財團法人醫藥品查驗中心
Taiwan Center For Drug Evaluation

財團法人醫藥品查驗中心

【再生製劑臨床試驗 AI 法規諮詢】

需求規格說明書

中 華 民 國 114 年 12 月

目 錄

壹、 專案說明概述

一、專案名稱

本專案名稱為【再生製劑臨床試驗 AI 法規諮詢】採購案（以下簡稱本專案）

二、專案背景

再生製劑之蓬勃發展為疾病治療帶來嶄新的契機與前景，然而再生製劑因其高度個體化、複雜製程以及對長期追蹤療效與安全性之要求，使其在研發與臨床試驗執行上，相較於傳統藥物開發之法規要求與遵循較為複雜。我國於 113 年通過再生醫療雙法(《再生醫療法》以及《再生醫療製劑條例》)，為產業發展奠定法規基礎，然而，雙法之通過也意味著相關子法規將陸續公告，使得醫藥產業界在執行再生製劑臨床試驗時，需在龐雜的條文及眾多公告中，迅速辨識並找到最符合自身產品需求的法規，以確保研發與送件的正確性與合規性。

傳統法規查詢需反覆瀏覽多個平臺與文件，耗時費力且易產生資訊斷裂。使用者若缺乏法規知識，可能無法正確辨識關鍵條文；即使具專業背景，仍因資料分散導致效率低落。法規掌握不足亦可能造成送件錯誤、重複修正與進度延宕，增加時間與資源成本。為有效協助醫藥產業掌握法規單位對於再生製劑臨床試驗的最新要求，提升送件資料的法規遵循，促進產業發展，查驗中心積極推動【再生製劑臨床試驗 AI 法規諮詢】專案。

本專案旨在建立一再生製劑臨床試驗智慧化法規諮詢系統，此系統將透過人工智慧，導入語言模型技術，將再生製劑相關法規文本轉化為可互動、可查詢之資料庫，此系統之建立將協助醫藥產業應對日益複雜之再生法規環境，從而加速再生製劑研發。

三、專案目標

本專案之目標為整合再生製劑臨床試驗法規，並利用 AI 大型語言模型技術，建立一套高效且高準確性之再生製劑臨床試驗智慧法規諮詢系統，強化醫藥產業之法規遵循能力。具體目標分述如下：

(一) 建立再生製劑法規資料庫：系統化、自動化蒐集及整合再生製劑臨床試驗相關之法規文件，建立一持續更新之再生製劑法規資料庫。此資料庫將作為再生製劑臨床試驗智慧化法規諮詢系統進行訓練、微調及檢索增強生成(Retrieval-Augmented Generation, RAG)的核心知識來源。

(二) 建立再生製劑臨床試驗智慧化法規諮詢系統：基於 AI 大型語言模型，發展再生製劑臨床試驗諮詢系統。此系統需理解使用者提出的自然語言法規問題，並結合再生製劑之法規要求，提供情境式、高準確性的專業法規指引與解答，最終實現高效率的法規知識提取，以協助產業大幅縮短確認送件要求與法規遵循。

四、專案範圍

本專案範圍旨在涵蓋再生製劑臨床試驗智慧法規諮詢系統從法規資料庫建置到系統交付的完整開發流程，具體範圍如下：

(一) 資料庫建置與資料準備：系統化地整合所有擬用於訓練大型語言模型的再生製劑臨床試驗相關法規文件，由本案建置廠商進行法規文件下載，並進行資料向量化處理，以建立再生製劑法規向量資料庫。

(二) 核心架構與數據介接：確立並建構查驗中心數據科學資料應用管理平臺與再生製劑法規資料庫之間的介接方式，確保模型回覆能夠準確地引用和依據最新的法規內容，並建立法規資料庫的自動化更新流程，包括對新增或修訂的法規文件進行監測、下載、擷取等功能，確保系統知識來源的即時性。

(三) 語言模型之評估與測試：使用語言模型 Google Gemini 2.5 以上版本建立系統，針對語言模型測試 QA 問答集及相關評估指標，以測試其在再生製劑臨床試驗法規領域的資料處理能力、自然語言問題理解能力、以及法規回覆的準確性與適用性。

(四) 系統開發：依據上述(一)至(三)點開發功能完整之再生製劑臨床試驗智慧化法規諮詢系統，並且完成使用者介面與體驗設計(UI/UX)之建構，包含前後臺建構、報表查詢。完成系統開發後，將系統交付於查驗中心。

五、專案時程

自決標日起至 115 年 12 月 31 日止。

六、專案經費

本專案預算金額為新臺幣 148 萬元整(含稅)，投標廠商報價不得逾預算金額，投標廠商報價超過預算者，即判為不合格標。本專案之契約價金包含廠商執行專案契約有效期間所需相關費用。

七、履約地點

財團法人醫藥品查驗中心（臺北市南港區忠孝東路六段 465 號 3 樓）

貳、 安全需求

一、資通系統籌獲各階段資安強化措施要求

本中心得聘請專家學者，協助本中心於專案重點里程碑中檢視履約(執行)程序與成果之相關管理作為，得標廠商應配合辦理，不得拒絕。

二、資通安全管理需求

(一) 得標廠商對業務上所接觸之本中心資料，應視同機密文件採必要之保密措施，

並應依本中心規定填具「委外廠商保密承諾書」及「保密承諾暨個人資料提供同意書」，併同本專案工作計畫書交付本中心備查。任何因得標廠商人員洩密所致之賠償及刑事責任，概由得標廠商負責，並列入本中心拒絕往來戶。

(二) 得標廠商服務人員除應遵守本中心相關規定外，並應對本中心資料保密。未經本中心同意不得將電腦硬體、軟體或資料任意變更或攜出原設置地點。凡對維護標的物硬體、軟體及資料之作為，均不得有所隱瞞，並不可對程式及軟體私設密碼。違者應自負法律責任，得標廠商並同意將之免職及賠償本中心之損失。本中心除扣除相關罰款之外，必要時，得終止契約。

(三) 本中心為資通安全責任等級 C 級之特定非公務機關，本專案系統防護需求分級為中級，須符合數位發展部-資通安全責任等級分級辦法-附表十-資通系統防護基準要求標準，且為 ISO/IEC 27001:2022 資安認證合格機構，得標廠商除應自行規範所有專案人員應遵守之資安規定外，並應遵守本中心 ISMS 各項資安管理規定，繳交委外人員應遵守之資安規範等相關文件。

(四) 為確保委外作業整體安全及個人資料維護措施與管理機制作業完善，得標廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本中心資通安全管理及保密相關規定。此外本中心保有依本中心與得標廠商同意之適當方式對得標廠商派員稽核、委由資通安全管理法主管機關籌組專案團隊稽核或其他適當方式執行相關稽核或查核的權利，稽核結果不符合本契約約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本中心通知後應於期限內完成改善；未依限完成改善者，核計逾期違約金。

(五) 得標廠商或本專案之專案成員如違反個人資料保護法規定造成損害，本中心除依契約罰則處理外，對於第三人所造成的損害賠償應負賠償之責，本中心保有對得標廠商追償之權利。

(六) 本採購屬行政院「大陸廠牌資通訊產品及委外經營公眾場域盤點原則」之範疇。

(七) 得標廠商介接本中心網路或處理本中心資訊業務之設備（含軟體、硬體及服務）不得有大陸廠牌資通訊產品。

(八) 弱點掃描：

得標廠商應於驗收前（測試結果併入專案結案報告）及系統保固期間，分別進行本系統之主機及網站弱點掃描，並完成中等級（含）以上風險弱點之修補；主機及網站弱點掃描應使用中央研究院資訊服務處認可工具（清單如：https://its.sinica.edu.tw/posts/154864），並請於服務建議書（企劃書）中提出。

(九) 本專案得標廠商所提供之產品(含軟體、硬體及服務）不得為大陸廠牌資通訊產品，應符合「各機關對危害國家資通安全產品限制原則」，且均不得安裝非公務

用軟體，執行本專案之團隊成員亦不得為陸籍人士。

(十) 得標廠商所提供之服務，如違反資通安全相關法令、知悉本中心或廠商發生資安事件時，均必須於 1 小時內通報本中心，提出緊急應變處理，並配合本中心做後續處理；必要時，得由資通安全管理法主管機關於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。

(十一) 得標廠商應於 TWCERT 和國家資通安全研究院公告資通系統弱點翌日起三個日曆天內(TWCERT 和國家資通安全研究院公告之漏洞值(CVSS)大於 7 分(含)者，應於公告資通系統弱點之次個上班日下午六點前)，通報本中心漏洞有關資訊、漏洞影響及得標廠商建議採行控制措施，並經本中心確認。

參、 專案執行

一、本專案執行內容，得標廠商應依照業務需求訪談結果後，進行系統設計、規劃與調整，提供規劃系統開發需求及架構，專案執行內容與具體要求如下：

(一) **再生製劑臨床試驗法規資料整合與資料庫建立：**

系統化整合再生製劑臨床試驗法規文件，並完成資料向量化處理，建立再生製劑臨床試驗法規資料庫，作為語言模型訓練資料來源。

(二) **語言模型與資料庫之介接**

1. 針對再生製劑臨床試驗法規資料庫與查驗中心數據科學資料應用管理平臺，建構一良好的介接方式。
2. 建立法規資料自動化更新機制以及更新異常通報機制，以確保系統知識來源之即時性與正確性。

(三) **語言模型評估方式與測試**

1. 查驗中心將依據再生製劑臨床試驗資料庫內容，準備至多 200 題之 Q&A 問答集，用於語言模型訓練與測試。
2. 針對語言模型對於再生製劑臨床試驗之問題理解與回覆適用性進行評估。
3. 針對語言模型回覆之評估結果，進行多輪次之語言模型調校與優化流程。
4. 自由測試階段：由查驗中心進行再生製劑臨床試驗智慧化法規諮詢系統測試，針對系統測試結果由廠商進行語言模型調校與優化，藉由需求訪談確定系統評估方法，測試準確率需達 80%。

(四) **使用者介面與體驗設計(UI/UX)**

建構一兼具專業性、直覺化以及實用性之使用者介面設計，包含前後臺建構、報表查詢，並將系統交付於查驗中心。

二、罰則

(一) 專案期間未依上述之需求執行，以『(二)計罰方式、1.未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『專案工作小組』會議同意，如未能配合『專案工作小組』會議開會，須先 mail『專案工作小組』成員並經半數(含)以上成員同意。

(二) 計罰方式

1. 未能於規定時間完成工作計罰

以日曆天計罰，計罰違約金不足 1 日以 1 日計，每日計罰契約價金 0.1%；未能於規定時間完成工作計罰之計算，為自本中心通知(書面、傳真、系統報修或電子郵件)之發生時間(工作時間)起算，經本中心人員確認止(日曆天之計算不含前 2 次本中心人員測至功能恢復正常運作且試時間，第 3 次起含本中心計算測試時間，計算方式詳如『未依規定時間完成工作計罰天數之計算說明表』；契約中不含本中心測試部分，依契約規定時間完成)。

2. 上述違約金依原因每件(申請單)獨立計罰，罰款天數以日曆天計。

3. 本案標的物如逾維修期限未修護或執行完成，且廠商無法提出令本中心同意之延遲原因時，本中心得另行招商修護，修護相關費用概由廠商負擔及賠償。

4. 本案功能新增修改部分仍受維護條款規範。

5. 本案每點違約金金額依契約規定，若契約未規定訂為每點新臺幣 3 仟元整。

(三) 其他相關罰則

1. 廠商應做好資通安全與防止個人資料外洩之相關配套措施。專案執行及保固期間，發生資安事件 2 級含以上、機敏資料外洩事件或其他因素而造成本中心不名譽事件等，且可歸責廠商者，每次予以本案得標總金額 5%懲罰性罰款，除限期改善外，並由承包廠商負責處理並承擔一切法律及賠償責任，本項罰款不列入契約所訂罰款上限金額，情節重大者，依刑法民法辦理相關條款；本中心發生資安事件 1 級含以下並經行政院國家資通安全會報技術服務中心發送事件通知或發生白帽駭客事件，且可歸責廠商者，每次予以懲罰性罰款 5 仟元整。

2. 其他詳如契約書及資訊委外共同說明書。

三、強制性需求

(一) 本案於契約期間內本中心所交付之資料不得複製外流並善盡保護管理責任，並於本案契約終止後應完整歸還。

(二) 執行本案如發生錯誤或資料漏失，經確認屬得標廠商責任者，應由廠商負責更正；另損及他人權利義務，廠商亦須負責。

(三) 得標廠商未依本案契約執行，又未於本中心要求期限內改善者，本中心得視情形終止契約。

(四) 廠商不得違反法令強制或禁止規定，公共秩序及善良風俗，且對本中心之經營管理及民眾權益不得有不利之影響，並應遵循資通安全法及其相關子法、國家機密保護法、個人資料保護法及其他法令之規定，廠商對本案契約之履行應留存紀錄，以供本中心定期或不定期之稽核。

(五) 廠商履約期間，違反個資法或資通安全相關法令或知悉資通安全事件時，應立即通知本中心、採行補救措施及配合本中心進行後續處理。

(六) 發生 1 級以上資安事件，廠商提出事件原因分析及不符合事項，如係因廠商未妥善規劃管理建議，得作成書面報告說明，經本中心同意確認後才可免罰，否則，本中心每次依二、罰則之（三）、其他相關罰則計罰。

四、本案採購標的範圍：

■本採購標的範圍之全部。

□除_____外，皆為主要部分。

肆、 管理需求

一、專案管理

(一) 廠商須於決標日起 30 個日曆天(以下簡稱日)內召開專案啟動會議，並與本中心進行需求訪談，實際內容須依本中心最終之要求而定，作成書面紀錄，得標廠商應確實配合辦理。

(二) 廠商依專案啟動會議訪談結果，須於會後 30 日內提交專案工作計畫書，內容應包括對本案之執行敘述，含專案組織、人力、分工、職掌、工作項目與進度、交付項目、測試計畫、經費明細表及其他相關事項等，本計畫書內容經本中心確認後執行，若有變更，則須經雙方同意。

(三) 廠商應於每月提供專案執行進度與狀態報告，會議需製作正式會議紀錄，並於會議結束後 14 日內交付。

(四) 廠商應依交付項目及注意事項之階段要求，於交付時程(含當日)完成各階段應交付項目。

二、資格要求

(一) 本案廠商應具備 ISO 27001 ISMS 相關證照。

(二) 廠商投標時於服務建議書須提供上述證照、具有與本中心類似領域之單位實績、近 3 年實績與著作等資料供本中心查驗。

三、服務管理

(一) 得標廠商於本案執行期間，若因無法達到服務水準，而須增加人力或投入額外資源時，所須費用均含於本案總金額中，不得另行要求本中心支付。

(二) 本中心如有必要，得要求廠商配合本中心召開專案進度會議報告專案執行進度；亦得因特殊需求，要求不定期召開會議，廠商不得拒絕。會議需製作正式會議紀錄，並於會議結束後 14 日內交付。

(三) 工作計畫書及本案產生之各項文件和會議紀錄，若有不一致時，以最新版為有效。

四、專案稽核

(一) 本中心得視本專案之執行狀況，對得標廠商提出外部稽核要求，由本中心指派人員不定期、但在事先知會的日期，至得標廠商執行本專案之辦公室或地點，執行稽核活動。以了解得標廠商是否依照本文件要求、投標服務建議書及專案規劃文件的承諾，執行本專案各項活動，得標廠商不得拒絕。

(二) 本中心指派之稽核人員得要求查看和本專案相關之所有文件、紀錄和系統設施，必要時，本中心指派人員得以訪談得標廠商參與本專案之人員，以了解專案成員是否具備執行本專案所需之技能與知識，如本中心人員認為得標廠商參與本專案之人員不符合執行本專案之需求，得要求得標廠商於一個月內更換專案成員，得標廠商不得拒絕。

五、文件衝突管理

得標廠商之服務建議書文件之建議事項，如和本需求規格說明書及契約內容有衝突或不一致，除另有書面紀錄約定外，應以本需求規格說明書及契約內容為執行及驗收依據。

伍、 交付項目作業及時程

一、交付項目作業方式及注意事項：

(一) 投標廠商須於專案工作計畫書中依所規劃之執行期程自訂各項文件產出之交付查核點，並可另依執行需要，自訂其他必要之交付項目及其查核點，於查核點前交付本中心審核，自訂查核點及自訂交付項目應審慎合理可行。得標廠商若未依下表及自訂之交付項目及時程執行，將依本文件之罰則計算違約金。

(二) 本案各項文件應於交付階段期限，正式函送交本中心書面文件一份及電子檔一份（採 A4 紙雙面列印、無須膠裝，並於文件封面註明案名、文件名稱、版本及文件產生日期）。

(三) 本案分成 4 階段，各階段工作內容說明如下：

項次	階段	交付項目	交付期限
1	第一階段	1. 專案工作計畫書(內容須包括專案工作項目及作業程序、時程規劃、工作進度表、甘特圖、細部執行計畫、經費明細表、成員組織架構及專案管理等項目)，含：委外廠商保密承諾書(附件 1)、保密承諾暨個人資料提供同意書(附件 2)、委外廠商資訊安全承諾書(附件 3)、系統安全需求項目檢核表(附件 4)、委外廠商稽核查檢自評表(附件 5)、採購契約範本附記條款特別聲明同意書/切結書(附件 6)	自啟動會議起 30 個日曆天內
2	第二階段	1. 需求規格書、測試建置計畫書	115 年 4 月 15 日
		2. 再生製劑臨床試驗智慧化法規諮詢系統雛型建置與測試期中報告初稿 1 份(內容須包括資料庫建立、語言模型與資料庫之介接、語言模型評估與測試規劃、使用者介面與體驗設計)	115 年 5 月 15 日。
		3. 再生製劑臨床試驗智慧化法規諮詢系統雛型建置與測試期中報告定稿 1 份(內容須包括資料庫建立、語言模型與資料庫之介接、語言模型評估與測試規劃、使用者介面與體驗設計) 4. 本專案系統雛形 1 式 (雛型系統須包含語言模型與資料庫須能介接，且能夠進行問題詢問以及回覆)	115 年 6 月 1 日。
3	第三階段	1. 再生製劑臨床試驗法規資料庫期末報告初稿 1 份 2. 再生製劑臨床試驗智慧化法規諮詢系統建置與測試期末報告初稿 1 份	115 年 8 月 15 日。
		1. 再生製劑臨床試驗法規資料庫期末報告定稿 1 份 2. 再生製劑臨床試驗智慧化法規諮詢系統建置與測試期末報告定稿 1 份	115 年 10 月 1 日。
4	第四階段	1. 系統保固服務計畫書初稿 1 份 2. 專案結案報告初稿 1 份(內容包含系統安全建議書、應用程式安全開發佐證文件)	115 年 12 月 1 日。

項次	階段	交付項目	交付期限
		1. 系統保固服務計畫書定稿 1 份 2. 專案結案報告定稿 1 份(內容包含系統安全建議書、應用程式安全開發佐證文件) 3. 系統原始程式碼及執行碼電子檔光碟	115 年 12 月 31 日。

註：

1. 上述各文件交付日期，以得標廠商來函之本中心**收文日**為準。
2. 上述各項文件，須於交付階段期限前送交本中心，並配合本中心視實際需要，由廠商加印足夠數量。
3. 屬每期付款應交付文件、工作項目，如涉罰責，以契約為準，併於當期計罰。

陸、 投標廠商基本資格及應檢附之資格證明文件

一、投標廠商基本資格（具下列■資格之一者）及應檢附之資格證明文件（廠商需提出資格文件影本繳驗，必要時本中心並得通知廠商提供正本供查驗）：

□財（社）團法人團體、公、協、學會
□公（私）立大專院校(或其院、系、所)
□政府機關及其附屬之研究機構
■經政府合法登記之公司、行號、機構
□經政府合法登記之醫療機構（含醫院、診所）

二、應檢附之資格證明文件：

(一) ■廠商登記或設立證明影本【如：如公司登記或商業登記證明文件、非屬營利事業之法人、機構或團體依法須辦理設立登記之證明文件、工廠登記證明文件、許可登記證明文件、執業執照、開業證明、立案證明或其他由政府機關或其授權機構核發該廠商係合法登記或設立之證明文件】。

上開證明，廠商得以列印公開於目的事業主管機關網站之資料代之。

(廠商附具之證明文件，其內容與招標文件之規定有異，但截止投標前公開於目的事業主管機關網站之該廠商最新資料符合招標文件規定者，本中心得允許廠商列印該最新資料代之。)

(二) □本採購屬經濟部投資審議司公告「具敏感性或國安（含資安）疑慮之業務範疇」之資訊服務採購，廠商不得為大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議委員會公告之陸資資訊服務業者。(上開業務範疇及陸資資訊服務業清單公開於經濟部投資審議司網站 https://www.moea.gov.tw/Mns/dir/home/Home.aspx

(三) 本案廠商納稅之證明：

1. **營業稅繳稅證明**：
   為營業稅繳款書收據聯或主管稽徵機關核章之最近一期營業人銷售額與稅額申報書收執聯。廠商不及提出最近一期證明者，得以前一期之納稅證明代之。新設立且未屆第一期營業稅繳納期限者，得以營業稅主管稽徵機關核發之核准設立登記公函代之；經核定使用統一發票者，應一併檢附申領統一發票購票證相關文件。(本項適用於依營業稅法須報繳營業稅者之情形)
2. **所得稅證明：**
   最近一期之所得稅申報證明文件。廠商不及提出最近一年證明文件者，得以前一年之納稅證明文件代之。
3. 營業稅或所得稅之納稅證明，得以相同期間內主管稽徵機關核發之無違章欠稅之查復表代之。
4. 依法免繳納營業稅或所得稅者，應繳交核定通知書影本或其他依法免稅之證明文件影本。

□ 廠商依工業團體法或商業團體法加入工業或商業團體之證明影本（如：會員證）。

□ 前述相關證明，下列單位得以組織條例、規程之影本或准予投標之公函正本(大專院校以院、系、所名義投標者，至少應附校方准予投標公函正本)(附於投標文件內)代之：

1.公（私）立大專院校(或其院、系、所)

2.政府機關及其附屬之研究機構

(四) ISO 27001 ISMS 相關證照

柒、 預算經費

一、採購金額：新臺幣 148 萬元整。

■本案預算金額：新臺幣 148 萬元整，內容如下：

□委託服務費用預算金額：新臺幣____萬元整。

□採固定金額給付之項目及費用：新臺幣____萬元整

1.項目如下：

2.採固定金額給付之經費，列入本案議價（約）範圍。惟決標後無須調整各項單價。

□核實支付項目及費用：新臺幣____萬元整。

1.核實支付項目如下：

2. 核實支付項目之費用：

□ 採固定金額給付：列入本案議價（約）範圍。惟決標無須調整各項單價。

□ 非採固定金額給付：列入本案議價（約）範圍，決標後須依決標金額比率調整各項單價。

(一)、投標廠商應依■委託服務費用、□固定金額給付、□核實支付項目，分別提列各項經費後加總填報總價投標。

(二)、注意：投標廠商報價不得逾預算金額，投標廠商報價超過預算金額者，列為不合格標，不予減價機會。

□本採購得依選擇一個項目。，保留未來向得標廠商增購之權利，擬增購之項目及內容：

(一)、本案保留後續擴充之期間為__年，其經費為新臺幣____元整。

(二)、本案保留後續擴充之項目及內容：

(三)、啟動條件：

捌、 服務建議書（企劃書）撰寫格式、內容及相關規定

一、 經費編列請依■**資訊服務委外經費估算原則**□**其他：**_____。

二、 除 A3 尺寸繪製之必要圖表（說）外，建議用 A4 縱向紙張，內文應以中文由左至右橫式繕打撰寫（如有必要時，得以英文註記）。宜加目錄、編頁碼（下方置中）、加封面（不須編頁碼）並裝訂成冊。

三、 封面應載明專案名稱、投標廠商，廠商之負責人姓名及提出日期。

四、 投標廠商應提出服務建議書（企劃書）一式 10 份【其中一份請勿裝訂，以利複製】(電子檔 1 份)與投標評審，所提服務建議書（企劃書）經提出後不得退換或更換補件。

五、 若於服務建議書（企劃書）中引用相關書籍資料，應加註引用書籍名稱，且不得有「互相抄襲」情形。如未予登載加註，且內容有雷同之處，由評審委員視其抄襲情節輕重，給予相對較低之分數。

六、 廠商不得以本中心名義，從事與履行契約工作項目無關之行為。違者視情節輕重，本中心中心得要求廠商停止履約至改善為止；逾期未改善或情節重大者，依契約有關契約終止、解除及暫停執行(一)相關規定，終止或解除契約。如造成本中心損害，本中心得請求損害賠償，並得自應付價金中扣抵。

七、 服務建議書（企劃書），其撰寫應至少包括下列內容：

1	目錄：目錄後請附上建議書中與評審項目相關之建議重點、頁次對照彙總表(請依「七、建議書項目對照表」填寫)。	
2	專案概述	
	2.1	專案名稱
	2.2	專案授權
	2.3	專案目標
3	團隊專業能力及經驗	
	3.1	專案組織(含括專案主持人及工作成員名單，各人員所任工作，與本案相關之學經歷、專業技術證照、取得與採購案相關認（驗）證、訓練合格證明、具備完善之資通安全管理措施或通過第三方驗證、**資通安全專業人員**配置及經驗、能力證明等情形，有何優良或不良事蹟等情形，所列人員如何投入本案工作，如何確保非僅掛名)
	3.2	專案管理(含主要工作人數及配置、工作計畫、預定進度、如何完整瞭解及配合本中心需求、如何如期如質履約之說明、尚在履約相關契約件數、金額及是否有逾期情形)
	3.3	專案監控(含專案執行、問題處理...等)、品質保證措施及方法、風險管理、需求變更管理
	3.4	廠商能力(含廠商於截止投標日前 5 年內與本案有關且已完成之證明)與信譽(含廠商於截止投標日前 5 年內受獎懲情形)
4	執行能力及規劃	
	4.1	本案執行工作內容服務規劃與實施
	4.3	資通安全管理機制及防護措施之規劃及執行
	4.4	機敏資料保護機制及防護措施之規劃及執行。
5	創新與建議(含其他與本採購標的有關，且含於標價內之附加或創新服務)	
6	價格分析 標價合理性；標價完整性及正確性	
7	廠商企業社會責任(CSR)指標：1.為員工加薪(如近一年內曾替員工普遍性加薪)。2.於投標文件載明後續履約期間給與全職從事本採購案之員工薪資 (不含加班費)至少超過勞動部公告最低工資 1.1 倍以上。3.提供員工「工作與生活平衡」措施等。	
8	附錄(相關證明文件影本)	

玖、 甄選作業方式及程序

一、受理投標方式：

(一) 廠商應將投標文件相關資格證明文件及服務建議書（企劃書）（一式 10 份【其中一份請勿裝訂，以利複製】及電子檔 1 份）等相關文件資料，以不透明容器密封，於截止投標期限前，以郵遞或專人送達招標指定場所。

(二) 投標廠商應於外標封詳填本標案「案名」「案號」、「廠商名稱」及「地址」等資料，以利審查。

(三) 投標廠商所送未通過審查之服務建議書（企劃書）與附件資料，除本中心保留部分數量作為備查使用，將於決標或無法決標後退還投標廠商。

二、審標與評審：本案採一次投標，不分段開標，並依**「資格規格審查」、「企劃書評審」及「議價」**三階段進行。

(一) 資格規格審查：依本案投標須知規定審查投標廠商之資格（應檢附資格證明文件）及規格（服務建議書（企劃書）應檢送份數及撰寫架構），經資格規格審查符合招標文件規定之投標廠商，始得進入後續評審。

(二) 服務建議書（企劃書）評審：符合資格者，由本中心通知進行現場評審，並由參與評審廠商進行簡報及答詢後，由各評審委員依評審評比表各項評審標準評分。

壹拾、 招標、決標、評審方式及原則

一、招標方式：

■公開招標：依本中心採購作業要點第 7 點第 4 項，取得 3 家以上廠商之書面報價(或企劃書)。

■另於第 1 次公告結果，如未能取得 3 家以上廠商之書面報價(或企劃書)時，依依中心採購作業要點第 7 點第 4 項第 2 款規定，得改採限制性招標。

□限制性招標：依□本中心採購作業要點第 6 點第 5 項第 9 款□政府採購法第 22 條第 1 項第 9 款，採限制性招標。

□委託專業服務 □委託資訊服務 □委託技術服務。

■公開評審，洽最符合需要廠商後辦理議價。

二、決標原則：

■依本中心採購作業要點規定，採取最有利標之精神(最符合需要者)為原則。

□依政府採購法第 52 條第 1 項 第 1 款。

三、決標方式：

(一) 採訂有底價並以總價決標。

(二) 本案採非複數決標。

四、評審方式及評定原則

(一) 本案採序位法－評分轉序位評比，並將價格納入評比。

(二) 由本中心依法組成採購評審小組辦理評審，並由各評審委員依據各投標廠商所提服務建議書（企劃書），按本案所列評審項目及配分，評定各廠商之得分。

(三) 全部評審項目之合計總分數（滿分）為 100 分，由各評審委員就評審項目及配分，填寫評比評分表（含序位）乙份，交由工作人員計算總平均分數及序位總和。

(四) 評審小組出席委員評分結果，**總平均分數達 70 分（含）以上者為合格廠商；總平均分數未達 70 分者為不合格廠商。經評定為不合格者，不得作為優勝廠商。**

(五) 評審委員對於廠商價格項目之給分，將考量該價格相對於所提供服務標的之合理性，以決定其得分，而非僅與其他廠商之價格高低相較而決定其得分。

(六) 評審小組之評審作業，以「記名方式秘密為之」為原則。會議中除評審委員就投標廠商所提資料、簡報有關內容提出發問外，其他列席人員於徵得主席同意後，得對廠商提出詢問，未經同意者不得發問。

(七) **優勝廠商評定方式：經計算各投標廠商之序位數總和結果，以總序位合計數最低且經評審小組出席委員過半數決定者為第一優勝序位廠商**，次低者為第二優勝序位廠商，依此類推。

(八) 評定優勝廠商之優勝序位後，依優勝序位及下列方式與優勝廠商辦理議價（議約）：

1. 優勝廠商為 1 家者，以議價方式辦理。
2. 優勝廠商在 2 家以上者，依優勝序位，自最優勝者起，依序以議價方式辦理。但有 2 家以上廠商為同一優勝序位者，以標價低者優先議價。

(九) 序位第一之廠商有 2 家以上且標價相同時，將依下列方式辦理，決定第一優勝序位廠商，次一優勝序位如有相同情形時，比照下列方式辦理：註：抽籤方式由工作小組製作籤卡(寫入廠商名稱或代號)及籤筒，並由主席代表行使抽籤，其抽出之第一籤，該籤卡廠商即為第一優勝序位廠商，主席每抽籤一次即應宣讀並簽名紀錄；後續順位如須抽籤依此類推。

擇獲得評審委員評定序位第一較多者為第一優勝序位廠商，仍相同者，抽籤決定之。

(十) 本案依優勝序位選出至多 2 名優勝廠商，並依序辦理議價，第一優勝序位廠商議價不成，則由第二優勝序位廠商遞補。

(十一) 本案經本中心衡酌個案特性及實際需要，不予公開評審委員會委員名單，名單於開始評審前應予保密。

五、評審項目、標準及配分

項次	評審項目	配分
1	團隊專業能力及經驗：計畫主持人及工作成員名單，各人員所任工作，與本案相關之學經歷、專業技術證照、取得與採購案相關認（驗）證、訓練合格證明，有何優良或不良事蹟等情形，是否具備完善之資通安全管理措施或通過第三方驗證、資通安全專業人員配置及經驗、能力證明等情形。	25
2	執行能力及相關服務主要工作人數及配置、工作計畫、預定進度、承攬經驗、履約能力、如何完整瞭解及配合機關需求、如何如期如質履約之說明、尚在履約相關契約件數、金額及是否有逾期情形。提供維護及諮詢之時間及方式。服務水準及其達成之方法及提供之承諾。軟體不中斷服務之風險管理。期間不另加價之功能更新及增修服務。其他創意及創新（與本採購標的有關，且含於標價內之附加或創新服務）。	25
3	對本計畫案內容之掌握及資安作為等(含資訊安全及個人資料保護規劃及執行方式、履約相關之資安事件通報、應變、處理之規劃機制)。	20
4	報價及經費組成內容之合理性分析（含資通安全檢測成本）。	20
5	廠商企業社會責任（CSR）指標：1.為員工加薪（如近一年內曾替員工普遍性加薪）。2.於投標文件載明後續履約期間給與全職從事本採購案之員工薪資 （不含加班費）至少超過勞動部公告最低工資 1.1 倍以上。3.提供員工「工作與生活平衡」措施等。	5
6	簡報及詢答。	5

六、本案之「評審評比表（序位法-評分轉序位法）」及「評審評比總表（序位法-評分轉序位法）」(詳如附件 7、8)。

七、簡報及答詢：

(一) 投標廠商至少應由負責人或指定授權人員 1 人出席評審委員會議簡報。列席簡報人數最多 3 人，所有參與人員請攜帶身分證件備查。

(二) 簡報之順序，將於本中心完成資格審查後，以中心收標案先後順序為主。廠商簡報時，其他廠商應退出場外。

(三) 簡報時間及地點，由本中心另行通知資格合格廠商。簡報型態由廠商自行決定，除會議室現有播放硬體設備外，其他必要設備由投標廠商自行攜帶準備。

(四) 資格審查合格廠商應就所提服務建議書（企劃書）內容對本案採購評審委員會

進行口頭簡報（15 分鐘）與答詢（5 分鐘）。簡報結束前 2 分鐘響鈴 1 聲提醒，簡報時間到響鈴 2 聲，廠商應即停止簡報。（參與簡報廠商如達 3 家以上，本中心得經所有參與簡報廠商同意後，酌予縮短簡報時間為 10 分鐘）

(五) 簡報時廠商若經本中心唱名三次未到者，視同放棄「簡報及答詢」機會，該項目以「0」分計，評審委員得逕依服務建議書（企劃書）內容進行評分。

(六) 簡報資料以服務建議書（企劃書）原有方案內容表達為主，現場不接受廠商補充資料，且簡報不得更改投標文件內容。廠商另外提出變更或補充資料者，該資料不納入評審。

(七) 問題答詢：簡報結束後，得由各評審委員就廠商簡報及服務建議書（企劃書）內容提出詢答。

(八) 所有參與評審廠商，均不給予任何經費補助。

(九) 評審合格者，如發現有資料提列不實或抄襲之情事者，由廠商自負相關責任，且本中心得立即取消其議價資格。

八、評審結果經本中心奉核後，另行通知各投標廠商，並依規定辦理後續作業。

壹拾壹、 驗收及付款

一、驗收方式：本案採分期查驗及期末成果報告 1 次驗收，其驗收得以書面資料審查方式進行，必要時得召開審查會議：

(一) 第 1 期：得標廠商依「伍、交付項目作業及時程」項次 1、項次 2 之履約交付項目，並於階段二最後一項交付後，經本中心查驗合格後，且無待解決事項後，撥付契約價金總額 50%。

(二) 第 2 期：得標廠商依「伍、交付項目作業及時程」項次 3、項次 4 之履約交付項目，並於階段四最後一項交付後，經本中心驗收合格後，且無待解決事項後，撥付契約價金總額 50%。

二、其他事項：得標廠商實際完成履約之日期，以本中心收文日為準。

壹拾貳、 其他相關事項

一、本案投標廠商投標文件應包括下列內容（請依本案投標須知辦理）：

(一) 投標廠商之資格文件。

(二) 投標廠商聲明書。

(三) 招標投標及契約文件(三用文件)。

(四) 標價清單。

(五) 投標廠商之服務建議書（企劃書）（一式 10 份）【其中一份請勿裝訂，以利複

製】(及電子檔 1 份)。

二、廠商投標時，請將前條所列投標文件裝入不透明容器（封套）密封，並於截止投標期限前以掛號、快遞或專人親送等方式送達本中心**【財團法人醫藥品查驗中心（臺北市南港區忠孝東路六段 465 號 3 樓)】**，逾時送達者概不受理，投標信封上應註明「本案採購案名」、「案號」及「投標廠商名稱」、「地址」。凡未載明採購案名、案號及投標廠商名稱、地址，以致無法判別為本標案者，皆視為無效標。

三、本案報價應含各細項費用及一切稅賦。

四、投標廠商報價不得逾預算金額，投標廠商報價超過預算金額者，列為不合格標，不予減價機會。

五、本案得標廠商應繳**履約保證金**金額(無者免填)：(請勾選■)

□ 一定金額：_____；■契約金額之一定比率：__10__%。

六、本案得標廠商應繳**保固保證金**金額(無者免填)：(請勾選■)

□ 一定金額：_____；■契約金額之一定比率：_3_%。

七、本案保固期限：自驗收合格之次日起算 1 年。

八、得標廠商之專業服務成果，如侵害第 3 人合法權益時，由廠商負責處理，並承擔一切責任。

九、本案需求說明書及廠商服務建議書（企劃書）之內容，決標後均視為契約之一部分，非因不可抗力之因素，經契約雙方書面同意，不得變更。

十、本案經費係屬_115_年度預算，若有刪減或刪除，將配合調整經費、終止或解除契約，倘遭凍結不能如期支付，得延後辦理支付，或因會計年度結束，本中心須依規定辦理該款項保留作業時，得視保留核定情形，再行支付，本中心不負延遲責任。

十一、本案契約總價曾經減價而確定者，得標廠商應於決標日起 3 日內，依下列規定，調整決標單價分析表經費：

(一) 調整後之各項單價，不得高於原報各項單價金額，另調整後之總價金額應與決標價相同。

(二) 調整後之單價分析表，應經請購單位人員審查確認無誤，始得辦理後續契約書印製事宜。

十二、委託製作之各項作品（含宣導）及設計附件，其著作財產權歸屬於本中心。

十三、本案規格承辦人，本中心諮詢輔導組 陳稚鴻 專案經理，地址：臺北市南港區忠孝東路六段 465 號 3 樓；電話：02-8170-6000 分機 738。

財團法人醫藥品查驗中心 委外廠商保密承諾書

附件 1

茲緣於本公司承做財團法人醫藥品查驗中心（以下簡稱查驗中心）專案，因業務往來需要得以接觸、取得、知悉該中心機密檔案。為保持所知悉或交付檔案之安全性，本公司遵守相關法律命令，並簽署本承諾書，恪遵下列事項：

第一條、 本承諾書所稱之「檔案」，係指一切尚未公開之文件或任何其他形式之記錄、複製品或儲存媒體等相關內容，包括但不限於書面、圖書、錄音、錄影、電磁紀錄等。

第二條、 本承諾書所稱之機密檔案係指明文標示為「密」、「機密」、「極機密」或其他同義字之一切機密，或雖未標示但依一般法律觀念，應視為機密之物品、文件及資料等。但下述情形不在此限：

一、 已有書面證據證明交付或告知之檔案為本公司所已知。

二、 已見於公開發行之刊物或出版品等欠缺機密性質之檔案。

三、 因政府、法院命令或相關法規範等要求必須揭露者。

第三條、 本公司應負善良管理人之注意義務維護查驗中心之機密檔案，非經查驗中心書面同意，絕不故意、過失洩漏、告知、移轉或以任何方式使任何第三人知悉、持有、利用之。

第四條、 本公司瞭解並同意凡利用查驗中心電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線電信，包括但不限網際網路等通訊封包，將依網路通訊監測管理規定進行管理。

第五條、 若違反本承諾書之約定或有任何因可歸責於本公司之事由，以各種方式致機密檔案被洩露者，本公司應依法負相關法律責任及損害賠償責任。

第六條、 本公司應採行一切必要措施，確保本公司之受任人、受僱人、代理人、承攬人或其他類似之履行輔助人，與本公司負擔相同程度之保密義務。若因可歸責於前述履行輔助人之事由致生損害於查驗中心者，準用第五條之規定。

第七條、 本承諾書於本公司契約期限內及其相關完成驗收後二年內均屬有效。

第八條、 非因本公司因素造成，當該等機密檔案對外公開或解除其機密性時，同時解除本公司對該等機密檔案之保密責任。

第九條、 本承諾書之條款，如部分無效或無法執行，不影響其他條款之效力。

第十條、 關於本承諾書引起之爭議，雙方同意先本誠信原則磋商之，如磋商未果須進行訴訟時，本公司同意以臺灣士林地方法院為第一審管轄法院。

第十一條、本承諾書正本由查驗中心留存。

此致

財團法人醫藥品查驗中心

公司：

負責人：

中華民國　　年　　月　　日

財團法人醫藥品查驗中心 保密承諾暨個人資料提供同意書

附件 2

茲緣於本人受僱承辦財團法人醫藥品查驗中心（以下簡稱查驗中心）專案，因業務往來需要得以接觸、取得、知悉查驗中心機密檔案。為保持所知悉或交付檔案之安全性，本人同意遵守「國家機密保護法」與「營業秘密法」。並簽署本承諾書，恪遵下列事項：

第一條、 本承諾書所稱之「檔案」，係指一切尚未公開之文件或任何其他形式之記錄、複製品或儲存媒體等相關內容，包括但不限於書面、圖書、錄音、錄影、電磁紀錄等。

第二條、 本承諾書所稱之機密檔案係指明文標示為「密」、「機密」、「極機密」或其他同義字之一切機密，或雖未標示但依一般法律觀念，應視為機密之物品、文件及資料等。但下述情形不在此限：

一、 已有書面證據證明交付或告知之檔案為本人所已知。

二、 已見於公開發行之刊物或出版品等欠缺機密性質之檔案。

三、 因政府、法院命令或相關法規範等要求必須揭露者。

第三條、 本人應負善良管理人之注意義務維護查驗中心之機密檔案，非經查驗中心書面同意，絕不故意、過失洩漏、告知、移轉或以任何方式使任何第三人知悉、持有、利用之。

第四條、 本人瞭解並同意凡利用查驗中心電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線電信，包括但不限網際網路等通訊封包，將依網路通訊監測管理規定進行管理。

第五條、 若違反本承諾書之約定或有任何因可歸責於本人之事由，以各種方式致機密檔案被洩露者，本人應依法負相關法律責任及損害賠償責任外。

第六條、 本承諾書於本人在專案契約期限內及其相關完成驗收後二年內均屬有效。

第七條、 非因本人因素造成，當該等機密檔案對外公開或解除其機密性時，同時解除本人對該等機密檔案之保密責任。

第八條、 本人同意查驗中心依個人資料保護法第 8 條第 2 項及第 19 條第 1 項之規定，基於其所負法定義務，於業務上有緊急狀況應變聯繫之需求，蒐集本人之姓名、職業、聯絡方式，做為建置通訊錄之用。

第九條、 本承諾書之條款，如部分無效或無法執行，不影響其他條款之效力。

第十條、 關於本承諾書引起之爭議，雙方同意先本誠信原則磋商之，如磋商未果須進行訴訟時，本人同意以臺灣士林地方法院為第一審管轄法院。

第十一條、 本承諾書正本由查驗中心留存。

此致

財團法人醫藥品查驗中心

個人簽名　　：

身分證字號　：

戶籍地址　　：

中華民國　　年　　月　　日

附件 3

財團法人醫藥品查驗中心

委外廠商資訊安全承諾書

【再生製劑臨床試驗 AI 法規諮詢採購案】

財團法人醫藥品查驗中心 （以下簡稱甲方）

立契約書人

○○○○○○○○○公司 （以下簡稱乙方）

茲因甲方向乙方採購【再生製劑臨床試驗 AI 法規諮詢】採購案，除採購相關文件外，因資訊安全管理要求，經雙方同意簽訂契約條款如下：

第一條、履約標的

(一)、 標的名稱：【再生製劑臨床試驗 AI 法規諮詢】採購案，契約編號：

(二)、 採購內容需求說明：詳如契約「需求規格說明書」及資訊委外共同說明書。

(三)、 乙方應依據採購內容需求，提供必要系統文件。文件內容至少可包括作業系統、應用程式伺服器、資料庫、開發語言與函式庫等資訊，以確保系統具備可更新與可維護性。

(四)、 契約期間：自決標日至 115 年 12 月 31 日。

第二條、教育訓練或維護服務

(一)、 乙方應提供管理或使用人員交付內容有關安全性之教育訓練，共__次，每次__小時。

(二)、 乙方應有到場支援或其他支援方式：本案以遠端連線或到場支援方式進行。

第三條、資訊安全管理要求

(一)、 乙方須遵守甲方以書面或口頭告知之資訊安全管理要求，並配合辦理相關事項以落實甲方資訊安全管理政策。

(二)、 資安法規

1. 乙方應配合甲方之資安政策、保密規定，遵循個人資料保護法與資通安全管理法相關法規，並簽署附錄 1 委外廠商保密承諾書、附錄 2 保密承諾暨個人資料提供同意書。
2. 乙方應遵循行政院公共工程委員會訂定之「採購契約範本附記條款特別聲明」(如附錄 6)，並簽署該聲明所附「使用資通訊產品禁制事項同意書/切結書」。
3. 乙方因執行本契約業務而違反個資法，致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。
4. 若交付項目係以行動應用程式（APP）為主，須配合「行政院及所屬各機關行動化服務發展作業原則」，並通過經濟部訂定之行動應用檢測基準之檢測。
5. 若交付項目為物聯網相關設備，應考量物聯網資安認驗要求，優先提供具有認證或受驗證之設備。

(三)、 帳戶安全

1. 乙方應協助甲方進行預設帳號與密碼之變更，並於適當時移除乙方使用帳戶或權限。

(四)、 網路管理

1. 系統或設備於建置或維護時，應關閉不必要連接埠或網路介面。必要時，應考量安全性，協助甲方變更預設連接埠或連線方式。
2. 乙方若採用遠端連線或到場維護，應先告知甲方並通過申請，方可進行作業處理。

(五)、 金鑰管理

1. 網站憑證或系統金鑰，應提供與告知金鑰產製、使用、保管、撤銷與效期等資訊。
2. 憑證協定應支援公認安全版本以上之版本，並關閉舊版之協定或技術使用。

(六)、 系統管理

1. 乙方應確保本專案之系統、網站應用程式及主機絕無任何形式之後門或漏洞，避免危害資通安全。
2. 配合甲方資安相關措施發現需改善之系統漏洞，應配合於契約有效期內提出改善計畫，並雙方議定後進行修補改正。若甲方進行資訊安全演練、入侵偵測、弱點掃瞄或其他安全檢測方式後，如發現需改善之系統漏洞，乙方應配合於契約有效期內提出改善計畫，並於雙方議定後進行修補改正，如資安弱點修補或改善超出本契約實際範圍，經雙方協議得酌收費用。
3. 乙方應協助甲方進行系統或設備之校時，並確保可提供持續的正確校時機制。
4. 乙方執行更新作業前，應提供「系統更新與錯誤回復計畫」，並於雙方同意後始得進行。

(七)、 營運作業

1. 乙方人員未經授權禁止輸入任何干擾程式或探取、損壞、消除、竊閱、洩漏甲方輸入資料。如有上列情形，願負一切法律上之責任。
2. 乙方應提供資料庫、電子檔案、系統程式碼、系統設定或日誌之備份或設置方法等管控措施說明，並於教育訓練過程說明與教學。
3. 乙方應配合甲方定期業務持續運作演練，提供短期必要技術文件或支援，確保演練時系統中斷或災害發生時之應對處理。

(八)、 事件事故

1. 乙方發現資通安全事件時，須依資通安全管理法子法「資通安全事件通報及應變辦法」與甲方資通安全事件通報及應變管理程序及相關資安規定所訂時限及方式進行通報、應變及處理。
2. 當系統發生重大事故、中斷、錯誤無法運行，或系統無法復原之情境，乙方應協助或支援備援資料還原或系統重新上線。
3. 乙方應提供緊急危難時之諮詢聯絡窗口，提供甲方於緊急且必要時可供聯絡。
4. 系統無法運作之緊急狀況時，乙方接獲通知應依需求規格說明書要求之時限內，提出回覆處理或排除錯誤方式。

第四條、系統開發管理要求

(一)、 乙方應於系統開發生命週期考量資訊安全，並確保於各階段有風險控管與安全機制。應視專案系統性質，參考行政院國家資通安全會報技術服務中心之共同規範，如「Web 應用程式安全參考指引與實作手冊」規劃適當安全機制或功能，並於開發過程確實測試各項安全機制或功能，以確保系統安全品質。

(二)、 乙方應具備軟體安全開發管理或資訊安全管理相關證照或證書，以確保開發人員在開

發過程對資訊之保護與管理安全情形。

(三)、 若因採購案有提出需求，乙方應提供程式原始碼及系統相關操作、說明文件，日後若系統升級或新增功能，乙方需主動提供系統變更的文件說明。

(四)、 乙方應對系統設置有輸入查驗（Input Validation）功能，並對使用者輸入資料之長度、型態、特殊字元及特殊指令等特殊指令等，確實加以過濾與處理。

第五條、安全驗收及文件交付

(一)、 乙方於測試與正式建置時，應提供計劃書與相關文件，並確保建置安全，包含如以下核選項目：(■為應提供項目)

(一) ■測試建置計畫書

(二) ■系統安全建議書：依採購系統規格架構，須至少考慮實體、軟體與資料安全等要求，提供相應安全設置規劃建議。

(二)、 乙方於交付時應提供系統文件與資安檢測報告，以確保系統安全，包含如以下核選項目：(■為應提供項目)

(一) ■弱點掃瞄報告：自行或第三方驗證之弱點檢測結果，並且無中風險等級（含）以上項目。

(二) ■網站效能檢測：提供滿足採購需求之效能測試結果。

(三) ■系統架構圖：足以說明系統建置架構之文件。

(四) ■系統建置手冊：足以在緊急或無人支援時，可進行基本系統重新建置或還原。

(五) ■系統管理手冊：管理者相關功能說明手冊

(六) ■系統操作手冊：使用者相關功能手冊

(七) ■程式原始碼：提供上線正式版，並須提供相關函式庫或相依套件等，足以重新建置運行之相關檔案。

(八) ■資料庫 Schema：提供上線正式版，包含資料表名稱、欄位名稱、欄位描述、欄位類型、長度、允許空值等。

(九) ■系統安全需求項目檢核表：按甲方提供之「系統安全需求項目檢核表」(參閱附錄4）回覆檢核結果，主要確認系統安全設計是否具備。

(十) ■委外廠商資安自主管理檢核表：廠商得以其他公認之認證文件提供，如 ISO 資安標準或 CMMI 等相關認證；或依甲方提供之「委外廠商資訊安全管理檢核表」(參閱附錄5）回覆檢核結果，確認乙方在資安管理之完善。

(三)、 乙方於維護或更新時，應提供系統文件與資安檢測報告，以確保系統維運之安全，包含如以下核選項目：(■為應提供項目)

(一) ■定期維護報告：定期維護依需求規格說明書內容進行維護作業，並以電子檔案或書面紙本方式提供現況資訊。可包含如：維護或變更紀錄、異常登入登出紀錄、異常權限變更情形、異常管理者活動、異常系統參數變更、資料存取失敗紀錄與相關系統設備硬體運作統計資訊。

第六條、權利及責任

(一)、 乙方所提供或使用之軟體、文件或圖片需合法並提供使用授權，不得違反智慧財產權行為，如有違反智慧財產權者，乙方應承擔所有法律責任。

(二)、 乙方履約結果涉及智慧財產權者，著作財產權歸甲方所有，乙方對甲方不行使著作人

格權。

(三)、　乙方公司與相關人員（包含到場與線上支援人員），應據實簽署「委外廠商保密承諾書」與「保密承諾暨個人資料提供同意書」。

(四)、　甲方提供一切機敏性資料、文件等均屬甲方之資產，約定期間或雙方無法合作、或技術移轉時，乙方應依甲方要求，無條件將所持有之原本交還，複製之機敏文件、資料、媒體應予銷毀。

(五)、　乙方派駐修人員發生嚴重不當行為違反相關資安政策，須立即暫停職務、存取權限與特權，必要時立即將其護送離開甲方場域。

(六)、　乙方派駐修人員違反相關資安政策，依契約相關罰則進行處置，如情節造成重大資安事件達「資通安全事件通報及應變辦法」等級 3 以上，甲方將立即終止及解除契約，並自負違反法律之責。

(七)、　甲方保有甲方及與第三方稽核單位或人員至乙方進行專案相關工作之執行、資料之處理及執行之紀錄，進行實地現場訪視或調閱資料之稽核權利，乙方應於契約時間內配合完成相關稽核要求改善事項。

第七條、違約及績效違約罰則

(一)、　乙方經評核未達所定服務水準及績效時，依評估結果按採購契約罰則處理。

(二)、　乙方若有違反前述安全要求事項，依違反情節嚴重程度，進行處罰或法律行動。

第八條、本承諾書書一式三份，由甲方留執二份、乙方留執乙份為憑。

立契約書人

甲　　方：財團法人醫藥品查驗中心

代 表 人：姜至剛

地　　址：臺北市南港區忠孝東路六段 465 號 3 樓

聯絡電話：（02）8170-6000

乙　　方：○○○○○○○○○公司

代 表 人：○○○

地　　址：○○○○○○○○○

聯絡電話：○○○○○○○○○

中　華　民　國　　年　　月　　日

財團法人醫藥品查驗中心系統安全需求項目檢核表

附件 4

No.	安全特性	安全需求項目	是	否	不適用
1-1	機密性	機敏資料傳輸時，採用加密機制	□	□	□
1-2		使用公開、國際機構驗證且未遭破解的演算法	□	□	□
1-3		使用演算法支援的最大長度金鑰	□	□	□
1-4		加密金鑰或憑證週期性更換	□	□	□
1-5		加密金鑰不與加密資料存放於同一系統中，並對於加密金鑰的存取進行限制	□	□	□
1-6		機敏資料儲存時，採用加密機制	□	□	□
2-1	完整性	於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性	□	□	□
2-2		針對開放下載的資料，也提供資料之雜湊值(HASH Value)供使用者比對其完整性	□	□	□
2-3		具有防範 SQL 命令注入攻擊(SQL Injection)之措施	□	□	□
2-4		具有防範跨站腳本攻擊(Cross-Site Scripting)之措施	□	□	□
2-5		驗證網頁重導(Redirects)與導向(Forwards)之目的地在合法名單內	□	□	□
2-6		重要系統資料或紀錄留存雜湊值以確保完整性	□	□	□
3-1	可用性	重要資料定時同步至備份或備援環境，並加以保護限制存取	□	□	□
3-2		採用「高可用性」(High Availability) 架構(分散式或叢集伺服器架構)	□	□	□
4-1	身分驗證	除了允許匿名存取的功能外，所有功能都必須已通過身分驗證才允許存取	□	□	□
4-2		身分驗證機制位於伺服器端且採用集中過濾機制(例如使用 Filter 過濾器)	□	□	□
4-3		身分驗證相關資訊(帳號、密碼等)不留存於程式原始碼中	□	□	□
4-4		確實規範使用者密碼強度（密碼長度12個字元以上、包含英文大小寫、數字，以及特殊字元）	□	□	□
4-5		使用者必須定期更換密碼，且至少不可以與前5次使用過之密碼相同	□	□	□
4-6		具備帳戶鎖定機制，帳號登入進行身分驗證失敗達3次後，至少30分鐘內不允許該帳號及來源 IP 繼續嘗試登入	□	□	□
4-7		身分驗證相關資訊不以明文傳輸	□	□	□
4-8		密碼添加亂數(Salt)進行雜湊函式(HASH Function)	□	□	□

No.	安全特性	安全需求項目	是	否	不適用
		處理後，分別儲存亂數及雜湊後密碼			
4-9		採用圖形驗證碼(CAPTCHA)機制於身分驗證及重要交易行為，以防範自動化程式之嘗試	□	□	□
4-10		重要交易行為要求使用者再次進行身分驗證	□	□	□
4-11		採用多重因素身分驗證(兩種以上驗證類型)	□	□	□
4-12		密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性令牌(Token)，檢查傳回令牌有效性後，才允許使用者進行重設密碼動作	□	□	□
5-1	授權與存取控制	執行功能及存取資源前，檢查使用者授權	□	□	□
5-2		採用伺服端的集中過濾機制檢查使用者授權	□	□	□
5-3		對使用者/角色，僅賦予所需要的最低權限	□	□	□
5-4		軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限執行	□	□	□
5-5		除特殊管理者權限外，其他角色或權限無法修改系統中授權資料及存取控制列表(ACL)	□	□	□
5-6		重要行為由多人/角色授權後才得以進行	□	□	□
5-7		具有防範「跨站請求偽造」(Cross-Site Request Forgery，CSRF)攻擊之措施	□	□	□
6-1	日誌紀錄	針對身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行日誌記錄	□	□	□
6-2		日誌紀錄包含以下項目1.識別使用者之 ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型或等級(priority)。5.事件描述	□	□	□
6-3		採用單一的日誌紀錄機制，確保輸出格式的一致性	□	□	□
6-4		對日誌紀錄進行適當保護及備份，避免未經授權存取	□	□	□
7-1	會談管理	使用者的會談階段，設定該帳號在合理的時間(至多30分鐘)內未活動即自動失效	□	□	□
7-2		使用者的會談階段在登出後失效	□	□	□
7-3		會談識別碼(Session ID)或使用者 ID 避免顯示於使用者可以改寫處(例如網址列)	□	□	□
7-4		會談識別碼(Session ID)採亂數隨機產生且不可預測	□	□	□
7-5		使用者登入後，重新賦予會談識別碼(Session ID)	□	□	□
8-1	錯誤及例外處理	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息	□	□	□
8-2		所有功能皆進行錯誤及例外處理，並確保將資源正確釋放	□	□	□
8-3		具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)	□	□	□

No.	安全特性	安全需求項目	是	否	不適用
9-1	組態管理	管理者介面限制存取來源或不允許遠端存取	□	□	□
9-2		作業平臺定期更新並關閉不必要服務及埠口(Port)	□	□	□
9-3		系統依賴的外部元件或軟體，不使用預設密碼	□	□	□
9-4		參數設定或系統設定存放處，限制存取或進行適當保護	□	□	□
9-5		針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新	□	□	□

檢核不符合事項說明表

不符合 項目編號	填寫日期	原因說明	主管確認

是否允以結案？ □ 單位主管核章：_____

財團法人醫藥品查驗中心委外廠商稽核查檢自評表

附件 5

<table>
<tr><td>受稽廠商名稱</td><td colspan="2"></td><td>受稽廠商代表</td><td></td></tr>
<tr><td>受稽廠商
聯絡人</td><td colspan="4">姓名：
職稱：
電話：
Email：</td></tr>
<tr><td>資訊安全管理系統(ISMS)實施情形</td><td colspan="4">○已驗證；驗證標準名稱：
最近一次通過驗證稽核時間：
○已導入；導入標準名稱：
最近一次更新管理文件時間：
○未導入或驗證</td></tr>
<tr><td rowspan="6">承作本中心所有委外案名
(表格列數請自行增刪)</td><td>項次</td><td>採購案名稱</td><td colspan="2">本專案配置之資通安全專業人員
(經適當之資格訓練、擁有資通安全業證照或具有類似業務經驗者)</td></tr>
<tr><td>1</td><td>ＯＯＯ</td><td colspan="2">姓名：
職稱：
證書名稱：</td></tr>
<tr><td>2</td><td></td><td colspan="2"></td></tr>
<tr><td>3</td><td></td><td colspan="2"></td></tr>
<tr><td>4</td><td></td><td colspan="2"></td></tr>
<tr><td>5</td><td></td><td colspan="2"></td></tr>
</table>

查核項目	查核內容	評估結果			說明 需提供佐證文件
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1 是否定義符合組織需要之資通安全政策及目標？	□	□	□	資通安全政策及目標 核准人員職稱： 文件名稱： 發佈日期：
	1.2 組織是否訂定資通安全政策及目標？	□	□	□	
	1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	轉知所有同仁佐證
	1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	管理審查會議日期： 會議紀錄(記載相關審查/調整佐證)
	1.5 是否隨時公告資通安全相關訊息？	□	□	□	公告日期： 公告訊息
2.設置資通安全推動組織	2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	資安長(單位+職稱)：
	2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	資安組織之章程或工作說明書等文件
	2.3 是否訂定組織之資通安全責任分工？	□	□	□	
3.配置適當之資通安全專業人員及適當之資源	3.1 是否訂定人員之安全評估措施？	□	□	□	說明人員進用之安全評估措施。
	3.2 是否符合組織之需求配置專業資安人力？	□	□	□	資安人員共____人。 具備證照：
	3.3 是否具備相關專業資安證照或認證？	□	□	□	
	3.4 是否配置適當之資源？	□	□	□	說明資安預算/資訊設備(軟硬體)/教育訓練(人員)之各類規劃(計畫/專案)。
4.資訊及資通系統之盤點及風險評估	4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	盤點資訊及資通系統資產日期： 資產筆數：

查核項目	查核內容	評估結果			說明 需提供佐證文件
		符合	不符合	不適用	
	4.2 各項資產是否有明確之管理者及使用者？	□	□	□	列舉本中心專案有關之資產並述明管理者及使用者(至少3項)
	4.3 是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	文件名稱： 發佈日期：
	4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	□	□	□	例：風險評鑑報告、風險處理計畫、管理審查會議紀錄。
5.資通安全管理措施之實施情況	5.1 人員進入重要實體區域是否訂有安全控制措施？	□	□	□	說明公司機房或大門之門禁管制措施或進出管制之規範文件名稱及發佈日期。
	5.2 重要實體區域的進出權利是否定期審查並更新？	□	□	□	最近1次門禁進出權限之審核日期： 審核筆數：
	5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	□	□	說明門禁管理規定
	5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	□	□	□	機房環控系統截圖證明
	5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	□	□	□	消防安全設備檢查紀錄 消防安全設備使用訓練紀錄
	5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	□	□	說明門禁管理之授權或監視作法。
	5.7 重要資訊處理設施是否有特別保護機制？ 防毒、定期掃毒(一個月一次)	□	□	□	說明開發環境主機之保護機制。

查核項目	查核內容	評估結果			說明 需提供佐證文件
		符合	不符合	不適用	
	5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？ 靠近梁柱的位置，有裝不斷電(半小時)。	□	□	□	開發環境主機設置地點：
	5.9 電源之供應及備援電源是否作安全上考量？	□	□	□	機房或開發環境是否設置備用電源(例:UPS)
	5.10 通訊線路及電纜線是否作安全保護措施？	□	□	□	通訊線路與電纜線定期檢修或抽換紀錄。
	5.11 設備是否定期維護，以確保其可用性及完整性？ 機房每個月巡檢一次/異常處理	□	□	□	開發環境主機定期維護紀錄
	5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	□	□	□	訂有場外維修保護措施之SOP/規範/程序/辦法文件名稱及發佈日期。
	5.13 可攜式的電腦設備是否訂有嚴謹的保護措施（如設通行密碼、檔案加密、專人看管）？	□	□	□	訂有可攜式電腦設備(例:USB、平板、手機、硬碟)保護措施之SOP/規範/程序/辦法文件名稱及發佈日期。
	5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	說明設備報廢前之資料清除方式。(例：消磁、覆寫等)
	5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	訂有相關妥為存放/收存之SOP/規範/程序/辦法文件名稱及發佈日期。
	5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	說明系統開發及測試主機位置。
	5.17 是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	開發環境主機更新病毒碼佐證紀錄。
	5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	開發環境主機病毒掃瞄佐證紀錄。
	5.19 是否定期執行各項系統漏洞修補程式？	□	□	□	最近1次漏洞修補執行時間： 修補說明：

查核項目	查核內容	評估結果			說明 需提供佐證文件
		符合	不符合	不適用	
	5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體（含病毒、木馬或後門等程式）？	□	□	□	訂有電子郵件附件及下載檔案之管理規範、規定、辦法文件名稱及發佈日期。
	5.21 重要的資料及軟體是否定期作備份處理？	□	□	□	原始碼、專案文件備份紀錄。
	5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	備份資料測試紀錄。
	5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	訂有機敏資訊傳送保護措施之管理規範、規定、辦法文件名稱及發佈日期。
	5.24 是否訂定可攜式媒體（磁帶、磁片、光碟片、隨身碟及報表等）管理程序？	□	□	□	訂有可攜式媒體之管理程序、管理規範、規定、辦法文件名稱及發佈日期。
	5.25 是否訂定用者存取權限註冊及註銷之作業程序？	□	□	□	訂有使用者存取權限註冊及註銷之作業程序、管理規範、規定、辦法文件名稱及發佈日期。
	5.26 使用者存取權限是否定期檢查（建議每六個月一次）或在權限變更後立即複檢？	□	□	□	開發環境使用者帳號權限清查紀錄。
	5.27 通行碼長度是否超過 6 個字元（建議以 8 位或以上為宜）？	□	□	□	訂有通行碼符合規定之管理規範、規定、辦法文件名稱及發佈日期。
	5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	
	5.29 是否依網路型態（Internet、Intranet、Extranet） 訂定適當的存取權限管理方式？	□	□	□	訂有網路或防火牆管理之管理規範、規定、辦法文件名稱及發佈日期。
	5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	□	□	□	
	5.31 是否訂定行動式電腦設備之管理政策（如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求）？	□	□	□	訂有行動式電腦設備(筆電)之管理規範、規定、辦法文件名稱及發佈日期。
	5.32 重要系統是否使用憑證作為身份認證？	□	□	□	說明開發環境主機身份認證機制。
	5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	□	□	□	最近1次系統變更之相關紀錄文件(變更單、測試報告、版更紀錄等文件)

查核項目	查核內容	評估結果			說明
		符合	不符合	不適用	需提供佐證文件
	5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	□	□	□	最近1次本中心專案系統弱點掃描及修補紀錄。
	5.35是否使用大陸廠牌之資通訊產品?	□	□	□	請說明本中心專案範圍是否使用大陸廠牌之資通訊產品。
	5.36專案人員是否有大陸籍人士？	□	□	□	請說明專案人員國籍
6.訂定資通安全事件通報及應變之程序及機制	6.1 是否建立資通安全事件發生之通報應變程序？	□	□	□	文件名稱： 發佈日期：
	6.2 同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	□	□	□	宣導佐證(例:公告、電子郵件、教育訓練等)
	6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	□	□	□	資通安全事件處理之紀錄文件
7.定期辦理資通安全認知宣導及教育訓練	7.1 是否定期辦理資通安全認知宣導？	□	□	□	宣導佐證(例:公告、電子郵件、教育訓練等)
	7.2 是否對同仁進行資安評量？	□	□	□	最近1次評量主題： 最近1次評量日期：
	7.3 同仁是否依層級定期舉辦資通安全教育訓練？	□	□	□	教育訓練紀錄
	7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	□	□	□	說明確效方式
8.資通安全維護計畫實施情形之精進改善與績效管考	8.1 是否設有稽核機制？	□	□	□	文件名稱： 發佈日期：
	8.2 是否定有年度稽核計畫並且定期執行？	□	□	□	最近1次稽核日期： 稽核缺失改善紀錄
	8.4 是否改正稽核之缺失並追蹤過去缺失之改善情形？	□	□	□	
	8.5是否訂定安全維護計畫持續改善機制？定期召開持續改善之管理審查會議？	□	□	□	訂定持續改善措施之規範、規定、辦法文件名稱： 發佈日期：

附件 6

採購契約範本附記條款特別聲明

(114.5.20修正)

一、茲特別聲明，以下附記條款優先於契約條款及投標須知以外其他文件附記條款之適用。

二、契約如約定廠商須於網路廣告平臺刊登廣告者，應遵守以下規範：

（一）廠商禁止於違反詐欺犯罪危害防制條例之網路廣告平臺刊登廣告。

（二）廠商於刊登廣告前，應提報擬刊登廣告之網路廣告平臺及擬刊登內容供機關審查，機關得就擬刊登內容予以審查，如擬刊登平臺違反實名制規定，機關應就本採購案禁止廠商於該平臺刊登廣告(違反實名制規定之網路廣告平臺名單由機關登入政府電子採購網查詢)。

（三）前開違反實名制規定，係指具實名制義務之網路平臺業者違反詐欺犯罪危害防制條例第30條第2項第1款實名制規定：「網路廣告平臺業者應建立下列管理措施：一、對其網路廣告服務，應以數位簽章、快速身分識別機制或其他安全性相當之技術或方式驗證委託刊播者及出資者之身分。」並經數位經濟相關產業主管機關（數位發展部）依同條例第40條第1項第2款令其限期改正。

三、契約如約定廠商須交付書面履約成果者，廠商就本採購案履約時使用資通訊產品之禁制事項：

（一）履約過程及履約標的禁止使用及採購中國大陸廠牌資通訊產品[含軟體、硬體及服務(含生成式 AI 程式如：Deepseek 等)，下同]。

（二）廠商不得向生成式 AI 提供本案涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及本案機敏或個人資料之事項，其經生成式 AI 產製之履約標的及相關文件，廠商應予以標明或揭露。

（三）廠商履約過程及成果需透過使用及採購生成式 AI 以產出履約標的內容或相關文件者，應先徵得機關同意始得為之。

（四）廠商應於得標後以「使用資通訊產品禁制事項同意書/切結書」(如附件)聲明其履約過程及履約標的遵循上述準則。

（五）廠商人員、代理人或使用人如有違反本點或簽署之同意書/切結書者，適用契約本文關於權利及責任條款之違約責任，就機關所受損害負賠償之責；致第三人權利受有損害者，廠商亦應負責。

四、廠商履約有下列情形之一，構成違反其他契約約定之情形，機關得以書面通知廠商終止或解除全部或部分契約：

（一）違反本特別聲明第3點第1款至第3款規定者。

（二）依本特別聲明第3點第5款簽署之同意書/切結書，切結內容不實者。

使用資通訊產品禁制事項同意書/切結書

本廠商＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿履行＿＿財團法人醫藥品查驗中心＿＿辦理之＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿案，已充分瞭解並遵行本特別聲明所定資通訊產品之禁制事項規範，於履約過程及履約標的均無違反前述禁制事項，如有違反，願賠償一切因此所生之損害，並擔負相關民、刑事責任。

立書人

投標廠商：　　（蓋章）

負 責 人：　　（蓋章）

中華民國　　年　　月　　日

附件 7

財團法人醫藥品查驗中心

廠商評審評比表（序位法-評分轉序位法）

採購案號：

採購案名：

日期：　年　月　日

評分 / 廠商名稱 評審項目及配分					
項次	評　選　項　目	配　分	評　分	評　分	評　分
1	團隊專業能力及經驗：計畫主持人及工作成員名單，各人員所任工作，與本案相關之學經歷、專業技術證照、取得與採購案相關認（驗）證、訓練合格證明，有何優良或不良事蹟等情形，是否具備完善之資通安全管理措施或通過第三方驗證、資通安全專業人員配置及經驗、能力證明等情形。	25			
2	執行能力及相關服務主要工作人數及配置、工作計畫、預定進度、承攬經驗、履約能力、如何完整瞭解及配合機關需求、如何如期如質履約之說明、尚在履約相關契約件數、金額及是否有逾期情形。提供維護及諮詢之時間及方式。服務水準及其達成之方法及提供之承諾。軟體不中斷服務之風險管理。期間不另加價之功能更新及增修服務。其他創意及創新（與本採購標的有關，且含於標價內之附加或創新服務）。	25			
3	對本計畫案內容之掌握及資安作為等（含資訊安全及個人資料保護規劃及執行方式、履約相關之資安事件通報、應變、處理之規劃機制）。	20			
4	報價及經費組成內容之合理性分析（含資通安全檢測成本）。	20			
5	廠商企業社會責任（CSR）指標：1.為員工加薪（如近一年內曾替員工普遍性加薪）。2.於投標文件載明後續履約期間給與全職從事本採購案之員工薪資（不含加班費）至少超過勞動部公告最低工資 1.1 倍以上。3.提供員工「工作與生活平衡」措施等。	5			

6	簡報及詢答。	5			
總　　分 (總滿分：　　)					
序　　位					
評審委員簽名：			意見	意見	意見

註：序位評比依下列方式辦理：就各評審項目分別評分並轉換為序位，再加總計算各廠商之序位數。

附件 8

財團法人醫藥品查驗中心
廠商評審評比總表 (序位法-評分轉序位法)

採購案號：

採購案名：

日期： 年 月 日

廠商名稱 / 標價 / 評分 / 序位 / 出席評審委員										
	評分	序位	評分	序位	評分	序位	評分	序位	評分	序位
A 委員										
B 委員										
C 委員										
D 委員										
E 委員										
F 委員										
G 委員										
序位合計數										
總評分/總平均分數										
是否達合格分數										
優勝廠商序位 (全部出席評審委員綜合考量及過半數決議)										
其他記事（詳會議紀錄）	1. 出席委員辦理廠商評審已就各評審項目、受評廠商資料及工作小組初審意見，逐項討論後為之。 2. 經確認本委員會或個別委員評審結果與工作小組初審意見有無差異及其處置方式。 3.經確認不同出席委員評審結果有無明顯差異及其處置方式。									

出席委員簽名								
	姓名							
	職業							
	姓名			請假委員	姓名			
	職業				職業			

註：受評廠商之總評分平均分數未達合格分數 70 分者，不得為優勝廠商。

財團法人醫藥品查驗中心
Taiwan Center For Drug Evaluation

財團法人醫藥品查驗中心

資訊委外共同說明書

目錄

壹、 前言

一、說明書圖例說明

✧ 以“□” 符號表示該項條文不適用

✧ 以“☑” 符號表示該項條文適用

✧ 無“□”及“☑”符號表示該項條文適用

✧ 字元以紅色字體表示本中心承辦人員需特別注意事項，如：「專案標的」

✧ 字元以網底表示廠商需特別注意事項，如：「會議中報告」

✧ 字元以黑色底線表示罰責說明，如：「違反本條任何所述者視同」

二、概述

本中心為配合政府資訊委外服務政策，將資訊服務委託民間辦理。為使本中心之委外專案能在符合資訊安全政策之前提下達成本中心之目標，特訂定此說明書，以期本中心所有資訊委外專案具有良好且一致之服務水準；資訊委外專案須考量是否為核心系統或第三方驗證範圍系統、是否涉及機密性或敏感性資料、系統是否對外部人員開放使用等，評估是否引用本說明書及調整適用條文。

三、適用性聲明

（一）資訊委外含概委託管理、委託建置及委託民間興建營運後轉移(Build-Operate-Transfer, BOT)之資通訊系統或關鍵資訊基礎設施。

（二）本文件屬於本中心資訊委外之通用性規範，除需求規格說明書另有規定者外，適用本說明書。

（三）需求規格說明書優於資訊委外共同說明書內之其他文件所附記之條款。但附記之條款有特別聲明者，不在此限。

（四）各專案須就各系統之特性，於需求規格說明書或契約本文載明下列事項，以明確定義適用範圍。

1. 專案標的(計畫執行工作內容)
2. 履約期限
3. 現況說明(如系統軟硬體架構、開發工具、系統功能、程式大約總支數或程式清單、資料筆數或占用空間)
4. 專案人員組成
5. 是否提供駐點人員或專線服務電話(5Ｘ8)
6. 新增及擴充需求
7. 資通安全與資料保護需求
8. 服務水準管理要求

9. 教育訓練需求

10. 應交付文件

11. 未來每年維護費占建置費比例(適用資訊系統建置案)

12. 滿意度調查結果報告是否列為交付文件

（五）本說明書所列附表之格式及內容僅為參考範本，本中心承辦人員得視實際需要進行修訂。

四、服務時限需求

（一）專案啟動會議：廠商須於**決標日次日**起 30 個日曆天內召開。

（二）專案工作計畫書：**自啟動會議**起 30 個日曆天內提交。

（三）☑資通系統異動維護變更申請單

1. ☑應用系統

(1) 系統資料維護：7 個日曆天完成。

(2) 系統資料下載：7 個日曆天完成。

(3) 系統程式錯誤維護：7 個日曆天完成。

(4) 系統功能錯誤維護：7 個日曆天完成。

(5) 其他：依雙方議定時程辦理完成。

2. □硬體維護

(1) A 級硬體維護：

A、本中心日常運作中之系統所使用設備屬本案維護標的者，若故障導致系統無法正常運作時，廠商須於接獲通知後 4 小時(日曆天)內恢復設備正常運作(含 OS 安裝、列印及網路)。

B、本案維護標的故障，惟所屬系統尚可運作(例如具有 Redundancy or HA 等機制)或非屬本中心日常運作系統，廠商須於接獲通知後 1 個日曆天內恢復設備正常運作(含 OS 安裝及列印)。

(2) B 級硬體維護：本中心通知廠商後，2 個日曆天內恢復設備正常運作(含 OS 安裝及列印)。

(3) 其他：本中心通知廠商後，3 個日曆天內恢復設備正常運作。

（四）☑系統維護之變更及新增管理：於 1 個月內完成需求訪談及確認並於需求確認後 1 個月內完成(含測試完成)，系統開發步驟請參考『系統開發流程』。

（五）契約中規範之事項，如未敘明完成時限，廠商以『資訊系統維護服務單』配合辦理。

（六）上述規範，違反本條任何所述者，以陸、一、(一)、『未依規定時間

完成工作計罰』規定計罰。如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

貳、 專案管理

一、專案執行計畫

(一) 工作計畫管理

廠商須以書面方式提交『專案工作計畫書』，內容請參考「文件及版本管制需求」之「文件製作規範」，作為雙方運作之依據，並於『專案啟動會議』或『工作小組』會議中通過，違反本條任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

二、廠商專案小組成員資格及工作內容

(一) 專案經理 (專案負責人)

1. 須具有管理系統、協調整合專案實績經驗。
2. 具備專案經理、☑分析師、☑設計師相關經驗。
3. 掌握專案進行情形。
4. 負責管理駐點人員相關事宜。
5. 出席專案會議。
6. □通過本中心需求規格說明書條文測驗及格。
7. 明瞭本中心駐點人員會議紀錄內容，並負責督促執行會議決議事項。

(二) □專案監控人員

1. 分析業務資料流之情形，並提供監視作業處理流程。
2. 監看資料流運作情形，並依本中心要求提供報表。
3. 配合本中心需求，至指定地點工作。

(三) ☑系統分析師

1、具備系統之需求分析與設計能力並具相關經驗。

2、須配合本中心需求，至指定地點工作。

(四) ☑程式設計師暨資料庫管理師

1、負責開發程式及維護系統。

2、須配合本中心需求，至指定地點工作。

(五) □資安技術師

1、國際電腦稽核師(CISA)證照或

2、國際資訊安全管理師（CISSP）證照或

3、認證道德駭客（CEH）證照。

（六）□管理顧問師

1、具備管理系統主任稽核員證照並具相關經驗。

2、ECSA Foundation 或 CSA CCSK 證照。

3、配合本中心需求，至指定地點工作。

（七）□主管理顧問師

1、具備管理系統主任稽核員證照並具相關經驗。

2、稽核輔導實稽經驗 5 年以上擔任主管理顧問師。

3、ECSA Foundation 或 CSA CCSK 證照。

4、配合本中心需求，至指定地點工作。

（八）資通安全專業人員

1. 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。

2. 負責資安相關文件之審核與簽署。

（九）☑文件及品質管理師，開會及測試會議須到場。

（十）□駐點人員

1. 人員選任

(1) □由廠商提供至少 5 倍候選名單，經本中心工作小組覆篩通過。

(2) 試用期為 1 個月，若未通過試用，則需重新指派。違反本條任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

(3) 須為大學畢業或曾於本中心服務表現良好者，本中心得要求廠商於每季報驗資料中提供相關證明。

(4) □具備資訊安全或網路安全相關實務資歷。

(5) 駐點人員中斷期間，廠商須於 1 個月內依契約規範找到駐點人員，期間廠商應先行派人代理職務。

2. 差假規定

(1) 駐點期間為全天之工作時間，上班日依行政院人事行政總處公告為準；每日上班為 8 小時(不含午休時間) ；上班時間□9 時

至 18 時或□工作滿 8 小時(不含午休時間)或☑依本中心彈性上下班規範，上下班時須刷卡，代理人員亦同；如忘記刷卡或遲到每月不得超過 1 次。超過 1 次以上時，專案經理〈專案負責人〉了解其原因後提出說明，並自第 2 次起陪同駐點人員於駐點期間到場駐點，每超過 1 次陪同駐點 1 天。

(2) 遇履約標的發生異常之狀況，如可歸咎於廠商，須配合本中心員工延長工時，本中心不另計加班費用；如不可歸咎於廠商，本中心得予加班補休，本中心不另計加班費用。

(3) 駐點人員請假，本中心專案負責人同意後方可請假。

(4) 駐點人員請假，廠商須另派人員代理職務；請假原因為病假或意外事故等不可抗拒之因素，廠商須於 2 小時內派人代理。

(5) 請假原因為加班補休或配合本中心活動給予公假時，廠商不須派員代理職務，但需本中心專案負責人同意。

(6) 違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

3. 工作內容

(1) 駐點人員須於本中心指定日期、指定地點執行有關履約標的或本中心指定之服務事項，其必要☑ OA 電腦或☑特殊工具軟體廠商須自行準備，並簽結本中心資安規範相關管理文件，且納入本中心資安相關規範管理。

(2) 駐點人員工作由本中心駐點所在地職員安排及管理，如遇駐點人員無法依限期處理解決問題時，廠商應即增派人員支援。

4. 教育訓練

本中心得要求廠商安排教育訓練計畫，以提升駐點人員專業能力，駐點人員應於工作小組會議進行心得報告。

三、專案小組成員審核及更換

（一）廠商應於本案『專案啟動會議』或『工作小組』會議中提出符合本案『專案小組』之人員，且須提出證明文件如勞保及公司證明文件、學歷及相關專長訓練證明文件，並提交『專案啟動會議』或『工作小組』會議同意後，負責處理與本中心聯繫及執行本專案之事宜。

（二）廠商所指派之專案小組人員如須更換，應於『工作小組』會議同意

後，始得更換；廠商之專案小組成員對於所應履約之工作有不適任之情形者，本中心得經『工作小組』會議決議要求廠商更換，且廠商應於收到通知後1個月內更換，不得拒絕。

（三）廠商於專案期間內專案人員異動時，新進成員應簽立『保密承諾暨個人資料提供同意書』，退離成員應對專案期間取得本中心資料進行銷毀或移轉。

（四）專案期間違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先mail『工作小組』成員並經半數(含)以上成員同意。

四、專案監控

（一）本中心為使專案順利進行且具一定之服務水準，依專案進行之需要，得召開不同型式之會議，對專案進行監控，以期可順利達成專案之目的；工作小組之組成，由本中心主導。

（二）會議種類

1. ☑專案啟動會議

廠商須召開「專案啟動會議」，報告專案之規劃。

2. ☑專案工作小組會議

(1) 廠商需於簽約後定期配合本中心時程召開，原則上以每月為週期，頻率可由『工作小組』會議決議後調整。

(2) 會議之目的在檢驗本專案執行狀況，明定未確定之作業規範，解決發生之問題，討論雙方應配合及協調事項。

3. 技術討論會議

(1) ☑本專案進行期間，本中心得視需要針對系統發生之問題要求廠商進行專題報告。

(2) ☑廠商需於得標後配合本中心召開全部廠商技術討論會，討論共同議題。

4. 進度管控會議

本專案進行期間，專案進度落後或待解決事項非本中心預期，本中心得不定期召開進度管控會議，會議之目的在即時協商及盡速解決問題，使本專案執行狀況達專案計畫之要求。

（三）會議規範

1. 適用會議種類：專案啟動會議、專案工作小組會議

2. 會議前準備工作

(1) 廠商參加人員須包含①專案經理、②文件及品質管理師、③□駐點人員 ④□管理顧問師 ⑤□主管理顧問師及相關必要人員。

(2) ☑廠商須於會議前到場並完成相關環境及資料準備，並依『會議前準備文件檢查清單』所規範之內容完成會議準備，本中心得視需要要求廠商提交『會議前準備文件檢查清單』供本中心確認，如準備不及或延誤需事先告知。

(3) 會議前應將報告事項及文件經本中心相關承辦人員或負責人完成確認。

（四）會議進行規範

1. 會議紀錄人員，不得兼任專案報告人員(如：專案經理)。
2. 會議報告內容，本中心得視管理需要增修內容。
3. 若廠商應報告內容準備不充份，會議主席得宣布散會，於廠商補齊資料後，再擇期召開。
4. □會議時必須進行錄音，錄音檔於會後 1 日(工作日)內提供本中心。

（五）其他

1. □廠商須於每次會議現場完成『會議紀錄』，同時請現場人員確認。並於會後 1 日(工作日)內以書面或傳真或電子郵件方式繳交。
2. ☑廠商須於每次會議 14 日(日曆天)內，完成「會議紀錄」，以書面或電子郵件方式提供本中心確認；並於本中心確認後 2 日(工作日)內以書面或電子郵件方式繳交正式文件至本中心。廠商須遵守會議決議事項，並於時限內完成工作項目。
3. □廠商須於每次會議準備 1 份檔案夾，放置相關歷次會議及合約書等資料，以利會議進行。
4. 會議決議如屬維護/變更需求，廠商應填寫『機房作業申請紀錄單』/『資通系統異動維護變更申請單』後，由本中心系統管理人員確認後辦理。

（六）專案期間違反上述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

參、 建構管理

一、系統維護管理

（一）資通系統異動維護變更申請單

當系統（含正式及測試環境）有下列之維護需求時，得由本中心專案負責人填寫本單，交由廠商進行維護工作：

1. 系統資料維護(系統無提供維護介面)；若因程式不正常之運作造成資料錯誤，由本中心專案負責人填寫『資通系統異動維護變更申請單』經業務單位確認修正內容後修正。
2. 系統資料下載(系統無提供下載介面)。
3. 系統程式錯誤維護(如:出現錯誤訊息視窗)。
4. 系統功能錯誤維護(如:未出現錯誤訊息視窗，但程式之運作結果，未達原系統設計之預期)。

(二) 技術諮詢及服務工作

1. 資料之傳輸、管理及整合之維護。
2. 系統功能之維護。
3. 緊急或異常狀況(包含當機及復原)處理。
4. 系統更新或擴充之技術支援。
5. 系統安全性之管理支援(如：系統使用紀錄及權限管制等措施)。
6. 系統問題排除。
7. 系統相關環境(作業系統及硬體)之問題追蹤。
8. 系統瑕疵與錯誤之修正。
9. 系統執行效能之調校。
10. 系統資訊安全弱點之修補。
11. ☑以源碼掃描工具進行系統原始碼弱點掃描並修補發現之中等級以上弱點。
12. 系統災難復原文件之製作及維護☑與系統災難復原演練。
13. 系統相關軟體環境之安裝與設定。
14. 系統操作與管理之技術諮詢。
15. 檢修並排除系統日誌中所警示之錯誤。
16. 協助排除作業系統事件檢視器之「系統」錯誤事件。
17. 系統文件之修訂。
18. ☑配合出席本中心召開之系統介接或技術討論會議。
19. 依本中心要求提交系統維護服務紀錄。
20. □廠商須提出提升教育訓練參與人數及問卷回收率之方案並執行，所需人力與費用，概由廠商負責。
21. 定期進行系統檢測與暫存資料清理。

(三) 非保固期間之維護工作，應包含保固責任所規範之內容。

二、系統變更及新增管理

（一）☑維護期間允許 10 %(以總程式支數估算)之彈性新增刪除且現有程式變更 3 支視為新增程式 1 支計算；廠商以『應用系統變更申請紀錄表』配合辦理，並依雙方議定時程辦理完成。

（二）程式完成修正上版至正式機前，廠商須與系統管理者即時聯繫，使本中心充分掌握狀況。

（三）廠商應負責維護正確安全之程式版本。

三、☑保固責任

（一）保固期間廠商需無償負責本章節所規範之事項。

（二）配合本中心環境異動，如系統移機及環境重建等。

（三）提供技術轉移服務並修訂系統相關文件。

（四）☑定期弱點掃描(含作業系統、網頁及原始碼)，並修正中等級以上風險弱點直到確認已無不可接受之風險弱點。

（五）配合系統相關會議之召開。

（六）釐清系統相關問題並修正系統功能錯誤。

（七）□依資訊系統維護服務單處理並回覆系統使用者相關問題。

（八）本中心通知後，仍不履行上述條款，本中心得逕行處理，所需費用，得自廠商保固保證金扣除。

四、☑系統基礎架構維護

本章節係為促進本中心整體基礎建設之推展，規範廠商通用性應配合項目，故需配合本中心整體環境及個別系統之特性，以使用單位實際需求訪談及工作小組會議決議為原則，廠商以『機房作業申請紀錄單』/『資通系統異動維護變更申請單』配合辦理，並依雙方議定時程辦理完成。

（一）☑廠商負責建置測試機，並置原始碼及提供開發環境，且可編譯成執行碼。

（二）□提供系統簡介之單張資料，內容須清楚描述系統概念、目的及架構等，並加裱框，尺寸大小由本中心規定。

（三）☑有關登入方式及權限管理，廠商須提供完整原始碼，作為資安驗證。

（四）☑Server 端程式錯誤之錯誤訊息須寫至事件檢視器。

（五）提供各項非客製化軟體之使用授權及操作手冊等文件；非客製化軟體須提供最新版本。

（六）☑配合現有 MS-SQL 資料庫整合，移至本中心指定之資料庫，環境

為 MS-SQL 2022 以上(版權由本中心提供)。

（七）☑配合內部系統 DB Table 介接需求，提供來源資料庫 Table 或 View。

（八）☑配合現有資料庫於所有欄位註記中文使用說明。

（九）資料庫資料表格關聯需建立外來鍵，不得使用程式控制為原則。

（十）配合系統移機作業將系統移至本中心指定之環境。

（十一）☑廠商需修改帳號登入程式及帳號申請流程，以配合本中心單一簽入。

（十二）☑系統目前介接如屬本中心內部系統介接，以使用 DB Table 介接方式為原則，廠商需負責至來源資料庫中擷取資料。

（十三）☑配合資料異動之重要資料庫表格(Table)皆須紀錄最後異動之時間(last modify date)及異動者(等 9 個基本欄位)之程式修改，詳『Table 增加 9 個欄位』(如相關表單)；需求範圍依專案工作小組會議決定。

（十四）配合本中心防火牆環境調整，作相對應設定。

（十五）☑提供網址列之識別圖檔(favicon.ico)。

（十六）☑須確保網站失效連結及無效檔案完全清除。

（十七）□配合本中心升級 IPv6 協定，系統作相對設定及調整。

（十八）□伺服器端產生 office 文件，以不安裝 office 軟體為原則。

（十九）配合本中心 office 及網頁瀏覽器環境升級，系統作相對調整。

（二十）☑廠商原則上不得使用 ActiveX 元件，如需使用必須經工作小組同意，且該 ActiveX 元件須經第三方公正單位驗證，所衍生費用由廠商支付。

（二十一）系統登入驗證

1、外部使用者

(1) □應採用【政府資料傳輸與多元驗證服務網】提供之 GSP 單一登入認證。

(2) ☑如系統未採用上述登入認證，則系統使用者密碼之長度、複雜度及更新期限，須遵循政府組態基準(Government Configuration Baseline，GCB)規範。

2、內部使用者

應整合本中心 AD 帳號為原則，如未整合本中心 AD 帳號，則使用者密碼之長度、複雜度及更新期限，須遵循依政府組態基準(Government Configuration Baseline，GCB)規範。

（二十二）□依循政府組態基準(GCB)規範，本中心資通訊終端設備(如:個人電腦)於套用 GCB 一致性的安全設定後，系統須維持正常運作，如未能配合，需經本中心專案工作小組同意後，填寫『GCB 例外原則申請單』備查。

（二十三）□依系統安全等級，資訊系統防護措施符合「資通安全責任等級分級辦法」附表十「資通系統防護基準」要求。

（二十四）□系統或網頁對不特定對象(如對民眾)開放時，優先以 HTML5 技術開發處理。

（二十五）☑對外開放網站首頁應標示本中心資訊安全政策及隱私權保護宣告。

（二十六）□對外開放網站若有提供可編輯文件供民眾下載時，應同時提供 ODF(Open Document Format 開放文件格式)文件。

（二十七）□特權帳號應具備雙因素(two-factor authentication)認證機制。

（二十八）□為確保開發之平台具備雲端特性，廠商建置之雲端平台應依據驗證時最新公告之「IaaS 服務雲端特性驗測作業程序」檢測項目，通過經濟部「雲端開發測試平台」（Cloud Open Lab）（http://www.cloudopenlab.org.tw）所建立雲端特性測試技術之驗證；驗證衍生之相關費用由廠商自行與驗證單位結算。

（二十九）☑廠商應定期(每年至少 1 次)清理舊資料，應清理之資料與頻率於工作小組會議決議，決議後廠商未執行依「未依會議決議執行」辦理。

（三十）□系統因故未採用 gMSA 帳號者，若未依規定定期變更 AD 帳號密碼而導致系統無法正常運作，每次計罰 1 點。

（三十一）系統應每至少 30 日曆天重新啟動一次，未依規定重新啟動，每次計罰 1 點。

（三十二）☑廠商為客製化資通系統開發者，應提供該資通系統之安全性檢測證明。

（三十三）☑非廠商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。

（三十四）□廠商應依 Host Monitor 監控系統之效能與容量，彙整結果對未來系統需求提前預作規劃，並收集系統負責人與系統管理者意見，於工作小組或期末提出報告。

（三十五）☑漏洞修補更新需求：廠商於本專案所提供各項軟硬體設備，在履約期間及本中心網路架構下，應能達成自動即時更新修補

漏洞目標，有效防止漏洞、弱點所造成危害，如相關漏洞、弱點無法自動即時更新，亦應提出替代方案，並說明改善方式及期程經本中心審查通過。

（三十六）資訊安全改善建議：廠商應隨時研究與注意最新資訊安全現況，遇有系統或設備原廠重大系統安全漏洞更新發布或外界重大安全事件發生，或接獲修正通知時，應向本中心發布資訊安全改善建議，並協助辦理防護及修正、修補工作。

（三十七）行動 App 開發安全：廠商應參考經濟部工業局(以下簡稱工業局)頒布之「行動應用 App 安全開發指引」開發行動 App，應用系統開發完成後，廠商應依工業局頒布之「行動應用 App 基本資安檢測基準」，委託第三方機構針對行動應用程式，進行資訊安全檢測。

（三十八）廠商交付之軟體、硬體及服務等產品，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」所公布禁止使用的危害國家資安產品清單，若因業務需求且無其他替代方案，應具體敘明理由，經本中心核可後，以專案方式購置，列冊管理，且不得與本中心公務網路環境介接。

（三十九）廠商執行專案若有遠距通訊之需要，須遵守行政院資安處訂定之國際會議使用具資安疑慮之遠端視訊會議軟體政府機關與會評估及採行原則。

（四十）公鑰憑證處理之安全檢查：廠商建置或維護之資訊系統若有使用公鑰憑證（包含 MOICA, MOEACA, GCA, XCA 憑證），不含 SSL 憑證，應依國發會頒布之「應用系統使用公鑰憑證處理之安全檢查表」(https://gca.nat.gov.tw/download/AP_CHECKLIST.odt)，針對安全檢查表內容逐項進行檢查，並納入驗收項目，以確保系統之安全性。

（四十一）□對外開放網站新設或改版時應依據國家通訊傳播委員會頒訂之「網站無障礙規範」檢測等級 AA 以上進行設計。

肆、 文件及版本管制需求

下列文件項目僅供參考，廠商以能符合本中心了解本專案實際運作、維護為基本原則。

一、文件製作範本

（一）專案工作計畫書

專案工作計畫書應包含下列事項：

1. 人力配置：維護系統之專案人員之人力配置。應於專案組織成員中，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，負責資安相關文件之審核與簽署，以符合資通安全管理要求。
2. 工作計畫項目(包含契約所有重要需求)。
3. 資訊安全管理計畫(具體敘明資安管理計畫)。
4. 個資適當安全維護計畫(具體敘明執行專案過程中所接觸的個資及安全維護計畫)。
5. 災難復原管理。

（二）需求規格書(SRS)

需求規格書應提供使用者角度的需求陳述且應包含下列事項：

1. 系統建置之目的
2. 需求示意圖(需描述使用對象及主要業務功能)
3. 業務功能描述(說明各項功能目的、資料來源及資料輸入者)
4. 權限及管理需求
5. 名詞定義

（三）系統分析及設計規格書(SDS)

1. 系統分析規格
   (1) 系統簡介：簡述系統之目的、功能、效益及結構等。
   (2) 系統功能定義：敘述主要功能及設計架構。
   (3) 系統介面及作業流程：說明本系統與其他應用系統之關連，及有關之作業程序。
   (4) 服務系統安全與控制：說明服務系統作業安全上應有之控制措施。
   (5) 物件關聯圖及說明：說明服務系統各物件間之關聯。
   (6) 共用模組(含概述及功能)。
2. 程式設計規格
   (1) 程式概論：包括依據／目的、程式概述、修正紀錄及輸出入檔案關聯圖。
   (2) 程式設計說明：包括程式設計要點及程式模組結構。
   (3) 處理程序：包括批次程序說明及線上操作說明。
3. 程式設計之細部設計說明

   撰寫格式參照『程式設計之細部設計說明』，內容應包含下列

項目：

(1) 螢幕/報表畫面。

(2) 使用之程式名稱說明。

(3) 使用時機及流程。

(4) 起始動作說明

(5) 欄位說明

A、使用時機。

B、欄位初始說明。

C、相關代碼/編碼說明。

D、檢核條件。

E、計算說明。

(6) 程式邏輯/產生邏輯。

(7) 相關資料表及資料庫。

(8) 動作(Button/Link)說明。

A、寫入之相關資料庫。

B、寫入檔案。

C、相關動作。

(9) 修正歷程及會議決議說明

4. 資料庫之資料庫綱要及實體關係資料模型(E-R Model)

本需求欄位總表主要是把主題計畫的需求經系統化，並列成表單供系統開發人員建置資料庫時設定欄位所用，同時也供程式設計人員在撰寫程式時參考使用。需求欄位說明如下：

(1) 資料表綱要

A、 項目名稱：所需著錄項目之中文名稱。

B、 英文名稱：項目名稱對應之英文名稱。

C、 資料型態：資料之資料型態。

D、 大小：欄位所需之空間。

E、 必填：標示“＊”者表示為必填欄位，建檔時須填寫該欄位之值，不能空白。

F、 多值：標示“◎”者表示為多值欄位，該組欄位資料可重覆著錄。

G、 屬性：標示該欄位的屬性，包括：

(A) 「唯一」表示欄位的值在資料庫中是唯一存在的。

(B) 「不開放」表示該欄位只供管理者使用，不對外開放。

(C)「下拉式選單」表示記錄方式為下拉式的選單。

(D)「系統自動產生」表示該欄位的值是由系統自動產生，非由著錄人員著錄。

H、 提供者：記錄這筆資料是由系統自動產生或由填表人所填入。

I、 備註(欄位檢核邏輯，如：必填、選填、不可填之關係及可作為註記上述未考慮之說明，如資料格式或限制)

(2) 欄位代碼表

5. 作業處理流程 Process flows

(1) 各項業務處理作業。

(2) 帳號申請/刪除處理作業。

(3) 密碼修改處理作業。

(4) 系統備份處理作業。

(5) 系統安裝處理作業。

(6) 系統事件處理作業。

(7) 系統維護處理作業。

(8) 系統轉介接處理作業。

(9) 其他處理作業。

（四）系統管理手冊

1. 系統簡介：包括系統之目的、功能及結構等。

2. 服務系統操作目錄說明：說明主要目錄(Menu)之各項功能說明。

3. 服務系統作業程序：包括各項定期作業，報表列印等各功能執行程序之參數維護、訊息顯示等作業流程及說明。

4. 服務系統維護須知：說明執行服務系統日常維護工作應注意事項，例如上下系統程序、經常性作業程序、系統意外事故處理程序、系統故障之分析與排除等。

5. 訊息說明與處理。

（五）系統操作手冊

1. 服務系統簡介：包括服務系統之目的、功能及結構等。

2. 服務系統編碼說明。

3. 輸入表單說明：說明須使用之表單格式及其輸入欄位之引用方式。

4. 服務系統作業說明：包括每日、月底、季末、年底等參考(標準)檔維護、系統資料維護等作業流程及說明；線上作業並應說明其使

用時機。

5. 服務系統操作說明：服務系統基本操作方式，各線上及批次功能使用方法，螢幕範例，報表列印及檔案維護方法等。
6. 報表列印。
7. 錯誤訊息說明與處理。

（六）系統安裝手冊(廠商依實際需求製作)

（七）災難復原手冊(廠商依實際需求製作)

（八）系統壓力測試報告

1. 說明使用之壓力測試工具、測試之軟硬體環境。
2. 依據測試數據提供下列結論：

(1) 目前正式環境及常態使用下之平均回應時間。

(2) 目前正式環境中最大使用者數與平均回應時間。

(3) 增加硬體資源後之最大使用者數與平均回應時間。

(4) 所需硬體環境由本中心提供。

（九）系統測試報告書

檢附單元(或整合)測試報告，其中須逐項敘明包括測試期間、測試項目、測試條件(或資料)、測試畫面、發現之問題數、與測試者簽名等。

（十）系統功能需求確認文件，需經本中心需求使用者確認。

二、版本管制需求

廠商所提供之服務，如為軟體或系統開發，須針對各版本進行版本管理，☑並於本中心測試機/開發機編譯後，再將其更新至正式機。

伍、 資訊安全

一、資訊安全政策說明

（一）廠商能力要求與工作說明

1. 廠商辦理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. 廠商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. 廠商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. 廠商應根據日常監控狀況，主動分析是否屬安全事件，並依照行政院國家資通安全會報相關通報應變標準啟動對應之處理程序，協助本中心執行相關處理程序。

5. 對於本中心發生之重大資安事件，廠商應提供 7 天 X 24 小時全年無休之緊急應變處理服務，在本中心要求下於規定時限內指派支援人員至本中心進行事件緊急應變協同處理。
6. 涉及資通訊軟體、硬體或服務等相關事務，廠商之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。廠商於履約期間因股份或資本額變動而成為陸資資訊服務業者，本中心得以書面通知廠商終止契約或解除契約之部分或全部，且不補償廠商因此所生之損失。

（二）委外廠商及人員管理

委外廠商及其專案人員應確實遵守本中心之資訊安全政策，且廠商及其專案人員應簽署『委外廠商資通安全承諾書』、『保密承諾暨個人資料提供同意書』。

（三）☑系統開發設計及變更維護管理

1. ☑機敏資料處理程序

以下所稱機敏資料係指本中心持有或保管之資訊，依國家機密保護法、個人資料保護法等相關法規及本中心實際需求訂定者；廠商以『資通系統異動維護變更申請單』配合辦理，並依雙方議定時程辦理完成。

2. 加解密

(1) ☑密等以上資料不得電子傳輸，如有傳輸需求應向專管單位申請加密機制專門使用，敏感資料在傳輸過程中應加密保護(如 TLS 1.2 及 TLS 1.3 等)以確保其機密性。

(2) ☑敏感資料儲存時，需使用加密技術或其他適當措施，確保其機密性。

(3) ☑廠商應遵循本中心訂定之資料保密規範或國際認可的加密技術(如 AES、3DES、Blowfish 等)，以確保符合安全要求。

(4) ☑敏感資料下載檔案須加密後才可下載。

(5) ☑系統採行加密編譯，廠商需符合 FIPS 140 規範之加密演算法，包括加密、雜湊以及簽署演算法。

3. ☑存取控制

(1) ☑敏感資料存取，系統或架構設計需可限制特定使用者 IP。

(2) ☑敏感資料下載或查詢等，使用者界面需顯示資安警語。

(3) ☑一般使用者查詢(含列印)敏感資料者時，個人資料(姓名、身分證統一編號、生日、居住地址、私人電話)不得顯示足以識別該個

人，如：身分證統一編號後 4 碼（即第 7 碼至第 10 碼）進行遮蓋，並以「*」取代，如另有特殊性用途則依相關規定辦理。

(4) ☑敏感資料使用者列印或查詢客製化報表，其輸出需產生註記(使用者姓名、日期、時間等)，必要時本中心得要求查詢介面提供驗證碼功能。

4. ☑功能測試：於測試機進行測試作業時，不得以正式資料、敏感資料進行測試。

5. 通行碼(密碼)管理

(1) 新增、修改通行碼時需驗證下列規則：通行碼長度應為 12 碼(含)以上，且包含英文大寫、小寫、數字、特殊符號(4 選 3)等。

(2) 系統應提供更新通行碼機制，包括期限參數設定、逾期鎖定、到期提示等。

(3) 通行碼輸入錯誤 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用本中心自建之失敗驗證機制：帳號登錄頁面與新申請頁面都有驗證碼欄位供使用者輸入。

(4) 使用者更換密碼時，至少不可以與前 3 次使用過之密碼相同。

6. ☑帳號管理

(1) 系統應依使用者權限提供系統帳號及權限查詢介面。

(2) ☑使用者帳號避免以身分證統一編號為帳號。

(3) ☑特殊情況需以身分證統一編號為帳號者，應以「*」取代方式處理後使用，同時需考慮相關延伸應用。

(4) ☑應於伺服器端採行集中過濾檢查使用者之權限作業。

7. ☑輸入資料確認

為防止 SQL Injection 等漏洞造成資訊系統中的輸入資訊錯誤、遺失與未經授權的修改或使用，系統中所有輸入欄位應進行資料格式、長度等檢查。

8. 系統日誌

(1) 需提供系統稽核軌跡(Log)，留存使用者帳號☑新增、☑異動、☑刪除記錄。

(2) ☑留存篩選資料之新增、異動、刪除記錄，必要時留存 SQL 指令。

(3) ☑採用單一日誌記錄機制，確保輸出格式一致性，且記錄必要的使用者資訊及管理者行為，排除敏感資訊。

(4) 系統日誌應至少備份留存 6 個月(含)以上。

9. ☑防駭及弱點掃描

(1) ☑檢查並確認作業系統、資料庫系統及相關套裝軟體是否已安裝最新修補檔，或關閉有漏洞服務，以減少有心人士利用已公布的系統弱點而產生的風險。

(2) ☑應用系統須通過本中心指定之資安原始碼掃描工具掃描及網頁弱點掃描工具進行驗證，若掃描結果有不可接受之風險弱點，則廠商需於系統弱點修補後，限期內申請復檢，廠商並應追蹤檢討直到確認已無不可接受之風險弱點。

(3) 以防毒及防駭軟體掃描應用系統程式，以確認程式中是否存在已知的木馬或後門程式。

(4) 檢查測試應用系統與資料庫連線是否正常 (資料庫與應用程式間之連結須設定，不可把資料庫存取權限開放給非應用程式主機來連線，原則上只限開放給應用程式連結資料庫)。

(5) 應用系統安裝其執行權限原則上不得使用 Administrator、sa、root 等管理群組執行。

(6) 嚴禁廠商私設遠端維護機制，以杜絕非法入侵管道。

(7) 網頁根目錄放置 robots.txt，虛擬目錄進行安全設定且應移除範例、預設目錄且不可使用預設值。

(8) 交付軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

(9) 違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先 mail『工作小組』成員並經半數(含)以上成員同意。

（四）☑日常作業

1. ☑程式原始碼管控

(1) ☑原始碼及編譯程式禁止置於正式作業環境之作業系統內。

(2) ☑應建立原始碼程式庫的更新活動稽核日誌。

(3) ☑程式換版應提供修改變更比較，並提供測試記錄及應用系統版更歷程紀錄表，經本中心人員審核後，才能換版，舊版程式原始碼需至少保留 3 代，以作為程式緊急回復措施之用。

2. 系統文件管理

(1) 系統相關文件(如：系統之操作手冊)應詳述資訊安全控制措施(如：備份與回復方式)，俾使使用者及技術支援人員瞭解系統之安全控制措施。

(2) 需提供『災難復原手冊』文件。

二、委外廠商執行事項

(一) ☑弱點掃描

1. ☑作業系統弱點掃描

系統運作之相關主機，須通過作業系統弱點掃描工具之驗證，若掃描結果有不可接受之風險弱點，則需於系統弱點修補後，申請復檢，直到確認已無不可接受之風險弱點。

2. ☑網站弱點掃描

應用系統須通過網站弱點掃描工具之驗證，若掃描結果有不可接受之風險弱點，則需於系統弱點修補後，申請復檢，直到確認已無不可接受之風險弱點。

3. ☑程式原始碼掃描

應用系統須通過源碼掃描工具，掃瞄系統所有程式，直到確認已無不可接受之風險弱點。

(二) ☑災難復原

1. 災難復原演練

(1) 廠商須配合本中心進行災難復原演練，並依『災難復原演練計畫』及『災難復原手冊』完成演練詳實記載於『營運持續演練計畫暨演練報告』，且依據演練結果調整『災難復原演練計畫』及『災難復原手冊』。

(2) □廠商於演練完成後次日起 7 天內進行資訊系統切換至正式營運區驗證復原有效性。超過 500 天之測試機應予以下架。

2.『災難復原演練計畫』及『災難復原手冊』文件正確性驗證

(1) ☑廠商應提供正確災害復原手冊，且確實維持完整性。

(2) ☑廠商須於本中心排定確認日期前完成更新合約範圍內的『災難復原演練計畫』及『災難復原手冊』，其內容須符合合約要求時限。

(3) □由系統負責人依『災難復原手冊』進行確認，並詳實記載演練過程，驗證文件正確性。

3. 系統故障無法運作之修復

(1) ☑應用系統：因系統故障無法運作時，如為本案範圍，廠商須於

接獲通知後4小時(日曆天)內到場處理，並於1個日曆天修復完畢。

(2) □硬體維護：同A級硬體維護之服務時限需求。

（三）參與資訊安全教育訓練

1. □配合本中心資訊安全政策，本專案全職及非全職人員均須配合本中心要求，參加本中心規定之資訊安全教育訓練及資安會議。
2. ☑廠商本專案人員應比照本中心人員每年應參與資訊安全教育訓練，依「資通安全責任等級分級辦法」規定，技術人員(如專案經理、系統分析師、程式設計師、資料庫管理師及其他技術相關職務)每人每年應接受三小時以上之資通安全專業課程訓練，其餘人員每人每年應接受三小時以上之一般資通安全教育訓練；本中心得要求廠商出具人員參與訓練證明(本中心資訊安全教育訓練或外部資訊安全教育課程)，廠商若無法提出證明，每人次計罰1點。

（四）□提供系統資訊安全風險評鑑相關文件及資訊資產清冊

廠商需提供系統資訊安全風險評鑑相關記錄文件(含「防護基準選用暨執行措施表(普）」或「防護基準選用暨執行措施表(中）」或「防護基準選用暨執行措施表(高）」、「風險辨識、分析與對策表」、「業務利害關係調查表」、「資訊系統安全等級評估表」及「資訊系統安全等級初估表」等)及資訊資產清冊等建議文件。

（五）廠商應配合提供符合「資通安全責任等級分級辦法」附表十資通系統防護基準要求之資通安全相關紀錄。

（六）廠商應配合並協助系統負責人及系統管理者，填畢「委外廠商稽核查檢自評表」各項查核項目執行情形，並視需要提供佐證資料。

（七）違反上述任何所述者，以陸、一、(一)、『未依規定時間完成工作計罰』規定計罰，如須延長日期或非廠商之問題(不納入計罰)，須經『工作小組』會議同意，如未能配合『工作小組』會議開會，須先mail『工作小組』成員並經半數(含)以上成員同意。

三、☑資安監控

（一）☑委外廠商稽核查檢

1. 本中心得定期或不定期以稽核或其他適當方式確認受託業務之執行情形。
2. 廠商需提供其內部資安控管之稽核項目供本中心參考，可參考『委外廠商稽核查檢自評表』，本中心得依廠商委外作業之各項資安風險等級進行評估後，不定期依相關稽核評估內容進行抽核。

3. 廠商應確實改善稽核查檢發現之缺失，於接獲本中心通知之期限內改善。若未於期限內改善或稽核查檢仍發現前次稽核發現之相同缺失未改善，每一缺失計罰 1 點。

（二）☑敏感資料及個人資料維護

1. 廠商需對本中心提供之業務或個人資料，包含紙本文件、電子檔案及電子郵件信箱附加檔案等任何形式存在之業務或個人資料應加以保護不得洩漏。
2. 廠商如需將專案複委託時，須事先獲得本中心同意，且廠商應要求複委託廠商遵守本規範。
3. 本中心正式環境之資料嚴禁廠商攜出，若需測試資料，須經特別處理以去除其機敏性。
4. 廠商於合約終止或解除前一個月，提出受委託期間曾接受本中心交付之業務或個人資料盤點清冊，其內容應包括交付各種紙本及載體。並於合約終止或解除時，提交具體指明相關資料銷毀、交還本中心或交給本中心指定之另一個機關之證明，內容包括銷毀或交還之項目、數量、時間、方式、簽收人等，並交付切結文件「合約終止資料處理聲明」證明未持有本中心之所有交付之資料。如因故未能銷毀、交還或交給本中心指定之另一個機關，應列冊載明原因及保存的期間、方式，於取得本中心之同意後進行保存。
5. 廠商對於個人資料保護需記錄下列各項執行結果，並定期提供本中心相關紀錄：
   (1) 廠商應確保專案成員明瞭專案可能涉及個人資料之蒐集、處理及利用之範圍、類別、特定目的及期間，並承諾僅就本中心指示範圍內蒐集、處理及利用個人資料。
   (2) 廠商執行個人資料蒐集、處理、利用之結果，其中包括蒐集、處理、利用個人資料數量、方式、範圍、時間以及是否符合本中心特定目的等內容，相關表單可評估加註標示：「**本資料因涉個人資料，請依法妥善蒐集、處理、利用及保管**」。
   (3) 廠商應遵守本中心所訂定之資訊安全相關規範、及個人資料保護法所要求採取之適當安全維護措施，並建立個資管理流程及做好防止使用者個人資料外洩之安全控制措施。廠商應定期繳交已實施個資法訂定適當安全維護措施之證明文件(如內外部稽核結果等)。

(4) 廠商或其員工違反個人資料保護法、其他個人資料保護法律，或其他法規命令時，應通知本中心違法之事實及欲採行之補救措施，並依個人資料保護法第 12 條之要求通知當事人及負個人資料保護法相關損害賠償責任。

(5) 廠商應遵守專案要求相關保留指示事項，並回報其遵循結果。

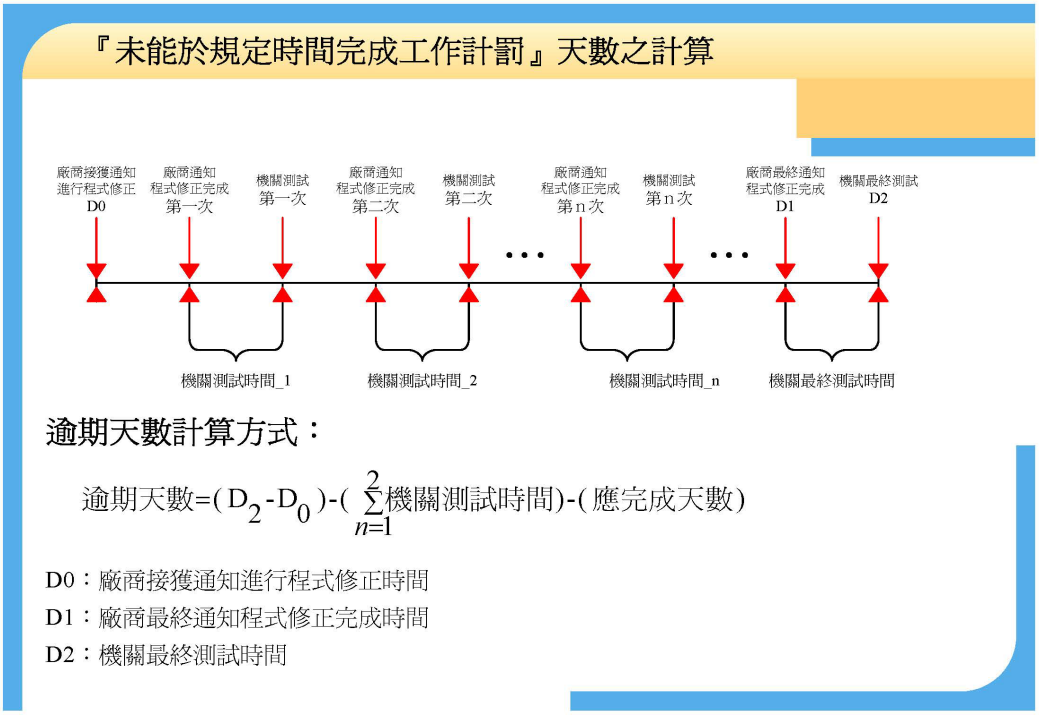
（三）廠商於發生資安事件時，有立即通報本中心之責任，並允許資通安全管理法主管機關得適時公開資安事件之處置內容等資訊。

陸、 罰則

一、計罰方式

（一）未依規定時間完成工作計罰

以日曆天計罰，計罰違約金不足 1 日以 1 日計，每日計罰契約價金 0.1%；未能於規定時間完成工作計罰之計算，為自本中心通知(書面、傳真、系統報修或電子郵件)之發生時間(工作時間)起算，至功能恢復正常運作且經本中心人員確認止(日曆天之計算不含前 2 次本中心人員測試時間，第 3 次起含本中心計算測試時間，計算方式詳如『未依規定時間完成工作計罰天數之計算說明表』；契約中不含本中心測試部分，依契約規定時間完成)。



（二）重覆報修定義

當案件發生多次報修，且經工作小組認定其原因相同，則罰款以最早

發生日期為起算點，並以最後結案時間為結算點。

（三）上述違約金依原因每件(申請單)獨立計罰，罰款天數以日曆天計。

（四）本案標的物如逾維修期限未修護或執行完成，且廠商無法提出令本中心同意之延遲原因時，本中心得另行招商修護，修護相關費用概由廠商負擔及賠償。

（五）本案功能新增修改部份仍受維護條款規範。

（六）凡在保固期內發現瑕疵，應由廠商於本中心指定之期限內負責免費無條件改正。逾期不為改正者，本中心得逕為處理，所需費用由廠商負擔，或動用保固保證金逕為處理，不足時向廠商追償。但屬故意破壞、不當使用或正常零附件損耗者，不在此限。

（七）本案每點違約金金額依契約規定，若契約未規定訂為每點新臺幣 3 仟元整。

二、其他相關罰則

（一）廠商應做好資通安全與防止個人資料外洩之相關配套措施。專案執行及保固期間，發生資安事件 2 級含以上、個資外洩事件或其他因素而造成本中心不名譽事件等，且可歸責廠商者，每次予以本專案得標總金額 5%懲罰性罰款，除限期改善外，並由承包廠商負責處理並承擔一切法律及賠償責任；本中心發生資安事件 1 級含以下並經國家資通安全研究院發送事件通知或發生白帽駭客事件，且可歸責廠商者，每次予以懲罰性罰款 5 仟元整。

（二）廠商所負責的專案與系統，對外服務經本中心人員測試發現有個資外洩情形，每頁外洩個資予以懲罰性罰款 3 仟元整。

（三）廠商所負責的專案與系統，經本中心滲透測試或攻防演練發現嚴重或高風險弱點，且未能限期完成改善(複測未通過)，每個弱點予以懲罰性罰款 3 仟元整。

（四）系統修改、新增或維護需以『資通系統異動維護變更申請單』為依據，如未經相關表單程序核可或資訊系統負責人或資訊系統管理者同意即異動系統程式、功能、資料，每次予以本專案得標總金額千分之 3 懲罰性罰款，惟以上罰款，最高上限 3 仟元整。

（五）廠商須協助系統負責人處理『異常處理單』，包括：建議資安事件等級(協助初判)、進行異常原因調查分析、損害控制與故障排除、漏洞修補、系統還原以及提出並執行改善措施。若『異常處理單』違反契約規範，每一張記罰 1 點。若未於 1 個月內提出改善措施者每次記罰 1 點。系統若發生不可接受之漏洞風險，且未於時限內修補

者，每次記罰 1 點，並累罰(以星期為單位)至改善為止。

（六）因系統功能發生異常本中心開立『資通系統異動維護變更申請單』，廠商如無法找出原因，每次記 1 次，超過 3 次(不含 3 次)以上每增加 1 次懲罰性罰款 3 仟元整或☑硬體廠商可以更換整台硬體設施代替罰則。

（七）□系統當機須重新開機或服務重啟，廠商如無法證明非系統問題，每次記 1 次(本中心以書面、傳真、系統報修或電子郵件紀錄)，超過 6 次(不含 6 次)以上每增加 1 次記罰 1 點。

（八）□廠商如需遠端管理系統須填寫『遠端連線申請表』申請遠端連線，每月 10 日前交付『遠端連線存取使用紀錄表』，如違反上述規定，每逾 1 日予以懲罰性罰款 1 仟元整；每月交付之『遠端連線存取使用紀錄表』

□漏列連線次數(閒置時間三十分鐘內可列同一次)或時間區間超過 30 分鐘(含) 等內容未確實填寫，若當年度累計達 3 次(以月為單位)將予以懲罰性罰款 3 仟元整；並累罰(以星期為單位)至改善為止。

□內容未確實填寫，經系統管理者判定情節重大者，將予以懲罰性罰款 6 仟元整；並累罰至改善為止(以星期為單位)。

□內容未確實填寫，將予以停用，改善完畢後至工作小組會議報告。

（九）廠商未依「**資通安全事故管理作業流程**」落實資安事件通報應變作業及提供資安紀錄等，致國家或社會受有重大損害時，將建議解除合約或依約罰款或不予續約；已遵循「**資通安全事故管理作業流程**」確實辦理資安事件通報及應變作業並提供資安紀錄，仍致本中心或民眾權益受損時，本中心得參酌減輕其責。

（十）除本中心同意外，廠商原則上需每月(得配合專案需求變更頻率及時間)就所維護系統虛擬主機完成 Windows update 作業，未於規定時間完成者，每次記罰 1 點。

（十一）廠商駐點人員使用之電腦，未於下班時間關機，無正當理由，經清查列表者，每次罰款 1 仟元整。

（十二）廠商所負責的專案與系統，經本中心第三方稽核與內部稽核開立不符合事項或次要缺失(不含觀察、建議事項)，且可歸責於廠商者，第三方稽核開立之每項缺失懲罰性罰款 3 仟元整，內部稽核開立之每項缺失懲罰性罰款 1 仟元整。