惠來醫療社團法人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（詳如附件一），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（詳如附件二），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：資通安全小組。

附件一

民國 114 年 11 月 1 日修訂

惠來醫療社團法人宏仁醫院資通安全防護評量表

本評量表用於協助承辦單位於採購、委外或技術導入前，初步辨識資通安全風險，作為後續資安審查、契約安全要求及管理強度之參考，填寫完成後送交專責單位審核。

一、 案件基本資訊

案件名稱		**評 量 日 期**	
申請單位		**申請人員姓名**	
廠商名稱		**申請人員員編**	
採購/委外類型	☐ 系統 ☐ 設備 ☐ 軟體 ☐ 服務	**申請人員分機**	

二、 標的物屬性與風險初評

1. 本案是否涉及資通訊相關項目，如：資訊系統、軟體、連網設備、維運服務、雲端服務等，詳附件說明 1
   （符合任一項目即屬**是**）
   ☐ 是 ☐ 否
2. 是否涉及中國（大陸）之資通產品，詳附件說明 2
   ☐ 是：品牌：_____ 型號：
   ☐ 否
3. 是否需連接院內網路（有線或無線）或對外網路
   ☐ 是 ☐ 否

三、 資料與系統影響評估

4. 系統或服務中斷是否可能影響院內關鍵業務或核心作業，如：門診、急診、住院、加護病房、檢驗檢查等
   ☐ 是 ☐ 否，防護等級低
5. 承上題，若發生中斷或異常，其影響程度為
   ☐ 嚴重影響醫療服務或營運，防護等級高
   ☐ 輕微影響或不影響
6. 是否涉及病人、員工或其他個人資料
   ☐ 可能性高或有使用，防護等級高 ☐ 可能性低或無使用
7. 是否涉及病人、員工或其他個人資料
   ☐ 可能性高或有使用，防護等級高 ☐ 可能性低或無使用
8. 是否會寫入病歷資料？
   ☐ 可能性高或有使用，防護等級高
   ☐ 可能性低或無使用，防護等級中

四、 資通訊設備資安自檢項，請勾選

9. ☐ Windows 系統須完成下表自檢項目並提供各項截圖畫面佐證

自檢項目	完成狀態
1. 安裝合規防毒軟體	☐是 ☐否
2. 完成 Windows Update 更新	☐是 ☐否

3. 網卡防火牆有開啟	□是 □否
4. 合乎本院對時機制	□是 □否

10. □非 WINDOWS 系統須提供弱點掃描報告，僅接受 LOW 及 INFO 等級。

審核報告：

專責單位（資訊室）

資安規範：□ 符合 □ 不符合 □ 不需會簽資安中心

資訊安全防護等級：□ 高 □ 中 □ 低

說明：

資安人員

審核結果：□ 通過 □ 不通過

說明：

附件說明

1. 名詞定義說明

本評量表所稱之資通訊相關項目，係參考《資通安全管理法》第三條之用詞定義，說明如下

1.1 軟體：

指各類資通訊系統（含套裝軟體）、應用軟體、行動應用程式（APP）、系統軟體、作業系統、開發工具及相關程式元件等。

1.2 硬體：

指具備連線能力、資料處理或控制功能之資通訊設備，包含但不限於個人電腦、伺服器、網路設備、印表機、儲存設備、可攜式裝置、物聯網設備及其他相關終端設備。

1.3 服務：

指提供資通訊相關之服務行為，例如系統維運、技術支援、駐點服務、雲端服務、資料處理或其他與軟硬體相關之服務。

2. 使用中國大陸品牌資通訊產品之管理原則

為降低資通安全風險，本院對於涉及中國大陸品牌之資通訊產品，訂定下列管理原則

2.1 公務或院務使用之資通訊產品，原則上不得採用中國大陸品牌，亦不得安裝或使用非核准之軟體。

2.2 已使用或已採購之中國大陸品牌資通訊產品，應納入管理清冊並訂定汰換或改善時程；於完成汰換或風險控管前，不得與本院正式網路或核心系統介接。

2.3 所稱「中國大陸品牌」，係由本院依管理需要採取從嚴認定原則，不論其產品產地位於我國、大陸地區或第三地區，凡具中國大陸品牌背景者，均應納入評估與填報範圍。

2.4 盤點及評估範圍包含本院各單位、委外廠商及分包廠商所使用，且可能連接或影響本院資訊環境之資通訊產品與服務。

2.5 如相關產品於汰換前須暫時與本院環境介接，應事前向資訊單位或資安承辦人員說明汰換時程、暫行配套措施及風險控管作法；如短期內確實無法完成汰換，應說明原因並提出替代性安全控管措施，供後續審查與裁示。

附件二

民國 114 年 11 月 1 日修訂

委外廠商資通安全承諾暨保密切結書

具切結廠商＿＿＿＿＿＿＿＿＿＿＿＿（公司名稱）及其指派執行人員＿＿＿＿＿（姓名），於 □ 投標 □ 執行，執行日期起訖：＿＿年＿＿月＿＿日 至＿＿年＿＿月＿＿日，於**惠來醫療社團法人宏仁醫院**（以下簡稱本院）之 ＿＿＿＿＿＿＿＿＿＿＿＿（案件/專案名稱）期間，因執行受託業務而取得或知悉之各項資訊（包含但不限於技術性、業務性或其他未公開資訊），除依法公開者外，均負保密義務，非經法令規定或本院事前書面同意，不得向任何第三人揭露或提供。廠商及其人員已知悉並同意遵循本院資通安全政策及相關規範，並確實配合執行；如因故意或過失違反，致本院權益受損，願依法及依契約約定負相關責任，特此切結。

立切結書人（廠商）：　　**立切結書人（廠商執行人員）：**

廠商名稱：　　姓　　名：＿＿＿＿＿（親簽）

統一編號：　　身分證字號：

聯絡電話：

（本人已瞭解並同意個人資料之蒐集、處理及利用）

中　華　民　國　　年　　月　　日

惠來醫療社團法人宏仁個人資料蒐集同意書

本院為蒐集、處理及利用個人資料，依《個人資料保護法》及相關法令規定，特以本聲明及同意書向您為書面告知，並徵求您的同意。***當您於主表單簽名處簽署本同意書時，即表示您已閱讀、瞭解並同意接受本同意書所載之一切內容。***

一、 基本資料之蒐集、處理及利用

（一） 本院依據中華民國《個人資料保護法》及相關法令規定，蒐集、處理及利用您的個人資料。

（二） 蒐集之個人資料，係為完成業務所必須之個人資料。

（三） 本院因執行業務所蒐集之個人資料，包含姓名、身分證統字號、聯絡電話及其他得以直接或間接識別個人身分之資料。

（四） 若您所提供之個人資料有任何異動，請主動向本院申請更正，以確保資料之正確性。

（五） 若您拒絕提供、不實提供或未完整提供個人資料，可能影響本院業務之執行或相關權益。

（六） 您得依《個人資料保護法》就您的個人資料行使以下權利：

1. 查詢或請求閱覽
2. 請求製給複製本
3. 請求補充或更正
4. 請求停止蒐集、處理或利用
5. 請求刪除

二、 蒐集個人資料之目的

（一） 本院蒐集、處理及利用您的個人資料，係基於業務管理、委外作業管理、資訊安全與相關行政作業之特定目的。

（二） 蒐集之個人資料，將於前述目的範圍內使用；如有其他利用目的，將依法另行取得您的同意。

（三） 自即日起至本院業務存續期間，或依法令規定之保存期間內利用。

三、 個人資料之保護

本院依《個人資料保護法》規定，採取合理且適當之安全維護措施，防止個人資料遭竊取、洩漏、竄改、毀損、滅失或其他不當利用。

惟如因天災、事變或其他不可抗力，或非可歸責於本院之事由，致您的個人資料發生竊取、洩漏、竄改或其他侵害情形時，本院將於查明相關情事後，依實際狀況以電話、信函、電子郵件或網站公告等方式，擇適當方法通知您。

四、 同意事項

（一） 您已充分瞭解並同意本院依本同意書所載內容，蒐集、處理及利用您的個人資料。

（二） 本院如因業務需要修訂本同意書內容，將依法於本院官方平台或網站公告修訂之事實，則不另行個別通知，修訂後內容自公告日起生效。如您於知悉修訂內容後，不同意前述增訂或修改事項，得依本同意書第一條第六款規定，向本院主張停止蒐集、處理或利用您的個人資料；未依前述方式主張停止蒐集、處理或利用，且仍持續與本院進行業務往來者，視為您已同意並接受本同意書修訂後內容之拘束。

五、 準據法與管轄

本同意書之解釋與適用，悉依中華民國法律為準據法；因本同意書所生之爭議，以臺灣彰化地方法院為第一審管轄法院。