屏東縣枋寮戶政事務所
資通安全維護計畫

108 年 8 月

資通安全維護計畫_C 級

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。

貳、適用範圍

本計畫適用範圍涵蓋本所全機關。

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
戶政業務管理	無	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 □為本機關依組織法執掌，足認為重要者 ■機關維運必要之業務	影響機關業務運作： 因無核心資通系統，故此項不評估。	因無核心資通系統，故此項不評估。

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。
2. 作業名稱：該項業務內各項作業程序的名稱。
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. 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
差勤服務-差勤系統	差勤系統失效時，影響機關差勤作業效率	24 小時

各欄位定義：

1. 業務名稱：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、郵件服務、用戶端服務等。(請依機關實際情形列出)
2. 作業名稱：該項業務內各項作業程序的名稱。
3. 說明：說明該業務之內容。
4. 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

為使本機關業務順利運作，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，本機關同仁應參與資通安全教育訓練，以提高資通安全意識。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 定期進行內部稽核，確保相關作業皆能確實落實。

二、資通安全目標

(一) 量化型目標

1. 本機關同仁每年皆完成 3 小時資通安全教育訓練。
2. 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。(年度 3 級以上事件發生≤1 次)。

3. 前次內部稽核發現事項，未完成改善之件數應≦2 件。

三、資通安全政策及目標之核定程序

資通安全政策由本機關戶籍資料及行政庶務股簽陳資通安全長核定。

四、資通安全政策及目標之宣導

1. 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、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。

2. 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，本機關訂定秘書為資通安全長，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，由資通安全長指派資通安全推動小組權責人員，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。

本機關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、專責(職)人力及資源之配置

1. 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Ｃ級，最低應設置資通安全專責人員１人(須以專職人員配置之)，其工作如下，本機關現有資通安全專責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。

(1) 負責推動資通系統防護需求分級、內部資通安全稽核、教育訓練、資通系統分級及防護基準、資通安全健診、資通安全防護設施建置、資通安全事件通報及應變及法遵義務執行事宜。

2. 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。

3. 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) 資安專職人員總計應持有 1 張以上資通安全專業證照。

(2) 資安專職人員總計應持有 1 張以上資通安全職能評量證書，並持續維持證書之有效性。

4. 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「資通安全保密同意書」，並建立人力備援制度

5. 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。

6. 專業人力資源之配置情形應每年定期檢討。

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。

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. 各單位如有資通安全資源之需求，應向資通安全推動小組提出，並以機關內部簽呈或填寫「資通安全需求申請單」，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。

4. 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. 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、軟體資產、實體資產、支援服務資產等。

2. 資訊及資通系統資產項目如下：

   (1) 資訊資產（資產類別代號：ID）：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（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) 實體資產（資產類別代號： HW）：電腦及網路設備、可攜式設備等。

   (4) 支援服務資產（資產類別代號： ES）：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（資產類別代號： PE）：系統管理者、設備管理者、委外駐點廠商等。

3. 本機關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. 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。

5. 權責單位：對資產具備管理權責之單位。

6. 每一個實體資產以及支援服務資產，只要是看得到/摸得到之主機/設備，都要標示。

7. 標籤內容：資產編號＋資產名稱

8. 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」。

二、機關資通安全責任等級分級

本機關因維運自行或委外開發之資通系統，為資通安全責任等級 C 級機關。

捌、資通安全風險評估

一、資通安全風險評估

1. 本機關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) x 可能性 x 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)，其評估標準請參考「資產價值評估量表」。

4. 資產風險計算需評估各事件可能性及衝擊性，其評估標準請參考「可能性及衝擊性評估量表」。

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，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，應儘量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) 資料備份

1. 系統中重要資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，且宜執行異地存放。

2. 敏感或機密性資訊之備份應加密保護。

(五) 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。

(六) 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、系統獲取、開發及維護

(一) 本機關之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，並填入「資通系統清冊」。系統等級為「高」者應完成附表十中資通系統防護基準，並注意下列事項：

1. 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

2. 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

3. 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

4. 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

四、資通安全健診

本機關每二年應辦理一次資通安全健診，其至少應包含下列項目，並檢討執行情形：

(一) 網路架構檢視。

(二) 網路惡意活動檢視。

(三) 使用者端電腦惡意活動檢視。

(四) 伺服器主機惡意活動檢視。

(五) 目錄伺服器設定及防火牆連線設定檢視。

五、資通安全防護設備

(一) 本機關應建置防毒軟體、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。

(二) 資安設備應定期備份日誌紀錄，定期檢視執行情形。

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，本機關應訂定資通安全事件通報、應變及演練相關機制，參閱「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。

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，稽核項目可參「委外廠商查核項目表」。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

1. 本機關依資通安全責任等級分級屬 C 級，資安及資訊人員每年至少 1 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。
2. 本機關之一般使用者與主管，每人每年接受 3 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，例如「資通安全認知宣導及

教育訓練簽到表」。

2. 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、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. 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。

4. 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

本機關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) 內部稽核機制之實施

1. 資通安全推動小組應定期(至少每二年一次)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. 內部稽核作業可以自評或各機關交互實地稽核等方式，以下說明作業方式：

(1) 自評：由資通安全推動小組依據「稽核自評表」各查核項目判斷實作現況，勾選適當查核結果，並於說明欄位描述所見情

形；當查核結果為不符合時，資通安全推動小組應提出改善措施填入說明欄位，並落實執行。

(2) 各機關交互實地稽核：由非本機關人員擔任稽核員，依據「稽核自評表」各查核項目進行稽核作業。稽核員依實作現況勾選適當查核結果，並於說明欄位描述所見情形；當稽核員提出查核結果為不符合時，資通安全推動小組應提出改善措施填入說明欄位，並落實執行。

3. 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。

三、資通安全維護計畫之持續精進及績效管理

1. 本機關之資通安全推動小組每年應以公文陳核或召開會議，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

本機關依據本法第 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

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. 安全軟體發展流程指引

8. 安全軟體設計指引

9. 安全軟體測試指引

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. 資通安全需求申請單
4. 資訊及資通系統資產清冊
5. 資產價值評估量表
6. 可能性及衝擊性評估量表
7. 威脅弱點對應表
8. 風險評估表
9. 風險改善計畫表
10. 資通系統清冊
11. 委外廠商執行人員保密切結書
12. 委外廠商執行人員保密同意書
13. 委外廠商查核項目表
14. 資通安全認知宣導及教育訓練簽到表
15. 稽核自評表
16. 改善績效追蹤報告
17. 資通安全維護計畫實施情形
18. 資通安全事件通報及應變管理程序