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，包括本中心所發生之費用，本中心並得請求損害賠償。
3. 得標廠商保證依本契約保證規定為本中心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，所取得或持有本中心之資料，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，皆屬於本中

心所有。除非為提供服務所需、法令規定或經本中心書面同意，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，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，避免本中心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. 得標廠商每年至少辦理 1 次弱點掃描作業及提交相關報告，如有掃描出高風險(含)以上弱點應於兩週內改善完成，弱點修補後應進行複掃，以確認弱點均已處理無遺漏，複掃處理結果仍有高風險(含)以上弱點因故無法修補者，應於「弱點處理報告單」（附件 5）說明無法修補之原因與因應方法。
5. 得標廠商應配合本中心執行弱點掃描作業，如有掃描出高風險(含)以上弱點應於兩週內改善完成，複掃處理結果仍有高風險(含)以上弱點因故無法修補者，應於「弱點處理報告單」（附件 5）說明無法修補之原因與因應方法。
6. 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。
7. 得標廠商於知悉本案相關產品弱點或本中心安全檢測、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本中心通知後，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)。
8. 得標廠商提供服務，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。

9. 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，以符合本中心對系統品質及資通安全的要求。
10. 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本中心之相關資料，或依本中心之指示返還或移交之，並保留執行紀錄。
11. 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。

系統開發及維運

1. 本案資通系統防護等級為____普____，得標廠商應依據本中心訂定資通系統防護需求分級原則及防護基準控制措施構面（附件 6）進行資安需求項目。
2. 得標廠商應依據安全系統發展生命週期(Secure System Development Life Cycle, SSDLC)執行，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，提供本中心每階段性的報告，以利本中心有效地管理安全性風險，從而提高應用程式的整體安全性和品質。
3. 建置新系統或系統重大變更時，得標廠商至少辦理 1 次安全性檢測（原始碼檢測及弱點掃描作業）及提交相關報告。
4. 得標廠商依本案提供本中心服務時，如使用開源軟體，應依該開源軟體之授權範圍，授權本中心利用，並以執行檔及原始碼共同提供之方式交付予本中心使用，得標廠商並應交付開源軟體清單（附件 7）（包括但不限於：開源專案名稱、出處資訊、原始著作權利聲明、免責聲明、開源授權條款標示與全文）。
5. 履約項目如涉及本中心既有資通系統之修改或資料介接，得標廠商應依約履行義務並交付成果(包含原始碼)。

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
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 3 日計 1 點
系統可用率	連續累計故障時數（不滿 1 小時，以 1 小時計）	不得超過 72 小時	每逾 1 小時計 2 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 3 點

評估項目	評斷方式	要求基準	違約金計點
	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 3 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 1 日計 3 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，按次數計 3 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，按次數計 3 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 1 日計 3 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	按次數計 3 點

評估項目	評斷方式	要求基準	違約金計點
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
其他	違反契約約定廠商應履行之項目	每次統計	按次數計 2 點

本案每點違約金金額為新臺幣 1500 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

附件 5

紀錄編號：＿＿＿＿＿＿＿＿　　填表日期：　　年　　月　　日

設備名稱		系統名稱		管理人員	
外部 IP		內部 IP		掃瞄時間	年　月　日

項次	等級	弱點名稱	修補情形	修補日期	未修補原因說明與防禦因應方法
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
			□已修補 □暫不修補		
覆核單位					
負責人簽章			權責單位主管簽章		

（註：等級為：風險等級「高」、「中」、「低」）

附件 6

資通系統資安防護基準要求與查核表

系統名稱：_____

廠商名稱：_____

填寫人：_____

填寫日期：_____ 安全等級：☐普 ☐中 ☐高

存取控制

帳號管理(Account Management)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	V	V	V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制（含帳號新增、停用、或刪除等申請表單紀錄） (系統主機非存置本中心，請說明系統帳號管理程序，並說明是否保留帳號新增、停用、或刪除等申請表單紀錄。)
已逾期之臨時或緊急帳號應刪除或禁用。	V	V	V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制。 (系統主機非存置本中心，請說明系統對於臨時或緊急帳號之管理程序。)
資通系統閒置帳號應禁用。	V	V	V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制。 (系統主機非存置本中心，請說明閒置帳號禁用方式，是否定期辦理帳號清查並留下清查紀錄。)
定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。	V	V	V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	依本中心 ISMS 程序書帳號管理機制（特權帳號每年審核 2 次，資通系統每年審核 1 次）。 (系統主機非存置本中心，請說明是否定期辦理帳號清查並留下清查紀錄。)
機關應定義各系統之閒置時間或可使用期限及資通系統之使用情況及條件。		V	V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	請說明系統之閒置時間或可使用期限及資通系統之使用情況及條件。
逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。		V	V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	請說明是否依規定設置系統閒置超時自動登出機制、設置時間為多久？
應依機關規定之情況及條件(如上班時間或指定 IP 來源)使用資通系統。			V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	請說明是否有系統使用時間規定、遠端連線來源 IP 限制？
監控資通系統帳號，如發現帳號違常使用時回報管理者。			V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	請說明系統本身是否有未經授權登入系統之監控及通報機制？機制為何？

最小權限(Least Privilege)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否依據權責設置帳號權限？

遠端存取(Remote Access)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	1.一般使用者須通過授權檢查後始可放行。 2.系統後臺及遠端維護管理功能，只開放具有相應權限之帳號使用，須完成身分驗證及授權檢查後，始可存取相關功能資源(如：透過 VPN 或 Citrix 平台，並搭配 idexpert 雙因子驗證)。
使用者之權限檢查作業應於伺服器端完成。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明使用者之權限檢查是否於伺服器端完成？
應監控遠端存取機關內部網段或資通系統後台之連線。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	本中心透過 SPS 側錄軟體監控廠商遠端連線之操作行為。 (系統主機非存置本中心，請說明監控方式)
應採用加密機制。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	1.請說明系統是否採加密安全通道，如 TLS1.2、RPC 通訊等。 2.本中心遠端維護系統 Citrix 採加密 TLS1.2 及 TLS1.3 安全通道。
遠端存取之來源應為機關已預先定義及管理之存取控制點。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	1.本中心遠端維護採廠商僅透過 Citrix 平台，並搭配 idexpert 雙因子驗證，通過授權後始可放行。 2.本中心 Citrix 系統設定防火牆限臺灣 IP 存取、資通系統主機非必要均不對外開放連線。 (系統主機非存置本中心，請就 1、2 項說明)

事件日誌與可歸責性

記錄事件(Audit Events)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	V	V	V	□是 □不適用 □否，預計完成時	請說明日誌(Log)保存方式與保存時間(依本中心規

				間　年　月　日	定，紀錄之保存期限須考量組織需求與法令法規要求，若無特別規定，至少須保存 6 個月)。
確保資通系統有記錄特定事件(如更改密碼、登錄失敗、資通系統存取失敗)之功能，並決定應記錄之特定資通系統事件。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明系統是否收集如左列特定事件之紀錄(log)，且於特定事件發生或發生次數異常時，是否發出異常警訊以供系統管理員查核？
應記錄資通系統管理者帳號所執行之各項功能。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明對[redacted]者帳號所為之各種操作是否留下稽核紀錄？
應定期審查機關所保留資通系統產生之日誌。		V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否留下定期審查日誌紀錄(log)之佐證資料？

日誌紀錄內容(Content of Audit Records)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明日誌紀錄是否包含左列安全需求，並採用單一(格式一致)的 Log 機制並依要求納入額外稽核紀錄？

日誌儲存容量(Audit Storage Capacity)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
依據日誌紀錄儲存需求，配置所需之儲存容量。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明是否已配置所需之日誌儲存容量？

日誌處理失效之回應(Response to Audit Processing Failures)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統於日誌處理失效時，應採取適當之行動。	V	V	V	□是 □不適用 □否，預計完成時間　年　月　日	請說明當系統記錄稽核紀錄之作業失效時，處理方式為何？
機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。			V	□是 □不適用 □否，預計完成時間　年　月　日	請說明特定稽核失效事件(資安事件達 1 級(含)以上)發生時，系統是否在 1 小時內通知相關權責人員？

時戳及校時(Time Stamps)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應使用系統內部時鐘產生日誌紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	V	V	V	☑是 □不適用 □否，預計完成時間　年　月　日	本中心各系統主機定時與本中心校時主機進行校時，基準時間源為國家時間與頻率標準實驗室。 (系統主機非存置本中心，請說明校時機制為何？)
系統內部時鐘應定期與基準時間源進行同步。	V	V	V	☑是 □不適用 □否，預計完成時間　年　月　日	

日誌資訊之保護(Protection of Audit Information)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
對日誌紀錄之存取管理，僅限於有權限之使用者。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明日誌紀錄的存取限制方式為何？(如僅提供特定權限人員可透過系統介面查詢)
應運用雜湊或其他適當方式之完整性確保機制。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否提供雜湊或其他方式確保日誌完整性，避免日誌遭竄改？
定期備份日誌至原系統外之其他實體系統。			V	□是 □不適用 □否，預計完成時間 年 月 日	儲存於資料庫之稽核紀錄，有採異地備份機制，餘網站服務 log、system log 等，則另備份於與系統不同實體之儲存媒體上。(系統主機非存置本中心，請說明備份機制為何？)

營運持續計畫					
資料備份(Information System Backup)					
安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定資料可容忍資料損失之時間要求。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	系統主機存置於本中心可容忍資料損失時間(RPO)為24 小時。 (系統主機非存置本中心，請說明可容許損失資料之時間(RPO)為何？)
執行資料備份。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	VM Guest OS 快照備份：每日備份，本地保留 7 份，異地保留 180 份。 (系統主機非存置本中心，請說明備份機制。)
應定期測試備份資料，以驗證備份媒體之可靠性及資訊之完整性。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	系統主機存置於本中心，依本中心營運持續演練規劃辦理。另每日監控備份情形，如發生備份失敗或異常情形，並有專人處理。 (系統主機非存置本中心，請說明是否定期執行備份還原演練？)
應將備份還原，作為營運持續計畫演練之一部分。			V	☑是 □不適用 □否，預計完成時間 年 月 日	本中心之營運持續演練，有將系統及資料庫備份還原納為執行項目。
應建立資料異地備份機制。			V	☑是 □不適用 □否，預計完成時間 年 月 日	本中心系統軟體與其他安全相關資訊之備份另外儲存於非伺服器本身的位置，且資料庫備份檔有異地備份措施(異地備份至汐止機房)。 (系統主機非存置本中心，

					請說明系統及資料是否異地存放？)

系統備援(Redundancy of Information Systems)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
訂定資通系統從中斷後至重新恢復服務之最大可容忍中斷時間要求。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	可容許資通系統中斷時間為(RTO)： ___小時。(請依系統安全等級評估表之可用性填寫對應數值。(填寫值：8 小時(高)、24 小時(中)、72 小時(普)) 註：應與資通系統安全等級評估表、營運衝擊分析表、及合約中之服務水準協議(SLA)一致
應定期測試原服務中斷時，於最大可容忍中斷時間內，由備援設備或其他方式取代並提供服務。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	可由備份還原或全機重建方式於可容忍中斷時間內提供服務，並有留存測試紀錄。 (系統主機非存置本中心，請說明還原機制可否於可容忍時間內提供服務，並提供測試紀錄予以佐證。)
應將備援啟動作為營運持續計畫演練之一部分			V	□是 □不適用 □否，預計完成時間 年 月 日	本中心之營運持續演練，有將備援啟動納為執行項目。

識別與鑑別

使用者之識別與鑑別(Identification and Authentication)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應識別及鑑別機關使用者，並禁止使用者使用共用帳號。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	本中心系統機制均與 AD 主機驗證，唯一識別且足供鑑別機關內部使用者，禁止使用共用帳號。 (系統主機非存置本中心，請說明系統機制是否可唯一識別且足供鑑別機關內部使用者，禁止使用共用帳號？)
對資通系統之存取採取多因子鑑別技術。			V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否具備多重認證或鎖定 IP 機制？

身分驗證管理

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
使用預設密碼初次登入系統時，應於登入後要求立即變更。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	本中心系統機制均與 AD 主機驗證，無預設密碼。 (系統主機非存置本中心，新帳號登入時是否要求變

					更預設密碼？)
身分驗證相關資訊不以明文傳輸。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	帳密驗證資料傳輸時是否有加密？
具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制（失敗 3 次，鎖定 15 分鐘）。 (系統主機非存置本中心，帳密驗證失敗的鎖定方式為何？)
使用密碼進行驗證時，應強制最低密碼複雜度；依機關密碼效期規定變更密碼。(非內部使用者，可依機關自行規範辦理。)	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制（密碼複雜度：至少 12 位元且需符合英文大小寫、數字、特殊符號 4 選 3；最短效期 1 天、最長效期 180 天）。 (系統主機非存置本中心，密碼複雜度與效期是否有要求？)
密碼變更時，至少不可以與前三次使用過之密碼相同。(非內部使用者，可依機關自行規範辦理。)	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制（密碼歷程 3 代）。 (系統主機非存置本中心，更換密碼是否有歷程之要求？)
身分驗證機制應防範自動化程式之登入或密碼更換嘗試。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	身分驗證是否有防止自動化方式登入(例如增加圖形驗證碼之輸入)？
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符記。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依資訊組 AD 帳號管理機制（須提出行政服務需求單，核准後始得變更）。 (系統主機非存置本中心，密碼重設時發送之驗證過程(如:驗證碼、驗證連結)是否有時效限制？)

鑑別資訊保護(Authentication Protect)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統應遮蔽鑑別過程中之資訊。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	系統登入時之密碼或機敏鑑別資訊是否不以明文顯示？
資通系統如以加密進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存		V	V	□是 □不適用 □否，預計完成時間 年 月 日	密碼是否加密或經雜湊處理後儲存？

系統與服務獲得

系統發展生命週期需求階段(System Development Life Cycle-Requirement)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
針對系統安全需求(含機密性、可用性、完整性)進行確認。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依據資通安全責任等級分級辦法附表九規定先評定系統資安等級，再使用

					「資通系統資安防護基準要求與查核表」進行安全需求確認。

系統發展生命週期設計階段(System Development Life Cycle-Design)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。		V	V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	各系統先進行高階風險評鑑(依據資通安全責任等級分級辦法附表九規定，評定系統資安等級)，資訊系統安全等級鑑別為高者或資訊資產安全等級為高者，再進行細部風險評鑑作業(風險評估表)。另透過 SSDLC 要求確認已將資安需求納入整個系統發展生命週期內。
將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		V	V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	是否將風險評估結果回饋至應用系統安全需求查檢表？

系統發展生命週期開發階段(System Development Life Cycle-Develop)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
應針對安全需求實作必要控制措施。	V	V	V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	是否已依系統安全等級實作必要控制措施？
應注意避免軟體常見漏洞及實作必要控制措施。	V	V	V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	是否定期執行資安檢測、code review 確保無常見漏洞？如定期交付資安檢測報告及漏洞修補。
發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	V	V	V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	請說明系統是否已避免於系統錯誤時顯示詳細錯誤訊息(如明確指出是帳號或密碼錯誤)，以免有心人士得知系統太多細節？
執行「源碼掃描」安全檢測。			V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	系統上線前是否有源碼檢測紀錄？
系統應具備發生嚴重錯誤時之通知機制。			V	☐是 ☐不適用 ☐否，預計完成時間 年 月 日	系統在嚴重錯誤時是否有通知機制？機制為何？

系統發展生命週期測試階段(System Development Life Cycle-Test)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
執行「弱點掃描」安全檢測。	V	V	V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	本中心內部系統每年均辦理一次弱點掃描安全檢測作業。 (系統主機非存置本中心，是否有弱點掃描紀錄？)
執行「滲透測試」安全檢測。			V	☑是 ☐不適用 ☐否，預計完成時間 年 月 日	本中心核心資通系統每年辦理 1 次滲透測試，其餘系統均依本中心規劃辦

					理。

系統發展生命週期部署與維運階段(System Development Life Cycle-Deployment and Maintenance)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
於部署環境中應針對相關資通安全威脅，進行更新與修補。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	依據本中心收到資安威脅情資，通知各系統廠商，進行弱點更新及修補事宜。
識別並關閉不必要服務及埠口。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	定期檢視系統運作需要所開啟之服務與埠口。相關服務或埠口之異動應提出申請並經核准始能異動。(系統主機非存置本中心，請說明服務或埠口管理方式？)
資通系統不使用預設密碼。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	1.機房使用之相關管理工具皆已變更密碼。 2.請說明資通系統使用之相關軟體是否使用預設密碼？ (系統主機非存置本中心，請就1、2項說明)
執行系統源碼備份	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	源碼多久備份？
於系統發展生命週期之維運階段，應執行版本控制與變更管理。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	版本版次之管理方式為何？系統變更是否填寫變更申請單？

系統發展生命週期委外階段(System Development Life Cycle-Outsourcing)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。	V	V	V	☑是 □不適用 □否，預計完成時間 年 月 日	資訊作業委外之資訊服務採購契約，已將資通系統資安防護基準要求與查核表納入委外合約中，請廠商依據系統資安等級實作各項安全控制措施。

獲得程序(Acquisition Process)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
識別資通系統使用之第三方軟體、服務、函式庫或其他元件。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	是否定期盤點系統所使用之第三方軟體、服務、函式庫或其他元件。
開發、測試及正式作業環境應為區隔。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	開發、測試及正式環境是否區隔？

系統文件(Information System Documentation)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
應儲存與管理系統發展生命週期之相關文件。	V	V	V	□是 □不適用	資訊系統從評估、規劃、

				□否，預計完成時間 年 月 日	招標、建置乃至維運過程之相關文件是否妥善保存？

系統與通訊保護					
傳輸之機密性與完整性(Transmission Confidentiality and Integrity)					
安全需求檢核項目	**資訊系統資安等級**			**是否符合**	**佐證資料或作法說明**
	普	**中**	**高**		
資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。			V	□是 □不適用 □否，預計完成時間 年 月 日	網站傳輸資料時，是否採用 HTTPS(透過 SSL 或 TLS 等加密協定)協定以確保資料以密文方式傳輸？
使用公開、國際機構驗證且未遭破解之演算法。			V	□是 □不適用 □否，預計完成時間 年 月 日	不使用自行創造的加密方式，採用公開、國際認可之演算法，例如 AES、RSA 及 SHA 安全雜湊等演算法。
加密金鑰或憑證應定期更換。			V	□是 □不適用 □否，預計完成時間 年 月 日	依據 GCA 政府憑證管理中心所核發憑證之有效期限，定期辦理憑證更新。
伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。			V	□是 □不適用 □否，預計完成時間 年 月 日	請說明針對使用的金鑰是否以密碼保護，並進行備份及妥善保管；且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。
資料儲存之安全(Protection of Information at Rest)					
安全需求檢核項目	**資訊系統資安等級**			**是否符合**	**佐證資料或作法說明**
	普	**中**	**高**		
資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。			V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統是否已定義哪些資料屬機密資料？其於資料庫或其他儲存裝置上是否加密儲存？以減少機敏資料因儲存媒體或裝置有其他存取管道而洩漏的風險。

系統與資訊完整性					
漏洞修復(Flaw Remediation)					
安全需求檢核項目	**資訊系統資安等級**			**是否符合**	**佐證資料或作法說明**
	普	**中**	**高**		
系統之漏洞修復應測試有效性及潛在影響，並定期更新。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否針對系統漏洞進行影響評估並定期更新修補？
定期確認資通系統相關漏洞修復之狀態。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明是否定期確認系統漏洞修復之狀態？
資通系統監控(Information System Monitoring)					
安全需求檢核項目	**資訊系統資安等級**			**是否符合**	**佐證資料或作法說明**

	普	中	高		
發現資通系統有被入侵跡象時，應通報機關特定人員。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	依本中心資訊安全事件管理規範及系統委外需求書對廠商資安通報之要求辦理。
監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	本中心透過 VISION ONE 及 watchdog 監控資通系統，以偵測攻擊與未授權之連線，並依據收到之資安威脅情資，確認惡意攻擊 IP 並於防火牆設定，加以阻擋。 (系統主機非存置本中心，請說明監控機制為何？)
資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。			V	☑是 □不適用 □否，預計完成時間 年 月 日	本中心透過 VISION ONE 及 watchdog 監控資通系統，並進行事件分析。 (系統主機非存置本中心，請說明是否對系統進出流量進行監控，於發現異常時之處置為何？)

軟體及資訊完整性(Software, Firmware, and Information Integrity)

安全需求檢核項目	資訊系統資安等級			是否符合	佐證資料或作法說明
	普	中	高		
使用者輸入資料合法性檢查應置放於應用系統伺服器端。	V	V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明對於使用者輸入欄位資料，是否於伺服器端進行合法性檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法？
使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。		V	V	□是 □不適用 □否，預計完成時間 年 月 日	請說明系統程式目錄是否已透過監控偵測機制(如 GIT 或 SVN 版控軟體)，確保程式、設定檔不被未經授權者變更。 (系統主機非存置本中心，請說明是否使用完整性驗證工具偵測軟體或資訊是否遭受未經授權之變更？)
發現違反完整性時，資通系統應實施機關指定之安全保護措施。		V	V	☑是 □不適用 □否，預計完成時間 年 月 日	當軟體與資訊經發現違反完整性時，依據本中心資通安全事件通報及應變管理規範進行通報，並即刻停止系統服務，經追查原因、復原系統及資料後，方能繼續系統服務。
應定期執行軟體與資訊完整性檢查。			V	□是 □不適用 □否，預計完成時間 年 月 日	是否定期執行軟體與資訊完整性檢查並留下紀錄？

附件 7

財團法人生物技術開發中心

（請填寫系統名稱）開源軟體清單

編號	軟體名稱	描述	主要功能	授權類型	官方網站
例	VLC Media Player	多媒體播放器	播放各種音頻和視頻格式	GPL	https://www.videolan.org
例	GIMP	圖像編輯軟體	圖像處理和編輯	GPL	https://www.gimp.org
例	LibreOffice	辦公軟體套件	文書處理、試算表、簡報等	MPL	https://www.libreoffice.org
例	Audacity	音頻編輯軟體	錄音和編輯音頻	GPL	https://www.audacityteam.org
例	Blender	3D 建模和動畫軟體	3D 建模、動畫、渲染	GPL	https://www.blender.org