

苗栗縣造橋鄉錦水國民小學

2.16.886.111.90007.90015.100003

苗栗縣國中小學校資通安全維護計畫

修訂人核章	
單位主管核章	
資安長核章	

Rev. 1.4

中華民國115年04月15日

目錄

壹、依據及目的	5
貳、適用範圍	5
參、核心業務及重要性	5
肆、資通安全政策及目標	7
一、資通安全政策.....	7
二、資通安全目標.....	7
三、資通安全政策及目標之核定程序	8
四、資通安全政策及目標之宣導	8
五、資通安全政策及目標定期檢討程序	8
伍、資通安全推動組織	8
一、資通安全長.....	8
二、資通安全推動小組.....	9
陸、專職人力及經費配置	10
一、專職人力及資源之配置	10
二、經費之配置	10
柒、資通系統之盤點	11
一、資通系統盤點	11
二、學校資通安全責任等級分級.....	12
捌、資通安全風險評估	12
一、資通安全風險評估	12
二、核心資通系統及最大可容忍中斷時間.....	12
玖、資通安全防護及控制措施	12
一、資訊及資通系統之管理	12
二、存取控制與加密機制管理.....	13

三、作業與通訊安全管理	14
四、系統獲取、開發及維護	17
五、業務持續運作演練	17
六、執行資通安全健診	17
七、資通安全防護設備	17
壹拾、資通安全事件通報、應變及演練相關機制	17
壹拾壹、資通安全情資之評估及因應機制	17
一、資通安全情資之分類評估	17
二、資通安全情資之因應措施	18
壹拾貳、資通系統或服務委外辦理之管理措施	19
一、選任受託者應注意事項	19
二、監督受託者資通安全維護情形應注意事項	19
壹拾參、資通安全教育訓練	20
一、資通安全教育訓練要求	20
二、資通安全教育訓練辦理方式	20
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	20
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	20
一、資通安全維護計畫之實施	20
二、資通安全維護計畫實施情形之稽核機制	21
三、資通安全維護計畫之持續精進及績效管理	21
壹拾陸、資通安全維護計畫實施情形之提出	22
壹拾柒、相關法規、程序及表單	22
一、相關法規及參考文件	22
二、相關表單	22

壹、 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13條及其施行細則第9條。
- 二、 其他相關業務法規名稱。

貳、 適用範圍

本計畫適用範圍涵蓋苗栗縣造橋鄉錦水國民小學

2.16.886.111.90007.90015.100003 (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
1.教務業務： 課程發展、課程編排、教學實施、學籍管理、成績評量、教學設備、教具圖書資料供應、教學研究及教學評鑑，並與輔導單位配合實施教育輔導等事項。 2.學生事務： 公民教育、道德教育、生活教育、體育衛生保健、學生團體活動及生活管理，並與輔導單位配合實施生活輔導等事項。 3.輔導業務： 學生資料蒐集與分	各校校務行政系統 (向上集中)	為上級機關指定之核心資通系統。	可能使本校校務行政業務中斷	由上級管理單位訂之

析、學生智力、性 向、人格等測驗之實 施，學生興趣、學習 成就與志願之調查、 輔導諮商之進行，並 辦理特殊教育及親職 教育等事項。 4.總務業務： 學校文書、事務及出 納等事項。				
--	--	--	--	--

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：該項核心業務所必須使用之資通系統名稱。
3. 重要性說明：說明該業務對學校之重要性，例如對學校財務及信譽上影響，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，學校業務運作有何影響。
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
公文系統(向上集中)	可能使本校公文業務中斷	由上級管理單位訂之
各校官方網站系統(向上集中)	可能使本校網站業務中斷	由上級管理單位訂之
網域名稱服務系統(向上集中)	可能使本校網站業務中斷	由上級管理單位訂之
郵件系統(向上集中)	可能使本校無法傳送公務信件	由上級管理單位訂之

各欄位定義：

1. 非核心業務系統：公務機關非核心業務相關之資通系統，如公文系統、用戶端服務等。
2. 業務失效影響說明：該項業務使用之系統失效後，學校業務運作有何影響。
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)。

肆、資通安全政策及目標

甲、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. 安全：確保資訊不遭竊取、竄改、滅失或遺漏。
2. 正確：資訊內容及處理過程精準無誤。
3. 迅速：對資安事件之處理、通報與回復能快速完成。

乙、二、資通安全目標

(一) 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。

(二) 量化型目標

1. 社交工程郵件開啟率應低於10%（含），社交工程郵件超連結點擊率應低於6%（含），社交工程郵件附件開啟率應低於6%（含）。
2. 資通安全專職人員以外之資訊人員，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，人員受訓人數達100%。
(含線上學習之人員)

3. 一般使用者及主管每人每年接受三小時以上之資通安全通識教育訓練，人員受訓人數達100%。(含線上學習之人員)
4. 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。

丙、三、資通安全政策及目標之核定程序

資通安全政策、資通安全目標由本校簽陳資通安全長核定。

丁、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，向學校內所有人員進行宣導。
2. 本校應每年向利害關係人(例如 IT 服務供應商、與學校連線作業有關單位)進行資安政策及目標宣導。

戊、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(與資安議題相關)中檢討其適切性，或以內部簽呈方式進行審查。

伍、資通安全推動組織

甲、一、資通安全長

依資通安全管理法第12條之規定，本校擇請校長兼任本校資通安全長，負責推動及監督機關內資通安全相關事項，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。

乙、二、資通安全推動小組

i. (一)組織

- ii. 本校設置「資通安全推動小組」負責督導機關資通安全相關事項，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。

iii. (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。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。跨部門資通安全事項權責分工之協調。
2. 訂定學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學校年度工作計畫。
4. 傳達學校資通安全政策與目標。
5. 其他資通安全事項之規劃。
6. 資通安全技術之研究、建置及評估相關事項。
7. 資通安全相關規章與程序、制度之執行。
8. 資訊及資通系統之盤點及風險評估。
9. 資料及資通系統之安全防護事項之執行。
10. 資通安全事件之通報及應變機制之執行。

11. 其他資通安全事項之辦理與推動。
12. 辦理資通安全內部稽核。
13. 每年定期召開內部會議（與資安議題相關），提報資通安全事項執行情形，留存相關紀錄備查。

陸、專職人力及經費配置

甲、專職人力及資源之配置

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，設置資通安全專職人員以外之資訊人員，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，負責本校各處室法遵義務執行事宜。
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，得洽請相關學者專家或專業機關(構)提供顧問諮詢服務。
3. 本校之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。

乙、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，應配合學校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，並經資通安全長核定後，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審查。

柒、資通系統之盤點

甲、資通系統盤點

1. 本校每年辦理資訊及資通系統資產盤點，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，分別為硬體設備、軟體、資料、服務四大類，說明如下表：

資產類別	說明
硬體設備 HW	<ol style="list-style-type: none">1. 網路交換器、防火牆、路由器、無線網路(Wifi)分享器等2. 電腦主機伺服器、個人電腦、筆記型電腦、平板電腦、印表機(事務印表機)、電子白板、數位電子看板等3. 儲存數位資訊之磁帶、光碟、隨身碟、網路附加儲存設備(NAS)等儲存媒介
軟體 SW	<ol style="list-style-type: none">1. 個人電腦、伺服器作業系統2. 能源管理系統
資料 DA	<ol style="list-style-type: none">1. 任何儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊，如資料庫、日誌檔案、業務資料電子檔等
服務 SV	<ol style="list-style-type: none">1. 資訊傳輸與交換之網路，如 LAN、ADSL、FTTB、T1、MDVPN。2. 機房相關之電力，如發電機、不斷電系統3. 空調4. 門禁管制設施、網路攝影機(監控系統)5. 消防設施

2. 本校每年度應依資訊及資通系統盤點結果，製作「資產清冊」。
3. 資訊及資通系統資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。
4. 各單位管理之資訊或資通系統如有異動，業務負責人應即時更新資產清冊。

乙、學校資通安全責任等級分級

本校因未維運自行或委外設置、開發之資通系統，為資通安全責任等級 D 級機關。

捌、資通安全風險評估

甲、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，因配合資訊資源向上集中計畫，資通系統已由上級或監督機關兼辦或代管，故資通系統風險評估由上級或監督機關統籌辦理，本校僅針對網路設備等資通訊設備進行評估。
2. 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」方法進行風險評估之工作。

乙、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，核心資通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「捌、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：

甲、資訊及資通系統之管理

i. (一) 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。

乙、存取控制與加密機制管理

i. (一) 網路安全控管

1. 本校配合資訊資源向上集中，防火牆政策之定期檢視及防火牆軟、

硬體之必要更新或升級，由上級機關兼辦。

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. 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。

ii. (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。

iii. (三) 特權帳號之存取管理

1. 資通系統之特權帳號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。

iv. (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。

丙、作業與通訊安全管理

i. (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.使用者不得私自安裝非合法授權之應用軟體，管理者並應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。

ii. (二)遠距工作之安全措施

本校原則無開放遠距維護工作。

iii. (三)電子郵件安全管理

- 1.本校配合資訊資源向上集中，校內無電子郵件伺服器，本校同仁均申請本府教育處電子郵件為公務信箱。
- 2.使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。
- 3.原則不得利用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. 使用者不得利用學校所提供電子郵件服務從事侵害他人權益或違法之行為。

iv. (四)確保實體與環境安全措施

1. 辦公室區域之實體與環境安全措施

- (1) 應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訊設備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訊設備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) 資訊或資通訊設備，未經管理人授權，不得被帶離辦公室。

v. (五)資料備份

1. 重要資料應進行資料備份，並盡量採取異地存放。
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。

vi. (六)媒體防護措施

1. 使用隨身碟或光碟等存放資料時，具機密性、敏感性之資料應進行加密或其他之防護措施，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紀錄。
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媒體，應保存於上鎖之櫃子，且需由專人管理鑰匙。

vii. (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. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循學校之通報程序通報。
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，以減少敏感性資訊遭破解或洩漏之機會。

viii. (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。

ix. (九)即時通訊軟體之安全管理

1. 使用即時通訊軟體傳遞學校內部公務訊息，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) 伺服器端之主機設備及通訊紀錄應置於我國境內。

x. (十)使用生成式 AI 資通安全規範

1. 業務承辦人不得向生成式 AI 提供涉及公務機密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。
2. 應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性。
3. 製作機密文件應由業務承辦人親自撰寫，禁止使用生成式 AI。

4. 生成式 AI 產出之資訊，須由使用者就其風險進行客觀且專業之最終判斷，不得取代使用者之自主思維、創造力。

丁、系統獲取、開發及維護

本校無自行或委外開發資通系統，故無系統獲取、開發及維護之相關需求。

戊、業務持續運作演練

本校全部核心資通系統已向上集中，業務持續運作計畫與演練由本縣教育網路中心統籌辦理。

己、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。

庚、資通安全防護設備

1. 本校應於各式電腦作業系統安裝防毒軟體，持續使用並適時進行必要更新或升級。
2. 公務用資通訊產品含軟體、硬體及服務等禁止下載、安裝或使用危害國家資通安全產品（含軟體、硬體及服務）。

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，本校依「臺灣學術網路各級學校資通安全通報應變作業程序」及「資通安全事件通報應變及演練辦法」辦理資通安全事件通報、應變及演練。

壹拾壹、資通安全情資之評估及因應機制

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。

甲、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：

i. (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。

ii. (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。

iii. (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。

iv. (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學校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。

乙、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。

i. (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。

ii. (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。

iii. (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。

iv. (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學校之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理措施

本校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

甲、選任受託者應注意事項

- i. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
- ii. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
- iii. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

乙、監督受託者資通安全維護情形應注意事項

- i. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
- ii. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
- iii. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
- iv. 受託者應採取之其他資通安全相關維護措施。
- v. 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時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

甲、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，資通安全專職人員以外之資訊人員，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；一般使用者與主管，每人每年接受3小時以上之資通安全通識教育訓練。

乙、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，以建立員工資通安全認知，提升學校資通安全水準，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。
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。
4. 資通安全教育及訓練之政策，除適用所屬員工外，對學校外部的使用者，亦應一體適用。

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「苗栗縣政府及所屬各機關學校公務人員平時獎懲標準表」、「公務機關所屬人員辦理資通安全事項作業辦法」及相關規定辦理之。

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

甲、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，相關單位於訂定相關文件、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。

乙、資通安全維護計畫實施情形之稽核機制

i. (一)稽核機制之實施

1. 資通安全推動小組應於每年或系統重大變更或組織改造後執行 1 次內部稽核作業(自我檢查作業)，以確認人員是否遵循本規範與學校之管理程序要求，並有效實作及維持管理制度。
2. 辦理稽核前資通安全推動小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。
3. 本校之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性。
4. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。
5. 本校應配合上級或監督機關之規定辦理查核作業，以確認人員是否

遵循本計畫與機關之管理程序要求，並有效實作及維持管理制度。

ii. (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、改善進度規劃，並落實執行。
- 2.本校於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
- 3.本校於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，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。
- 4.本校應定期審查缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
- 5.本校於執行改善措施時，應留存相關之執行紀錄，並提出稽核結果及改善報告。

丙、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定期召開內部會議(與資安議題相關)，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。

壹拾陸、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14條之規定，應依主管機關規定期限向上級或監督機關，提出上年度資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全維護計畫實施情形。

壹拾柒、相關法規、程序及表單

甲、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.資通安全事件通報應變及演練辦法
- 5.資通安全情資分享辦法

6. 公務機關所屬人員辦理資通安全事項作業辦法
7. 資通系統風險評鑑參考指引
8. 苗栗縣政府及所屬各機關學校公務人員平時獎懲標準表
9. 臺灣學術網路各級學校資通安全通報應變作業程序

乙、 相關表單

1. 資通安全推動小組成員表(附表1)
2. 資產清冊(附表2)
3. 風險評估表(附表3)
4. 帳號清查紀錄單(附表4)
5. 稽核項目紀錄表(附表5)

附表1 資通安全推動小組成員表

NO	角色	處室	職稱	連絡電話 (分機)	E-mail
1	資通安全長	校長室	校長		
2	資通安全推動 小組委員	教務處			
3		學務處			
4		人事室			
5		會計室			
6		資訊老師			
7	資通安全專職 人員以外之資 訊人員	總務主任			
8	稽核人員	教導主任			

附表2 資產清冊

NO	財產編號	資產名稱	資產說明(用途)	數量	地點	使用者	管理者

附表3 風險評估表

NO	財產編號	資產名稱	風險項目	改善措施	預計完成日

資通安全推動小組：

資通安全長：

附表4 帳號清查紀錄單

系統/設備名稱		
清查日期		
清查結果	<input type="checkbox"/> 正常 <input type="checkbox"/> 異常 異常說明： 異常處理： ※帳號清冊/列表如附	
簽核	管理人員	單位主管

附表5 稽核項目紀錄表

項次	檢核項目	查核結果	備註
1.	是否了解本校資安政策及目標?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2.	是否開啟螢幕保護程式? a. 時間設定為15分鐘以內 b. 密碼保護打勾	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
3.	是否設定登入密碼長度8碼以上?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
4.	是否設定登入密碼複雜度包含英文大小寫、數字及符號混合(四擇三)?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
5.	是否定期三個月變更密碼?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
6.	機敏資料(含紙本文件、報表或電子資料)是否已妥善保存(放置特定場所或進行加密管控)?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
7.	是否已建置防毒軟體? a. 防毒是否啟用 b. 病毒碼是否更新	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
8.	是否將 Windows 系統更新至最新版本?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
9.	是否無安裝來路不明或未授權之軟體?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
10.	是否設定鐘訊同步?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
11.	是否已關閉郵件預覽功能?	<input type="checkbox"/> 是 <input type="checkbox"/> 否	

