臺中市豐原地政事務所資通安全維護計畫

中華民國 108 年 1 月 17 日訂定

108 年 10 月 8 日豐地資字第 1080009686 號函修正

109 年 12 月 9 日豐地資字第 1090012020 號簽修正

110 年 12 月 7 日豐地資字第 1100011605 號簽修正

112 年 12 月 6 日豐地資字第 1120012438 號簽修正

目 錄

壹、 依據及目的 2
貳、 適用範圍 2
參、 核心業務及重要性 2
肆、 資通安全政策及目標 2
伍、 資通安全推動組織 2
陸、 專職(責)人力及經費配置 3
柒、 資訊及資通系統之盤點 4
捌、 資通安全風險評估 4
玖、 資通安全防護及控制措施 5
壹拾、 資通安全事件通報、應變及演練相關機制 5
壹拾壹、資通安全情資之評估及因應 5
壹拾貳、資通系統或服務委外辦理之管理 6
壹拾參、資通安全教育訓練 7
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 ... 7
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 ... 7
壹拾陸、資通安全維護計畫實施情形之提出 9

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臺中市豐原地政事務所全機關(以下簡稱本機關)。

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	重要性說明	業務失效影響說明	最大可容忍中斷時間
地政業務	為主管機關核定資通安全責任等級 C 級機關所涉業務	地政業務失效時，影響民眾財產交易、紀錄及機關信譽。	48 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
臺中市豐原地政事務所全球資訊網	無法提供民眾市政資訊，影響民眾取得公開資料，影響機關聲譽	48 小時
地價區段劃分及區段地價估價作業系統	影響機關行政效率	48 小時
地政資料掃描建檔資訊系統	影響機關行政效率	48 小時

肆、資通安全政策及目標

依據本機關資訊安全管理系統文件編號 ISMS-1-003「臺中市政府地政局暨所屬地政事務所資訊安全政策與目標」辦理。

伍、資通安全推動組織

依據本機關資訊安全管理系統文件編號 ISMS-2-008「臺中市政府地

政局暨所屬地政事務所資通安全組織架構及作業程序書」辦理。

陸、專職(責)人力及經費配置

一、專職(責)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Ｃ級,最低應設置資通安全專職(責)人員１人,負責本機關之法遵義務執行事宜。本機關現有資通安全專責人員名單及職掌應列冊,並適時更新。

(二) 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。

(三) 資安專職(責)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。

(四) 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,應簽署書面約定,並視需要實施人員輪調,建立人力備援制度。

(五) 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。

(六) 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動小組提出,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。

(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、軟體資產、實體資產、服務資產等。

(二) 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、永續運作計畫、稽核紀錄及歸檔之資訊等。
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：電腦及通訊設備、可攜式設備及資通系統相關之設備等。
4. 服務資產：相關基礎設施及其他機關內部之支援服務，如電力、消防等。

(三) 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：資訊及資通系統名稱、資產名稱、資產類別、擁有者、管理者、使用者、存放位置、防護需求等級。

(四) 資訊及資通系統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。

(五) 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產清冊。

二、機關資通安全責任等級分級

本機關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

依據本機關資訊安全管理系統文件編號 ISMS-2-004「臺中市政府地

政局暨所屬地政事務所風險評鑑作業程序書」辦理。

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 ISO 27001 資訊安全管理系統，全機關之防護及控制措施詳如 ISO 27001 資通安全管理系統文件。

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，本機關依行政院訂定「各機關資通安全事件通報及應變處理作業程序」辦理資通安全事件通報、應變及演練。

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

(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

依據本機關資訊安全管理系統文件編號 ISMS-3-034「臺中市政府地

政局暨所屬地政事務所委外作業安全管理作業說明書」辦理。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

(一) 本機關依資通安全責任等級分級屬 C 級，資通安全專職人員每人每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練。

(二) 資通安全專職人員以外之資訊人員每人每2年至少接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練。。

(三) 本機關之一般使用者與主管,每人每年接受 3 小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

依據本機關資訊安全管理系統文件編號 ISMS-2-013「臺中市政府地政局暨所屬地政事務所資訊安全人員教育訓練作業程序書」辦理。

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、臺中市政府及所屬各機關學校公務人員平時獎懲案件處理要點，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. 資通安全推動小組應定期(至少每 2 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. 辦理稽核前資通安全推動小組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。
3. 辦理稽核時，資通安全推動小組應於執行稽核前 10 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至稽核結果及改善報告中，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（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）。

(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) 本機關之資通安全推動小組每年應召開會議，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。

(二) 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，以作為持續精進及績效管理執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本機關依據資通安全管理法第 12 條之規定，依主管機關規定期限向上級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。