「特權帳號安控稽核系統」
建置計畫案

徵求建議書說明文件

案件編號：A115-000154

馬偕紀念醫院 資訊室 臺北系統維護課 編撰

2026 年 02 月 25 日

目　　錄

一、簡介

1.1 徵求建議書說明文件背景

馬偕紀念醫院本院(以下簡稱本院)為提昇應用系統運用效能，提升資訊防護安全性及可靠性，擬建置「**特權帳號安控稽核系統建置計畫案**」，以期達整體資訊系統運作順暢，穩定及安全之目標。

依本院資訊系統採購程序規定得公開徵詢廠商建議書，做為本案執行評估程序之參考，為使投標廠商瞭解本案需求，故製作本「徵求建議書說明文件」。

1.2 徵求建議書說明文件目的

本徵求建議書說明文件之目的，係向廠商說明本院即將採購「**特權帳號安控稽核系統建置計畫案**」之需求與期望，俾供廠商據以提出符合本案需求之建議書。

本院配合主管機關—衛服部稽核要求，並有效控管本院資訊系統管理人員與廠商存取主機系統、各業務所需共用帳戶、資料庫、虛擬化平台、網路與資安設備等作業，擬建置集中式單一入口特權帳號安控稽核系統，強化資訊安全並落實本院資訊安全管理制度，敬邀有意願之廠商依此需求規格說明提出符合本院需求之解決方案。

本徵求建議書說明文件之目的，係向廠商說明本院即將建置「特權帳號安控稽核系統」之需求與期望，俾供廠商據以提出符合本案需求之建議書。

1.3 徵求建議書說明文件範圍

本徵求建議書說明文件範圍，主要規定投標廠商針對本案所提出之建議書應包含的內容，包括：專案概述、專案需求建議、成本分析、專案計畫執行能力、廠商信譽等。

針對本案“資訊系統/設備 詢價品項規格表”，需要提出達規說明書(若有需要需檢附證明，所送達標書內容或品項規格不符、不實等情況若發生，將不予與驗收)，並在徵求建議書的最後一頁提供本案報價單。

二、專案概述

2.1 專案承辦單位

本專案主辦單位為臺北系統維護課。

2.2 專案名稱

本專案名稱為「**特權帳號安控稽核系統**」建置計畫。

2.3 專案目標

(1). 落實本院管理規範並符合主管機關—衛服部稽核規範要求。

(2). 依據衛服部頒布「醫院面對勒索軟體攻擊的應變指南」規範要求，系統所自動產出之亂數密碼必須符合加強密碼原則(至少 8 碼以上、包括英數大小寫及特殊符號)，並具備自動機制檢查高權限帳號是否有異常活動。

(3). 針對各業務所需共用網域帳戶必須在不影響現行醫護人員使用方式的前提下，實現定期**自動/手動/自定義**變更密碼內容。

(4). 本專案之特權帳號管理系統必須施以定期自動檢查密碼內容是否正確之機制，避免密碼遺失或擅自變更。

(5). 透過特權帳號管理避免特權密碼使用揭露風險，並結合「代登入」機制，防範內部威脅及外部攻擊，有效保護主機系統、資料庫、虛擬化平台、網路與資安設備等。

(6). 留存特權帳號操作使用之軌跡紀錄至少乙年，並整合申請覆核機制，有效控管並清楚勾稽識別真實人員身分、回溯歷程紀錄、追究資安根因。

2.4 專案範圍

有關本專案系統之範圍與工作項目如下：

(1)安裝與建置：

A. 依照本院「 特權帳號安控稽核系統」建置案主要應用目標進行規畫建構。

B. 本案採購相關系統之安裝。

C. 與現有系統/網域整合與連接。

D. 相關教育訓練。

(2)軟體系統保固：

參與投標廠商須具備原廠授權證明書,以利提供合約保固期內軟體系統之完善售後服務，自驗收日起提供 1 年原廠免費軟體升級及 7*24 原廠技術支援服務，以維持系統正常運作。

2.5 專案時程規劃

本專案時程分為兩階段，第一階段為徵求建議書階段，合乎本院需求意向者進行議價；第二階段為系統建置階段。得標廠商自簽訂合約後依相關時程規定辦理並完成所有工作。廠商須於建議書中提出以簽約後開始並於三個月內完成建置之時程建議。

相關時程本院初步規劃如下：

(1) 徵求本專案建置建議書，廠商於接獲邀請後請於二週內完成建議書投遞。

(2) 合格投標廠商於本院指定之日期時間參加密封報價及議價。

(3) 於議價後第四週內進行合約簽訂工作。

(4) 自簽訂合約起第二週內廠商提交專案執行計劃書(需含交貨，建置、驗收與教育訓練等時程以及其他未盡事項)。

(5) 自簽訂合約起第四週內與專案負責人開會協調，由雙方確認及協調各項工作時程以確保可以順利執行。

(6) 自簽訂合約起第六週內貨品交付。

(7) 自簽訂合約起第八週內完成軟硬體安裝與建置。

(8) 自簽訂合約起第十二週內完成各項功能測試與驗收。

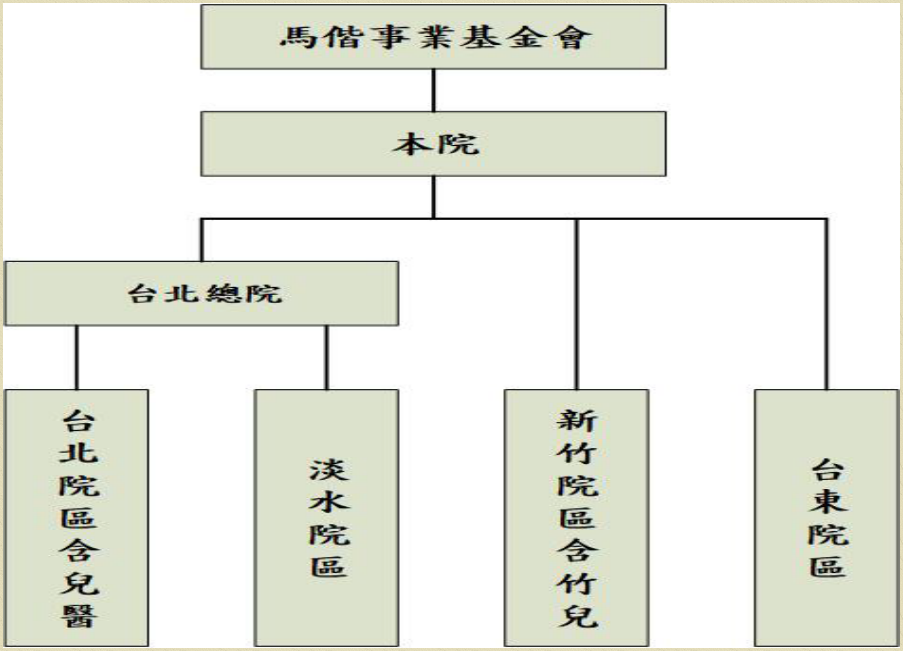
(9) 完成驗收第二週內廠商提交保固期執行計劃書。

☛以上專案時程規劃為本院基本需求，投標廠商若有時程出入應提出說明。
☛本專案自驗收作業完成後，廠商提供白金級保固及相關諮詢服務。

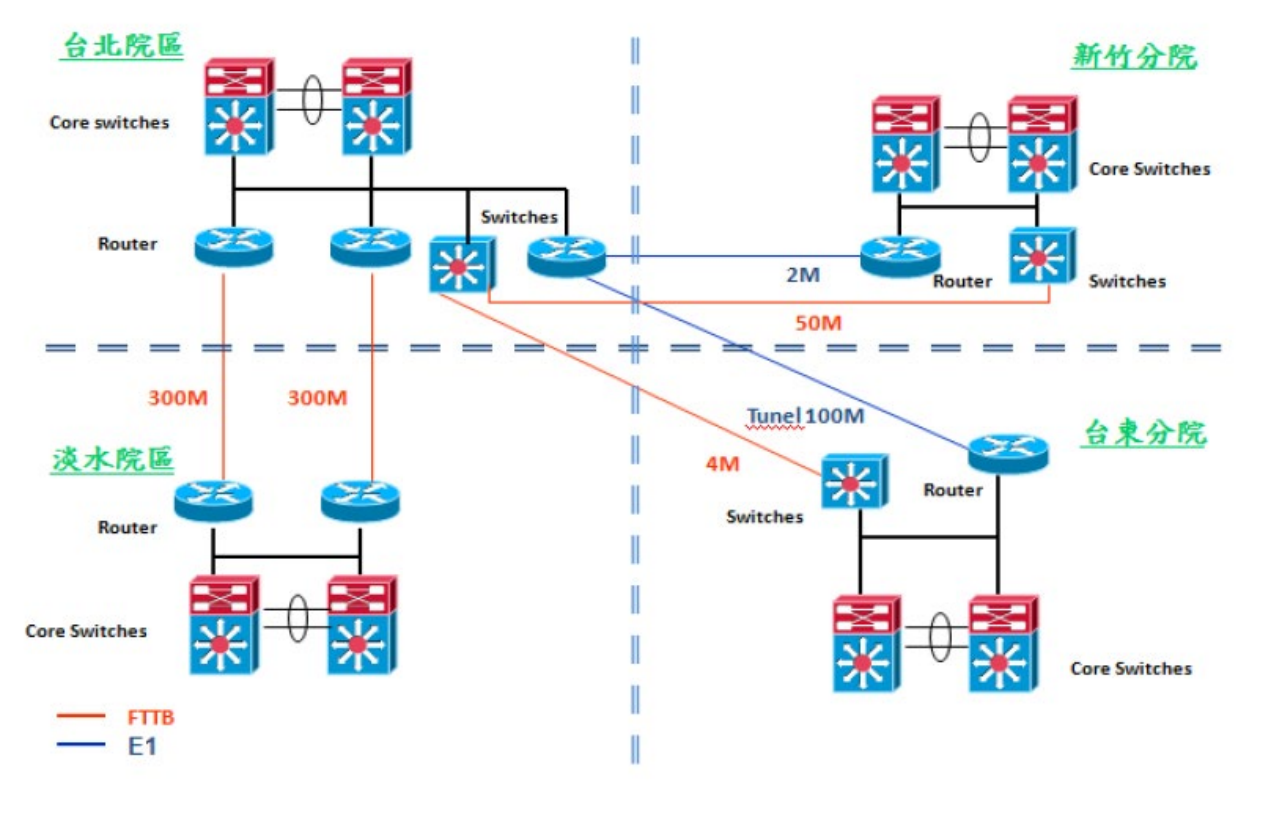
三、作業環境說明

3.1 馬偕醫院體系

本院組織架構圖如下，本案應用於臺北院區。



3.2 現行系統概況

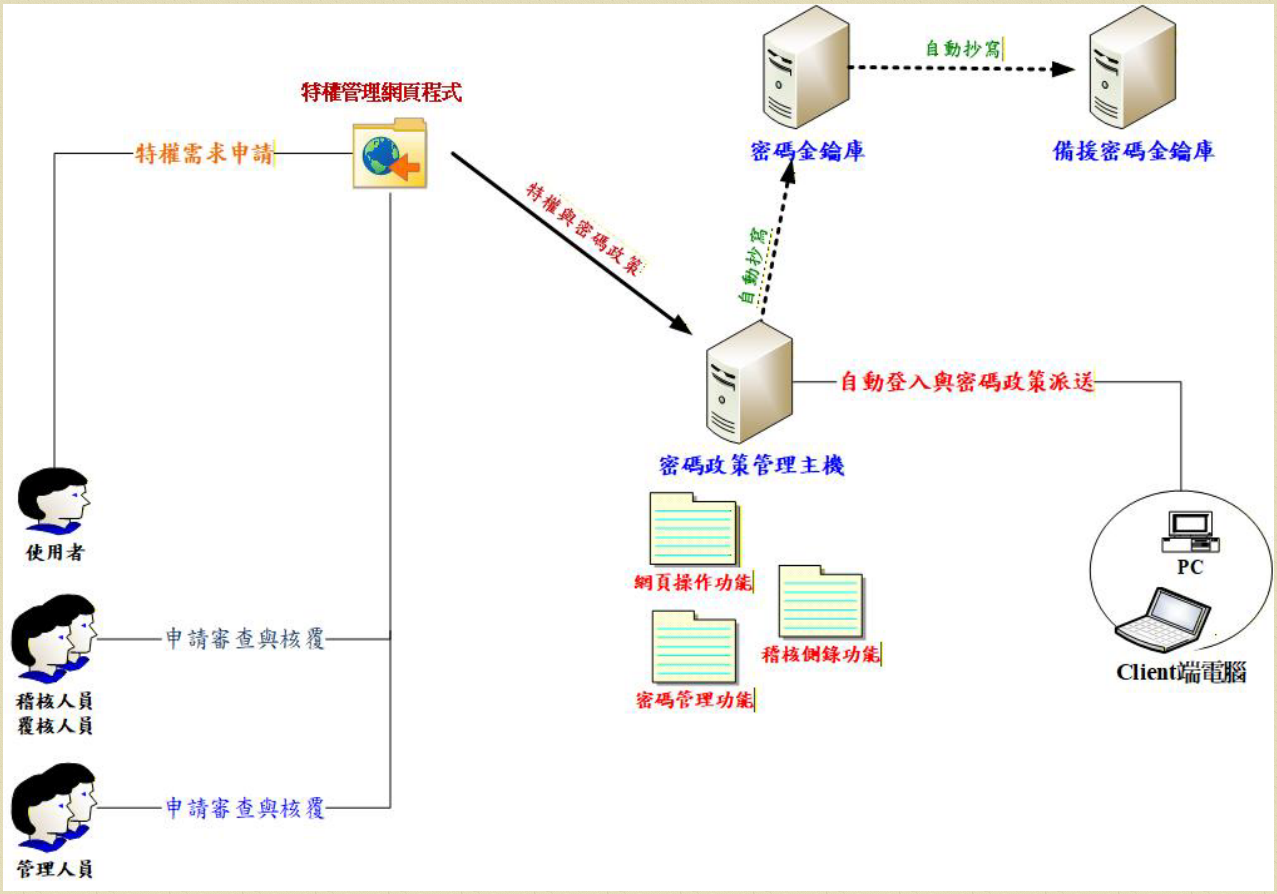


現行系統相關網路環境示意圖如下：

1. 業務 Server：Oracle ExaData。
2. 網管 Server：Windows Server 2008/2012/2016/2019/2022。
3. 虛擬 Server：VMWare vSphere ESXi。
4. 資料庫引擎：ORACLE 11g。
5. 使用者端 OS：Windows 7/8/10/11 等。
6. 開發語言：Microsoft dotNET 等。
7. 網路通訊模式：TCP/IP 1,000/10,000 Mbp。

3.3 預期完成目標的架構

預期完成的系統架構如下圖：



3.4 系統建置原則及技術

(1). 參與本案廠商需有建置相關環境架構的經驗及技術人員，同時必須具備有規劃相關專業人員及維護支援技術團隊，也必須與本專案中提供參與上述需求的企業經驗案例。

(2). 本案由得標廠商負責協助建置特權帳號安控稽核系統環境架構，並包含現有環境架構的融入，能確保資料保存完整及備援的可用性。

(3). 本案系統提供全域政策，統一定義密碼檢查與變更週期，亦可依受管理主機系統設定例外政策。

(4). 提供管理人員連線登入特權帳號安控稽核系統授權並內含多重要素驗證(MFA)機制。

(5). 須提供提供完整使用者操作與密碼使用等稽核紀錄功能，並可直接登入 Web 圖形化(GUI)介面進行查詢。

(6). 系統架構具備中央儲存伺服器，所有存放在系統中的檔案為加密檔案，並符合 FIPS 140-2 安全需求規範。

(7). 系統架構具備災難復原 DR(Disaster Recovery)機制，(本案至多提供 4 個 DR 金庫)可於中央儲存伺服器停止運作時自動連線至備援系統，不會影響日常運作。

(8). 提供相關系統技術教育訓練。

(9). 本案與其它系統連結部分，得標廠商需提供相關技術協助及諮詢服務。

(10). 本案所需項目、程式、元件等皆安裝於本院，所需主機部分由院方提供。

四、需求說明

4.1 整體性需求

- 功能性需求
  1. 本專案之系統功能及內容，需進一步與本院主辦單位進行需求訪談及確認。
  2. 本專案系統之使用者介面設計應具親和力與未來之擴充性。
- 安全規範需求
  1. 應用業務之權限控管管理需與本院權限控管整合。
  2. 應能防止非系統允許之合法授權人進入系統內存取資料，能識別使用者身份並決定使用者對資料及系統之使用權限。
  3. 承包廠商對業務上所接觸之本院電腦資料，應視同機密文件採必要之保密措施，任何因承包廠商人員洩密所致之賠償及刑事責任，概由承包廠商負責，並列入本院拒絕往來戶。
  4. 需訂定故障排除程序及完善備援機制，便於復原及緊急處置。
- 專案管理需求
  1. 專案開發期本院得視需要召開開發會議，承包廠商需派專案經理率技術人員前來參加並做報告。
  2. 專案管理應進行整體測試、壓力測試，以達成完善的軟硬體測試及驗證程序，來確保本專案之品質。
  3. 專案完成後本院得視需要召開維護會議，承包廠商派需專案經理率技術人員前來參加並做報告。
- 教育訓練需求
  1. 提供系統操作及使用訓練。
  2. 提供教材或講義。
  3. 訓練梯次及時間由雙方協調訂定。
- 驗收管理需求
  1. 承包廠商應依合約所訂之交付項目與時程，依序進行專案工作，本院得視需要要求廠商提供進度報告。
  2. 為確保承包廠商所交付系統能滿足本院作業需求，本案需進行系統測試，由承包廠商提供各測試項目執行及結果報告以作為驗收依據。
  3. 建置系統後，必須派員至本院協同進行各項功能測試，由本院確認無誤後始可完成測試報告文件。
  4. 驗收方式：
     (1) 資產性驗收：主機及相關設備必須詳列規格清單，並逐一清點。
     (2) 功能性驗收：本案軟硬體功能需求規範需逐項測試驗收。
     (3) 相關文件：系統建置白皮書、產品規格書及其他文件。

產品交付

1. 交付品項規格表列項目。

馬偕紀念醫院
Mackay Memorial Hospital

資訊系統/設備　詢價品項規格表

預算項目：特權帳號安控稽核系統　　案件編號：A115-000154

名稱：	(中) 特權帳號安控稽核系統
	(英) Privileged Access Management

項次	品　　項／規　　格	數 量	單位
1.	規格： 1. 提供至少 10U 以及一年訂閱授權使用者連線登入特權帳號安控稽核系統授權並內含多重要素驗證(MFA)機制。 2. 系統提供收納側錄 200 個設備或 1000 個帳號:密碼管理、稽核側錄與威脅分析功能。 3. 系統架構具備災難復原 DR(Disaster Recovery)機制，(本案至多提供 4 個 DR 金庫)可於中央儲存伺服器停止運作時自動連線至備援系統，不會影響日常運作。 4. 系統提供全域政策，統一定義密碼檢查與變更週期，亦可依受管理主機系統設定例外政策，以及可自訂密碼歸與週期。 5. 系統提供使用者登入系統後僅顯示被授權登入的受管理主機系統。 6. 系統提供分段式密碼存取方式，依使用者權限只能看到前段或後段密碼。 7. 系統提供密碼設定不顯示功能(密碼不揭露)，僅允許使用者代登入受主機系統。 8. 系統提供一層或階層覆核流程機制，並可同時採用批次方式進行大量的申請使用與核准請求。 9. 系統提供登入 Web 圖形化(GUI)操作介面。 10. 提供預先申請密碼使用區間，如:下班後或假日作業，待覆核後，僅能在申請使用區間作業。 11. 系統提供密碼版本控管功能，當需要使用舊版本密碼時可由被授權使用者取得，例如受管理系統被備份檔還原後。 12. 系統提供受管理設備帳號密碼批次或一次上傳功能，管理設備及帳號批次建立。 13. 系統提供內建電子郵件事件通知引擎，並支援提供變數允許管理者自訂郵件範本內容。 14. 系統提供 Web 圖形化(GUI)統一管理與使用者操作介面，並至少支援英文、繁體中文。 15. 系統至少於線上保留一年報表、影片、稽核紀錄等資料，以供隨時調閱稽查。 16. 系統提供透過 syslog 轉送單位現有 SOC 資安監控平台。 17. 系統密碼管理功能，必須以不安裝代理程式(Agent-less) 方式，且不須因密碼變更機制而必須額外新增帳號執行。 18. 系統支援管理 Windows 服務啟動帳號與排程工作的密碼。 19. 系統可設定自動更改密碼的週期，並可由本院自行定義具備有可邏輯化且可輪序的密碼內容。	1	組

資訊系統/設備　詢價品項規格表

預算項目：特權帳號安控稽核系統　　案件編號：A115-000154

名稱：	(中) 特權帳號安控稽核系統
	(英) Privileged Access Management

20. 系統提供密碼依需求限制於特定時間變更，如：04:00~06:00。
21. 系統提供自動檢查受管理主機系統上的特權密碼是否與系統相同，若不一致可主動發出電子郵件警告通知管理者，可於兩者密碼不同時自動重置密碼，使受管理設備密碼與系統相同。
22. 系統支援一次性密碼(One-Time Password)功能，經授權取得密碼後，可依政策規定，在一定時間後自動更新密碼(預設 60 分鐘，最短為 5 分鐘)。
23. 系統提供將受管理主機系統帳號設定為統一密碼內容群組，一次性變更相同密碼。
24. 系統稽核側錄功能，必須以不安裝代理程式(Agent-less)方式執行。
25. 系統提供側錄下列通訊協定或軟體：①.SSH、②. Remote Desktop（RDP）、③. SQL Server Management Studio、④.網頁（HTTP、HTTPS）
26. 系統提供連續錄影(非操作鍵盤滑鼠才開始錄影)，並將側錄影片自動壓縮加密儲存於中央儲存伺服器。
27. 系統提供線上即時監看，經授權的使用者可即時監看或中斷操作過程，並可與原始使用者同時操作受管理主機系統。
28. 系統提供 Web 圖形化(GUI)介面直接播放側錄檔案、亦可將側錄檔案下載在本機播放。
29. 系統提供依單位資安政策要求，暫停(Suspend)外部廠商使用者可執行的 Linux 指令(如：adduser、rm)與 Windows 動作(如：新增帳號、遠端桌面)，並能夠即時透過電子郵件警示。
30. 系統須提供提供完整使用者操作與密碼使用等稽核紀錄功能，並可直接登入 Web 圖形化(GUI)介面進行查詢。
31. 系統提供指令搜尋功能，可輸入關鍵字快速查詢操作過或違反政策的指令。
32. 系統提供提供即時安全事件風險儀表板，至少包含風險評分、發生時間、事件數量、帳號名稱、主機名稱等。
33. 系統提供報表排程寄送與手動產出，並至少包含下列類型報表：
34. 特權帳號納管狀況報表
35. 特權帳號密碼變更合規性報表
36. 特權帳號授權使用報表(週報、月報或年報)
37. 活動日誌報表，包含使用者存取密碼、何時被修改、申請理由、授權原因等。
38. 系統架構具備中央儲存伺服器，所有存放在系統中的檔案為加密檔案，並符合 FIPS 140-2 安全需求規範。
39. Server 端：
    (1) 三個月密碼自動更改（或可自訂週期）
    (2) 指定帳戶密碼週期變動。
    (3) 特定帳號降權。(申請提權，時間限制)

資訊系統/設備　詢價品項規格表

預算項目：特權帳號安控稽核系統　　案件編號：A115-000154

名稱：	(中) 特權帳號安控稽核系統
	(英) Privileged Access Management

	40. Client 端： (1). 三個月密碼自動更改（或可自訂週期） (2). 自訂密碼政策。 (3). 用戶端自動代登入。 41. 本案所需項目、程式、元件等皆安裝於本院，所需主機部分由院方提供。
備註	1. 上列項目為必需項目，廠商如有增加項目(不可減少)則需於建議書中規劃增列並說明。 2. 本專案之系統功能及內容，如有需要可進一步與本院主辦單位進行需求訪談及確認。 3. 以上含免費到場軟體系統安裝及系統架設服務，並檢附原廠保固證明書、維護廠商到府維護書、軟體弱掃證明，以及其它佐證文件。 4. 需包含此專案所採購系統安裝服務及相關教育訓練。 5. 自驗收日起提供保固，需提供當年度新品證明文件，保固期間內廠商應負責免費維護服務，以維持系統正常運作。 6. 本案自驗收日起提供 1 年原廠免費軟體保固及升級服務，同時為 7*24 原廠技術支援服務，以維持系統正常運作，保固期過後的維護費用比率，將於議價會議時依據得標含稅金額一併訂定之。

五、廠商須知

5.1 實績要求

承包廠商所屬團隊需具備相關領域之建置之工作實績經驗(乙)案以上，並表列之，如下。

對象	建置日期	建置規模	備註

5.2 人員要求

檢送參與本專案工作人員之學經歷背景，專案過程中非經本院公函同意不得任意更換專案人員。

承包本專案之廠商應成立工作小組，成員及成員資格需包括下列:

1. 本案專案經理應具2年以上相關工作經驗，並執行各項技術及管理工作。
2. 本案專案經理需具備相關資格證明，廠商需提出相關文件，以保障本專案系統開發之品質控管。
3. 參與專案人員均需為承包廠商全職工作人員，並應於專案簽約前提交與建議書相符之專案人員相關資料(含該人員之到職日期、健保卡正面影本、學經歷及在本案擔任工作等)檢送本院備查。

5.3 損害賠償

廠商於得標後須保證履行契約規定，若於合約進行時使本院蒙受之損失或有設備系統安全受損害，無法正常運作時，概由廠商負責賠償，而本院得自應付價金中扣抵。

5.4 權利瑕疵擔保

(1) 廠商應保證本案交付本院之產品未侵害他人之著作權及其他權利，如有侵害他人合法權益時，應由廠商負責處理並承擔一切法律及賠償責任。

(2) 廠商所提供之產品因侵害他人著作權或其他權利時，應按下列方式擇一解決，並且負責賠償本院因侵權引起之相關費用：

- ☞ 修改侵權部份，使該產品無觸犯他人權利之處。
- ☞ 徵得權利人授權，使本院能繼續使用該產品。

5.5 工作項目時程要求

本專案開發工作項目時程與相關產品交付階段如下表：

項次	工作項目	產品項目	專案時程
1	提報建議書作業	系統建議書 (請依建議書製作規則)	截止日內郵寄或送交採購單位
2	參與院內評估作業	請廠商到院簡報說明或 提報相關文件	必要時由本院召開會議
3	密封報價	依『採購品項規格表 EDP-P-04』 廠商密封報價單	由本院採購單位通知
4	參與議價	請廠商到院參與 押標金憑證(500 萬以上案件)	由本院採購單位通知
5	簽訂合約	依照本院合約範本填寫	由本院採購單位通知
6	專案啟動	專案執行計劃文件	簽約後依 2.5(4)項時程內
7	專案建置	建置文件	簽約後依 2.5(5)項時程內
8	交貨、安裝	品項規格表列項目	簽約後依 2.5(6)(7)項時程內
9	專案驗收	驗收報告、文件	簽約後依 2.5(8)項時程內

5.6 履約保證金規定

得標廠商應於簽定合約時，繳交履約保證金，金額為付款總額之 10％，於驗收完成，且無待解決事項後 30 日內無息退還。

說明：

若本合約總價新台幣一百萬元以上，乙方於簽定合約時，應繳交履約保證金。

(一)金額：付款總額之 10%；若合約中含軟硬體，軟體部份之履約保證金為軟體付款總額之 100%，硬體部份之履約保證金為硬體付款總額之 10%

(二)方式：履約保證金可以現金、金融機構簽發之本票或支票、保付支票、郵政匯票、無記名政府公債、設定質權之金融機構定期存款單、銀行開發或保兌之不可撤銷擔保信用狀繳納，或取具銀行之書面連帶保證、保險公司之連帶保證保險單為之。

(三)執行：因可歸責於乙方之事由，致甲方遭受損害，其所造成損失、額外費用或懲罰性違約金之金額，甲方得自應付價金中扣抵，若仍有不足者，甲方得自履約保證金中扣抵。

(四)期間：履約保證金於驗收入庫完成且無待解決事項後 30 日內無息退還。

5.7 保固保證金規定

取回履約保證金時，應同時繳交保固保證金，金額為付款總額之 5 %，俟本案保固期屆滿，且無待解決事項後 30 日內無息發還。

說明：

(一)保固責任：如保固保養合約。

(二)保固保證金：取回履約保證金時，應同時繳交保固保證金。

(三)金額：付款總額之 5%；若合約中含軟硬體，軟體部份之保固保證金為軟體付款總額之 30%，硬體部份之保固保證金為硬體付款總額之 5%。

(四)期間：驗收入庫完成日起至保固期滿，且無待解決事項後 30 日內無息發還

5.8 本院付款方式

本專案費用將分四期支付

1. 第一期款項為整體專案費用百分之十，得標廠商於完成正式簽約手續後，提出專案啟動計劃書，經本院相關單位確認無誤後撥付。
2. 第二期款項為整體專案費用百分之三十，得標廠商於完成需求調查分析後，提出系統規劃設計書，經本院相關單位審核無誤後再行撥付。
3. 第三期款項為整體專案費用百分之三十，得標廠商於完成產品製造程序後，提出安裝測試報告書，經本院相關單位審核無誤後再行撥付。
4. 第四期款項為整體專案費用百分之三十，得標廠商於完成所有安裝測試，依本院驗收程序驗收後，交付相關文件，並經本院相關單位審核無誤後再行撥付。

5.9 資通安全管理義務

一、定義：

1. 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
2. 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。
3. 資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
4. 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。
5. 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或

間接方式識別該個人之資料。

6. 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
7. 蒐集個人資料：指以任何方式取得個人資料。
8. 處理個人資料：指為建立或利用個人資料檔案所為資料之記錄、輸入儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
9. 利用個人資料：指將蒐集之個人資料為處理以外之使用。
10. 安全維護事項：採取技術上及組織上之必要措施，並符合資通安全、個人資料保護相關法規之安全控制。

二、資通安全與個人資料保護保證

乙方茲向甲方聲明、保證並同意遵守以下事項：

1. 乙方需遵循本合約、甲方資通安全管理系統及個人資料保護安全維護事項相關文件之規定。
2. 乙方更換專案人員應提供資歷供甲方審查，並經甲方同意後，始得更換。
3. 乙方執行本合約內容期間，違反資通安全、個人資料保護相關法令，應於知悉 4 小時內通知甲方，並配合甲方之要求採行補救措施。
4. 如係因可歸責於乙方之事由，造成甲方發生資通安全事件時，應於知悉 1 小時內，將事件發生之事實及已採取之因應措施通報甲方，並於 15 日曆天內依甲方指定之方式，送交調查、處理及改善報告。
5. 因乙方執行合約內容期間造成甲方發生資通安全事件時，乙方需負損害賠償責任。
6. 乙方交付之資通系統、資通服務，應於合約期間配合原廠、CVE 網站（https://cve.mitre.org/）漏洞公告，提供修補或防止該漏洞造成甲方發生資通安全事件之建議，並配合甲方之要求，由乙方安排專人進行更新，並確保資通系統、資通服務正常運作。
7. 乙方自甲方取得之個人資料，在蒐集、處理、利用個人資料時，應遵守法令及甲方主管機關相關法規命令之規定，建立適當安全維護事項，防止資通安全事件發生，限於本合約目的範圍內，於甲方指定之處所內使用。乙方同意取得或知悉甲方之資料，應僅提供、告知有需要知悉該秘密之團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書。本條款所

指安全維護事項包含採取技術上及組織上之必要措施，並符合資通安全、個人資料保護相關法規。

8. 乙方承攬本合約，若有合作夥伴與分包廠商，應事先提交名單經甲方同意，並依其對甲方資料之存取程度，由乙方要求建立相對應之安全維護事項，以防止資料被竊取、竄改、毀損、滅失或洩漏。
9. 乙方提供服務所使用之資通訊軟硬體設備，不允許使用大陸地區產品；亦不得使用行政院依據「各機關對危害國家資通安全產品限制使用原則」公布之廠商清單所提供之產品，或甲方主管機關公告之禁用廠商名單，如產品係由上述廠商進行設計（Original Design Manufacturer, ODM）或製造（Original Equipment Manufacturer, OEM）者，同屬限制範圍。
10. 乙方提供之服務，或所使用之軟硬體設備，如經甲方主管機關以正式函文、新聞稿或類此方式公告有資安疑慮時，甲方得請乙方提出說明並綜合一切情事決定是否暫停乙方服務被訂購、或採取暫停履約等措施。
11. 乙方保證承攬本合約所涉及之人員未具有陸籍身分。
12. 本合約若包括客製化資通系統開發者，乙方應提供該資通系統之安全性檢測證明；涉及利用非乙方自行開發之系統或資源者，乙方應標示非自行開發之內容與其來源及提供授權證明，例如：jQuery、NativeBase 等第三方元件。
13. 乙方承攬本合約期間，在經甲方同意下開放資通系統遠端連線，乙方應建立以下安全維護事項：
    A. 應監控資通系統遠端連線。
    B. 資通系統應採用加密機制。
    C. 資通系統遠端存取之來源應為乙方已預先定義及管理之存取控制點。
    D. 依維運需求，授權透過遠端執行特定之功能及存取相關資訊。
    E. 乙方執行資通系統遠端連線之資訊設備，每次連線甲方網路前，必須先以商業版合法防毒軟體最新病毒碼進行全系統掃描，確認沒有病毒，且作業系統之漏洞修補程式已更新至最新狀態，方可存取甲方網路。
    F. 對於每一種允許之遠端存取類型，均應先取得甲方授權，建立使用

限制，並留有使用紀錄。

14.甲方得不定期派員稽核乙方提供之服務是否符合本合約之規定，乙方應以合作之態度在15日曆天內提供甲方相關書面資料，或協助約談相關當事人。若配合主管機關、司法單位執行上述稽核，甲方得以不預告之方式進行之，乙方不得拒絕或規避。稽核應符合乙方合理的保密、安全及業務要求。稽核費用由甲方自行負擔。

15.乙方應配合甲方所辦理之稽核工作，針對缺失於收到甲方書面通知日起限期改善，如乙方未依限完成，依本合約相關規定辦理。

16.乙方僅得於甲方指示之範圍內，蒐集、處理或利用個人資料。乙方認甲方之指示有違反個人資料保護法規，或基於個人資料保護法規所發布之命令規定情事，應立即通知甲方。

17.本合約委託關係終止或解除時，乙方應配合甲方之要求，返還、移交、刪除或銷毀履行合約而持有之資料。

馬偕紀念醫院

委外契約共同條款表

文件編號：MMH-ISMS-4-GE-029　　文件版本：1.3　　生效日期：2024.07.25

保存期限：依據契約標的保存期限　　機密性等級：一般

一、 定義

1. 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
2. 資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。
3. 資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
4. 資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

5. 個人資料：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
6. 個人資料檔案：指依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。
7. 蒐集個人資料：指以任何方式取得個人資料。
8. 處理個人資料：指為建立或利用個人資料檔案所為資料之記錄、輸入儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
9. 利用個人資料：指將蒐集之個人資料為處理以外之使用。
10. 安全維護事項：採取技術上及組織上之必要措施，並符合資通安全、個人資料保護相關法規之安全控制。

二、 資通安全與個人資料保護保證

乙方茲向甲方聲明、保證並同意遵守以下事項：

1. 乙方需遵循本契約、甲方資通安全管理及個人資料保護安全維護事項相關文件之規定。
2. 乙方更換專案人員應提供資歷供甲方審查，並經甲方同意後，始得更換。
3. 乙方保證符合資通安全管理法施行細則第四條規定之受託者要求：
   (1) 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。
   (2) 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。
   (3) 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。
   (4) 受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
   (5) 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之

安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

(6) 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。

(7) 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

(8) 受託者應採取之其他資通安全相關維護措施。

4. 甲方有權定期或於知悉乙方發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

5. 乙方執行本契約內容期間，違反資通安全、個人資料保護相關法令，應於知悉 1 小時內通知甲方，並配合甲方之要求採行補救措施。

6. 因乙方造成甲方發生資通安全事件時，應於知悉 1 小時內，將事件發生之事實及已採取之因應措施通報甲方，並於 15 日曆天內依甲方指定之方式，送交調查、處理及改善報告。

7. 因乙方執行契約內容期間造成甲方發生資通安全事件時，乙方需負損害賠償責任。

8. 本契約委託關係終止或解除時，乙方應配合甲方之要求，□返還 □移交□刪除□銷毀履行契約而持有之資料，並於驗收時，提交履行本款規定之佐證資料。

9. 乙方交付之資通系統、資通服務，應於契約期間配合原廠、CVE 網站（https://cve.mitre.org/）漏洞公告，提供修補或防止該漏洞造成甲方發生資通安全事件之建議，並配合甲方之要求，由乙方安排專人進行更新，並確保資通系統、資通服務正常運作。

10. 乙方自甲方取得之個人資料，在蒐集、處理、利用個人資料時，應遵守法令及甲方主管機關相關法規命令之規定，建立適當安全維護事項，防止資通安全事件發生，限於本契約目的範圍內，於甲方指定之

處所內使用。乙方同意取得或知悉甲方之資料，應僅提供、告知有需要知悉該秘密之團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書。本條款所指安全維護事項包含採取技術上及組織上之必要措施，並符合資通安全、個人資料保護相關法規。

11. 乙方承攬本契約，若有合作夥伴與分包廠商，應事先提交名單經甲方同意，並依其對甲方資料之存取程度，由乙方要求建立相對應之安全維護事項，以防止資料被竊取、竄改、毀損、滅失或洩漏。
12. 乙方提供服務所使用之資通訊軟硬體設備，不允許使用大陸地區產品；亦不得使用數位發展部依據「各機關對危害國家資通安全產品限制使用原則」公布之廠商清單所提供之產品，或甲方主管機關公告之禁用廠商名單，如產品係由上述廠商進行設計（Original Design Manufacturer,ODM）或製造（Original Equipment Manufacturer,OEM）者，同屬限制範圍。
13. 乙方提供之服務，或所使用之軟硬體設備，如經甲方主管機關以正式函文、新聞稿或類此方式公告有資安疑慮時，甲方得請乙方提出說明並綜合一切情事決定是否暫停乙方服務被訂購、或採取暫停履約等措施。
14. 乙方保證承攬本契約所涉及之人員未具有陸籍身分。
15. 本契約若包括客製化資通系統開發者，乙方應提供該資通系統之安全性檢測證明；涉及利用非乙方自行開發之系統或資源者，乙方應標示非自行開發之內容與其來源及提供授權證明，例如：jQuery、NativeBase 等第三方元件。
16. 乙方承攬本契約期間，在經甲方同意下開放資通系統遠端連線，乙方應建立以下安全維護事項：
    （1）應監控資通系統遠端連線。
    （2）資通系統應採用加密機制。
    （3）資通系統遠端存取之來源應為乙方已預先定義及管理之存取控制點。

（4）依維運需求，授權透過遠端執行特定之功能及存取相關資訊。

（5）乙方執行資通系統遠端連線之資訊設備，每次連線甲方網路前，必須先以商業版合法防毒軟體最新病毒碼進行全系統掃描，確認沒有病毒，且作業系統之漏洞修補程式已更新至最新狀態，方可存取甲方網路。

（6）對於每一種允許之遠端存取類型，均應先取得甲方授權，建立使用限制，並留有使用紀錄。

17. 甲方得不定期派員稽核乙方提供之服務是否符合本契約之規定，乙方應以合作之態度在 15 日曆天內提供甲方相關書面資料，或協助約談相關當事人。若配合主管機關、司法單位執行上述稽核，甲方得以不預告之方式進行之，乙方不得拒絕或規避。稽核應符合乙方合理的保密、安全及業務要求。稽核費用由甲方自行負擔。
18. 乙方應配合甲方所辦理之稽核工作，針對缺失於收到甲方書面通知日起限期改善，如乙方未依期限完成，依本契約相關規定辦理。
19. 乙方僅得於甲方指示之範圍內，蒐集、處理或利用個人資料。乙方認甲方之指示有違反個人資料保護法規，或基於個人資料保護法規所發布之命令規定情事，應立即通知甲方。

六、建議書製作規則

6.1 簡述

(1) 投標廠商建議書製作，應符合本節之規定。

(2) 建議書不得逾期投遞，否則視為棄權。

(3) 建議書於投遞時間截止後，不得修改或增訂。

6.2 裝訂及交付

(1) 裝訂

請用 A4 規格式印刷，內容以中文橫式由左至右繕打，並標註頁數。請提供一式一份。

(2) 投遞

截止日期及時間：依公告日期為準。

(3) 投遞地點

馬偕紀念醫院總院 總務室採購課(台北市中山北路二段 92 號 8 樓)

(4) 投遞方式

投標廠商將建議書送達本院。

6.3 一般要求

(1) 建議書交付後，本院不得交付本院及評選單位以外之第三者參閱。製作建議書及合約簽訂前所費之成本，由投標廠商自行負擔，建議書所有權歸本院。

(2) 投標廠商對於徵求建議書說明文件內容有疑問時，請於公告截止前之上班時間以電話（25433535#2476 梁煌達）提出意見或問題，本院不另舉辦說明會；另為使投標廠商瞭解本院現行資訊系統，廠商得於公告截止前之上班時間至資訊單位洽詢討論或借閱相關文件。

(3) 本院對投標廠商建議書中所提實績經驗有疑問時，得請廠商提出證明文件。

6.4 建議書內容

投標廠商所撰寫「建議書」內容應包括下列主要項目：

1. 建議書封面(如附件一範例)
2. 目錄
3. 專案概述
   - 3.1 專案名稱
   - 3.2 專案目標
   - 3.3 專案範圍
   - 3.4 專案時程及交付品項
4. 專案需求建議
   - 4.1 技術建議：包括系統功能設計、架構、資料庫技術等
     - 4.1.1 規格、架構及說明
     - 4.1.2 解決方案描述(包含方法、技術與工具)
     - 4.1.4 保固保養(維護)計畫
   - 4.2 教育訓練建議(課程綱要及時數)
   - 4.3 系統管理者教育訓練計畫
5. 專案計畫執行能力
   - 5.1 如期完成專案之規劃
   - 5.2 驗證系統效能之規劃
6. 廠商信譽
   - 6.1 公司之簡介、經驗及實績
   - 6.2 技術能力證明及說明
   - 6.3 參與專案團隊及人員相關資料
   - 6.4 後續保固維護服務能力
7. 其它建議事項

附件一

七、附件

「特權帳號安控稽核系統」

建置計畫案

建議書

案件編號：A115-000154

2026 年　　月　　日

	公司章	負責人章
用印欄		

公司名：

聯絡人：

電　話：

傳　真：

大哥大：

e-mail：