桃園市政府主計處

資通安全維護計畫
(V1.4)

版本修訂紀錄表

項次	年度	版次	修訂日期	備註
1	108	V1.0	108/01/30	新編
2	109	V1.1	109/03/06	依本府資訊科技局109年2月13日府資設字第1090018424號函知範本修改
3	111	V1.2	111/02/22	依資通安全管理法及本處ISMS程序書與表件資料修改
4	112	V1.3	112/02/15	本處業已導入ISMS，修改資通安全維護計畫，俾利與現行ISMS四階文件規定一致
5	113	V1.4	113/03/20	修正文字內容。 因應本府組織改造及業務移撥，修正本府資訊相關主辦機關為「智慧城鄉發展委員會」。

目　　錄

壹、依據及目的

本計畫依據據下列法規訂定：

一、資通安全管理法第 10 條及施行細則第 6 條訂定。

二、桃園市政府主計處資通安全管理系統相關程序及規範。

貳、適用範圍

本計畫適用範圍涵蓋桃園市政府主計處(以下簡稱本機關)。

參、核心業務及重要性

- 依據行政院資通安全責任等級分級辦法，本機關資安責任等級為C級機關。

- 資通安全責任等級C級之公務機關應辦事項如下表：

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級；其後應每年至少檢視一次資通系統分級妥適性；並應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。

制度面向	辦理項目	辦理項目細項	辦理內容
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全弱點通報機制		一、 初次受核定或等級變更後之二年內，完成資通安全弱點通報機制導入作業，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。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成資通安全弱點通報機制導入作業，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。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持
		網路防火牆	

制度面向	辦理項目	辦理項目細項	辦理內容
		具有郵件伺服器者，應備電子郵件過濾機制	續使用及適時進行軟、硬體之必要更新或升級。
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別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。

本機關之核心業務及重要性如下表：

核心業務名稱	作業名稱	重要性說明	MTPD
歲計業務	預算編製及決算編造	依市政建設之輕重緩急，將有限財源作最經濟有效之分配運用，達成財政健全，妥適分配本府有限資源。	4 小時
會計業務	財務及預算執行之管理	發揮財務管理功能，將預算執行及財務活動情形確實記錄，以了解計畫執行之績效，並透過督導各機關內部審核，以符合法令並減少浪費，增進本府財務效能。	4 小時
統計業務	蒐集政府施政相關之資料及分析	蒐集與政府施政及社會經濟有關之資料，加以整理、分析，適時提供決策之參據，發揮統計支援決策功	4 小時

		能，協助推動市政建設。	

本機關核心業務係使用中央維運之資通系統，故本機關使用之資通系統屬非核心系統，說明如下表：

非核心業務名稱	非核心資通系統	業務失效影響說明	MTPD
公務統計資訊管理	公務統計行政管理系統	影響機關行政效率。	18 小時
桃園市市政資料整合	桃園市市政資料整合平台	影響機關行政效率。	24 小時

各欄位定義：

1. 核心業務名稱：機關內的核心業務名稱。
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. MTPD：最大可容忍中斷時間。

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，確保資訊資料、系統、設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或毀損等風險，特制訂「資通安全政策(ISMS-01-001)」(以下簡稱本政策)，本政策未規定事項依政府其他資通安全法規辦理，以達成資訊之機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）及適法性(Compliance)。

二、資通安全目標

為確認資通安全落實程度，本機關資通安全管理系統目標係針對「資通安全實施程序書(ISMS-02-002)」之「三、資通安全管理系統目標」辦理，相關單位應對各項目標進行統計並分析，並紀錄於「資通安全管理系統目標與評量機制查核表（02-002-01）」，以確認

目標的達成情形。

三、資通安全政策及目標之核定程序

由「資通安全推動組織」下設之「文件管理分組」簽陳資通安全長核定。

四、資通安全政策及目標之宣導

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。

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、資通安全推動組織

資通安全推動作業之權責依據本機關「資通安全組織程序書(ISMS-02-001)」辦理，設置「資通安全推動組織」，並定期維護與更新「資訊安全組織名冊（02-001-01）」。

陸、專責人力及經費配置

一、專職人力資源之配置

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職人員 1 人，並適時更新。
2. 本機關職責及人員能力需求依據「資通安全組織程序書(ISMS-02-001)」於「資通安全推動組織」下設「資安處理小組」(「資通安全組織名冊（02-001-01）」負責執行資通安全相關業務及技術之推動)。
3. 資通安全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]：至少一名資通安全專職人員，分別持有資通安全專業證照及資通安全職能評量證書各一張以上，並持續維持證照及證書之有效性。

[1] 各機關應依據其資通安全責任等級分級辦法所規範之資通安全專責人員、認知與訓練之要求，配置適當之資源於資安人員專業職能之培養。

二、經費之配置

1. 資通安全推動組織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]。

2. 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，應配合機關預算規劃期程向資通安全推動組織提出[3]，由資通安全推動組織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，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

本機關已訂定「資產管理制度暨風險評鑑程序書(ISMS-02-006)」，每年定期辦理資訊及資通系統資產盤點；如遇設備更新或汰換時，須重新執行資產盤點。並產出「資產清冊暨風險評鑑表（02-006-01）」。

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、資通安全風險評估及因應

1. 本機關已訂定「資產管理制度暨風險評鑑程序書(ISMS-02-006)」，每年定期進行風險評估，針對資訊資產進行風險評估，相關威脅脆弱點鑑別、風險值鑑別及風險處理等，產出「資產清冊暨風險評鑑表（02-006-01）」進行「風險評鑑」、「風險排序與風險處理措施」、「高風險處理方案」。

2. 每年依據「資通安全責任等級分級辦法」之規定，分別就機密

[2] 為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動組織於資源規劃或編製預算時，應考量機關之責任等級、資通安全政策及目標。

[3] 各機關可填具資通安全需求申請單。

性、完整性、可用性、法律遵循性等面向評估係自行或委外開發之資通系統防護需求分級，並應於初次受核定或等級變更後之二年內，完成防護需求分級對應之資通系統防護基準控制措施。

玖、資通安全防護及控制措施

依據資通安全風險評估結果、資通安全責任等級 C 級之應辦事項及資通系統防護基準，採行相關之防護及控制措施，本機關業導入「ISO 27001 資訊安全管理系統」，有關防護及控制措施將依本機關資通安全管理系統相關規範辦理。另本機關無維運核心資通系統，非核心資通系統應準用相關程序書、標準書內容進行資安防護。

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，有效降低其所造成之損害，本機關已訂定資通安全事件通報及應變管理程序，詳細規範及作業流程參照「資通安全事件管理程序書(ISMS-02-009)」。

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「資通安全推動組織之資安處理小組」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

由資通安全專職人員或系統管理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

「資通安全推動組織」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

本機關已訂定「資通委外安全管理程序書(ISMS-02-011)」，於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，執行相關委外管理作業及要求等。

壹拾參、資通安全教育訓練

依據「資通安全實施程序書(ISMS-02-002)」之「玖、執行資通安全 一、人員安全」，每年度均配合本府智慧城鄉發展委員會規劃之教育訓練項目及時程，完成當年度相關人員須接受之資通安全訓練。

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「桃園市政府及所屬各機關學校人員資通安全事項獎懲基準」審酌辦理。

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紀錄。

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

「資通安全推動組織」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。內稽作業流程規範參照「資通安全稽核管理程序書(ISMS-02-010)」。

(二) 稽核改善報告

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。相關作業規範參照矯正管理程序書(ISMS-02-007)」。

三、資通安全維護計畫之持續精進及績效管理

本機關應於每年（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之實施情形，確保其持續適切性、合宜性及有效性。作業流程規範參照「資通安全實施程序書(ISMS-02-002)」。

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，應每年向上級或監督機關，提出資通安全維護計畫實施情形[4]，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

本計畫參考相關法規請參照「外來文件管制表(02-005-01)」，本機關已訂定相關程序及表單請參照「四階文件清冊(02-005-02)」。

[4] 資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項。