**天主教輔仁大學附設醫院**

**資安管理制度維運暨委外續評驗證服務需求書**

**一、專案概述**

 本院為符合ISO 27001：2013相關規範驗證準則要求，辦理資安管理制度續評驗證工作，爰辦理本案採購。

**二、專案名稱**

 天主教輔仁大學附設醫院「資安管理制度維運暨委外續評驗證服務案」勞務採購案(以下簡稱本案)。

**三、專案範圍**

1. 資安管理制度維運暨委外續評驗證服務(驗證範圍包含資訊室、資訊室維運機房、HIS、PACS及電子病歷系統)
	* + 1. 資安管理制度維運作業
2. 工作研討
3. ISMS相關作業規範與文件紀錄檢視協助
4. 內部稽核執行。
5. 內部稽核後改善建議
	* + 1. 外部稽核驗證服務(含第三方驗證費用)

外部稽核到場陪同

外稽後矯正改善建議與諮詢

**四、服務地點**

 輔仁大學附設醫院：資訊室、資訊室維運機房。

**五、專案時程**

 於本案發包下訂日後於「外部稽核續評驗證」前完成本案維運作業事項，如需與本院設備廠商配合與協調之工作事項，請於工作會議協調事項與配合時間。

**六、本案需求**

* 1. 資安管理制度維運

協助檢視、修訂資訊安全相關作業規範與文件：瞭解本院各單位組織及業務現狀，以使本院資訊安全管理制度更為健全，並讓本院符合ISO 27001：2013相關規範。

1. 實施資訊安全管理相關工作研討實務作業：對相關人員實施資訊安全管理制度架構、資訊資產價值評估及分類分級、風險評鑑、風險管理、業務持續運作、委外管理、內部稽核作業、管理審查作業、矯正改善等工作實務研討作業。
2. 資安目標達成計畫與量測表

協助輔導本院接受資訊安全第三方外部稽核並通過驗證。

* 1. ISMS專案管理需求

到場顧問諮詢服務與協助本院所提出之相關事項(含括配置之人員、設備技術與程序表單等資源)。

* 1. 強制性需求

作業時如發生錯誤或資料漏失，經確認屬承包廠商責任者，應由承包廠商負責更正；另損及他人權利義務，承包廠商亦須負責。

承包廠商未依本案契約執行，又未於本院要求期限內改善者，本院得終止契約。

**七、專案組織與管理**

1. 專案成員資格
2. 輔導顧問
3. 應具備15年以上資訊服務工作經驗，曾參與資訊安全管理制度專案建置及輔導經驗10案(含)以上。
4. 具備ISO/IEC 27001資安管理制度、ISO/IEC 27701 隱私資訊管理系統、IEC 62443-2-1 工控系統 及ISO/IEC 9001主導稽核員（Lead Auditor）主導稽核員之國際證照(請檢附證明文件)。
5. 稽核顧問
6. 具參與醫療院所ISMS稽核工作之經驗。
7. 具備ISO/IEC 27001資安管理制度、ISO/IEC 27701 隱私資訊管理系統、IEC 62443-2-1 工控系統及ISO/IEC 9001主導稽核員（Lead Auditor）主導稽核員之國際證照有CEH道德駭客認證證照尤佳(以上均請檢附證明文件)。

 上述成員資格等相關證明文件，請檢附於投標文件，供承辦人員審查確認。

1. 專案管理
2. 專案工作小組成員如有異動，廠商應於兩週前通知本院同意，並檢附接替人員相關學歷、專長、負責本案之工作項目及內容、相關在職證明，並須由本院查核通過始得更換，本院對不符需求之人員得要求更換。
3. 專案人員有異動時，應指派代理人代理其工作，代理人須為本計畫執行人員以外之人員，且應具被代理人相當資格。
4. 專案配置人力不符本院需求或未盡到專案職責分工，本院有權要求增加或更換相關人員，廠商不得拒絕。
5. 履約人員有不適任之情形者，本院有權要求增加或更換相關人員，廠商不得拒絕，並應於15日曆天內指派經同意之適當人員擔任。

**八、工作時程、交付項目與付款**

本案工作時程、工作項目應符合下表所列之要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 項次 | 工作項目 | 交付項目 | 數量 | 交付日期與付款 |
| 驗收 | 1. 協助完成資產清冊、風險評鑑報告及風險處理計畫
2. 內部稽核與查檢紀錄
3. 外部驗證完成後之報告
4. 外稽改善建議等相關文件
 | 一式 | 依驗收付款百分比：完成資安外部驗證，依規定辦理階段驗收合格後，由本院支付得標金額全額費用。 |

**九、資訊安全**

1. 廠商所有履約人員，均應依本院相關資安規定簽署保密協定，始得執行相關業務，且須配合資安相關稽核資料整理與提供。
2. 廠商不得違反法令強制或禁止規定，公共秩序及善良風俗，且對本院之經營管理及民眾權益不得有不利之影響，並應遵循國家機密保護法、個人資料保護法、其他法令及本院資訊安全政策與資訊安全相關之規定，廠商對本案契約之履行應留存紀錄，以供本院定期或不定期之稽核。
3. 廠商對業務上所接觸之資料及產生文件，應適當分級及標示，並採取必要之保密措施，參與本案人員均應依本院規定簽具保密切結書，任何因輔導廠商人員洩密所致之賠償及刑事責任，概由廠商負責。廠商對所處理之資料，應盡善良管理人之義務，確保傳輸、交換或處理過程之安全性。(其有錯誤、毀損、滅失、洩漏或其他不當處理情事者，依個人資料保護法等相關法令辦理。)
4. 廠商所交付之文件，應有必要之安全保護機制，並依據本院相關程序進行交付，電子文件非經授權不得攜出。
5. 廠商履約人員嚴禁使用電腦設備於本院網路環境進行與業務無關或未被允許之活動，履約期間用於處理本院資訊設備，非經許可不得攜出。
6. 廠商及其分包廠商所有履約人員應負保密之責於本案服務期間所蒐集與本案相關之個人、公務及機密資料與各類統計報表(報)，其所有權歸屬本院，非經本院書面同意不得自行使用或提供第三者參考使用。
7. 軟體須提供合法版權。