國立花蓮高級農業職業學校

115 年資通安全維護計畫

114 年 2 月 16 日初訂
114 年 11 月 26 日第一次修訂
115 年 05 月 26 日第二次修訂

115 年 06 月

目　　錄

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條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫（以下簡稱本計畫）。為因應資通安全管理法及資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、適用範圍

本計畫適用範圍涵蓋國立花蓮高級農業職業學校全機關（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	資通系統分級
校務系統（教務、學務、輔導）	校務系統	為本校依組織法執掌，足認為重要者	影響機關行政效率以及無法登入及查詢成績，影響教師及學生權益	24小時	普
學習歷程系統（向上集中）	學習歷程系統	為本校依組織法執掌，足認為重要者	影響機關行政效率及無法登錄學習歷程，影響學生權益	24小時	普
會計業務（辦理歲計、會計業務等事項）	主計請購系統（艾富）	為本校依組織法執掌，足認為重要者	無法請購，影響機關行政效率。	24小時	普
學校官網（向上集中—成大）	學校官網	為本校依組織法執掌，足認為重要者	影響學校最新訊息發布以及外部查找學校相關資訊的管道	24小時	普
DNS（向上集中—東華大學）	DNS	為本校依組織法執掌，足認為重要者	影響機關行政效率及機關信譽，影響民眾對本校觀感	24小時	普

各欄位定義：

- 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。
- 核心資通系統：支援核心業務運作必要之系統。

- 重要性說明：說明該業務對機關之重要性。
- 業務失效影響說明：當系統失效時對學校所造成的衝擊及影響。
- 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	資通系統分級
公文交換系統	將無法正常收發電子公文及辦理公文交換作業，影響公文傳遞、簽收及行政流程之時效，可能造成重要公文延誤處理。	48 小時	普
差勤服務系統	將無法辦理教職員出勤、請假、加班及簽核等作業，影響人事管理及行政作業之正常運作，並可能導致出勤資料無法即時登錄與查詢，影響相關人事業務處理。	48 小時	普
圖書館藏借閱系統	將無法辦理館藏查詢、借閱、歸還及續借等作業，影響圖書館服務品質及館藏管理效率，並可能造成借閱資料無法即時更新，增加人工處理作業及管理負擔。	48 小時	普
出納系統	將無法辦理各項收付款撥付及帳務管理作業，影響經費收支管理及行政作業正常運作，並可能造成帳務處理延誤。	48 小時	普
無聲廣播系統	將無法即時發布校內公告、緊急通知及災害應變訊息，影響師生接收重要資訊之時效，降低校園緊急事件應變效率。	48 小時	普
電力系統	將造成資訊設備及相關電力需求設施停止運作，影響行政、教學及資訊服務之持續提供。	48 小時	普
財產管理系統	無法辦理財產管理、盤點及異動等作業，影響財產資料維護及行政管理正常運作。	48 小時	普

各欄位定義：

- 非核心業務：公務機關之非核心業務至少應包含輔助單位之業務名稱。

肆、資通安全政策及目標

依本校「資通安全政策」如附件一施行。

伍、資通安全推動組織

依本校「資通安全組織」辦法如附件二成立資通安全委員會並成立資訊安全小組，「資通安全組織成員表」如附件三。

陸、人力及經費配置

一、資通安全人力及資源之配置

- 依據行政院 112 年 10 月 30 日院授數資安字第 1120004855 號函，依據資通安全責任等級分級辦法第 6 條辦理，並考量本校已有核心系統向上集中規劃，依同法第 10 條第 4 款調降等級為 D 級。本校依資通安全責任等級分級辦法之規定，設置資通安全專責人員 1 人，並將人員職掌填寫於「資通安全推動小組成員表」如附件三，應適時更新之。
- 本校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，並提升校內資通安全專業人員之資通安全管理能力。本校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。
- 本校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，若負有機密維護責任者，應簽屬「資通安全保密同意書」，並建立人力備援制度。
- 資安專責人員專業職能之培養（如證書、證照、培訓紀錄等），應參加主管機關辦理之相關專業研習，並鼓勵取得資通安全專業證照及資通安全職能評量證書。
- 本校所有人員皆有教職員生個資維護責任，應簽屬「保密切結書」如附件四。
- 本校之首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。
- 專責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

- 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。
- 各單位於規劃建置資通系統時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配或勻支資通安全預算所佔之比例。
- 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

依本校「資訊資產管理」規定如附件五施行。

二、機關資通安全責任等級分級

依據行政院 112 年 10 月 30 日院授數資安字第 1120004855 號函，依據資通安全責任等級分級辦法第 6 條辦理與同法第 10 條第 4 款調降等級為 D 級機關。

捌、資通安全風險評估

一、資通安全風險評估

依本校「風險評鑑與管理」規定如附件六施行。

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，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

依本校「資訊資產異動作業」規定如附件七施行。

二、存取控制與加密機制管理

依本校「存取控制與加密機制管理」規定如附件八施行。

三、作業與通訊安全管理

依本校「實體安全管理」規定如附件九、「通信與作業管理」規定如附件十施行。

四、業務持續運作演練

本校應針對尚未向上集中之核心資通系統制定業務持續運作計畫，並每二年辦理一次未向上集中之核心資通系統持續運作演練。

五、資通安全防護設備

1.本校應建置防毒軟體、網路防火牆，持續使用並適時進行軟、硬體之必要更新或升級。

2.資安設備應定期備份日誌紀錄，並由主管定期檢視複核執行成果，並檢討執行情形。

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，，詳如附件十一「資通安全事件通報及應變管理程序」。

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、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、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

（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

由資通安全專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。

壹拾貳、資通系統或服務委外辦理之管理

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。

一、選任受託者應注意事項

- 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。
- 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。
- 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

- 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。
- 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。
- 受託者應採取之其他資通安全相關維護措施。
- 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」與「委外廠商執行人員保密同意書」。
- 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

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，資安專責人員每年至少接受 12 小時以上之資安專業課程訓練或資安職能訓練。一般使用者及主管，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

- 承辦單位應於每年公告請同仁進行實體或線上學習，以建立同仁資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。
- 本校資通安全認知宣導及教育訓練之內容得包含：
  - 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）。
  - 資通安全法令規定。
  - 資通安全作業內容。
  - 資通安全技術訓練。
- 教職員報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

- 資通安全教育及訓練之政策，除適用所屬教職員生外，對機關外部的使用者，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「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，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

- 資通安全推動小組應於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。
- 稽核作業可分為自評及各機關交互實地稽核等方式。辦理稽核前資通安全小組應擬定「內部稽核計畫」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（稽核委員簽署「保密切結書」）、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。
- 辦理稽核時，資訊安全稽核小組應於執行稽核前 30 日，通知受稽核單位，並將稽核期程、「稽核項目紀錄表」及稽核流程等相關資訊提供受稽單位。
- 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；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至「內部稽核報告」，並提供給受稽單位填寫辦理情形。
- 稽核結果應對相關管理階層（含資通安全長）報告，並留存稽核過程之相關紀錄以作為稽核事件之證據。

（二）稽核改善報告

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議改善措施，並落實執行。

三、資通安全維護計畫之持續精進及績效管理

- 本校之資通安全推動小組每年至少一次召開資通安全管理審查會議，確認「資通安全維護計畫」及「資通安全維護計畫實施情形」，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」如有需改善之事項，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

本校依據本法第 12 條之規定，依照上級或監督機關所訂時限提出「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

- 資通安全管理法
- 資通安全管理法施行細則
- 資通安全責任等級分級辦法
- 資通安全事件通報及應變辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法
- 資訊系統風險評鑑參考指引
- 政府資訊作業委外安全參考指引
- 網路架構規劃參考指引
- 行政裝置資安防護參考指引
- 安全軟體發展流程指引
- 本機關資通安全事件通報及應變程序

二、附件表單

- 資通安全推動小組成員及分工表
- 資通安全保密同意書
- 資訊及資通系統資產清冊
- 風險評估表
- 風險改善計畫表
- 委外廠商執行人員保密切結書
- 委外廠商查核項目表
- 資通安全認知宣導及教育訓練簽到表
- 稽核項目紀錄表
- 資通安全維護計畫實施情形
- 資通安全事件通報及應變管理程序