宏仁醫院資通安全規範

民國 114 年 11 月 1 日修訂

一、 凡本院使用之資訊系統、電腦設備及相關周邊，凡具備與外部環境連結能力者，包括透過有線或無線方式連接其他設備、使用可攜式儲存媒體（如 USB、CD、DVD）或連線至網際網路，均屬本規範管理範圍，為降低資通安全事件發生風險，確保醫療服務及院內作業之安全與穩定，特訂定本規範。

二、 基本規範

（一） 資通系統防護需求分級原則

1. 本院於新建置、引進或進行重大調整之資通系統、資通訊設備或相關服務，應依《資通安全管理法》及「資通安全責任等級分級辦法」規定，由資訊室辦理資通系統防護需求等級評估，並填寫資通系統防護需求等級評估表（如附件一），作為資通安全管理與防護措施規劃之依據。
2. 經評估之資通系統，應依其防護需求等級，採行與風險程度相符之資通安全管理與防護措施，並得視本院實際營運需求及資源狀況，分階段執行；相關防護基準得於本院資通安全制度成熟後，另行訂定或補充。

（二） 名詞定義

本規範所稱資通訊產品，參考《資通安全管理法》第三條用詞定義，說明如下：

1. 軟體：指資通訊系統相關軟體，如應用軟體、系統軟體、開發工具、客製化或套裝軟體、行動應用程式（APP）及電腦作業系統等。
2. 硬體：指具備連網能力、資料處理或控制功能之資通訊設備，包括個人電腦、伺服器、印表機、網路通訊設備、可攜式設備及物聯網設備等。
3. 服務：指資通服務，如系統維運、客服支援及軟硬體資產維護等相關服務。

（三） 資通訊產品範圍與責任確認

各單位於引進或使用資通訊產品前，應先確認該項業務內容是否涉及硬體/韌體、作業系統、應用服務、應用軟體或系統及網路連線等範圍，並釐清相關管理與維運責任後，依本規範辦理。

（四） 採購與廠商資安要求

1. 廠商接獲本院採購中心詢價或招標邀請時，應遵循本資通安全規範，並依案件性質提供相關資安證明文件及委外廠商資安承諾暨保密切結書（如附件），併同報價文件提供採購中心承辦人員。
2. 經評估屬具網路連線或資安風險之案件，得要求報價或得標廠商提供近三個月內之弱點掃描檢測報告且須蓋公司章以茲證明，並確認完成中風險以上弱點之修補；若提供有效期間內之資安認證或標章證明文件者，得視同符合前述要求。

（五） 資通安全維運與監控原則

具網路連線之資通系統，應依其重要性及風險程度，採取適當之安全管理措施，包括帳號存取控管、防止未授權存取及異常行為之基本防護作為，並持續進行安全監控、定期檢測網路運作環境之安全漏洞予以修補，並設有專員定期檢視及進行安全管理。

（六） 大陸廠牌資通訊產品管理原則

1. 本院公務用之資通訊產品不得使用大陸廠牌，且不得安裝與公務無關之軟體。
2. 已使用或既有之大陸廠牌資通訊產品，應由資訊室統籌列冊管理，並規劃汰換時程；於汰換前，不得與院內網路介接。
3. 大陸廠牌之認定，由資安管理單位依「從嚴認定」原則辦理，凡屬大陸廠牌者，無論其原產地為我國、大陸地區或第三地區，均應納入盤點範圍。
4. 盤點範圍應涵蓋本院、委外廠商及其分包廠商。
5. 因業務需要於汰換前須與院內環境介接者，應向資安管理單位提報相關配套措施；如短期內無法完成汰換，應說明原因及汰換前之風險控管作為。

三、 硬體/韌體（Hardware/Firmware）

（一）對具網路連線或具資安風險之硬體與韌體設備，應留意其已知安全漏洞，並於可行範圍內依原廠建議進行更新或修補。

（二）原則上應停用非業務所需之 USB、CD/DVD、有線或無線網路、藍牙、紅外線及其他資料傳輸介面（如：RS-232、RS-485 等）；如因業務需求須啟用者，應採取適當之管理或控管措施。

四、 作業系統（OS，Operating System）

（一）具備稽核或紀錄功能之資通系統，應視其重要性留存必要之操作或事件紀錄，以利資安事件發生時之追蹤與查證。

（二）前述紀錄內容原則上應包含使用者識別、事件時間、系統或設備識別資訊及事件簡要說明。

（三）資通系統之使用者帳號，應定期進行清查，原則上至少每半年辦理一次。

（四）系統時間應與院內標準時間來源進行校正，以確保相關紀錄時戳之一致性。

（五）作業系統應實施基本身分驗證管理措施，包括但不限於：

1. 使用預設密碼登入者，應於首次登入後變更密碼
2. 身分驗證資訊避免以明碼方式傳輸
3. 具備登入失敗次數限制或延遲機制
4. 訂定基本密碼複雜度與效期原則
5. 避免使用者重複使用近期已使用之密碼

五、 應用軟體/系統（Application Software/System）

（一）應建立帳號管理機制，包含帳號申請、啟用、異動及停用等基本程序。

（二）系統應具備自動登出或閒置中斷機制，以降低未授權使用風險。

（三）系統應限制登入失敗三次，採取中斷連線之措施。
（四）對於異常登入或操作行為，系統應視功能可行性留存相關紀錄。
（五）系統得提供登入歷史資訊或異常提示機制，以協助使用者辨識可能之帳號風險。
（六）對於涉及機密性或敏感性資料之系統，於資料傳輸或儲存時，應視實際情況採取適當之加密或防護機制（如：以 SSL 加密）。
（七）新建置或重大調整之應用系統，於正式上線前須提供源碼掃描檢測合規報告，資料庫則須提供 SQL 隱碼檢測合規報告，若有對外網開放則須提供滲透攻擊測試報告，作為資安評估之參考。

六、 配合事項
（一）廠商於執行定期維護作業時，應依合約約定或系統性質，提供相應之維護報告，其內容原則上得包含主機安全性更新（如：Windows Update）、系統運作狀況（如：主機硬碟剩餘容量、CPU 效能、記憶體紀錄、伺服器相關紀錄等）及防毒軟體掃描等相關作業說明。
（二）廠商應配合本院依實際需求辦理之弱點掃描與改善措施，並針對資通安全或弱點掃描稽核所提建議事項，於合理期限內完成修補，或提出具體改善方案供本院確認。
（三）廠商應配合本院辦理之資安或相關稽核作業，包含但不限於資料安全控管、系統維護管理及備援或緊急應變相關措施之查核。
（四）本院得依實際需要，定期或不定期派員檢查或稽核廠商提供之服務是否符合契約及本規範之約定；廠商應於合理時間內提供必要之書面資料或配合訪談，其範圍以法令或契約約定事項為限。
（五）經本院查核或稽核結果確認不符合契約或本規範者，廠商應於本院通知之期限內完成改善或提出改善計畫。

七、 委外廠商管理原則
（一）本院委外辦理資通系統建置、維運或資通服務時，應依《資通安全管理法》及相關法規規定，於選任及監督受託者時，將資通安全要求納入評估與管理。
（二）受託者應具備與其受託業務相符之資通安全管理能力，並配置具備相關訓練或經驗之人員，負責執行受託業務之資通安全相關事項。
（三）受託業務如涉及複委託，應於契約中明訂其範圍、對象及資通安全管理要求，並確保分包或轉包廠商同樣遵循本院資通安全規範。
（四）受託業務涉及客製化資通系統開發或具高度資安風險者，得依案件性質要求受託者提供相關安全性檢測或測試資料，作為資安評估之參考。
（五）受託者於執行受託業務期間，如發現或知悉資通安全事件，應即時通知本院，並配合採行必要之補救或因應措施。
（六）委託關係終止或解除時，應依契約約定，確認受託者返還、移交、刪除或銷毀因履行契約而持有之本院資料。

（七）受託者應配合本院資通安全管理要求，採取必要之其他資安維護措施，包括但不限於專案管理人員指派、使用設備之基本安全控管及不得使用大陸廠牌資通訊產品等事項。

八、 業務主辦單位：資安中心。