馬偕紀念醫院
MacKay Memorial Hospital

ISO27001 資訊安全管理系統輔導暨驗證及資通安全顧問服務案

規格說明書

2025 年 10 月 21 日

壹、 服務對象

一、台灣基督長老教會馬偕醫療財團法人馬偕紀念醫院

（以下簡稱台北馬偕）。

二、台灣基督長老教會馬偕醫療財團法人淡水馬偕紀念醫院

（以下簡稱淡水馬偕）。

三、台灣基督長老教會馬偕醫療財團法人台東馬偕紀念醫院

（以下簡稱台東馬偕）。

四、台灣基督長老教會馬偕醫療財團法人新竹馬偕紀念醫院

（以下簡稱新竹馬偕）。

五、台灣基督長老教會馬偕醫療財團法人馬偕兒童醫院

（以下簡稱兒童醫院）。

六、新竹市立馬偕兒童醫院(委託台灣基督長老教會馬偕醫療財團法人興建經營，以下簡稱新竹馬偕兒童醫院)

貳、 專案範圍

一、輔導資訊單位提供之資訊安全管理活動，涵蓋醫療資訊系統、醫療影像系統、健保醫療資訊雲端查詢系統批次下載、電子病歷系統之開發、維護管理，及其相關之電腦機房實體安全、網路安全管理、醫事單位提供之醫務管理業務、病歷資料管理作業、病歷存放實體安全、掛號批價作業、健保申報業務、人事單位提供之 HCA 醫事憑證管理中心醫事人員行動憑證管理服務窗口作業(RAO)、遠距照護服務提供之遠距醫療作業(通訊診察治療辦法）之資訊安全管理系統，且取得經我國標準法主管機關委託機構之公正第三方驗證，於合約有效期間維持 ISO/IEC 27001:2022

證書之有效性及顧問輔導服務，

二、輔導台北馬偕(含兒童醫院)與淡水馬偕配合「資通安全法」與衛生福利部、數位發展部等……主管機關之要求，協助持續維護資通系統分級及防護基準，協助 OT 醫療儀器導入與維護資通系統分級及防護基準，協助 OT 其他(工務)支援設施導入與維護資通系統分級及防護基準。

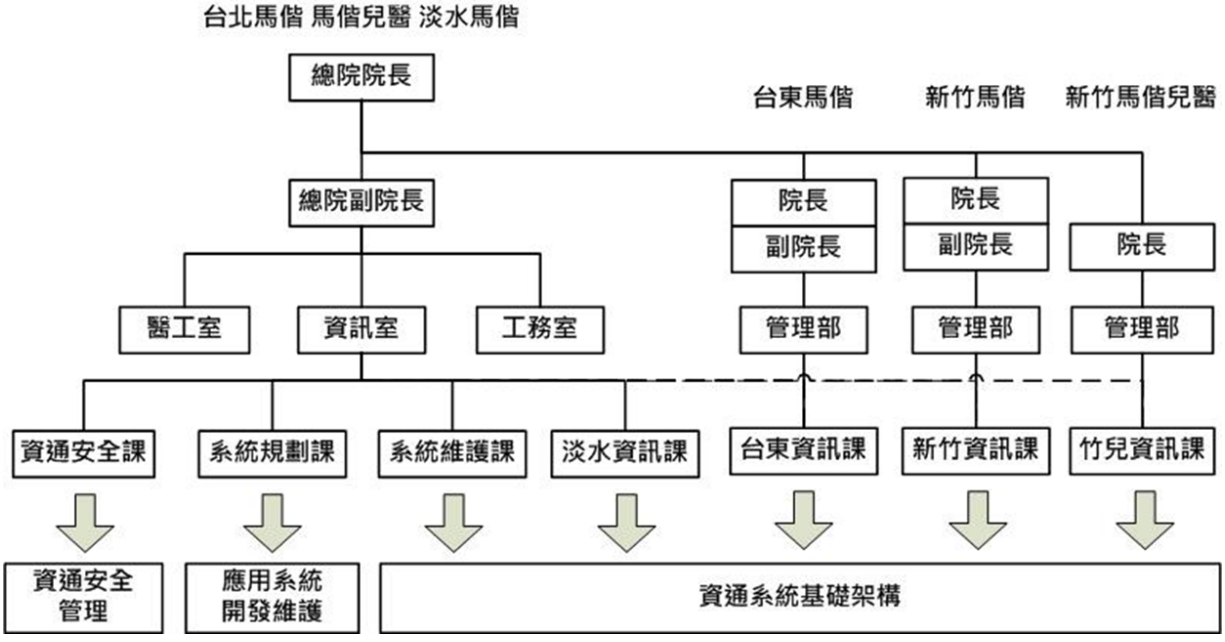
三、台東馬偕、新竹馬偕、新竹馬偕兒童醫院配合於驗證範圍內「資通安全法」與衛生福利部、數位發展部等……主管機關之要求，協助持續維護資通系統分級及防護基準。

參、 專案期間

自 115 年 01 月 01 日起至 116 年 12 月 31 日止，共二年。

肆、 現況說明

一、 資訊單位組織運作



二、 本院資訊軟體系統分為下列九種：

(一)醫療資訊系統 (HIS)

(二)醫療影像系統（PACS）

(三)電子病歷系統(EMR)

(四)醫療支援業務

(五)醫療行政業務

(六)行政管理

(七)全球資訊網

(八)行動裝置 APP

(九)雲端服務

三、 資通安全管理現況說明

(一)行政院核定台灣基督長老教會馬偕醫療財團法人馬偕紀念醫院（包含淡水馬偕）為資通安全責任等級Ａ級之非公務機關。

(二)新竹馬偕、台東馬偕為關鍵基礎設施提供者「重度級急救責任醫院」。

(三)本院於 2020 年 11 月通過 ISO/IEC 27001:2013 初評驗證，2025 年 10 月轉版驗證完成。驗證範圍：資訊單位提供之資訊安全管理活動，涵蓋醫療資訊系統、醫療影像系統、健保醫療資訊雲端查詢系統批次下載、電子病歷系統之開發、維護管理，及其相關之電腦機房實體安全、網路安全管理、醫事單位提供之醫務管理業務、病歷資料管理作業、病歷存放實體安全、掛號批價作業、健保申報業務、人事單位提供之 HCA 醫事憑證管理中心醫事人員行動憑證管理服務窗口作業（RAO）、遠距照護服務提供之遠距醫療作業（通訊診察治療辦法）。

(四)台東馬偕將於115年進行醫院評鑑,新竹馬偕兒童醫院為BOT案。

備註：若廠商需瞭解本院現行資訊環境，請與承辦人員聯繫。

伍、 台北馬偕(含兒童醫院)與淡水馬偕需求內容

一、 資通系統分級及防護基準

(一)依據「資通安全責任等級分級辦法」、衛生福利部規定，廠商應指導資訊單位進行分類分級與鑑別，每年綜整各項資通系統「資通系統防護需求等級評估表」，製作「資通系統清冊」，並指導資訊單位交付資通系統分級資料予衛生福利部。

(二)廠商應指導資訊單位從事資通系統防護需求等級評估，依據「資通安全責任等級分級辦法」附表十之控制措施，填寫相對應等級之「普級資通系統防護基準評估表」、「中級資通系統防護基準評估表」與「高級資通系統防護基準評估表」。

(三)資訊單位遵循「資通安全責任等級分級辦法」規定，但資訊單位資通系統程式之修改、軟硬體採購，不在本專案服務範圍。

(四)廠商進行本階段人員，建議需有1位具有效期間之Information Systems Security Architecture Professional(CISSP - ISSAP)或Information Systems Security Engineering Professional(CISSP - ISSEP)資通安全專業證照。

二、 資通安全風險評估

(一)資通系統及資訊業務（IT）

1. 依據「ISO 31000風險管理－原則與指導綱要」（以下簡稱ISO 31000）、「MMH-ISMS-2-GE-003資訊資產管理規範」、

「MMH-ISMS-2-GE-006 資通安全風險管理規範」規定，執行本項作業。

2. 於合約有效期間，協助每年更新風險評估因子，並指導資訊單位更新「風險評估因子定義表」。
3. 協助與指導驗證範圍內單位維護與更新「資產清冊」與資訊單位相關資通系統及資訊業務之「組態清冊」、「資通系統清冊」、「雲服務專案管理表」。
4. 分辨資訊資產潛在威脅之來源與弱點，評估現有管控措施，以及進行業務衝擊分析，決定風險等級，產出「風險評估報告」。
5. 依據「風險評估報告」結果，針對不可接受之風險等級，擇定控制目標與控制點，交付「風險處理計畫」。
6. 廠商進行本階段人員，建議至少需有 1 位具有效期間之 Certified in Risk and Information Systems Control (CRISC) 資通安全專業證照。

(二)醫療儀器及其他(工務)支援設施 (OT)

1. 針對衛生福利部、主管機關對於醫療儀器、其他支援設施風險評估需求，由廠商提供範例與顧問諮詢，指導醫工單位與工務單位撰寫「醫療儀器盤點與風險評估作業規範」、「其他(工務)支援設施盤點與風險評估作業規範」(實際名稱由院方決定)。
2. 廠商需指導醫工單位與工務單位依據衛生福利部、主管機關、「醫療儀器盤點與風險評估管理規範」、「其他(工務)支援設施盤點與風險評估作業規範」(實際名稱由院方決定)之

規定，於合約期間每年進行醫療儀器、其他(工務)支援設施盤點與風險評估。

3. 針對 OT 醫療儀器盤點，於合約期間每年指導本院進行風險評估，產出「OT 資產風險評估上傳表」（若未來主管機關有要求，其他(工務)支援設施盤點須比照辦理）。
4. 廠商每季至少一次應針對 OT 領域進行資安輔導（不含矯正、維護計畫、實施情形填寫會議、內部稽核）。
5. 廠商需協助 OT 單位確認系統架構之設計是否符合資安要求，專案結束時應提供成果報告及未來建議方向。
6. 廠商須具有輔導醫工單位及工務單位之經驗或能力。
7. 廠商進行本階段人員，建議至少需有 1 位具有效期間之以下資通安全專業證照：
   (1) 1 位具有 HealthCare Information Security and Privacy Practitioner(HCISPP) 或 Information Systems Security Management Professional(CISSP – ISSMP)。
   (2) 1 位具有 Certified in Risk and Information Systems Control (CRISC)。

三、 資通安全維護計畫維護與實施情形申報協助，及其他主管機關所要求填報事項：

(一)廠商需配合衛生福利部、數位發展部及主管機關、院方之要求，指導院方人員每年維護「資通安全維護計畫」，計畫內容須包含資通系統及資訊（IT)、醫療儀器及其他支援設施（OT）資通安全管理。

(二)廠商應協助院方，配合衛生福利部要求，指導院方人員每年申報「資通安全維護計畫」實施情形，以符合「資通安全管理法施行細則」之規定。

(三)廠商需指導院方，針對以下情形撰寫改善報告，以符合「資通安全管理法」、「資通安全管理法施行細則」之規定：

1. 衛生福利部、數位發展部及主管機關認定本院之資通安全維護計畫實施有缺失或待改善者。

2. 本院發生資通安全事件。

(四)廠商需指導院方，填報主管機關所要求之事項：國家層級資通安全風險評估作業、IT 資安治理成熟度評估作業及 OT 資安治理成熟度評估系統作業，並輔導達主管機關之要求。

(五)廠商進行本階段人員，建議至少需有 1 位具有效期間之 Certified Information Security Manager(CISM)資通安全專業證照。

四、 資通安全管理文件修改

(一)資通系統及資訊（IT）

1. 廠商應依據衛生福利部、主管機關要求，及院方實際作業需求，與資訊安全管理系統 ISO/IEC 27001:2022 驗證機構之要求，配合提供撰寫範例與顧問諮詢之方式，指導修改現行資訊安全管理系統四階文件規定。

2. 配合 ISO/IEC 27001:2022 要求，廠商必須產出符合規範之差異分析報告。

3. 廠商需指導資訊單位，依據「各機關資通安全事件通報及應變處理作業程序」，更新資安應變標準作業程序，以符合衛生

福利部、數位發展部等機關之規定。

4. 台北馬偕與淡水馬偕依據「資通安全維護計畫」，每年辦理核心資通系統業務持續運作演練，廠商需指導兩院區，辦理並參與核心資通系統業務持續運作演練。

5. 廠商需指導驗證範圍內之單位進行資安應變演練。

(二)醫療儀器及其他支援設施（OT）

1. 廠商需依據資通安全管理法、資通安全管理法施行細則、衛生福利部之要求，針對院方之醫療儀器、其他(工務)支援設施，由院方人員撰寫，廠商提供撰寫範例與顧問諮詢之方式，協助指導製作與審查相關資通安全管理文件。

2. 廠商需依據資通安全事件通報及應變辦法、衛生福利部、數位發展部之要求，針對院方之醫療儀器、其他(工務)支援設施，由院方人員撰寫，廠商提供撰寫範例與顧問諮詢之方式，指導訂定相關通報與應變機制。

(三)廠商進行本階段人員，至少需有 1 位以下證照人員：

1. ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor。

2. ISO 22301 Business Continuity Management System(BCMS) Auditor/Lead Auditor。

3. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor。

(四)廠商進行本階段人員，建議具有以下證照人員尤佳：

1. 具有效期間之 Certified Information Security

Manager(CISM)證照。

2. 具有效期間之 Information Systems Security Architecture Professional(CISSP - ISSAP) 證照。

五、 資通安全內部稽核

(一)廠商需依據「資通安全維護計畫」規定，每年執行 2 次資通安全內部稽核，範圍包括全機關資訊、醫療儀器、其他(工務)支援設施，且符合「資通安全法」及其子法等相關法規以及資訊安全管理系統 ISO/IEC 27001:2022 證書驗證範圍，交付「資通安全管理內部稽核報告」。

(二)廠商每次稽核前應訂定稽核計畫，計畫內容須符合「資通安全法」及其子法等相關法規以及 ISO/IEC 27001:2022 之規定。

(三)廠商擔任稽核之人員，須具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor 資通安全專業證照，並建議具有 Certified Information Systems Auditor (CISA)證照尤佳。

六、 資通系統安全檢測

(一)針對院方於資通安全維護計畫內提報主管機關之核心資通系統，廠商於合約期間，每年進行一次所有核心資通系統滲透測試，交付「滲透測試報告」並說明報告內容及建議改善方式，於初掃報告完成 3 個月內執行複掃。

(二)針對院方於資通安全維護計畫內提報主管機關之核心資通系統，及本院對外官網（1 個 URL），每年進行一次弱點掃描，交付「弱點掃描報告」並說明報告內容及建議改善方式，於初掃報告完成 3

個月內執行複掃：

1. Web 網頁弱點檢測：針對網頁安全弱點進行檢測，檢測項目應符合 OWASP TOP 10 2025 項目(官方網站如有公布更新資訊內容，請廠商以最新內容檢測)。
2. 主機系統弱點檢測：針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點檢測的檢測項目，應符合 Common Vulnerabilities and Exposures(CVE)發布的弱點內容(最新版)。

(三)廠商擔任資通系統安全檢測人員至少有 1 名 Certified Ethical Hacker(CEH)或 CompTIA PenTest (CompTIA PenTest+)證照。

七、 受託者資通安全稽核

(一)院方每年指定資訊 2 家受託者，醫工 1 家受託者，由廠商執行受託者資通安全稽核。

(二)廠商每次稽核前，應依據每家被稽核之受託者產出「受託者資通安全稽核計畫」，由本院依據該計畫通知受託者，確認實際稽核日期與行程。

(三)廠商應依據每家被稽核之受託者，交付「受託者資訊安全稽核報告」，交由資訊單位進行後續改善追蹤。

(四)廠商擔任稽核之人員，皆須具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor 資通安全專業證照。

八、 管理審查協助

廠商需依據「資通安全維護計畫」、ISO/IEC 27001:2022 之規定，於合約有效期間指導院方準備管理審查會議資料，並安排專案人員 1 名出席該會議。

九、 第三方驗證協助

(一)廠商需依據院方資訊安全管理系統驗證範圍，安排驗證機構進行年度稽核，以協助本院取得經我國標準法主管機關委託機構之公正第三方驗證之 ISO/IEC 27001:2022 證書，並維持證書之有效性。

(二)廠商需於驗證機構執行稽核前，協助院方準備驗證機構稽核所需相關文件。

(三)廠商應於外部驗證期間安排顧問人員到場陪同與協助院方通過稽核。

(四)依據驗證機構稽核結果所提出之相關不符合事項，提供改善措施之規劃與執行建議，並符合「MMH-ISMS-2-GE-007 改善措施管理規範」規定。

(五)廠商選擇之驗證機構，須為通過我國標準法主管機關委託機構認證之機構，且需經院方同意，且驗證文件核發之證書單位應有前開委託機構之認證標誌及國際論壇（International Accreditation Fourum，IAF）認證機構認可之驗證機構。

十、 資通安全教育訓練

(一)廠商需於合約期間，每年舉辦以下教育訓練：

1. 針對院方使用者與主管，每年舉辦 3 堂資通安全通識教育訓練，每堂課 1 小時。

2. 針對院方資訊人員，每年舉辦2堂符合「資通安全責任等級分級辦法」規定之資通安全專業教育訓練，每堂課3小時，人數限制最多30人。

3. 針對醫療儀器、其他(工務)支援設施，每年舉辦2堂「OT資通安全教育訓練」，每堂課3小時。

4. 課程內容應提前交付並經過院方同意。

陸、 台東馬偕、新竹馬偕及新竹馬偕兒童醫院之需求內容

一、 資通安全風險評估

(一)依據「ISO 31000風險管理－原則與指導綱要」(以下簡稱ISO 31000)、「MMH-ISMS-2-GE-003資訊資產管理規範」、「MMH-ISMS-2-GE-006資通安全風險管理規範」規定，執行本項作業。

(二)於合約有效期間，協助每年更新風險評估因子，並指導資訊單位更新「風險評估因子定義表」。

(三)協助與指導驗證範圍內單位維護與更新「資產清冊」與資訊單位相關資通系統及資訊業務之「組態清冊」、「資通系統清冊」、「雲服務專案管理表」。

(四)分辨資訊資產潛在威脅之來源與弱點，評估現有管控措施，以及進行業務衝擊分析，決定風險等級，產出「風險評估報告」。

(五)依據「風險評估報告」結果，針對不可接受之風險等級，擇定控制目標與控制點，交付「風險處理計畫」。

(六)廠商進行本階段人員，建議至少需有1位具有效期間之Certified in Risk and Information Systems Control (CRISC)資通安全專

業證照。

二、 資通安全維護計畫填寫與實施情形申報協助，及其他主管機關所要求填報事項：

(一)廠商需配合衛生福利部、數位發展部及主管機關、院方之要求，指導院方人員每年維護「資通安全維護計畫」，計畫內容須包含資通系統及資訊（IT）資通安全管理。

(二)廠商應協助院方，配合衛生福利部要求，指導院方人員每年申報「資通安全維護計畫」實施情形，以符合「資通安全管理法施行細則」之規定。

(三)廠商需指導院方，針對以下情形撰寫改善報告，以符合「資通安全管理法」、「資通安全管理法施行細則」之規定：

1. 衛生福利部、數位發展部及主管機關認定本院之資通安全維護計畫實施有缺失或待改善者。

2. 本院發生資通安全事件。

(四)廠商需指導院方，填報主管機關所要求之事項：國家層級資通安全風險評估作業、IT 資安治理成熟度評估作業，並輔導達主管機關之要求。

三、 廠商進行本階段人員，建議至少需有 1 位具有效期間之 Certified Information Security Manager(CISM)資通安全專業證照。

四、 資通安全管理文件修改

(五)配合衛生福利部、數位發展部等主管機關要求，及本院實際作業需求，與資訊安全管理系統 ISO/IEC 27001:2022 驗證機構之要求，配合提供撰寫範例與顧問諮詢之方式，指導修改現行資訊安全管理

系統四階文件規定。

(六)配合 ISO/IEC 27001:2022 要求，廠商必須產出符合規範之差異分析報告。

(七)廠商進行本階段人員，至少需有 1 位具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor 資通安全專業證照。

五、 資通安全內部稽核

(一)廠商每年需依據資訊安全管理系統驗證範圍，訂定符合「資通安全法」及其子法等相關法規執行台東馬偕、新竹馬偕及新竹馬偕兒童醫院各 2 次資通安全內部稽核，並交付「資通安全管理內部稽核報告」。

(二)廠商每次稽核前應訂定稽核計畫，計畫內容應包含稽核說明與頻率、稽核準則、稽核範圍、受稽核單位、預計稽核日期、稽核人員與職責且符合「資通安全法」及其子法等相關法規。

(三)廠商擔任稽核之人員，皆須具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor 資通安全專業證照，並建議具有 Certified Information Systems Auditor (CISA)證照尤佳。

六、 受託者資通安全稽核

(一)台東馬偕與新竹馬偕每年各指定 1 家受託者，由廠商執行受託者資通安全稽核。

(二)廠商每次稽核前，應依據每家被稽核之受託者產出「受託者資通安全稽核計畫」，由院方依據該計畫通知受託者，確認實際稽核日

期與行程。

(三)廠商應依據每家被稽核之受託者，交付「受託者資訊安全稽核報告」，由各院資訊單位進行後續改善追蹤。

(四)廠商擔任稽核之人員，皆須具有 ISO/IEC 27001:2022 Information Security Management Systems(ISMS) Auditor/ Lead Auditor 資通安全專業證照。

七、 管理審查協助

廠商需依據「資通安全維護計畫」規定，於合約有效期間指導院方準備管理審查會議資料，並安排專案人員 1 名出席該會議。

八、 第三方驗證協助

(一)廠商需依據院方資訊安全管理系統驗證範圍，安排驗證機構進行年度稽核，以協助本院取得經我國標準法主管機關委託機構之公正第三方驗證之 ISO/IEC 27001:2022 證書，並維持證書之有效性。驗證文件核發之證書單位應有前開委託機構之認證標誌及國際論壇（International Accreditation Fourum，IAF）認證機構認可之驗證機構

(二)廠商需於驗證機構執行稽核前，協助本院準備驗證機構稽核所需相關文件。

(三)依據驗證機構稽核結果所提出之相關不符合事項，提供改善措施之規劃與執行建議，並符合「MMH-ISMS-2-GE-007 改善措施管理規範」規定。

(四)廠商選擇之驗證機構，需經院方同意。

九、 資通安全教育訓練

（一）針對台東馬偕、新竹馬偕(含新竹馬偕兒童醫院)使用者與主管，每年舉辦3堂資通安全通識教育訓練，每堂課1小時。

（二）針對台東馬偕、新竹馬偕(含新竹馬偕兒童醫院)資訊人員，每年舉辦1堂符合「資通安全責任等級分級辦法」規定之資通安全專業教育訓練，每堂課3小時，人數限制最多30人。

（三）課程內容應提前交付並經過院方同意。

柒、 專案管理需求

一、 專案管理

得標廠商應就本專案之規劃管理、組織、時程及進度查核等方面撰寫專案執行計畫書，內容應包含專案規劃及執行方式說明、專案管理、專案組織、人力配置、交付項目、專案時程及進度查核、工作對應窗口、專案驗收及本院配合事項等。

二、 專案組織與人力

(一)得標廠商應研擬評估預計投入本專案之人員配置與資歷（學經歷背景與技術專長)。參與本專案之專案成員需3人以上，且為承包廠商連續在職1年以上之全職員工，並依各項服務需求所要求具備之證照，於專案執行計畫書中提出相關證明，並填具委外廠商專案人員資格審查表(附件一)。

(二)本院有權要求更換專案成員，得標廠商應於接獲本院通知後1個月內完成更換。

(三)得標廠商於專案執行計畫書提出之專案組織與人員應與實際執行本專案之人員相符，得標廠商若欲異動專案成員須於1個月前通

知本院，並經本院同意後始可異動。

三、 廠商投標資格

(一)具輔導醫療機構 ISO/IEC 27001:2022 經驗。

(二)具輔導資通安全責任等級 A 或 B 級以上機關辦理應辦事項之能力。

(三)需政府機關登記合格，無不良紀錄之廠商（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。

四、 安全需求

(一)得標廠商參與本案之專案人員進行本案之相關專案工作時，應注意資訊安全之防護措施，須依照本院規定簽訂保密切結書（詳附件二)，以及合作廠商保密切結書(詳附件三)並確實要求所屬人員遵守保密規定，倘經發現因前述事由而洩密者，一切損害由得標廠商負責，並依法追究刑事責任。

(二)得標廠商參與本案之專案人員因工作之便所接觸之資料不得私自進行留存、備份、篡改或販售等行為，如因疏失造成本院各項資訊作業與文件資料之毀損與損失，由得標廠商負責賠償責任，本院並保留損失估計權利。廠商使用之資通訊工具需符合國家安全規定。

(三)得標廠商須將本院委外契約共同條款表（詳附件四）簽訂於合約規範中，並確實要求所屬人員遵守規定。

五、 強制性需求

(一)本專案於合約期間內所取得之資料，於本專案合約終止後應完整

歸還，不得複製。

(二)第三方驗證協助之驗證機構稽核報告其驗證結果若為無效，其缺失改善再複驗所產生之費用，將由得標廠商負擔。

(三)得標廠商未依本專案合約履行者，本院得解除或終止合約。

(四)得標廠商於簽約時須同時簽訂保密與責任條款。

捌、 附件

一、 馬偕紀念醫院委外廠商專案人員資格審查表

二、 馬偕紀念醫院人員保密切結書

三、 馬偕醫療財團法人體系合作廠商保密同意書

四、 馬偕紀念醫院委外契約共同條款表