財團法人生物技術開發中心
資訊服務採購資安規範

投標廠商資格

一、本案內容涉及國家安全，不允許大陸地區廠商、第三地區含陸資成分廠商、在臺陸資廠商參與，及分包廠商亦不得為大陸地區廠商或第三地區含陸資成分廠商，為證明承諾規定，請填具資料所在地及跨境傳輸切結書（附件 1）。

二、投標廠商須具有資通安全之專業能力，並應提送以下證明文件：

1. 投標廠商除提供具備完善之資通安全管理措施之證明（如符合 CNS27001、CNS 27018 任一國家標準，或通過 ISO 27001、ISO27018 任一國際認證，或具有資通安全管理相關內控規章或查核紀錄等）外，請填具資安管理作業自我評估表（附件 2），以證明具備資通安全之專業能力。
2. 投標廠商需提供技術人員具資通安全證照之證明（如行政院公告之資通安全專業證照清單之證照或其他足資證明文件），以證明具備資通安全之專業能力。
3. 投標廠商具有安裝、維修及售後服務之專業能力，應提送維修人員及技術人員經專業訓練之證明（如相關之證照或訓練課程證明）。

得標廠商履約管理及責任

1. 得標廠商應於得標日次日起◯個日曆天（未載明者依 20 個日曆天計算）內，提交團隊成員簽署之委外廠商保密切結書（附件 3）及委外廠商人員保密切結書（附件 4）提交本中心，並要求其工作人員嚴守工作契約內容、本案契約內容及業務機密。任何因得標廠商或其工作人員洩密所致之民、刑事及其他相關法律責任，概由得標廠商負責，本中心並將提報行政院公共工程委員會列為不良廠商。
2. 得標廠商履約，其有侵害第三人合法權益時，應由廠商負責處理並承擔一切法律責任及費用，包括委託者所發生之費用，委託者並得請求損害賠償。
3. 得標廠商保證依本契約保證規定開發或維護應用軟體時，係全部為自己所開發或已獲得第三人之授權或第三人公開允許不特定人得使用，絕無抄襲或侵害任何第三人之著作物或智慧財產權之情事。如因可歸責於廠商之事由，致第三人對本中心或委託者提出智慧財產權侵權之賠償請求或訴訟時，廠商應即出面以自己之名義承受該請求或訴訟，並賠償本中心及委託者因此而致之損失。
4. 廠商依本契約提供本中心服務時，所取得或持有委託者之資料，包括文字、影像、圖形、聲音，不論其儲存於印刷、磁性、光學或其他媒體上，皆屬於委託

者所有。除非為提供服務所需、法令規定或經委託者書面同意，不得複製、揭露或交付第三人。

得標廠商資通安全責任

1. 得標廠商應遵守 CNS 27001 國家標準、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。此外本中心保有對廠商執行稽核的權利。
2. 得標廠商提供之資通訊產品(含軟體、硬體及服務)不得使用大陸廠牌，資料如存放於雲端，亦不得存放至大陸地區（含港澳），得標廠商應遵守資通安全管理法規定限制使用危害國家資通安全產品：不得採用行政院核定之廠商生產、研發、製造或提供之危害國家資通安全產品，避免委託者公務及機敏資料外洩或造成國家資通安全危害。
3. 得標廠商交付之軟硬體及文件，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)，提出安全性檢測證明，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。廠商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。
4. 得標廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
5. 得標廠商於知悉本案相關產品弱點或委託者安全檢測、監控、行政院網路攻防演練或國家資通安全研究院警訊通知發現安全漏洞時，得標廠商須於知悉時起或接獲委託者通知後，立即對本專案之軟體提出改善措施且依本中心規定時程無條件進行漏洞修補(若無法即時完成修補，得標廠商須另提出有效之風險處理措施)。
6. 得標廠商提供服務，如違反資通安全相關法令、知悉本中心及委託者或廠商發生資安事件時，均必須於 1 小時內通報本中心，提出緊急應變處置，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。
7. 得標廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合對系統品質及資通安全的要求。
8. 契約履約或終止後，得標廠商應刪除或銷毀執行服務所持有委託者之相關資料，或依委託者之指示返還或移交之，並保留執行紀錄。
9. 除上述需求外，本專案各項作業均應符合政府資訊安全作業之要求。

得標廠商違約及服務績效違約金

評估項目	評斷方式	要求基準	違約金計點
定期維護	未依契約規定維護	每次（季）統計	每逾○○日（或小時）計○點/按次數計○點
故障排除、系統修復	經本中心通知（不限形式）後，未依契約規定，修復或提供相同系統（設備）供本中心暫時使用	每次統計	每逾○○日（或小時）計○點
系統可用率	系統各項功能，可正常提供使用者之時間百分比，不得低於○○%	每季統計	每不足○○%計○點
	單日累計故障時數（不滿 1 小時，以 1 小時計）	每日不得超過○○小時	每逾○○小時計○點
資安指標	知悉發生資安事件之通報、損害控制或復原作業時效	應於 1 小時內通知本中心（或接獲本中心通知 1 小時內），並採取適當之應變措施	每逾 1 小時計○點
	完成損害控制或復原作業之時效	應於知悉資通安全事件後 72 小時(重大資安事件為 36 小時)內完成損害控制或復原作業	每逾 1 小時計○點
	調查及處理資安事件之時效	完成損害控制或復原作業後，應於 1 個月內送交調查、處理及改善報告（或協助本中心調查處理）	每逾○○日計○點

評估項目	評斷方式	要求基準	違約金計點
	本中心資料之機密性及完整性	本中心擁有之敏感資料應採取適當之防護措施，以避免不當外洩或遭竄改	廠商於本契約承接範圍內，因未採取適當防護，致本中心敏感資料外洩或遭竄改時，按受影響資料筆數，每筆計◯點/按次數計◯點
	個人資料之機密性及完整性	本中心所擁有之個人資料應採取適當之防護措施，以避免不當外洩或遭竄改	廠商於本契約承接範圍內，因未採取適當防護，致本中心個人資料外洩或遭竄改時，按受影響資料筆數，每筆計◯點/按次數計◯點
	經本中心通知（不限形式）後，未依稽核改善缺失限期改善者	每次統計	每逾◯◯日（或小時）計◯點
	違反本中心 ISMS 資安規定	1. 同一事件連續發生 2 次(含)以上事件 2. 於稽核發現列為主要或次要不符合規定事項	每筆計◯點/按次數計◯點
文件交付	1. 開發系統每階段性需求報告（包含需求分析、安全性設計、安全性編碼、安全性測試、安全性部署及安全性維護等） 2. 安全性檢測報告（如：原始碼檢測、弱點掃描等） 3. 依合約規定須交付之文件（如：保密切結書、資通系統資安防護基準要求與查核表、開源軟體清單等）	每次統計	缺少相關報告或文件，按次數計 2 點

評估項目	評斷方式	要求基準	違約金計點
派駐本中心服務人員	累計遲到及早退之總時數(不滿1小時，以1小時計)	每季不得超過___小時	每逾○○小時計○點
其他	違反契約約定廠商應履行之項目	每次統計	每筆計○點/按次數計○點

本案每點違約金金額為新臺幣○○○元（未載明者依契約價金總額1‰計算，未達新臺幣○仟元者，以新臺幣○仟元計)。

附件 1

資料所在地及跨境傳輸切結書

本廠商＿＿＿＿＿＿參與財團法人生物技術開發中心辦理（標的名稱）招標案，對於廠商之責任，包括刑事、民事與行政責任，已充分瞭解相關之法令規定，並願確實遵行，簽結承諾事項如下：

一、本公司目前是否有中國大陸地區廠商或人民持股情形？

□本公司無中國大陸地區廠商或人民持股情形。

□有中國大陸地區廠商或人民持股情形，其佔比情形及相關說明如下：

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

二、本公司及涉及本案之分包廠商是否為中國大陸地區廠商？

□本公司及涉及本案之分包廠商皆非屬中國大陸地區廠商。

□有中國大陸地區廠商，說明如下：

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

三、執行本案之團隊成員是否有中國大陸國籍人士(多重國籍者，若有屬中國大陸國籍者亦屬之)？

□執行本案之團隊成員皆無陸籍人士。

□本案之團隊成員有陸籍人士，說明如下：

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

四、本公司及涉及本案之分包廠商，是否於中國大陸地區(含香港、澳門)設立相關團隊據點？如是，則該據點與本案履約間之關係為何？

□否，本公司及涉及本案之分包廠商，皆未於中國大陸地區設立相關團隊據點。

□是，該據點與本案履約間之關係，說明如下：

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

五、本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、備份及備援之實體所在地是否有置於中國大陸地區(含香港、澳門)之情形？或跨該等境內傳輸相關資料？

□否，本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、儲存、備份及備援等作業，皆無置於中國大陸地區(含香港、澳門)之情形，且未經該等境內傳輸相關資料。

□是，有置於中國大陸地區(含香港、澳門)或該等境內傳輸相關資料，說明如下：

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

切結廠商：　　（簽名蓋章）

負責人：　　（簽名蓋章）

中華民國　　年　　月　　日

附件 2

（廠商名稱）參與財團法人生物技術開發中心辦理（標的名稱）案之相關資安管理作業自我評估表

日期： 年 月 日

評估項目	辦理情形
1.管理面	
1.1 辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	□辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ □辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □本專案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2 本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	□本專案之資安負責人(專案主管)為____ □本專案之資安人員為____ □本專案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3 本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	□本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於____文件，已(將)採取對應之控制措施詳____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □未就本專案進行資安風險評估 備註：_____
1.4 本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	□本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含____ □未就本專案訂定相關資安事件通報及應變程序 備註：_____
1.5 由招標公告日起算，過去 3 年是否發生因管理議題肇因之重大資安事件	□過去 3 年無發生因管理議題肇因之資安事件 □是，共__次，事件發生主要根因為____ 備註：_____

2.技術面	
2.1 本專案範圍內之資通系統，包含主要履約標的之資通系統及其他執行本專案業務所需使用之業務、行政相關資通系統，辦理安全性檢測	□本專案範圍內之資通系統將規劃執行_____(如源碼掃描、弱點掃描、滲透測試)，檢測項目及本案範圍為：_____ □未就本專案範圍內之資通系統規劃安全性檢測 備註：_____
2.2 辦理本專案受託業務環境及設備導入之相關資通安全防護措施	□本專案受託業務之環境及設備已(將)導入(啟用)_____(如防毒軟體、防火牆、電子郵件過濾機制、入侵偵測及防禦機制等)，導入項目及本案範圍為：_____ □本專案受託業務之環境及設備未導入相關資通安全防護措施 備註：_____
2.3 本專案範圍內之資通系統及專案資料之存取控制等權限管理機制，如 PM、系統管理員、一般使用者帳號之權限分級原則及控管方式	□本專案範圍內之資通系統帳號或使用者權限分成__種等級，相關存取控制、權限管理機制說明如下：____ □未規劃本專案範圍內之資通系統及專案資料相關存取控制及權限管理機制 備註：_____
3.認知訓練面	
3.1 本專案直接履約相關人員之資安教育訓練	□本專案直接履約相關人員之資安教育訓練包含__小時之資安通識教育訓練，對象包含____；__小時之資安專業教育訓練，對象包含____ □未規劃相關資安教育訓練 備註：_____
3.2 本專案團隊人員取得之資通安全專業證照	□本專案具資安證照之團隊成員有：__位 □本專案團隊人員未具備資通安全專業證照 備註：_____

註：本表評估項目及辦理情形等欄位內容，機關得視個案特性及實際需要，自行調整或增刪。

切結廠商：　　（簽名蓋章）

負責人：　　（簽名蓋章）

中華民國　　年　　月　　日

附件 3

紀錄編號：＿＿＿＿＿＿　　填表日期:　年　月　日

＿＿＿＿＿＿＿＿＿＿＿＿公司（以下簡稱乙方）受財團法人生物技術開發中心（以下簡稱甲方）委託辦理「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿案」（以下簡稱本專案），乙方執行本專案接觸之公務（機密）資料，具結依下列規定保密並履行責任：

一、乙方於本專案進行期間因進行調查、搜集依合約所產生或所接觸之業務（機密）資料，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知悉之上述業務（機密）資料，乙方須負保密責任。

二、業務（機密）資料保密期限，不受本專案工作完成（結案）或合約到期及乙方不同工作地點及時間之限制，乙方持有或獲知業務（機密）資料，未經甲方書面同意或授權，不得洩漏或轉讓於第三者。

三、乙方違反資訊安全保密切結書之規定，致造成甲方或第三者之損害賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供絕無異議。

四、乙方有完全約束所屬員工之責，包括分包廠商人員及臨時性人員，所有作業之工作人員皆須簽署委外廠商人員保密切結書。

此致

財團法人生物技術開發中心

具切結書廠商：＿＿＿＿＿＿＿＿＿＿（公司章）

代　表　人：＿＿＿＿＿＿＿＿＿＿

統 一 編 號：＿＿＿＿＿＿＿＿＿＿

公 司 地 址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

電　　話：＿＿＿＿＿＿＿＿＿＿

本中心蒐集本表單上所列之個人資料，作為辨識您為簽署本保密切結書之本人，並為追溯違反本保密切結相關規定用途，不做其他目的範圍外之利用，並遵循個人資料保護法與本中心個資保護之要求辦理。

中　華　民　國　　年　　月　　日

附件 4

紀錄編號：＿＿＿＿＿＿　　填表日期:　　年　　月　　日

立切結書人＿＿＿＿＿＿＿＿（以下簡稱乙方）參與財團法人生物技術開發中心（以下簡稱甲方）辦理「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿案」，謹聲明恪遵甲方下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經甲方權責人員之核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，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，絕無異議。

一、未經申請核准，不得私自將甲方之資訊設備、媒體檔案及公務文書攜出。

二、未經甲方業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接甲方網路。若經申請獲准連接甲方網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、廠商駐點服務及專責維護人員原則應使用甲方配發之個人電腦與週邊設備，並僅開放使用甲方內部網路。若因業務需要使用甲方電子郵件、目錄服務，應經甲方業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經甲方業務相關人員之確認並代為申請核准。

四、甲方得定期或不定期派員檢查或稽核乙方是否符合上列工作規定。

五、本保密切結書不因乙方離職而失效。

六、乙方因違反本保密切結書應盡之保密義務與責任致生之一切損害，乙方所屬公司或廠商應負連帶賠償責任。

此致

財團法人生物技術開發中心

具切結書廠商：＿＿＿＿＿＿＿＿

立切結書人：＿＿＿＿＿＿＿＿

地　　址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本中心蒐集本表單上所列之個人資料，作為辨識您為簽署本保密切結書之本人，並為追溯違反本保密切結相關規定用途，不做其他目的範圍外之利用，並遵循個人資料保護法與本中心個資保護之要求辦理。

中　華　民　國　　年　　月　　日