國立花蓮高級農業職業學校

114 年資通安全維護計畫

113 年 2 月 16 日初訂
113 年 11 月 26 日第一次修訂
114 年 06 月 03 日第二次修訂

114 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
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
學習歷程系統(向上集中-暨大)	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
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
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
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

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：支援核心業務運作必要之系統。
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：當系統失效時對學校所造成的衝擊及影響。
5. 最大可容忍中斷時間單位以工作小時計(一天為 8 小時)。

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
公文交換	電子公文無法即時送達機關，影響機關行政效率。	40 小時
差勤服務	無法進行差假申請作業，影響機關行政效率。	40 小時
圖書館藏查詢	無法借還書，影響機關行政效率。	40 小時
出納系統	費用無法撥付，影響機關行政效率。	40 小時
財務管理	校內財產、物品無法登錄、查詢，影響機關行政效率。	40 小時

各欄位定義：

1. 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，如差勤服務、用戶端服務等。
2. 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。
3. 最大可容忍中斷時間單位以工作小時計(一天為 8 小時)。

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），特制訂本政策如下，以供全體同仁共同遵循：

1. 應因應資通安全威脅情勢變化，本校同仁應參與資通安全教育訓練，以提高資通安全意識。
2. 應確認相關人員熟悉資安事件通報機制，有效完成通報作業。
3. 確保機關網路服務維持一定水準的可用性。

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。每年不依適當通報程序反應，並予以適當的調查及處理 0 件。
2. 控制全年度非預期網路服務中斷件數，能於最大可容忍中斷時間內及時恢復資通系統，確保各業務穩健執行。每年未能於最大可容忍中斷時間內恢復資通系統，並造成的本校損害事件 0 件。

(二) 質化型目標

1. 達成資通安全責任等級之要求，並降低遭受資通安全風險之威脅。
2. 提升人員資安防護意識、有效偵測與預防外部攻擊。

三、資通安全政策及目標之核定程序

資通安全政策簽陳資通安全長核定。

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，向校內所有人員進行宣導，並檢視執行成效。
2. 本校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檢討其適切性，若需調整簽陳資通安全長核准。

伍、資通安全推動組織

一、資通安全長

依本法第 11 條之規定，本校由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：

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

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，由資通安全長召集各業務部門主管/副主管，並指派適當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. 資通安全政策及目標之研議。
6. 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。

7. 依據資通安全目標擬定機關年度工作計畫。

8. 傳達機關資通安全政策與目標。

9. 資通安全技術之研究、建置及評估相關事項。

10. 資通安全相關規章與程序、制度之執行。

11. 資訊及資通系統之盤點及風險評估。

12. 資料及資通系統之安全防護事項之執行。

13. 資通安全事件之通報及應變機制之執行。

14. 辦理資通安全內部稽核。

15. 每年提報資通安全維護計畫之實施情形。

16. 每年定期召開資通安全管理審查會議，或在內部行政會議中提報資通安全事項執行情形並進行管理審查。

本校資通安全推動小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。

陸、人力及經費配置

一、資通安全人力及資源之配置

1. 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」，應適時更新之。

2. 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，並提升機關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。

3. 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。

4. 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。

5. 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。

6. 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

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. 各單位於規劃建置資通系統建置時，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。

3. 資通安全經費、資源之配置情形應每年定期檢討。

柒、資訊及資通系統之盤點

一、資訊及資通系統盤點

1. 依本校「資訊資產管理」規定施行。

2. 資訊及資通系統資產項目如下：

(1) 資訊資產：以數位等形式儲存之資訊，如 Office 電子檔、資料庫等。

(2) 軟體資產：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) 實體資產：電腦及網路設備、可攜式設備等。

(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、空調等。

(5) 人員資產：系統管理者、設備管理者、委外駐點廠商等。

3. 本校每年度應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，欄位應包含：資產編號、資產類別、資產名稱、權責單位、存放位置、數量、資訊及資通系統名稱。

4. 權責單位：對資產具備管理權責之單位。

5. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新「資訊及資通系統資產清冊」。

6. 本校不得使用對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務，自行或委外營運，提供公眾活動或使用之場地，亦不得使用前述所定造成危害風險之產品。本校將前段規定事項納入委外契約或場地使用規定中，並督導辦理。

7. 本校應向所屬人員宣導使用危害國家資通安全產品之風險。

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

1. 本校應每年針對資訊及資通系統資產進行風險評估，並填寫「風險評估表」。

2. 風險評估項目及計算公式如下：

(1) 資產風險計算需考量資產價值(C+I+A)、可能性及衝擊性等項目。

(2) 資產價值＝資產之[機密性(C)＋完整性(I)＋可用性(A)]。

(3) 資產風險＝ 資產價值(C+I+A)× 可能性 × 衝擊性

(4) 風險分佈：

低風險	中風險	高風險
3~37	38~73	74~108

(5) 當資產風險為高風險時，應填寫「風險改善計畫表」進行風險改善作業。

3. 資產價值應考量機密性(C)、完整性(I)及可用性(A)。

4. 資產風險計算需評估各事件可能性及衝擊性。

5. 威脅暨弱點評估：

(1) 將應進行威脅弱點評估之資產，可能面臨之事件(威脅-弱點)分為五類，請參考「威脅弱點對應表」，其類別包括：

A. 資訊資產風險：包含資料、文件之建立、維護、控管、傳遞不當等所產生之風險。

B. 軟體資產風險：包含系統設計、維護、操作不當等所產生之風險。

C. 實體資產風險:包含缺少實體安控或環境監控不足等所產生之風險。

D. 支援服務資產風險:包含容量不足或維護之不當等所產生之風險。

E. 人員資產風險：包含因人員有意或無意行為、安全訓練不足等所產生之風險。

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、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. 本校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. 本校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

1. 防毒軟體、防火牆置應適時進行軟、硬體更新及維護作業。

2. 防毒軟體、防火牆設定檔必要時應進行備份作業。

四、業務持續運作演練

本校應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

五、執行資通安全健診

本校每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

1. 網路架構檢視。

2. 網路惡意活動檢視。

3. 使用者端電腦惡意活動檢視。

4. 伺服器主機惡意活動檢視。

5. 安全設定檢視。

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，依「資通安全事件通報及應變管理程序」辦理。

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、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

1. 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。
2. 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。
3. 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

1. 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。

2. 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。

3. 受託者應採取之其他資通安全相關維護措施。

4. 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」。

5. 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

1. 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。

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。

(4) 資通安全技術訓練。

3. 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。

4. 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

1. 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。

2. 稽核作業可分為自評及各機關交互實地稽核等方式，以下說明作業方式：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。

3. 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。

4. 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。

5. 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

1. 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。
2. 「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

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. 數據公益運作指引
18. 隱私強化技術應用指引
19. 本機關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. 資訊及資通系統資產清冊
4. 風險評估表
5. 風險改善計畫表
6. 委外廠商執行人員保密切結書
7. 委外廠商查核項目表
8. 資通安全認知宣導及教育訓練簽到表
9. 稽核項目紀錄表
10. 資通安全維護計畫實施情形
11. 資通安全事件通報及應變管理程序

1. 資通安全推動小組成員及分工表

國立花蓮高級農業職業學校
資通安全推動小組成員及分工表

編號：2024-11-26-1

製表日期：113 年 11 月 26 日

職稱	職級	名稱	職掌事項	分機	備註	代理人
資通安全長	校長	梁宇承	資通安全管理政策、相關規章及年度計畫之核定 資通安全責任與資源的分配協調 資安防護與事件的檢討監督 召開資通安全推動小組會議	303		
資通安全推動小組組長	組長	李幸蓉	提報年度資通安全管理工作計畫。 推動資通安全相關政策 落實資通安全事件通報及相關應變處理 辦理資通安全內部稽核	338	資通安全專責人員	
委員	秘書	蔡金智	研議資通安全政策及目標 傳達本校資通安全政策與目標	303		
委員	教務主任	黃俊霖	研議資通安全政策及目標 傳達本校資通安全政策與目標	305		
委員	學務主任	陳凱群	研議資通安全政策及目標 傳達本校資通安全政策與目標	307		
委員	總務主任	江金安	研議資通安全政策及目標 傳達本校資通安全政策與目標	312		
委員	實習主任	林政仁	研議資通安全政策及目標	325		

			傳達本校資通安全政策與目標			
委員	輔導主任	蘇延任	研議資通安全政策及目標 傳達本校資通安全政策與目標	323		
委員	圖書館主任	江春梅	研議資通安全政策及目標 傳達本校資通安全政策與目標	327		
委員	人事主任	何瑞鳳	研議資通安全政策及目標 傳達本校資通安全政策與目標	318		
委員	主計主任	楊庭偉	研議資通安全政策及目標 傳達本校資通安全政策與目標	365		
委員	農經科主任	黃士庭	研議資通安全政策及目標 傳達本校資通安全政策與目標	349		
委員	園藝科主任	吳靖隃	研議資通安全政策及目標 傳達本校資通安全政策與目標	343		
委員	畜保科主任	李佩昭	研議資通安全政策及目標 傳達本校資通安全政策與目標	341		
委員	森林科主任	楊逸晴	研議資通安全政策及目標 傳達本校資通安全政策與目標	351		
委員	生機科主任	盧禮宏	研議資通安全政策及目標 傳達本校資通安全政策與目標	331		
委員	食品科主任	張靜華	研議資通安全政策及目標 傳達本校資通安全政策與目標	347		
委員	土木科主任	黃志鵬	研議資通安全政策及目標 傳達本校資通安全政策與目標	333		
委員	餐飲科主任	張雅芳	研議資通安全政策及目標 傳達本校資通安全政策與目標	329		
委員	資處科主任	姚蘭香	研議資通安全政策及目標 傳達本校資通安全政策與目標	336		

委員	特教組組長	苗繼之	研議資通安全政策及目標 傳達本校資通安全政策與目標	321		
委員	生輔組組長	劉李韓	研議資通安全政策及目標 傳達本校資通安全政策與目標	311		
委員	資通組員	馬浚瑄	協助執行資通安全防護措施 協助辦理資通安全教育訓練 協助資通安全事件通報	312		
委員	資通組員	劉仲達	協助執行資通安全防護措施 協助辦理資通安全教育訓練 協助資通安全事件通報	312		
委員	資媒組協行教師	黃品學	協助執行資通安全防護措施 協助辦理資通安全教育訓練 協助資通安全事件通報			

2. 資通安全保密同意書

國立花蓮高級農業職業學校

資通安全保密同意書

編號：

立同意書人_____於民國___年__月__日起於_____任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。

二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：_____(簽章)

身份證字號：_____

服務機關：_____

中　　華　　民　　國　　年　　月　　日

3. 資訊及資通系統資產清冊

國立花蓮高級農業職業學校
資訊及資通系統資產清冊

編號：

製表日期：113 年　月　日 (配合每年學校盤點)

資產編號	資產類別	資產名稱	權責單位	存放位置	數量	備註
						(財產編號)

4. 風險評估表

國立花蓮高級農業職業學校

風險評估表

編號：

風險評估表										
填寫日期：										
項次	資產編號	資產名稱	機密性	完整性	可用性	威脅	弱點	可能性	衝擊性	風險值
1	HW-001	個人電腦	3	2	1	作業人員或使用者錯誤	使用者認知不足	2	3	36
2	HW-002	防火牆	3	3	2	技術失能	技術設施維護不恰當	1	3	24
3	HW-003	門診系統主機	4	3	4	技術失能	技術設施維護不恰當	1	3	33
4	SW-001	防毒軟體	2	2	1	軟體程式錯誤	缺少有效的型態管理控制	1	3	15
6	SW-003	作業系統(Windows7)	2	2	1	入侵	未更新或安裝作業系統/軟體的修補程式	1	2	10

承辦人員：　　單位主管：

註：陳核層級請機關依需求調整

(1)機密性(C)量表

機密等級	資產類別	評估標準	數值
一般	資訊/軟體/實體/支援服務資產	此資訊資產無特殊之機密性要求。	1
	人員資產	無涉及機密性資訊處理之人員。	
內部	實體資產	此資訊資產僅限機關人員存取。	2
	人員資產	機關員工。	
	資訊/軟體/支援服務資產	此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供機關員工使用。	
密	實體資產	此資訊資產僅限機關相關業務承辦人員存取。	3
	人員資產	可接觸密級資產、資料人員。	
	資訊/軟體/支援服務資產	此資訊資產僅供機關相關業務承辦人員存取。	
機密	資訊/軟體/實體/支援服務資產	此資訊資產所包含資訊為機關或法律所規範的機密資訊。	4
	人員資產	可接觸機密級資產、資料人員。	

(2)完整性(I)量表

完整等級	資產類別	評估標準	數值
微或無	資訊資產	資料不正確或不完整時，不會造成任何影響或其影響是可忽略的。	1
	實體資產	硬體或通訊服務發生損壞或故障時，不會造成任何影響或其影響是可忽略的。	

	軟體資產	不當使用軟體時，不會造成任何影響或其影響是可忽略的。	
	支援服務資產	所使用之環境服務發生中斷時，不會造成任何影響或其影響是可忽略的。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，不會造成任何影響或其影響是可忽略的。	
低	資訊資產	資料不正確或不完整時，將對機關業務之營運造成輕微影響。	2
	實體資產	硬體或通訊服務發生損壞或故障時，將對機關業務之營運造成輕微影響。	
	軟體資產	不當使用軟體時，將對機關業務之營運造成輕微影響。	
	支援服務資產	所使用之環境服務發生中斷時，將對機關業務之營運造成輕微影響。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，將對業務之營運造成輕微影響。	
中	資訊資產	資料不正確或不完整時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	3
	實體資產	硬體或通訊服務發生損壞或故障時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	
	軟體資產	不當使用軟體時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	
	支援服務資產	所使用之環境服務發生中斷時，將對機關業務之營運造成中度影響，但不至於造成業務停頓。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，將對業務之營運造成中度影響，但不至於造成業務停頓。	

高	資訊資產	文件及電磁紀錄具有完整性要求，當完整性被破壞時，將對機關業務之營運造成高度影響且致使業務停頓。	4
	實體資產	硬體或通訊服務發生損壞或故障時，將對機關業務之營運造成高度影響且致使業務停頓。	
	軟體資產	不當使用軟體時，將對機關業務之營運造成高度影響且致使業務停頓。	
	支援服務資產	所使用之環境服務發生中斷時，將對機關業務之營運造成高度影響且致使業務停頓。	
	人員資產	人員所負責之作業，因操作錯誤造成的資訊不完整，將對業務之營運造成高度影響且致使業務停頓。	

(3) 可用性(A)量表

可用等級	評估標準	數值
微或無	「可容忍該資訊資產失效時間」≧24 小時。	1
低	16 小時「可容忍該資訊資產失效時間」＜24 小時。	2
中	8 小時「可容忍該資訊資產失效時間」＜16 小時。	3
高	「可容忍該資訊資產失效時間」＜8 小時。	4

上述單位小時為工作小時；1 日工作小時為 8 小時

(4) 可能性量表

可能性	評估標準	數值
低	■ 很少發生。 ■ 對於可預期之資訊安全威脅具有動機但能力不足以利用脆弱點造成資安事件。	1

	■ 資訊安全事件因控制措施執行得當，有效降低脆弱點被利用，致使威脅發生之可能性極低。 ■ 一年發生之次數約 1 次，或三年 1 次以上 3 次以下。	
中	■ 偶爾發生。 ■ 對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ■ 已採行部份資訊安全措施，脆弱點仍未被有效降低或減少，致使威脅發生之機率略高。 ■ 一季發生之次數約 1 次，或一年 1 次以上 4 次以下。	2
高	■ 經常發生。 ■ 對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ■ 未實行資訊安全措施或安全措施無效，脆弱點仍未被有效降低或減少，致使威脅發生機率偏高。 ■ 一個月發生次數 1 次以上，或一季發生 2 次。	3

(5)衝擊性量表

分數	衝擊	評估標準	
1	低	資料保護受到損害	資料外洩或竄改僅導致個人權益輕微受損。 資通安全事件發生時，對資產會造成輕微的損失。
		影響業務運作	對於整體營運或業務執行影響不大。 修復或進行復原的措施可以在很短時間（1 小時）內完成。 造成的損害可能僅影響單一業務或系統。 可以由內部人員進行復原。
		影響法律規章遵循	導致組織違反法律規章並伴隨輕微不良後果。
		人員傷亡	

		損害組織信譽	對組織的信譽有輕微負面衝擊。
		其他	
2	中	資料保護受到損害	資料外洩將導致個人權益嚴重受損。 資通安全事件發生時，對資產會造成較大的損失。 資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成間接或輕微的影響。
		影響業務運作	對於本組織數項業務營運或執行造成停頓。 復原可能要數個小時到 1 天才能完成。 造成的損害可能影響多種業務、數個系統、多個部門或合作夥伴。 復原的措施必須由專業人員才能進行。
		影響法律規章遵循	導致機關違反法律規章並伴隨嚴重不良後果。
		人員傷亡	可能造成人員遭遇危險或受到輕微傷害。
		損害組織信譽	對組織的信譽有嚴重的負面衝擊。
		其他	
3	高	資料保護受到損害	資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成直接且嚴重的影響。 資通安全事件發生時，對資產會造成嚴重的損失。 資料外洩將危及國家安全、導致個人權益非常嚴重受損、或造成極大規模之個人權益嚴重受損。
		影響業務運作	對於本組織全部業務營運或執行造成停頓。 復原無法於 1 天內完成。 造成的損害可能影響全關或利益相關

			者。 復原的措施僅能由外部特定專業人員才能進行或修復人員不易取得。
		影響法律規章遵循	導致組織從根本上違反法律規章。
		人員傷亡	可能造成人員遭遇危險或受到嚴重傷害。
		損害組織信譽	威脅到組織的未來。
		其他	

(6)資訊資產威脅弱點對應

威脅	脆弱性
火災	使用易燃性之材質，如紙或盒子。
未授權存取資料	網路存取規劃不當。
	非單位內人員進出未有適當人員陪同。
	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
作業人員或使用者錯誤	安全訓練不足。
	使用者認知不足。
	缺少文件。
	缺少有效的型態管理控制。
	複雜的使用者介面。
作業失能	備份失效
	保存不當

委外作業失能	未釐清委外協議的權責。
社交工程	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
冒充	未保護密碼(password)檔。
	缺乏身份鑑別與辨識機制。
	密碼易被人識破/取得。
破壞	存取權限不對。
	缺少實體安控。
	缺少變更管理控制。
	缺少邏輯上(技術或系統)的存取安控。
	對有計畫的破壞行動缺乏懲戒處分。
竊聽	未規範行動與遠端裝置之使用。
	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺乏交換資訊協議。
	通訊未加密。
	資料通訊室或中心缺少實體安控。
偷竊	未控制資料及/或軟體複製。

(7)軟體資產

威脅	脆弱性
軟體程式錯誤	不清楚或不完整之開發規格。
	技術不足的人員。
	系統發展生命週期程序不足。
	缺少有效的型態管理控制。

通訊失能	未規劃與建置通訊線路。
	缺少備援與備份設備。
	缺乏意外處理機制。
惡意破壞資料與設施	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。
惡意程式碼	未定期更新防毒軟體(病毒碼及掃瞄引擎)。
	未規劃與建置通訊線路。
	沒有防毒軟體。
	對人員在軟體病毒的教育不足。
	未實施程式碼檢驗。
	對有計畫的破壞行動缺乏懲戒處分。
詐欺	缺乏應用系統控管導致不實的付款。
傳輸錯誤	佈線不當。
	缺乏意外處理機制。
資料外洩	資料分級錯誤或處理不當。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。
入侵	未更新或安裝作業系統/軟體的修補程式。
	開發或設定標準不足。
阻斷服務攻擊	網路管理不足。

	缺乏備援系統。
未授權軟體變更	缺少軟體變更管理規範與程序。
	缺少備份。
	缺少變更管理軟體。
	軟體失能的處理或報告不恰當。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
未授權撥接存取	缺少使用者身份辨識。
作業人員或使用者錯誤	使用者認知不足。
	缺少有效的型態管理控制。
技術失能	使用者認知不足。
	變更管理流程失誤。
使用盜版軟體	未限制複製軟體。
	缺少人員使用合法軟體的規範。
	缺少軟體稽核。
	軟體派送安裝機制不足。
委外作業失能	未釐清委外協議的權責。
社交工程	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
破壞	存取權限不對。
	缺少變更管理控制。
軟體程式錯誤	不清楚或不完整之開發規格。
	技術不足的人員。
	系統發展生命週期程序不足。

	缺少有效的型態管理控制。
惡意程式碼	未定期更新防毒軟體(病毒碼及掃瞄引擎)。
	未控制由網際網路下載及使用軟體。
	沒有防毒軟體。
	資通安全政策不足。

(8)實體資產

威脅	脆弱性
水災	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
火災	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	使用易燃性之材質，如紙或盒子。
	缺少火災偵測設備。
	缺少自動滅火系統。
	缺少實體安控。
	備份檔案或系統無法使用。
未授權存取資料	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
地震	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
有害動物(蟲、鳥、獸)	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
污染	位於易受環境影響的地區。

	沒有回復資訊與資訊資產的營運持續管理與程序。
污染(放射線)	設備與設施缺乏維護。
	備份檔案或系統無法使用。
作業人員或使用者錯誤	使用者認知不足。
技術失能	由於不當的規劃或維護而導致網路容量不夠。
	技術設施維護不恰當。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	使用者認知不足。
	缺少備份設施或流程。
	缺乏環境保護。
	變更管理流程失誤。
委外作業失能	沒有回復資訊與資訊資產的營運持續管理與程序。
	備份檔案或系統無法使用。
破壞	缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。
偷竊	缺少實體安控。
通訊服務失能	網路管理不足(路徑彈性)。
惡意破壞資料與設施	缺少實體安控。
	缺乏溝通導致離職同仁可存取系統。
	對有計畫的破壞行動缺乏懲戒處分。
極端的溫濕度	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。

	環境監控不足。
電力供給失能	電力供應設備容量不足。
電子干擾	位於易受環境影響的地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
電源不穩	位於易有電源不穩定地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。
	沒有電力調節設備。
暴風雨(土石流,颱風)	位於易有天然災害地區。
	沒有回復資訊與資訊資產的營運持續管理與程序。

(9)支援服務資產

威脅	脆弱性
干擾	傳輸介面易遭破壞或干擾。
中斷	缺乏應變計劃。
	容量不足。
	未釐清委外協議的權責。
	維護不當。
誤用	缺乏線路圖或標示不明。
	未釐清委外協議的權責。
	缺乏使用規範。

(10)人員資產

威脅	脆弱性
未授權存取資料	未規劃與建置通訊線路。

	非單位內人員進出未有適當人員陪同。
	缺少實體安控。
	傳輸機密資料未加適當防護。
	對有計畫的破壞行動缺乏懲戒處分。
罷工	沒有回復資訊與資訊資產的營運持續管理與程序。
	缺乏勞資協議。
未授權軟體變更	缺少接收訊息證明。
	缺少軟體變更管理規範與程序。
	缺少備份。
	軟體失能的處理或報告不恰當。
	軟體開發者與作業人員的職責未釐清。
	程式人員監督不週。
	傳輸機密資料未加適當防護。
作業人員或使用者錯誤	安全訓練不足。
	使用者認知不足。
	缺少文件。
	缺少有效的型態管理控制。
	複雜的使用者介面。
否認	未使用數位簽章。
	缺少收送訊息證明。
使用盜版軟體	未限制複製軟體。
委外作業失能	未釐清委外協議的權責。
社交工程	使用分享的乙太網路意即訊號會廣播到區域網路中之每一部機器。
	缺少要求同仁不可在電話上提供資訊的規範。
	缺少資訊諮詢的規範：待釐清詢問者的身份再給予資訊。
	缺乏交換資訊協議。
	通訊未加密。
	資訊相關辦公室或機房缺少實體安控。
	對有計畫的破壞行動缺乏懲戒處分。

破壞(偷竊,詐欺,竄改)	對有計畫的破壞行動缺乏懲戒處分。
偷竊	未控制資料及/或軟體複製。
詐欺	缺乏應用系統控管導致不實的付款。
誤傳	使用者訓練不足。
	缺少接收訊息證明。
	傳輸機密資料未加適當防護。
竄改或任意變更	缺少實體安控。
	缺少邏輯上(技術或系統)的存取安控。
	缺乏加解密規範與控管機制。
	缺乏有效的軟體變更管理導致未授權軟體變更而製造詐欺事件。

5. 風險改善計畫表

國立花蓮高級農業職業學校

風險改善計畫表

編號：

製表日期：113 年　月　　日

風險改善計畫表						
項次	資產編號	資產名稱	風險值	改善措施	執行人員/完成日期	殘餘風險值
1	SW-004	作業系統(WindowsXP)	81	1.限制上網功能 2.禁止使用可攜式媒體 3.編列預算，升級作業系統及電腦主機		(2+4+3)*1*3=27
填寫人員：				主管：		

承辦人員：　　單位主管：

註：陳核層級請機關依需求調整

6. 委外廠商執行人員保密切結書

國立花蓮高級農業職業學校
委外廠商執行人員保密切結書

立切結書人＿＿＿＿＿＿（簽署人姓名）等，受＿＿＿＿＿＿（廠商名稱）委派至＿＿＿＿＿＿（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經機關權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、 未經機關業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接機關網路。若經申請獲准連接機關網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接機關網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經機關業務相關人員之確認並代為申請核准。

五、 機關得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：

姓名及簽章	身分證字號	聯絡電話及戶籍地址
＿＿＿＿＿＿	＿＿＿＿＿＿	＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿	＿＿＿＿＿＿	＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

立切結書人所屬廠商：

廠商名稱及蓋章	廠商負責人姓名及簽章	廠商聯絡電話及地址

填表說明：

一、 廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連結機關網路者為限）及經常到機關洽公之業務人員皆須簽署本切結書。

二、 廠商駐點服務人員、專責維護人員及經常到機關洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

7. 委外廠商查核項目表

國立花蓮高級農業職業學校
委外廠商查核項目表

編號：

填表日期：年月日

查核人員：

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	(下列灰色字體內容為範例)
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	□	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	定期進行政策及目標之檢視、調整。
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	指派副首長擔任資通安全長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	機關內部訂有資安責任分工組織。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	□	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	機關依規定配置資安人員1人。
	3.3 是否具備相關專業資安證照或認證？	□	□	□	專業人員具備ISO27001之證照
	3.4 是否配置適當之資源？	□	□	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	資產依規定指定管理者及使用者。
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	資訊訂有分級處理之作業規範。
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	□	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	□	□	□	機房訂有門禁管制措施。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	離職人員之權限未刪除。
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	□	□	對於進出人員並未監督其活動。
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	□	□	□	按時檢測機房物理面之情況。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	□	□	□	依規定定期檢查並按時提供同仁安全設備之使用運練。
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	□	□	並未陪同或監視第三方支援人員。
	5.7 重要資訊處理設施是否有特別保護機制？	□	□	□	對於核心系統主機並未設置特別保護機制。
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	□	□	□	定期檢查物理面之風險。
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	有設置備用電源。
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	電纜線老舊，並未設有安全保護措施。
	5.11 設備是否定期維護，以確保其可用性及完整性？	□	□	□	設備按期維護。
	5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	□	□	□	訂有相關之保護措施。
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設密碼、檔案加密、專人看管)？	□	□	□	攜帶式設備訂有保護措施。
	5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	設備報廢前均有進行資料清除程序。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
	5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	人員下班後並未將機敏性公文妥善存放。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	系統開發測試與正式作業區隔。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	按時更新病毒碼。
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	定期進行相關系統之病毒掃瞄。
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	定期進行漏洞修補。
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	□	□	□	系統設有檢查之機制。
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	有定期做備份處理。
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	備份資料均有測試。
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	均有設加密之保護措施。
	5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	□	□	□	訂有可攜式媒體之管理程序。
	5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	訂有使用者存取權限註冊及註銷之作業程序。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
	5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	□	□	未定期檢視使用者存取權限。
	5.27 密碼長度是否超過 6 個字元(建議以 8 位或以上為宜)？	□	□	□	密碼符合規定。
	5.28 密碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	密碼符合規定。
	5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	□	□	□	依規定訂定適當之存取權限。
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	□	□	□	對於特定網路有訂定相關之控制措施。
	5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	□	□	□	有針對行動式電腦訂定管理政策。
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	針對重要系統設有身份認證。
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	□	□	□	系統更新後相關措施仍有效。
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	□	□	□	可即時取得系統弱點並採取應變措施。
6.訂定資通安全事件通報	6.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	有訂定通報應變程序。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	(下列灰色字體內容為範例)
及應變之程序及機制	6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	□	□	□	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	□	□	□	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	□	□	□	有定期辦理宣導。
	7.2 是否對同仁進行資安評量？	□	□	□	按期進行資安評量。
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	□	□	□	有定期辦理教育訓練。
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	□	□	□	同仁均瞭解單位之資通安全政策及目標。
8.資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？	□	□	□	訂有稽核機制。
	8.2 是否定有年度稽核計畫？	□	□	□	有訂定年度稽核計畫。
	8.3 是否定期執行稽核？	□	□	□	有按期執行稽核。
	8.4 是否改正稽核之缺失？	□	□	□	訂有稽核後之缺失改正措施。
9.資通安全維護計畫及實施情形之績效管考機制	9.1 是否訂定安全維護計畫持續改善機制？	□	□	□	有訂定持續改善措施。
	9.2 是否追蹤過去缺失之改善情形？	□	□	□	有追蹤缺失改善之情形。
	9.3 是否定期召開持續改善之管理審查會議？	□	□	□	定期召開管理審查會議。

單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

8. 資通安全認知宣導及教育訓練簽到表

國立花蓮高級農業職業學校

資通安全認知宣導及教育訓練簽到表

編號：

課程名稱：_____

時　　間：_____

地　　點：_____

單　位	職　稱	姓　名	簽　名

9. 稽核項目紀錄表

國立花蓮高級農業職業學校稽核項目紀錄表

編號：

填表日期：年月日

查核人員：

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	(下列灰色字體內容為範例)
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	□	□	□	已訂定資通安全政策及目標。
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	政策及目標符合機關之需求。
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	依規定按時進行教育訓練之宣達。
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	定期進行政策及目標之檢視、調整。
	1.5 資通安全目標是否達成？	□	□	□	資通安全目標皆達成。
	1.6 是否隨時公告資通安全相關訊息？	□	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	指派副首長擔任資通安全長。
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	機關內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	□	□	□	有訂定人員錄用之安全評估措施
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	機關依規定配置資通安全人員1人。
	3.3 是否具備相關專業資安證照或認證？(D 級機關可勾選不適用)	□	□	□	專業人員具備ISO27001之證照
	3.4 是否配置適當之資源？	□	□	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	依規定建置資產目錄，並定時盤點。
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	資產依規定指定管理者及使用者。
	4.3 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	□	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	設備報廢前均有進行資料清除程序。
	5.2 是否遵守網路安全規定？	□	□	□	無私裝電腦及網路通訊等相關設備。
	5.3 是否遵守電腦使用之安全管理？	□	□	□	個人電腦不使用時，登出或啟動螢幕保護功能。
	5.4 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	人員下班後並未將機敏性公文妥善存放。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
	5.5 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	按時更新病毒碼。
	5.6 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	定期進行相關系統之病毒掃瞄。
	5.7 是否定期執行各項系統漏洞修補程式？	□	□	□	定期進行漏洞修補。
	5.8 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	□	□	□	系統設有檢查之機制。
	5.9 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	均有設加密之保護措施。
	5.10 是否訂定使用者存取權限註冊及註銷之作業程序？(如無負責系統帳號管理則勾選不適用)	□	□	□	訂有使用者存取權限註冊及註銷之作業程序。
	5.11 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？(如無負責系統帳號管理則勾選不適用)	□	□	□	未定期檢視使用者存取權限。
	5.12 密碼長度是否超過 8 個字元？	□	□	□	密碼符合規定。
	5.13 密碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	密碼符合規定。
	5.14 是否定期維護資通安全防護設備？	□	□	□	定期執行防火牆軟、硬體更新及設定檔備份作業。
6.訂定資通安全事件通報	6.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	有訂定通報應變程序。

查核項目	查核內容	查核結果			說明 (下列灰色字體內容為範例)
		符合	不符合	不適用	
及應變之程序及機制	6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	□	□	□	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	□	□	□	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1 同仁是否每年完成3小時資通安全教育訓練？	□	□	□	已參與教育訓練。
	7.2 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	□	□	□	同仁均瞭解單位之資通安全政策及目標。
8.資通安全維護計畫實施情形之精進改善機制	8.1 是否設有稽核機制？	□	□	□	訂有內部稽核機制。
	8.2 是否定期執行稽核？	□	□	□	有按期執行內部稽核。
	8.3 是否改正稽核之缺失？	□	□	□	訂有內部稽核後之缺失改正措施。
9.資通安全維護計畫及實施情形之績效管考機制	9.1 是否訂定安全維護計畫持續改善機制？	□	□	□	有訂定持續改善措施。
	9.2 是否追蹤過去缺失之改善情形？	□	□	□	有追蹤缺失改善之情形。
	9.3 是否定期審查資通安全維護計畫之實施情形？	□	□	□	定期以公文陳核或召開會議。

單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

10. 改善績效追蹤報告

國立花蓮高級農業職業學校改善績效追蹤報告

編號：

製表日期：

稽核發現			
稽核日期	＿＿＿年＿＿月＿＿日＿＿時	受稽核單位	
稽核區域	■　電腦機房　　委外業務之監督措施　　自動備份系統之安全措施		
缺失或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 缺失項目：委外廠商未定期為保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		

改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。
技術面			
人力面			

資源面	更新相關電腦機房設備，並確保備份設備及機制運作效果。	電腦機房電源設備更新，並採用不斷電系統，於停電時可維持 12 小時運作。	已進行採購作業。
作業程序			
其他			

績效管考			
改善措施確認	■合格／完成 □待追蹤(追蹤期限：_____年_____月_____日) □不合格(說明：_____)		
經費需求或編列執行金額	萬元。	經費執行情形	已進行相關電腦機房設備更新採購，共執行萬元。
預定完成日期	108 年 11 月 20 日	實際完成日期	108 年 11 月 20 日
完成進度或情形說明	定期檢視委外廠商之監督維護責任。		
改善成效考核			
後續成效追蹤			
資通安全推動小組		資通安全長	

註：陳核層級請機關依需求調整

11. 資通安全維護計畫實施情形

國立花蓮高級農業職業學校
資通安全維護計畫實施情形

編號：

本校(單位)之業務因涉及自行辦理資通業務，經主管機關核定後本單位之資通安全責任等級為 D 級 ，依資通安全管理法第 12 條之規定，向 鈞部（院）提出本 113 年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形及佐證資料說明 （下列內容為範例，請機關依自身情形填寫對應的說明，並提供證明，如計畫、程序、記錄或相關公文等）
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	本校核心業務及重要性詳參資通安全維護計畫。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本校已訂定資通安全政策，詳參資通安全維護計畫，並經資通安全長核定(詳附件-維護計畫陳核簽呈)。
	2.2 資通安全目標之訂定	本校已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本校為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本校已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性 (詳會議記錄) 。
3. 設置資通安全推動組織	3.1 設定資通安全長	本校已指定長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本校已設置資通安全推動小組，其組織、分工及職常詳參

		資通安全維護計畫。
4. 專責人力及經費之配置	4.1 專職(責)人員配置	本校依規定設置資通安全人員1人。
	4.2 經費之配置	本校今年視需求已合理分資安經費，資安經費佔資訊經費之%。
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本校已於今年月盤點本校之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本校依資通安全責任等級分級辦法，為資通安全責任等級D級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本校已於今年月完成本校之資訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本校已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資通安全防護及控制措施	本校已依安全維護計畫辦理。
	7.2 資訊及資通系統之保管	本校已依安全維護計畫辦理。
	7.3 存取控制與加密機制管理	本校已依安全維護計畫辦理。
	7.4 作業及通訊安全管理	本校已依安全維護計畫辦理。
	7.5 系統獲取、開發及維護	本校已依安全維護計畫辦理。
	7.6 執行資通安全健診	本校已依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本校已依規定訂定資通安全事件通報應變程序。(詳附件)
	8.2 資通安全事件通報、	本校已依規定進行資通安全事

	應變及演練	件通報。 本校已依規定於今年、月辦理社交工程演練，並於月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本校接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本校已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本校資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本校已依規定監督受託者資通安全維護情形，客製他資通系統開發者 ，已要求其出具安全性檢測證明....(請機關依實際情形列出)。
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本校人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本校已於今年月辦理資通安全教育訓練。
12. 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	12.1 訂定考核機制並進行考核	本校已建立考核機制，並已依規定進行平時及年終考核。
13. 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	13.1 資通安全維護計畫之實施	本校已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本校已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管	本校已依規定以公文陳核或召開會議，確認資通安全維護計

	理	畫之實施情形，確保其持續適切性、合宜性及有效性。
其他說明		

承辦人員：　　資通安全長：

註：陳核層級請機關依需求調整

12. 資通安全事件通報及應變管理程序

壹、 目的

本校為遵照資通安全管理法第 14 條及本校資安全維護計畫之規定，建立本校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、本校所屬人員於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本校應於資通安全事件發生前，確保所屬或監督之公務機關是否制定及落實資通安全事件通報及應變管理程序，並依規定指定其知悉資通安全事件之通報以及完成應變作業後之結案登錄方式。

三、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本校進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

四、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依上級或監督機關及行政院指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、 事件通報窗口及緊急處理小組

一、本校之資通安全事件通報窗口及聯繫專線為：李幸蓉/03-8312338

二、本校應以適當方式使相關人員明確知悉本校之通報窗口及聯絡方式。

三、本校所屬人員發現資通安全事件後，應立即向所屬單位主管及本校之通報窗口通報。

四、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，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

五、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。

六、事件經初步判斷認為可能屬重大資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校所屬機關或受託廠商所通報之資通安全事件時，亦同。

七、緊急處理小組成員由資通安全長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。

八、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)除事件之等級外，權責人員或緊急處理小組亦應對資通安全事件之影響範圍、損害程度及本校因應之能力進行評估。

(三)本校權責人員或緊急處理小組於完成資通安全事件等級之判斷及相關評估後，應盡速報資通安全長核准。

(四)除因網路或電力中斷等事由，致無法依上級或監督機關及行政院所指定或認可之方式通報外，應於知悉資通安全事件後一小時內上級或監督機關及行政院所指定或認可之方式，進行事件通報。

(五)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，應於知悉資通安全事件後一小時內以電話或其他適當方式，將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，分別告知所屬之上級或監督機關及行政院，並於事由解除後，依原方式補行通報。

(六)資通安全事件等級如有變更，權責人員或緊急應變小組應告知通報窗口，使其續行通報作業。

(七)本校於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，應即向本校之權責人員或窗口，以指定之方式進行通報。

(八)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，權責人員或緊急處理小組應於知悉資通安全事件後一小時內，將該事件依上級機關或行政院所指訂或認可之方式，通知該機關。

(九)本校執行通報應變作業時，得視情形向直屬上級機關或縣政府提出技術支援或其他協助之需求。

二、接獲自身、所屬（監督）機關通報之評估作業程序

(一) 本校之權責人員或緊急處理小組，於接獲所屬（監督）機關之資通安全事件通報後，應於以下時限內，完成資通安全事件通報等級及相關事項之審核：

1. 通報為第一級或第二級之資通安全事件，於接獲通報後八小時內。

2. 通報為第三級或第四級之資通安全事件，於接獲通報後二小時內。

(二) 本校之權責人員或緊急處理小組進行本條第一項之審核過程中，得請求通報之公務機關提供級別判斷所需之資料或紀錄。

(三) 本校於必要時得依據審核之結果，逕行變更資通安全事件之等級，並應於決定變更後一小時內，將審核結果及級別變更之決定通知行政院，並提供做成決定所依據之相關資訊。

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，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，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. 資安事件相關鑑識及其他調查作業。

4. 資安事件之調查與處理及改善報告之方式。

5. 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，應依據本校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七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三) 本校完成通報及應變程序之辦理後，應依所隸屬之上級機關或行政院所指定或認可之方式進行結案登錄。

(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、 資安事件後之復原、鑑識、調查及改善機制

一、本校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、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行政院提出前項之報告，以供監督與檢討。

四、本校指示隸屬於本校之所屬機關提出第二項報告之期限，若其逾期未提出，本校除應使其盡速提出外，並應為其他必要之監督及指示。

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「資通安全事件通報單」上留存完整之紀錄，該文件並應經承辦之權責人員、資通安全長簽核。

二、本校於完成資通安全事件之通報及應變程序後，應依據「資通安全事件通報單」之內容及實際處理之情形，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。