國立臺北護理健康大學

資通系統採購建議納入資安要求事項

（115.7.30 修正）

（一）專案團隊成員限制與設備管制

1. 廠商執行團隊成員不得為陸籍人士。
2. 全面禁止採購與使用大陸廠牌之資通訊產品。
3. 廠商之個人資通訊設備（含智慧型手機、平板、筆電等）不得處理本校之公務事務，亦不得與本校之公務網路及系統環境介接。

（二）系統分級與安全開發規範

1. 本系統之資通系統防護需求分級為 □普□中□高 級，服務期內廠商應協助執行 □普□中□高 級資通系統防護相對應之防護措施，並配合填寫「資通系統防護基準控制措施檢核表」。
2. 本專案若涉及系統建置或開發，其發展生命週期各階段均需將機密性、可用性、完整性等安全需求納入，並確實依本校規定填寫「應用系統 SSDLC 檢核表」進行確認。若涉及雲端服務之採購或使用，應配合進行「雲端服務資通安全措施評估表」之檢核。

（三）個人資料保護與合約終止資料處置

1. 得標廠商執行本契約若涉及蒐集、處理或利用本校個人資料，應確實遵守《個人資料保護法》及《個人資料保護法施行細則》之規定，且配合本校個人資料管理制度運作；若有違反情事發生致本校受有損害，廠商應無條件負損害賠償之責。
2. 本契約關係終止或解除時，得標廠商應確實將履行本契約而持有之本校資料（含備份）予以返還、移交、刪除或銷毀。執行資訊刪除時，應確實留存紀錄以備查核。

（四）系統上線與安全性檢測

1. 得標廠商於系統上線前，應通過資訊安全檢測（如弱點掃描），並繳交弱點掃描檢測報告，不得有嚴重、高以上之風險存在，以降低遭受駭客攻擊之風險。若涉及客製化資通系統開發者，廠商於驗收時應交付包含原始碼檢測（源碼檢測）、滲透測試等證明文件（如「系統安全性檢測證明」），以確認系統之安全；涉及利用非自行開發之系統或資源者，廠商應標示其內容來源並提供授權證明

2. 系統之密碼管理應符合安全性規範（如：首次登入強制變更密碼、密碼複雜度要求等），嚴禁使用不安全之設計技術（如硬編碼/Hard-coding 通行碼）。

（五）廠商自我檢核

得標廠商應填寫「國立臺北護理健康大學委外廠商資通安全檢核表」並提供相關佐證資料，完成自我檢核。

（六）稽核與監督

1. 本校保有對廠商稽核之權利，得於定期或知悉廠商發生可能影響受託業務之資通安全事件時，對專案相關工作之執行、資料處理及執行紀錄進行實地現場訪視或調閱資料。此外，有權對廠商使用之工具軟體及處理作業之執行紀錄進行稽核，廠商應留存異常處理紀錄，以供本校隨時查核。
2. 廠商應配合本校（或資安法主管機關籌組之專案團隊）進行稽核作業；若稽核發現缺失，須於接獲本校通知後限期改善。

（七）廠商得標後簽署文件

1. 得標廠商應簽署「承包廠商保密同意書」，廠商相關人員應簽署「承包廠商員工保密同意書」，克盡保密之責。
2. 得標廠商應簽署「資通系統開放維運委外之資通安全條款」(委外開發系統用)、「資通服務委外之資通安全條款」。

（八）資通安全事件通報與應變

得標廠商執行受託業務時，若違反資通安全相關法令或知悉資通安全事件（包含系統異常狀況）時，應立即通報本校，並採取必要之損害控制與復原等補救措施。

（九）人員離職與異動規範

得標廠商相關系統之開發或負責人員離職、調職或職務異動時，廠商應確實收回其作業權限。