宜蘭縣員山鄉員山國民小學

資通安全維護計畫

修訂人核章	教師兼任資訊組長 游勇強
單位主管核章	教師兼代教務主任 林珊
資安長核章	校長 陳碧卿

版次：**V2.0**

中 華 民 國 114 年 09 月 16 日

目次

資通安全維護計畫

文件制/修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人	核定人（資安長）
V1.0(初版)	108年4月15日	新擬訂文件	教務處	游勇強	任立誠
V1.1	109年3月25日	更正引用法條，原引用法條為「資通安全管理法」第11條，更正為第12條	教務處	游勇強	任立誠
V2.0	114年9月16日	改版	教務處	游勇強	陳碧卿

壹、依據及目的

本計畫依據「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宜蘭縣員山鄉員山國民小學全機關。

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： 學籍管理、成績評量	無	為本機關依組織法執掌，足認為重要者。	無	無
學務業務： 校安通報、性平事件通報	無	為本機關依組織法執掌，足認為重要者。	無	無
總務業務： 出納業務、主計業 務、文書業務、事 務業務	無	為本機關依組織法執掌，足認為重要者。	無	無

二、非核心業務及說明

本機關非核心業務及說明：無

肆、資通安全政策及目標

一、資通安全政策

為使本機關業務順利運作，防止資訊或資通系統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，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）並，特制訂本政策如下，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)保護資訊及資通系統避免受到未被授權的存取，保持資訊及資通系統的機密性。

(三)防護未經授權的修改以保護資訊及資通系統之完整性。

(四)確保經授權之使用者當需要時能使用資訊及資通系統。

(五)符合法令與法規要求。

(七)評估各種人為或天然災害之影響，訂定核心資通系統之復原計畫，以確保核心業務可持續運作。

(八)落實資通安全教育訓練，以提高員工之資通安全意識。

(九)落實人員辦理業務涉及資通安全事項之獎懲機制。

二、資通安全目標

(一)量化型目標

1.知悉資安事件發生，未能於規定的時間完成通報、應變及復原作業之件數≤0。

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。

4.加強資安區域防禦作業，提升區域防禦廣度與組織防護縱深。

三、資通安全政策及目標之核定程序

資通安全政策由本校總務處簽陳資通安全長核定。

四、資通安全政策及目標之宣導

(一)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、張貼公告或e-mail等方式，向機關內所有人員進行宣導，並檢視執行成效。

(二)本機關應每年向利害關係人(例如IT服務供應商、與機關連線作業有關單位)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資通安全管理審查會議中檢討其適切性。

伍、資通安全長

依資通安全管理法第11條之規定，本機關指定陳碧卿校長擔任資通安全長，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。

陸、資通安全推動組織

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，由資通安全長指定機關一、二級主管及相關業務承辦人成立「資通安全推動小組」(簡稱：推動小組)，其任務包括：

(一)跨部門資通安全事項權責分工之協調。

(二)應採用之資通安全技術、方法及程序之協調研議。

(三)整體資通安全措施之協調研議。

(四)資通安全計畫之協調研議。

(五)其他重要資通安全事項之協調研議。

二、分工及職掌

本機關之資通安全推動小組依資通安全長之指示負責下列事項。本機關資通安全推動小組分組人員名單及職掌應填寫於「資通安全推動小組成員及分工表」，並適時更新之：

(一)資通安全政策及目標之研議。

(二)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。

(三)依據資通安全目標擬定機關年度工作計畫。

(四)傳達機關資通安全政策與目標。

(五)資通安全技術之研究、建置及評估相關事項。

(六)資通安全相關規章與程序、制度之執行。

(七)資訊及資通系統之盤點及風險評估。

(八)資料及資通系統之安全防護事項之執行。

(九)資通安全事件之通報及應變機制之執行。

(十)辦理資通安全內部稽核。

(十一)每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。

(十二)其他資通安全事項之規劃、辦理與推動。

柒、專責人力及經費配置

一、專職(責)人力資源之配置

(一)本機關依「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。本機關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。本機關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。

(二)本機關負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，以符職權分離原則。若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，以建立人力備援制度。

(三)本機關之首長及各級業務主管，應督導所屬人員之資通安全作業，以防範不法及不當行為。

(四)資通安全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

(一)「推動小組」於規劃配置相關經費及資源時，應考量本機關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)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「推動小組」提出，以利依整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置事宜。

(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。

捌、資訊及資通系統之盤點

一、資訊及資通系統盤點

(一)本機關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，分別為資訊資產、服務資產、軟體資產、硬體資產及人員資產資產等五類。

(二)資訊及資通系統資產項目如下：

1.資訊資產(類別代號：ID)

以數位等形式儲存之資訊，如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、稽核紀錄及歸檔之資訊等。

2.軟體資產(類別代號：SW)

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.硬體資產(類別代號：HW)

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(類別代號：ES)

相關基礎設施及其他機關內部之支援服務，如電力、消防、空調等。

5.人員資產(類別代號：PE)

管理、執行或提供支援給所負責的業務流程之人員，例如：管理者、系統管理員、資料管理員、機房管理員、委外駐點廠商等。

(三)本機關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：資產編號、資產類別、資產名稱、資產說明(資訊及資通系統名稱)、權責單位、存放位置、數量。

(四)前述資產編號規則：資產類別代號＋三碼流水號，例如電腦之資產編號為HW-001。權責單位：對資產具備管理權責之單位。

(五)資通系統及資訊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。核心資通系統及相關資產，並應加註標示(標示內容：資產編號＋資產名稱)。

(六)各單位管理之資通系統或資訊資產如有異動，應即時通知資通安全推動小組更新資產清冊。

二、機關資通安全責任等級分級

本機關因自行辦理資通業務，未維運自行或委外開發之資通系統，為資通安全責任等級D級機關。

玖、資通安全風險評估

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。

(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、資通安全風險之因應

(一)本機關之資通系統於完成資通系統分級後，應依「資通安全責任等級分級辦法」之規定，以及考量本機關之資源，以決定可接受之風險值（級別），並選擇或採行相關之防護及控制措施。

(二)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。

壹拾、資通安全防護及控制措施

本機關依據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，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.使用者不得於辦公室內私裝電腦及網路通訊等相關設備。

2.使用者應遵守網路安全規定，如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利。

(二)權限管理

1.密碼設置原則，應避免使用易猜測或個人資訊為設定。

2.應依使用者業務需要開通帳號權限，且不得共用帳號。

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帳號。

(三)加密管理

1.機密資訊於儲存或傳輸時應進行加密。

2.加密保護措施應避免留存解密資訊，若加密資訊具遭破解跡象，應立即更改之。

二、作業與通訊安全管理

(一)防範惡意軟體之控制措施

1.本機關之主機及個人電腦應安裝防毒軟體，並時維護軟、硬體。

2.任何形式之儲存媒體所取得之檔案，應確定有無惡意程式或病毒。

3.使用者未經同意不得私自安裝來路不明、有違法疑慮或與業務無關

的軟體。

(二)電子郵件安全管理

1.使用者使用電子郵件時應提高警覺，避免讀取來歷不明之郵件。

2.原則不得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。

3.使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

4.本機關應配合上級機關舉辦電子郵件社交工程演練，並檢討執行情形。

(三)確保實體與環境安全措施

1.應考量採用辦公桌面的淨空政策，以減少機密資訊、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.資訊或資通系統相關設備應妥善存放，未經管理人授權，不得被帶離辦公室。

(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。

(五)電腦使用之安全管理

1.個人電腦不使用時，應立即登出或啟動螢幕保護功能。

2.禁止安裝使用未經合法授權軟體。

3.個人電腦應定期進行更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

4.如發現資安問題，應主動循機關之通報程序通報。

5.重要資料應定期備份。

三、資通安全防護設備

(一)防火牆應適時進行軟、硬體更新及維護作業。

(二)防火牆設定檔必要時應進行備份作業。

壹拾壹、資通安全事件通報、應變及演練相關機制

一、為即時掌控資通安全事件，並有效降低其所造成之損害，本機關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及應變處理作業程序。

二、本機關指定總務處主任擔任通報專責人員，並由資訊組長或資訊業務承辦人協助辦理，依業務狀況辦理移交(含名單異動)。

壹拾貳、資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、可用資源及可接受之風險等，決定以最適當之方式因應，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

本機關接受資通安全情資後，應指定資通安全專職人員進行情資分析，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：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，均屬之。

(二)入侵攻擊情資

資通安全情資之內容，如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，列屬入侵攻擊情資。

(三)機敏性之情資

資通安全情資之內容，如：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，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：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，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

本機關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)資通安全相關訊息之情資

由「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)入侵攻擊之情資

由資通安全專職(責)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，另應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

「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。

壹拾參、資通系統或服務委外辦理之管理

本機關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。

一、選任受託者應注意事項

(一)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。

(二)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。

(三)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。

二、監督受託者資通安全維護情形應注意事項

(一)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。

(二)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。

(三)受託者應採取之其他資通安全相關維護措施。

(四)與受託者簽訂契約時，應審查契約中保密條款，並要求受託者之業務執行人員簽署「委外廠商執行人員保密切結書」。

(五)本機關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，稽核項目如「委外廠商查核項目表」。

壹拾肆、資通安全教育訓練

一、資通安全教育訓練要求

本機關資通安全責任等級分級屬「D級」，一般使用者及主管等，每人每年至少接受三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

(一)承辦單位應於每年2月份前，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，以深化員工資通安全認知，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。

(二)本機關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、作業流程、資通安全事件通報程序、資通安全要求事項及人員責任等)。

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。

(三)員工得至數位學習資源整合平臺「e等公務園+學習平臺」(https://elearn.hrd.gov.tw)線上修習包含資安管理制度、社交工程攻擊防護、個人資料保護、行動裝置使用安全、物聯網資安威脅等資安課程。

(四)員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

(五)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。

壹拾伍、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

本機關所屬人員之平時考核或聘用，遵循宜蘭縣政府依據「公務機關所屬人員資通安全事項獎懲辦法」所制訂之「宜蘭縣政府及所屬機關人員辦理資通安全事項獎懲要點」。

壹拾陸、資通安全維護計畫及實施情形之持續精進與績效管理機制

一、資通安全維護計畫之實施

為落實本安全維護計畫，確保本機關資通安全管理有效運作，除訂定各階程序文件、流程或控制措施時，並與資通安全政策、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.「推動小組」得視需求(例如：系統重大變更、組織改造或其他事由)執行內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，以確保資通安全維護計畫有效運作。

2.「推動小組」應於辦理稽核前擬定資通安全稽核計畫並選派稽核成員。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（查檢表）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.辦理稽核時，「推動小組」應於執行稽核前15日，通知受稽核單位，並將稽核期程、稽核查檢表及稽核排程等相關資訊提供受稽單位。

4.本機關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；如有聘任稽核委員應填具「稽核委員聘任同意保密切結書」備查，另於執行稽核時，應依稽核查檢表填具稽核紀錄或工作底稿，待稽核結束後，應將稽核發現彙整至稽核報告，並提供給受稽單位採取矯正預防措施，以持續改善。

5.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。

6.稽核人員於執行稽核時，應至少執行一項特定之稽核項目。

(二)稽核改善報告

1.受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失

或待改善之項目研採改善措施、規劃改善進度，並加以落實。

2.受稽單位於稽核實施後發現有缺失或待改善事項，應分析其發生之原因，並評估是否有類似、潛在之缺失，以及可能之待改善項目。

3.受稽單位於找出缺失或待改善之原因後，應據此提出並矯正及預防措施，以及改善進度規劃，必要時得修訂現行資訊安全管理制度或對相關文件進行變更。

4.機關應定期審查受稽單位缺失或待改善項目所採取之矯正預防措施、改善進度規劃及佐證資料之有效性。

5.受稽單位於執行矯正預防措施時，應留存相關之執行紀錄，並依填寫「稽核結果及改善報告」。

三、資通安全維護計畫之持續精進及績效管理

(一)本機關之「推動小組」每年至少召開一次資通安全管理審查會議，以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。

(二)管理審查議題應包含下列討論事項：

1.過往管理審查之處理狀態。

2.與資訊安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、「推動小組」決議事項等。

3.資通安全維護計畫內容之適切性。

4.資訊安全績效之回饋，包括但不限於：

(1)資通安全政策及目標之實施情形。

(2)資通安全人力及資源之配置之實施情形。

(3)資通安全防護及控制措施之實施情形。

另，得視年度需求納入以下議題：

(1)內、外部稽核結果。

(2)不符合項目及矯正措施。

5.風險評鑑結果及風險處理計畫執行進度。

6.重大資通安全事件之處理及改善情形。

7.利害關係人之回饋。

8.持續改善之機會。

(三)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。

壹拾柒、資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第12條之規定，應依主管機關來函限期內，提出資通安全維護計畫實施情形，使其得瞭解本機關之年度資通安全計畫實施情形。

壹拾捌、相關法規、程序及表單

一、相關法規

(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)資通安全事件通報及應變辦法

(五)資通安全情資分享辦法

(六)公務機關所屬人員資通安全事項獎懲辦法

(七)特定非公務機關資通安全維護計畫稽核辦法

(八)宜蘭縣政府及所屬機關人員辦理資通安全事項獎懲要點

二、表單

(一)資通安全推動小組成員及分工表

(二)資通安全保密同意書

(三)資訊資產清冊

(四)資安威脅弱點評估表

(五)風險評鑑報告

(六)資安風險處理計畫

(七)資通安全事件通報處理結案單

(八)威脅情資彙處表

(九)委外廠商執行人員保密切結書、保密同意書

(十)委外廠商查核項目表

(十一)年度資通安全教育訓練計畫

(十二)資通安全認知宣導及教育訓練簽到表

(十三)年度資通安全稽核計畫

(十四)稽核項目紀錄表

(十五)稽核委員聘任同意暨保密切結書

(十六)稽核結果及改善報告

(十七)矯正措施表

(十八)資通安全維護計畫實施情形

三、參考文件

(一)資訊系統風險評鑑參考指引

(二)政府資訊作業委外安全參考指引

(三)無線網路安全參考指引

(四)網路架構規劃參考指引

(五)行政裝置資安防護參考指引

(六)政府行動化安全防護規劃報告

(七)安全軟體發展流程指引

(八)安全軟體設計指引

(九)安全軟體測試指引

(十)安全控制措施參考指引

(十一)資通系統防護基準驗證實務