馬偕紀念醫院特權管理要求

1. 特權管理系統主要項目需包含：
   (1).特權帳號密碼管理：
      A. 密碼集中管理。
      B. 自動變更密碼。
      C. 密碼不落地。
   (2).特權帳號申請簽核
      A. 代登入系統。
      B. 流程管理：使用者提出申請、多層級核准、指定使用時間、Just-In-Time Access。
      C. 支援共享帳號管理。
      D. 整合 Teams 或 Line 簽核(手機簽核)。
   (3).特權連線側錄與監控：
      A. 不需安裝 Agent。
      B. 全程錄影側錄。
      C. OCR 全文搜尋。
   (4).特權行為分析與風險偵測：
      A. 即時阻斷危險操作。
      B. 使用者異常行為分析。
      C. 滿足稽核需求。
      D. 稽核追蹤，包含：時間戳記、數位簽章、防竄改紀錄。
   (5).提供 Restful API，與本院內部流程簽核系統整合。
2. 主機與系統需求規範：
   (1).特權管理系統軟體程式需能符合 ISO27001 資安需求與提出弱點掃描證明。
   (2).主機作業系統需提供最新版本或近 3 年內無 EOSL（End of Service Life）之作業系統，並已完成中、高漏洞修補。
   (3).特權管理系統所需主機資源超過本院能提供虛擬機標準規範（需事先與本院訪談），得標廠商得另外提供實體主機（相關主機規範需配合本院）。
3. 特權管理數量：需提供至少 300 台伺服器管理授權，可連線使用者與管理數量不限。
4. 維護起迄時間：2027 年 01 月 01 日至 2028 年 12 月 31 日止。
5. 服務等級（SLA）：維護期間除維護廠商 5*8 軟體及系統叫修及技術支援服務外，並含免費保固及升級服務，以維持系統正常運作。
6. 特權管理功能需求規範：
   (1). 無代理式（Agentless）程式或需代理程式皆可，建議以無代理式（Agentless）程式架構為佳。
   (2). 管理介面：Admin 管理介面及 User Access Gateway（UAG）使用者入口，分離管理與連線操作，建議以網頁由佳。

(3). 使用者認證：可建立本機使用者，使用密碼、公鑰或憑證等方式登入，也能可整合 Active Directory／LDAP，作為外部認證及使用者同步來源。

(4). 多因素認證：支援 OATH TOTP／HOTP、DUO、SMS、RADIUS、Google Authenticator 等認證方式，建議以本院的微軟 Authenticator 為佳。

(5). 需具備遠端連線代登入功能，讓維運人員或外部廠商能夠順利登入目標設備進行操作，但完全「不揭露」目標主機的實際帳號與密碼/金鑰。

(6). 登入失敗鎖定：可設定登入失敗次數門檻，達到門檻後自動封鎖指定使用者。

(7). 角色權限管理：可建立自訂角色，控制使用者可查看及操作的管理功能。

(8). 特權帳號連線申請：

A. 使用者可申請立即或排程按照所需時間連線使用，而特權管理簽核者可核准、拒絕，並可查詢相關申請歷程。

B. 特權帳號連線申請：可設定一人或多人核准，並支援以 E-Mail 通知或 Line 等。

C. 可支援連線行為分析，如 SSH、RDP 使用行為並顯示威脅程度，協助辨識異常使用。

(9). 特權帳號申請需能提供簽核頁面與流程，並能與本院公文簽核系統（OA）或 VPN 流程透過 API 介接由佳。

(10). 連線協定與使用方式：

A. 連線方式應為 Web Client（使用者可透過瀏覽器啟動 SSH、RDP 等連線，不需安裝專用 Client）或下載安裝 Native Client，使用 mstsc、PuTTY、OpenSSH、WinSCP、SSMS 等既有工具連線，或 2 者皆可為最佳。

B. 支援 SSH Shell、SFTP、SCP、Port Redirection、X11 及常見 Native Client。

C. 支援 RDP、NLA、TLS、RemoteApp、多螢幕、Web Client 及 Native Client。

D. 支援 Rendered 與 Non-rendered HTTP／HTTPS；Rendered 模式可錄影與 OCR。

E. 其他支援連線模式視為本案最佳選擇。

(11). 連線錄影、監控與稽核：

A. 提供連線時全程錄製，並記錄畫面、鍵盤、滑鼠、指令、來源 IP、User、Server、Account、Safe 及 Listener 等資訊。

B. 管理者可即時觀看正在進行的連線。

C. 管理者可加入使用者的連線畫面，進行協同處理或遠端支援，可產生分享連結，提供唯讀或可互動的協作方式，同時管理者可 Pause、Resume 或 Terminate Session，並留下事件紀錄。

D. 連線錄影觀看可播放、暫停、快轉、拖曳時間軸、略過 Idle 及查看使用者動作，以及提供搜尋與篩選，以及 OCR 與全文搜尋，並可將錄影檔案下載，轉換為支援格式如 MP4 或 AVI 等格式離線觀看。

(12). 帳號與密碼管理：

A. 保存或取得目標帳密並由特權帳號系統進行代登入，使用者不需知道實際密碼，以增加安全度。

B. 密碼變更政策：可設定密碼複雜度、變更頻率及 Session 結束後變更等條件，並可設定密碼複雜度、變更頻率及 Session 結束後變更等條件

(13). 連線行為分析與報告：

A. 支援預設報表、隨選報表及週期報表，可依條件產生與下載。

B. 可分析使用者連線活動時間、閒置時間、Session 活動比例及比較結果，並可產出報表（如週報、月報等），分析結果可產生 HTML、CSV 或 PDF 報表。

C. 特權管理系統支援可將 Event Log 傳送至外部 Syslog 或 SIEM 平台。

D. 特權管理系統支援透過 SMTP E-Mail 發送報表與訊息通知。

(14). 其它：

A. 提供 API 管理 User、Server、Account、Safe、Listener、Session、Request、Report 等物件。

B. 支援連線外部備份、設定匯出及必要時的資料還原。

C. 可設定連線資料保存期限及重要連線的保留鎖定。

D. 可支援配置外部 NAS 儲存，擴充連線錄影資料保存空間。

E. 所提供特權管理系統本身支援 Upgrade、Hotfix、Diagnostics、Health Check、Call Home 及系統狀態檢查。