花蓮縣政府
資通安全維護計畫

4.3

115 年 3 月 9 日

目錄

壹、依據及目的

本計畫依據資通安全管理法第 13 條及施行細則第 9 條訂定。

貳、適用範圍

本計畫適用範圍涵蓋花蓮縣政府（以下簡稱本機關）全機關。

參、核心業務及重要性

一、核心業務及重要性：

本機關依法辦理自治事項、執行中央機關委辦事項，並監督所轄鄉（鎮、市）自治。
https://glrs.hl.gov.tw/glrsout/LawContent.aspx?id=GL000556

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
機房與網路服務（含電力）	無	■為本機關依組織法執掌，足認為重要者	影響其他機關業務運作(相依性)： 機房與網路服務，如無法正常運作時，將影響機關行政效率。	4 小時
縣府同仁人事差勤之管理	電子差勤管理系統	■為本機關依組織法執掌，足認為重要者	影響其他機關業務運作(相依性)： 影響本機關業務運作，刷卡資料無法進電子差勤管理系統，同仁無法請假，無法查詢差假狀況。	12 小時
縣府內部及外部之行政溝通	公文整合資訊系統	■為本機關依組織法執掌，足認為重要者	影響其他機關業務運作(相依性)： 如失效將影響本機關使用公文系	16 小時

			統之機關(單位)，造成無法接收、發送及繕打公文，造成行政效率低落。	
	公務雲系統	■為本機關依組織法執掌，足認為重要者	影響其他機關業務運作(相依性)： 提供員工入口網及即時通訊功能，如失效將造成公務聯繫、辦公效率降低，影響行政效率。	12 小時

二、非核心業務及說明：

本機關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
內部管理業務	本機關內部管理業務等，如無法正常運作時，將影響機關行政效率。	72 小時
民眾服務業務	本機關民眾服務業務等，如無法正常運作時，將影響機關行政效率。	72 小時

肆、資通安全政策及目標

一、資通安全政策

為強化資通安全管理，建立安全及可信賴之電子化政府作業環境，以確保資料、系統、設備及網路安全，保障民眾權益，特訂定本機關資通安全政策及目標，詳細內容詳本機關資通安全管理系統四階文件「1-01-01 資通安全政策」。

二、資通安全目標

為維護本機關資通訊資產之機密性、完整性與業務服務之可用性，期藉由本機關全體同仁共同努力以達成下列目標：

(一) 確保資通訊資產之機密性，資通訊資產須經適當授權方可存取。

(二) 確保資通訊資產之完整性，資通訊資產應避免未經授權或非預期之變更或修改。

(三) 確保業務服務之可用性及持續運作。

(四) 確保業務服務之執行符合相關法令或規範之要求。

三、資通安全政策及目標之核定程序

資通安全政策經資通安全推行委員會審核後實施，修正時亦同。

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內部會議、張貼公告等方式，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、資通安全組織

一、資通安全推行委員會

(一) 組織

為提升整體資通安全，明確規定本機關資通安全及組織之角色及職掌，期使內部組織及內部控制達到最佳化，依本機關資通安全管理系統四階文件「2-03-01 資通安全管理組織管理辦法」設立資通安全推行委員會。詳細資通安全組織之角色及職掌得參照「2-03-01 資通安全管理組織管理辦法」內「四. (二)資通安全推行委員會」。

(二) 分工及職掌

本機關之資通安全推行委員會依資通安全長之指示進行責任分組，詳細之分工與負責事項得參照「2-03-01 資通安全管理組織管理辦法」內「四. (四)資通安全長」、「四.(五)資安工作小組」、「四.(六)稽核工

作小組」與「四.(七)文件管理工作小組」。

陸、專職人力及經費配置

一、專職人力及資源之配置

(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 B 級，最低應設置資通安全專職人員 2 人，其分工如下：

1. 資通安全管理面業務 1 人，負責推動資通系統分級及防護基準、資訊安全管理系統導入及驗證、內部資通安全稽核、業務持續運作演練、資安治理成熟度評估及資通安全教育訓練等業務之推動。

2. 資通安全技術面業務 1 人，負責資通安全監控管理機制、政府組態基準導入，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. 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。

4. 資安專職人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

(1)資安專職人員分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。

(2)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，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，建立人力備援制度。

(3)本機關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。

(4)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) 資通安全推行委員會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資通安全預算所佔之比例。

(三) 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資通安全推行委員會提出，由資通安全推行委員會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。

(四) 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、資通系統之盤點

本機關每年度應辦理資通系統盤點及資訊資產盤點：

一、資通系統盤點

本機關由資訊科統籌，請所有系統管理員定期盤點資通系統於「本府系統清單」。

二、資訊資產盤點

(一) 幕僚單位五處依本計畫規定，定期進行資訊資產盤點，其他處室參准辦理。

(二) 詳細程序詳本機關資通安全管理系統四階文件「2-04-01 資訊資產暨風險管理辦法」及「3-04-01 資訊資產管理程序」。

三、機關資通安全責任等級分級

本機關因持有區域性或地區性民眾個人資料檔案，並負責區域性或地區性跨公務機關共用性資通系統之維運，為資通安全責任等級B級公務機關。

捌、資通安全風險管理

本機關每年度應辦理資通系統之風險評估及資訊資產風險評估：

一、資通系統之風險評估

本機關應系統管理員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，依「資通安全責任等級分級辦法」附表九完成資通系統分級，並完成附表十之控制措施；並應每年至少檢視一次

資通系統分級妥適性。

二、資訊資產風險評估

(一) 幕僚單位五處依本計畫規定，定期進行資訊資產風險評估，其他處室參准辦理。

(二) 依據本機關資通安全管理系統四階文件「2-04-01 資訊資產暨風險管理辦法」及「3-04-02 資訊資產風險管理程序」進行評估。

(三) 本機關應每年針對資訊資產盤點之鑑價後，進行風險評估並完成「4-04-03 資訊資產風險評估表」，依據程序產出「4-04-06 風險評鑑報告」。

玖、資通安全防護及控制措施

本機關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，由於本機關核心資通系統已導入並通過 ISO 27001 驗證，全府之防護及控制措施詳如 ISO 27001 資通安全管理系統文件，並針對資通安全責任等級分級辦法中資通安全責任等級 B 級公務機關應辦事項採行相關之防護及控制措施如下。

一、執行資通安全健診

(一) 本機關應每二年辦理資通安全健診，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. 目錄服務系統設定及防火牆連線設定檢視。

6. 核心資通系統資料庫安全檢視。

二、安全性檢測

(一) 弱點掃描

全部核心資通系統每年辦理一次。

(二) 滲透測試

全部核心資通系統每二年辦理一次。

三、資通安全監控管理機制

建置監控管理機制，並持續維運及依主管機關指定之方式提交監控管理資料。

四、政府組態基準

導入本機關政府組態基準作業，並持續維運。

五、資通安全防護

(一) 應建置防毒軟體、網路防火牆、電子郵件過濾機制、入侵偵測及防禦機制及應用程式防火牆，持續使用並適時進行軟、硬體之必要更新或升級。

(二) 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形，詳本機關資通安全管理系統四階文件「2-07-01 通訊與作業管理辦法」。

六、資通安全弱點管理

導入資通安全弱點管理作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

七、端點偵測及應變機制

導入端點偵測及應變機制，並持續維運及依主管機關指定之方式提交偵測資料。

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，本機關資通安全事件通報、應變相關機制詳本機關資通安全管理系統四階文件「2-10-01 資通安全事故管理辦法」、「3-10-01 事件通報管理程序」；本機關演練相關機制，詳本機關資通安全管理系統四階文件「**2**-11-01 營運持續管理辦法」、「3-11-01 緊急應變計畫管理程序」。

壹拾壹、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、本機關可接受之風險及本機關之資源，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，詳細程序詳本機關資通安全管理系統四階文件「2-13-01_委外管理辦法」。

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。

(四) 受託業務涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，於招標公告、招標文件及契約中，註明受託者辦

理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

(五) 前點適任性查核得在必要範圍內就下列事項查核，查核前應經當事人書面同意：

1. 曾犯刑法妨害電腦使用罪章之罪，經有罪判決確定，或通緝有案尚未結案。

2. 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。

3. 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。

4. 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

5. 其他與國家機密保護相關之具體項目。

二、監督受託者資通安全維護情形應注意事項

(一) 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。

(二) 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。

(三) 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。

(四) 受託者應採取之其他資通安全相關維護措施。

(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。

壹拾參、資通安全教育訓練

本機關依資通安全責任等級分級屬 B 級公務機關，依本機關資訊安全管理系統四階文件「2-05-01 人力資源及訓練管理辦法」辦理本機關人員資通安全教育訓練。

壹拾肆、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，依據公務機關所屬人員辦理資通安全事項作業辦法及本機關各相關規定辦理之。

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，使本機關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，應與本機關之資通安全政策、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. 資通安全推行委員會應每年一次或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. 依資通安全管理法第 15 條「公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形」，本機關應定期檢視所屬或監督機關之資通安全維護計畫實施情形，因應機關(單位)眾多，本項檢視採抽測方式執行，執行項目另以本機關所屬及監督機關資通安全稽核計畫定之。

3. 辦理稽核前資通安全推行委員會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。

4. 辦理稽核時，資通安全推行委員會應於執行稽核前 14 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。

5. 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；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提供給受稽單位，並由受稽單位進行矯

正措施。

6. 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。

7. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼）。

8. 詳本機關資通安全管理系統四階文件「2-12-01 資訊稽核管理辦法」。

(二) 稽核改善矯正

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議改善措施、改善進度規劃，並落實執行。

2. 受稽單位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. 受稽單位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. 機關應定期審查受稽單位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. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫「4-10-01 矯正紀錄單」。

三、資通安全維護計畫之持續精進及績效管理

(一) 本機關之資通安全推行委員會應每年召開一次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。

(二) 管理審查議題應包含下列討論事項：

1. 過往管理審查議案之處理狀態。

2. 與資通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、資通安全推行委員會決議事項等。

3. 與資訊安全管理系統相關關注方之需要及期望的變更。

4. 資通安全維護計畫內容之適切性。

5. 資通安全績效之回饋，包括：

(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。

(4) 內外部稽核結果。

(5) 不符合項目及矯正措施。

(6) 風險評鑑結果及風險處理計畫執行進度。

(7) 重大資通安全事件之處理及改善情形。

(8) 利害關係人之回饋。

(9) 持續改善之機會。

(三) 持續改善機制之管理審查相關紀錄應予保存，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

本機關依據本法之規定，應每年向主管機關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。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

(一) 資通安全管理法

二、附件表單

(一) 本府系統清單

(二) 1-01-01 資通安全政策

(三) 2-03-01 資通安全管理組織管理辦法

(四) 2-04-01 資訊資產暨風險管理辦法

(五) 2-05-01 人力資源及訓練管理辦法

(六) 2-07-01 通訊與作業管理辦法

(七) 2-10-01 資通安全事故管理辦法

(八) 2-11-01 營運持續管理辦法

(九) 2-12-01 資訊稽核管理辦法

(十) 3-04-01 資訊資產管理程序

(十一) 3-04-02 資訊資產風險管理程序

(十二) 3-10-01 事件通報管理程序

(十三) 3-11-01 緊急應變計畫管理程序

(十四) 4-03-02 資安目標有效性量測統計表

(十五) 4-03-04 資通安全相關法令標準規範彙總表

(十六) 4-04-03 資訊資產風險評估表

(十七) 4-04-06 風險評鑑報告

(十八) 4-10-01 矯正紀錄單

(十九) 2-13-01 委外管理辦法