網中心排程進行相關受稽核作業，以確認是否遵循資安規範與管理程序要求，並有效實作及維持管理制度。

2.受稽核前，校內應擬定並安排受稽核成員，並確認受稽核之內容是否已完成，並將前次稽核之結果納入稽核範圍。

3.稽核結果應對資安長報告，並留存稽核結果，以利改進。

(二)稽核改善報告

1.本校於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施並處理。

2.本校如也有缺失或待改善項目者，應判定其發生原因，評估是否有其類似之缺失或待改善之項目存在，必要時得考量對現行資通安全管理制度或相關文件進行變更。

3.應於上級機關規定之時程內，回復改善採取之措施、進度及資料。

依拾陸、資通安全維護計畫實施情形之提出

依據本法第14條之規定，於每年10月前向上級機關提報新學年之核准計畫書，於每年5月底前向監督機關（資安署），提出資通安全維護計畫實施情形。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

(一)資通安全管理法

(二)資通安全管理法施行細則

(三)資通安全責任等級分級辦法

(四)資通安全事件通報應變及演練辦法

(五)資通安全維護計畫實施情形稽核辦法

(六)資通安全情資分享辦法

(七)公務機關所屬人員辦理資通安全事項作業辦法

(八)危害國家資通安全產品審查辦法

(九)國家資通安全會報設置辦法

二、附件表單

(一)資通安全推動小組成員及分工表

(二)資通安全需求申請單

(三)資通安全維護計畫實施情形

(四)稽核項目紀錄表

(五)資通安全保密同意書

(六)稽核結果及改善報告

(七)改善績效追蹤報告