澎湖縣湖西國民小學

資安通報應變管理程序書

機密等級：一般

承辦人簽章：約僱人員 陳慶龍

單位主管簽章：教師兼教導主任 王有榮

資安長簽章：澎湖縣湖西鄉湖西國民小學校長 辛武震

校長簽章：澎湖縣湖西鄉湖西國民小學校長 辛武震

簽章日期：114. 8. 1

資通安全維護計畫

目　　錄

依據及目的

本計畫依據下列法規訂定：

一、 資通安全管理法第10條及其施行細則第6條。

二、 其他相關業務法規名稱。

適用範圍

本計畫適用範圍涵蓋澎湖縣湖西國民小學（以下簡稱本校）。

核心業務及重要性

一、 核心業務及重要性：

本校之核心業務及重要性如下表：

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
教務業務	學務管理系統（向上集中） 學生資源網（向上集中）	為本校依組織法執掌，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
學生事務	學務管理系統（向上集中）	為本校依組織法執掌，足認為重要者。	無	無
總務業務	公文系統（向上集中）	為本校依組織法執掌，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
輔導業務	教育部心測輔導系統（向上集中） 學務管理系統（向上集中）	為本校依組織法執掌，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

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 7 條之規定列示。

2. 核心資通系統：該項核心業務所必須使用之資通系統名稱。

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. 業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

5. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

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	業務失效影響說明	最大可容忍中斷時間
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
資通安全防護-防毒軟體	未安裝容易造成校園電腦中毒	24小時
資通安全防護-校園防火牆、無線網路分享器(向上集中)	可能使本校部分業務中斷	由上級管理單位訂之
資通安全教育訓練	無	無

各欄位定義：

1. 非核心業務系統：非核心業務相關之資通系統可依機關實際情形增加列出。

2. 業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

3. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

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：

1. 建立校園資通安全保護及管理機制，確保資訊不會遭到竊取、竄改、滅失或遺漏。
2. 保護校內資訊內容之機密性與完整性，確保未經授權的存取與竄改，並確認處理過程精準無誤。
3. 針對資安事件之處理、通報與回復能快速完成。
4. 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高同仁之資通安全意識，本校同仁亦應確實參與訓練。
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/同意書。

二、 資通安全目標

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. 提升校內人員資安防護意識與預防外部攻擊等預防方法。

三、 資通安全政策及目標之核定程序

資通安全政策由本校湖西國小簽呈校長核定並公告之。

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，向機關內所有人員進行宣導。

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資通安全管理審查會議中檢討其適切性。

資通安全推動組織

一、 資通安全長

依本法第11條之規定，本校擇請_校長/辛武震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：

1. 資通安全管理政策及目標之核定、核轉及督導。
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) 本校設置「資通安全推動小組」負責督導校內資通安全相關事項，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，由資通安全長召集人員代表成立資通安全推動小組，其任務宜包括：

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，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) 其他資通安全事項之規劃。

(6) 資通安全相關規章與程序、制度之執行。

(7) 資訊及資通系統之盤點及風險評估。

(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。

(10)每年得需參加縣市辦理之相關資訊研習

專職(責)人力及經費配置

一、 專職(責)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，其分工如下。

(1) 資通安全認知與訓練業務，負責推動資通安全教育訓練等業務之推動。

(2) 資通安全防護業務，資通安全防護設施建置及資通安全事件通報及應變業務之推動。

(3) 資通安全管理法法遵事項業務，負責本校對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。

2. 本校之承辦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。

3. 本校校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。

4. 本校專業人力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。

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. 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。

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。

資訊及資通系統之盤點

一、 資訊及資通系統盤點

1. 本校應每年辦理資訊及資通系統資產盤點，依管理責任及使用人員指定其對應之資產管理人，其項目包括資訊資產、軟體資產、實體資產、支援服務資產、人員資料等，以利交接作業。

2. 相關資產項目如下：

(1) 資訊資產：以數位等形式儲存之資訊，如學籍資料、網站資料、資料檔案、操作手冊、訓練教材、稽核紀錄及歸檔之資訊等。

(2) 軟體資產：應用軟體、系統軟體、電腦作業系統及防毒軟體等。

(3) 實體資產：電腦(含桌機、筆電)、電腦螢幕、單槍投影機、液晶電視、影音設備、可攜式設備等相關設備。

(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) 人員資料：校內各項資訊系統使用之人員帳號清冊。

二、 機關資通安全責任等級分級

依據教育部臺教資(四)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。

資通安全風險評估

一、 資通安全風險評估

1. 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。

2. 執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

3. 本校應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

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。

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、資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。

2. 系統管理人應確保資訊及資通系統被妥善的保存或備份。

3. 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) 資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統前應經其管理人授權。

2. 本校同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

3. 本校同仁使用資訊及資通系統後，應依規定之程序歸還。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。

4. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製或散播資訊。

5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

(三) 資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 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。

2. 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。

3. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。

4. 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。

5. 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) 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在

干擾。

(3) 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(4) 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. 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。

(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) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。

3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5. 資通系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四) 加密管理

1. 本校之機密資訊於儲存或傳輸時應進行加密。

2. 本校之加密保護措施應遵守下列規定：

(1) 應避免留存解密資訊。

(2) 一旦加密資訊具遭破解跡象，應立即更改之。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校之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。

(1) 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。

(2) 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。

(3) 確實執行網頁惡意軟體掃描。

2. 使用者未經同意不得私自安裝應用軟體，管理者並應每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. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二) 遠距工作之安全措施

1. 本校資通系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。

2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。

(三) OpenID 安全管理(含電子郵件安全管理)

1. 本校人員到職後應經教育網路中心申請 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。

2. 定期進行 OpenID 帳號清查，令使用者需定期依本法修改通行碼。

3. 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。

4. 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。

5. 使用者應確保電子郵件傳送時之傳遞正確性。

(四) 確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理

(1) 資料中心、電腦機房或相關設備，應進行實體隔離。

(2) 校內人員或來訪人員應申請及授權後方可進入資料中心及電腦機房，資料中心及電腦機房管理者並應定期檢視授權人員之名單。

(3) 校內人員應隨時注意身分不明或可疑人員。

(4) 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。

(5) 人員及設備進出資料中心及電腦機房應留存記錄。

2. 資料中心及電腦機房之環境控制

(1) 資料中心及電腦機房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。

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) 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。

(五) 資料備份

1. 重要資料應定期進行資料備份，並執行異地存放。

2. 本校應定期確認資料備份之有效性。

3. 敏感或機密性資訊之備份應加密保護。

(六) 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. 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。

3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

4. 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。

(七) 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. 下班時請務必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。

7. 支援資訊作業的相關設施如影印機、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。

(八) 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

(九) 即時通訊軟體之安全管理

1. 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。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。

2. 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。

(3) 應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。

(4) 伺服器端之主機設備及通訊紀錄應置於我國境內。

(5) 伺服器通訊紀錄（log）應至少保存六個月。

四、 系統獲取、開發及維護

1. 配合教育部系統向上集中之規定，如校內另有系統相關開發及維護等需求，需另訂規範，其餘需求者請向上級機關申請、尋求協助。

五、 業務持續運作演練

本校為D級機關無需針對核心資通系統制定業務持續運作計畫與演練。

六、 執行資通安全健診

本校為D級機關無需執行資通安全健診作業。

七、 資通安全防護設備

1. 本校應建置防毒軟體、防火牆，持續使用並適時進行軟、硬體之必要更新或升級。前項之防火牆若為向上集中管理，則由上級單位統一辦理更新與升級。

2. 資安設備設定異動應保留相關修改紀錄，並定期檢討執行情形。

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。

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、本校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。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

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

由經指派之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。

(四) 涉及核心業務、核心資通系統之情資

資通安全推動小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

資通系統或服務委外辦理之管理

本校如需委外辦理資通系統之建置、維運或資通服務之提供時，可由上級機關認證後，考量其之專業能力與經驗、委外項目之性質及資通安全需求，而後選任適當之受託者，並監督其資通安全維護情形。

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，校內人員與主管，每人每年接受6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. 校內應每年考量管理、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，以建立資通安全認知，提升其資通安全水準，並保存相關教育訓練紀錄，相關專責人員則需參加上級機關辦理之相關教育訓練。

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、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。

3. 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)。

4. 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。

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。

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定期召開資通安全管理審查會議，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。

資通安全維護計畫實施情形之提出

本校依據本法第11條之規定，應於次年向上級或監督機關，提出上年度資通安全維護計畫實施情形，使其得瞭解本校上年度資通安全計畫實施情形。

相關法規、程序及表單

一、 相關法規及參考文件

1. 資通安全管理法
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. 本校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.資訊工作日誌
4.管制區域人員進出登記表
5.資訊設備進出/維護紀錄表
6.委外廠商執行人員保密切結書、保密同意書

7.年度資通安全教育訓練計畫

8.資通安全認知宣導及教育訓練簽到表

9.資通安全維護計畫實施情形

澎湖縣湖西國民小學

學校資通安全事件通報及應變管理程序

目錄

壹、 目的

澎湖縣湖西國民小學(以下簡稱本校)為遵照資通安全管理法第 14 條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、 適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、 責任

一、本校資通安全事件發生時，立依本程序或權責人員之指示，執行通報及應變相關事務。

二、本校應視必要性，制定其資通安全事件通報及應變管理程序，並於知悉相關事件後至「教育機構資安通報平台」內進行通報，並於完成事相關程序後，校內存取相關之紀錄或資料。

肆、 事件通報窗口及緊急處理小組

一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

（一） 聯絡電話：(07)525-0211

（二） 網路電話：98400000

（三） 電子郵件：service@cert.tanet.edu.tw

二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平台」(https://info.cert.tanet.edu.tw)登錄相關聯絡資料，如有異動亦應立即上網更新。

三、本校之資通安全事件通報窗口及聯繫專線為：

聯絡人姓名	職稱	電話	E-mail
辛武震	校長	06-9921008#209	jerry9920646@gmail.com
陳慶龍	約僱人員	06-9921008#115	ph2001220@hotmail.com

四、本校應以公告布告欄、校園網站等適當方式，使校內人員明確知悉本機關之通報窗口及聯絡方式。

五、本校權責人員知悉資通安全事件後，應立即至教育機構資安通報平台(https://info.cert.tanet.edu.tw)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷且持續達一小時以上者，應即將該情況告知相關人員，並提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向澎湖縣教育網路中心匯告，由教育網路中心成立緊急處理小組，立即協助進行處理；接獲本校所屬分校或受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由澎湖縣教育網路中心指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、 通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1. 事件涉及核心業務或關鍵基礎設施業務之資訊與否。
2. 事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。
3. 事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。
4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。
5. 事件其他足以影響資通安全事件等級之因素。

(二)本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確

認資安事件條件成立後1小時內，與本縣教育網路中心及通報應變小組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

(三)資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單位，使其續行通報作業。

(四)本校如委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

(五)本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依教育部或行政院所指訂或認可之方式，通知該機關。

(六)本校執行通報應變作業時，得視情形向本縣教育網路中心人員提出技術支援或其他協助之需求。

陸、 應變程序

一、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，規劃業務持續運作計畫，參與本縣辦理之相關研習，並於每年參加演練實施及更新資通安全聯絡人員，以預防資安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。
4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方式。
5. 重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。
7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後一小時內於平台內通報，並於七十二小時內完成相關控制或復原作業，並留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後一小時內於平台內通報，並於三十六小時內完成損害控制或復原作業，並留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、 重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

捌、 紀錄留存及管理程序之調整

一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至教育部資訊及科技教育司覆核備查。

二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、 演練作業

一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。

二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程。

(二)資安事件通報及應變

(三)網路攻防

(四)情境演練

(五)其他資安演練