臺中市和平區衛生所

資通安全維護計畫

版本 V4.0

中華民國115年4月1修訂

文件制/修訂履歷

制/修訂版次	制/修訂日期	制/修訂說明	備註
1.0	108/1/22	初版發行	
2.0	109/8/4	依臺中市政府衛生局109年7月29日指示辦理修正	
3.0	112/12/25	依臺中市政府衛生局指示辦理修正	
4.0	115/4/1	配合資安法修法修正計畫	

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本衛生所全機關。

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	系統失效影響說明	系統最大可容忍中斷時間
婦幼衛生、社區護理、疾病防治、預防接種、國民營養、精神衛生、衛生教育、衛生統計、食品衛生、營養衛生、家戶衛生及醫藥管理等事項	傳染病個案通報系統 健保資訊網服務系統 (由衛生福利部維護)	為本機關依組織法執掌，足認為重要者	業務系統失效時，影響業務運作效率，需改以紙本方式處理	由資通系統管理單位訂之
門診醫療、巡迴醫療、緊急救護及實驗診斷等事項	醫療保健資訊系統 (門診掛號系統) (由衛生福利部維護)			

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
臺中市政府網站整合	無法提供民眾機關資訊，影響民眾取得	由上級或中

服務平台(公版官方網站)	公開資料，影響機關聲譽	央管理單位訂之
臺中市政府陳情整合平台	無法處理民眾陳情意見，影響機關行政效率	
E化公務入口網	無法使用相關應用系統，影響機關行政效率	
差勤及費用請領表單系統	影響機關同仁差假申請權益	
公文整合資訊系統	影響機關行政效率	
電子郵件服務系統	無法使用e-mail，影響機關行政效率	
AD系統	影響機關同仁內部系統之使用，降低行政效率	
防毒系統等	失效時提高資安風險	

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：

(一) 強化人員知能。

(二) 避免資料外洩。

(三) 確保服務可用。

二、 資通安全目標

(一) 確實參與中央機關、上級機關辦理之資安教育訓練，提高人員資通安全之意識與強化其對相關責任之認知。

(二) 保護業務活動資訊，避免未經授權的存取與修改，確保其正確完整。

(三) 知悉資安事件發生，於規定時間完成通報、應變及復原作業。

三、 資通安全政策及目標之核定程序

由本機關資訊業務主責人員簽陳資通安全長核定。

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。

(二) 本機關應每年向利害關係人(例如駐點 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內部會議檢討其適切性。

伍、 資通安全推動組織

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，由本機關資通安全長擔任召集人，召集各業務部門代表成立資通安全推動小組，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，其任務包括：

(一) 跨部門資通安全事項權責分工之協調。

(二) 應採用之資通安全技術、方法及程序之協調研議。

(三) 整體資通安全措施之協調研議。

(四) 資通安全計畫之協調研議。

(五) 資通安全政策及目標之研議。

(六) 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。

(七) 傳達機關資通安全政策與目標。

(八) 資通安全相關規章與程序、制度之執行。

（九）資料及資通系統之安全防護事項之執行。

（十）資通安全事件之通報及應變機制之執行。

（十一）辦理資通安全內部稽核。

（十二）每年至少召開1次會議，提報資通安全事項執行情形。

（十三）配合執行資通安全稽核工作。

陸、 人力及經費配置

一、 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Ｄ級，設置資通安全專責人員1人(由正式人員兼任)，負責本機關之法遵義務、教育訓練及資通安全事件通報及應變等業務之推動，並將人員職掌填寫於「資通安全推動小組成員及分工表」，適時更新之。

（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）本機關業務主管人員，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。

（四）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）資通安全經費、資源之配置情形應每年定期檢討。

柒、 資通安全長之配置

依資安法第12條之規定，本機關由主任擔任資通安全長，負責督導、核定機關資通安全相關事項，其任務包括：

（一）資通安全管理政策及目標之核定、核轉及督導。

（二）資通安全責任之分配及協調。

（三）資通安全資源分配。

（四）資通安全防護措施之監督。

（五）資通安全事件之檢討及監督。

（六）資通安全相關規章與程序、制度文件核定。

（七）資通安全管理年度工作計畫之核定

（八）資通安全相關工作事項督導及績效管理。

（九）其他資通安全事項之核定。

捌、 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、支援服務資產等

（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、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. 支援服務資產：相關基礎設施及其他機關內部之支援服務，如電力、消防、網路等。

(三)本機關每年度應依資訊及資通系統盤點結果，製作「資訊資產清冊」，欄位應包含：資產名稱、廠牌名稱、型號、資產類別、管理者、存放位置、數量、安全等級。

（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、規格等資訊。

（五）管理之資訊或資通系統如有異動，應即時通知資通安全專責人員更新資產清冊。

二、 機關資通安全責任等級分級

本機關自行辦理資通業務，但未維運自行或委外開發之資通系統，為資通安全責任等級 D 級機關。

玖、 資通安全風險管理

一、 本機關應每年針對資訊及資通系統資產進行風險評估，評估結果填寫於「資訊資產清冊」。

二、 風險評估分級說明如下：

（一）參照「資通安全責任等級分級辦法」「附表九 資通系統防護需求分級原則」，分析「機密性、完整性、可用性、法律遵循性」4個構面，並依「低、中、高」3個安全等級，進行資訊資產安全等級分級。

（二）風險評估分佈：依前述4個構面中安全等級最高者，評定安全等級，風險定義如下：

1. 低風險：低。
2. 中風險：中。
3. 高風險：高。

三、 當資產風險為高風險時，應填寫「風險改善計畫表」並進行風險改善作業。

壹拾、 資通安全防護及控制措施

本機關依據自身資通安全責任等級 D 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. 本機關內部網路之區域應做合理之區隔，使用者應經授權後在授權範圍內存取網路資源。
2. 遵循上級機關規定，使用者應依規定方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

3. 無線網路防護

(1)機密資料不得透過無線網路及設備存取、處理或傳送。

(2)行動通訊或紅外線傳輸等無線設備不得攜入涉及或處理機密資料之區域。

(3)用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二)資通系統權限管理

1. 本機關之資通系統應設置通行碼(密碼)管理，通行碼之要求需滿足(適用ｅ化入口網規則)：

(1)通行碼長度12碼以上。

(2)通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3)使用者每180天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者ID，除有特殊營運或作業必要經核准並紀錄外，不得共用ID。

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ID，資通系統管理者應定期清查使用者之權限。

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，並適時進行軟、硬體之必要更新或升級。

2. 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

3. 使用者未經同意不得私自安裝應用軟體，管理者並應定期針對管理之設備進行軟體清查。

4. 使用者不得私自使用已知或有嫌疑惡意之網站。

5. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二) 電子郵件安全管理

1. 本機關人員到職後應經申請方可使用電子郵件帳號，並應於人員離職後停用該員電子郵件帳號。
2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
3. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。
4. 原則上不得以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。
5. 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。
6. 本機關應配合臺中市政府電子郵件社交工程演練，並檢討執行情形。
7. 遵循臺中市政府電子郵件使用管理要點。

(三) 確保實體與環境安全措施

1. 機密性及敏感性資訊，不使用或下班時應上鎖。
2. 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。
3. 資訊或資通系統相關設備，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、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。
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，並應保留傳送及簽收之記錄。
3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。
4. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

（五）電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過10分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循機關之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低敏感性資訊遭洩漏之機會。

（六）行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。
2. 機敏會議或場所不得攜帶未經許可之行動設備進入

壹拾壹、 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「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。

壹拾貳、 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。

壹拾參、 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

（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。

二、 監督受託者資通安全維護情形應注意事項

（一）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。

（二）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。

（三）受託者應採取之其他資通安全相關維護措施。

（四）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」。

（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，以稽核或其他他適當方式確認受託業務之執行情形。

壹拾肆、 資通安全教育訓練

一、 資通安全教育訓練要求

(一)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)資通安全專職人員以外之資訊人員：每人每二年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。

二、 資通安全教育訓練辦理方式

（一）每年參加中央機關、上級機關辦理之資通安全教育訓練或利用數位學習，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。

（二）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。

（三）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。

壹拾伍、 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」、「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。

壹拾陸、 資通安全維護計畫與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，相關單位於訂定資通安全文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及相關內容相符，並應保存相關執行成果。

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. 內部稽核：依據「資安項目自我檢核表」各檢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. 查核作業：本機關應配合上級或監督機關之規定辦理查核作業，以確認人員是否遵循本計畫與機關之管理程序要求，並有效實作及維持管理制度。

（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、改善進度規劃，並落實執行。

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應每年至少1次召開內部會議，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）持續改善機制應做成改善績效追蹤報告，相關紀錄並應予保

存，以作為審查執行之證據。

四、 資通安全維護計畫實施情形之提出

本局依據資安法第14條之規定，依主管機關規定期限向上級或監督機關，提出資通安全維護計畫實施情形[1]，使其瞭解本機關之年度資通安全計畫實施情形。

[1] 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。