

財團法人台灣設計研究院

「設計導向 AI 知識基礎建置及驗證」採購案

徵求建議書 (案號：1151003758)

1、 專案名稱

財團法人台灣設計研究院「設計導向 AI 知識基礎建置及驗證」採購案
(以下簡稱本專案)。

2、 專案背景與目標

(1) 專案背景

- 財團法人台灣設計研究院執行「設計領域科技研發暨產研共創應用計畫 (以下簡稱本計畫)」，長期累積設計研究、設計方法、產業輔導、專案案例、研究報告、資料庫及其他設計相關知識資產，資料來源與格式多元，部分資料已具備一定之分類或結構化基礎，惟整體仍以文件、資料夾及既有資料庫分散管理為主，尚未形成可持續擴充、可供人工智慧應用之整合知識基礎。
- 隨生成式人工智慧、檢索增強生成 (Retrieval-Augmented Generation, RAG)、知識圖譜及 AI Agent 等技術發展，設計知識可由單純文件保存，進一步轉化為可檢索、可追溯、可比較及可支援設計研究流程之知識服務。本計畫規劃分階段建立設計知識庫及人工智慧應用基礎，逐步將既有知識內容與實際研究、設計及產業服務流程整合。
- 因應 AI 技術發展，本計畫規劃建立設計導向 AI 知識基礎建置及驗證之平台 (以下簡稱本平台)：把本計畫與合作企業長期累積、散

落且隱性的設計知識，轉化為可檢索、可溯源、可跨案重用的知識服務，協助設計研究與產品設計流程，運用 AI 加速設計研究、刺激創意發想並優化設計工作環節。

- 本平台透過以企業合作示範案，由企業提供資料與需求，驗證系統需要的設計知識建構，逐步成為設計產業可共用的知識底層。
- 本案為四年期發展規劃之第一階段，115 年重點在於資料整理與知識庫建立，包含可用資料盤點、知識分類與重構、資料匯入與處理機制、權限分級、基礎 AI 搜尋與問答，以及企業場域驗證。後續年度將另案依資料權利盤點、知識累積、技術成熟度及實際使用情境，逐步擴充 AI 應用基礎架構、工作流程整合及正式服務平台。
- 本案另規劃以合作企業場域進行 PoC 驗證，選定一家具工業產品設計背景之企業作為示範場域。將累積大量研發與製造知識（設計檢討、規格、製程經驗、品質問題與對策等）等非結構化文件匯入本平台。系統須讓 AI 給出符合該企業判斷邏輯的答案（而非通用回答），用以驗證平台在真實場域的可用性與可信度；但其知識架構、方法論與公用共享層須設計成可複製到其他企業之應用形式。

(2) 專案目標

- 盤點本計畫及示範場域可供本案使用之資料來源、文件格式、授權狀態、機敏程度、結構化程度及預期應用方式，建立後續資料持續納入之基礎機制。
- 建立適用於設計知識之分類、標註、Metadata、知識重構及資料匯入機制，使原始資料得轉換為可供檢索、追溯與人工智慧應用之知識內容。
- 建立具擴充性之知識庫架構，支援不同知識層級、不同來源及不同權限資料之管理，並保留後續串接外部工具、AI 應用與企業自有知識之彈性。

- 建置基礎 AI 知識搜尋與問答能力，提供自然語言查詢、語意檢索、內容摘要、比較與整合、設計建議及決策判斷等功能，且應盡可能呈現回應所依據之知識來源，降低無來源生成之風險。
- 於示範場域完成企業知識庫及 AI 設計輔助應用之 PoC，驗證既有研發知識、流程文件及案例資料導入後之實際可用性。
- 建立資料權限與存取分級原則，針對可上雲資料、限制性資料、企業私有資料及需另行確認授權之資料，採取適當之隔離、存取控制、處理或替代方案。
- 完成 PoC 技術驗證、使用者回饋與後續發展建議，作為後續年度知識累積與 AI 應用基礎架構建置之規劃依據。

3、 專案執行範圍

- (1) 本案採資訊服務與 PoC 系統開發建置方式辦理。廠商應依本計畫核定之需求完成資料整理、知識庫 PoC、AI 搜尋與問答、企業場域驗證、文件交付及必要之技術支援。各項功能之實作方式、模型選擇、畫面配置及底層技術，得由廠商依技術成熟度提出適當方案，但不得影響本案主要目標、資料權限及驗證需求。
- (2) 「設計導向 AI 知識基礎建置及驗證」申請與審查作業、期程與各階段應繳交資料之線上系統化及流程化方法，並依服務建議書與得標廠商實際了解本計畫需求後，執行本案之系統建置。

4、 專案執行時間

決標次日起至 115 年 12 月 15 日止。

5、 專案預算

新臺幣 3,200,000 元整 (含稅) 。

6、規格需求

項次	項目	說明
資訊服務需求		
1	技術選型與系統架構需求	(1)本案採資訊服務與 PoC 系統開發建置方式辦理。廠商應依本計畫核定之需求完成資料整理、知識庫 PoC、AI 搜尋與問答、企業場域驗證、文件交付及必要之技術支援。各項功能之實作方式、模型選擇、畫面配置及底層技術，得由廠商依技術成熟度提出適當方案，但不得影響本案主要目標、資料權限及驗證需求。
2	導入需求確認與現況盤點	(2)廠商應於履約初期與本計畫指定人員辦理需求確認會議，確認本計畫現行資料來源、知識管理方式、使用角色、預期應用情境、部署限制及 PoC 驗證範圍。 (3)廠商應協助盤點本計畫提供之資料，至少記錄資料來源、資料類型、檔案格式、更新頻率、授權狀態、機敏程度、建議處理方式及預期應用。 (4)針對示範場域，廠商應辦理需求訪談與資料現況盤點，確認企業研發工作流程、知識使用情境、可提供之資料範圍、可使用方式、企業資料安全要求及 PoC 成效評估方式。

項次	項目	說明
3	知識架構與資料整理需求	(1)本計畫與示範案例知識之整理，宜能表達專案問題、背景、研究過程、使用方法、關鍵發現、決策、成果及回饋等脈絡。實際欄位與標註方式由廠商提出並經本計畫確認。 (2)廠商應建立知識重構與資料處理規則，至少涵蓋格式解析、文字切分、Metadata 建立、來源保留、去除重複、版本處理、分類標註及必要之品質檢查。 (3)廠商應提供資料匯入流程，支援本案選定之常見文件與結構化資料格式，如遇不支援之格式，應說明限制與替代處理方式。 (4)知識內容應保留可追溯資訊，包括原始來源、文件或資料識別碼、處理日期、版本、知識類別、權限層級及必要之處理紀錄。 (5)廠商應依本計畫既有規劃及需求訪談結果，提出設計知識分類與資料模型。知識層級原則可涵蓋：通用設計知識（Design Foundation）、領域知識（Domain Knowledge）、示範案例知識（Project Knowledge）及企業專屬知識（Enterprise Knowledge）。
4	資料權利與使用原則	(1)本案僅得使用經本計畫或資料權利人確認可供本案處理、分析或建置之資料。廠商不得自行擴張資料授權範圍。 (2)公開取得或本計畫既有可合法使用且得上雲之資料，得依本案核定架構進行雲端處理。 (3)涉及著作權、智慧財產權、契約限制或其他使用權

項次	項目	說明
		利尚待確認之資料，應由本計畫逐案確認其可使用範圍。在未確認前，不得逕自上傳至外部雲端或納入模型訓練。 (4)對於經本計畫確認可進行內容整理但不宜直接保存原始全文之純文字資料，得依核准範圍進行摘要、主題分類、關鍵概念、設計方法、案例特徵或其他知識重構。 (5)不適合上雲之原始資料，得依本計畫核定之部署方式於地端或受控環境完成必要之解析與知識抽取，再將經確認可使用之知識單元匯入知識庫。 (6)示範場域之企業私有資料應與本計畫共用知識適當隔離，並依使用者角色與權限控管存取；未經企業及本計畫同意，不得挪作其他用途、公開揭露或作為一般模型訓練資料。 (7)資料生命週期管理：應建立明確之資料保存期限與自動銷毀機制，並於專案結案後，針對所有機敏數據執行符合資安規範之合規抹除作業。
5	企業場域驗證需求	(1)廠商應與本計畫及示範場域共同確認 PoC 驗證情境、使用角色、測試資料、權限設定及測試方式，選定適合之範圍完成資料處理與知識導入。 (2)應至少辦理一次場域操作測試或工作坊，蒐集實際使用者對搜尋結果、AI 回應、操作流程及實務價值之回饋。 (3)完成「企業場域 PoC 驗證報告」，說明導入資料、測試情境、測試結果、限制、問題、改善建議及後續擴充方向。

項次	項目	說明
		(4)本年度以知識庫、資料治理與基礎 AI 應用驗證為主，應涵蓋至少一項合作企業實際需求應用情境作為驗證標的。
系統建置與驗收需求		
6	系統功能及技術面需求	(1)資料匯入與處理：具備可重複執行之資料匯入與處理機制，得依資料格式進行解析、清理、切分、Metadata 建立、分類及索引，支援的資料格式至少包含 PDF、Word(.docx)、Excel(.xlsx)、csv、純文字、Markdown、圖片格式(.jpg, .png) 等。 (2)知識庫管理：支援知識內容之新增、編輯、更新、查詢、批次上傳 / 下架、版本管理、來源追溯、權限分級及操作紀錄，並建立知識分類、標籤及 Metadata 管理機制，支援文字、圖片、表格、簡報等多元格式及多模態資料之匯入與管理。知識內容應具備審核、發布、更新及下架機制，並支援知識有效期限、版本追蹤及重複內容檢核，以確保知識之正確性、時效性與可追溯性。 (3)語意搜尋：支援關鍵字與語意檢索，檢索算法需涵蓋檢索精準度提升機制（例如 BM25/全文檢索、Cross-encoder、Reranking...）並依照第十項之驗收需求證明其效能，並得依知識類別、資料來源、場域、時間或其他 Metadata 進行篩選。 (4)AI 問答：支援基於知識庫之自然語言問答，並提供可追溯之引用或來源資訊；對無足夠知識依據之問題，應切換成使用大語言模型內建之知識，並提示

項次	項目	說明
		回應不確定性。 (5)知識重構：支援將經核准之原始資料轉換為摘要、主題、關鍵概念、案例特徵、設計方法或其他結構化知識單元。 (6)結構化知識單元轉化：能將非結構化文本自動/半自動提煉為結構化範本，如「關鍵概念」、「案例特徵」、「設計方法論」、「SOP 標準作業程序」等。 (7)關聯知識推薦：依據重構後之知識單元，自動建立相關知識節點間之關聯，便於使用者擴展閱讀。 (8)權限管理：至少支援本計畫共用知識與企業私有知識之隔離，並具備資料存取權限控制。 (9)操作介面：應提供可供本計畫與示範場域測試之網頁介面或其他易於操作之使用方式，至少包含搜尋、問答、來源檢視及基本管理等功能。 (10) 擴充性：系統架構應考量後續串接外部資料來源、即時爬蟲、模型服務、AI Agent workflow、其他設計工具及企業應用之可能性，宜採模組化設計，至少區分資料處理、知識儲存與檢索、AI 模型推論服務及應用操作介面等主要元件，並於技術文件中說明擴充方式。
7	AI 應用與 PoC 使用情境	(1)本案應建置基礎 AI 知識搜尋與問答功能，支援自然語言提問及語意檢索，並得依情境提供摘要、重點整理、跨資料比較、案例搜尋、知識整合、設計建議及決策判斷等。 (2)AI 回應應以本案可使用之知識內容為主要依據；於

項次	項目	說明
		適用情況下，應提供來源文件說明、知識單元或其他可供使用者追溯之依據。 (3)廠商應提出降低生成式 AI 幻覺、來源錯置、敏感資料外洩之設計，例如檢索限制、系統提示、權限過濾、回答拒絕或不確定性提示等。 (4)本案之 AI 應用屬輔助性質，不應取代設計師、研究人員或企業人員之專業判斷；系統應避免將生成內容呈現為未經人工確認之正式決策。 (5)示範場域 PoC 應至少選定一項具體研發或設計工作情境進行驗證，例如：市場趨勢研析、可製造性設計（DFM）、材質挑選與建議等，或經本計畫與示範場域共同確認之其他情境。 (6)示範場域 PoC 應以企業現有資料與實際工作情境為基礎，完成資料導入、權限設定、功能展示、使用者測試及回饋彙整。
8	技術開發規劃及商模建議	(1) 技術發展藍圖：依據本計畫長期專案計劃目標，考量市場技術發展進程與成熟度，提出本平台未來歷年需發展的關鍵技術/核心技術、技術發展路徑圖/策略藍圖（四年期）、研發工作分解結構、成效指標等策略建議。
交付項目與規範需求		
9	AI 知識基礎建置及驗證平台	建置符合規格需求之可運作平台系統，並且知識需符合資訊服務需求。
10	期末驗收報告	(1)系統架構文件：解釋目前的 PoC 系統架構

項次	項目	說明
		(2)知識架構暨資料處理設計說明：如知識分類與資料模型、Metadata、權限分級、資料處理流程 (2)需求確認暨資料盤點：資料來源、類型、格式、權限分類等，含示範場域需求與資料現況 (3)驗證題組 (golden set) 與評測結果：根據本計畫與合作企業共同擬定的題組，實作評測方法與評測結果。 (4)核心功能測試：資料匯入、語意搜尋、AI 問答、來源追溯、權限隔離之測試結果，量化標準請參考項次 11：量化驗收指標。 (5)AI 關鍵技術說明：本專案使用到的 AI 技術如選用模型, Prompt, skills, workflow, RAG 等方法說明 (6)場域驗證結案：導入資料、測試情境、結果、限制、問題、改善建議、後續擴充方向 (7)部署與環境文件：依實際部署形態之部署與環境設定 (8)技術開發規劃及商模建議：工作分解結構 (WBS)、時程、里程碑、風險與溝通機制、Token 費用與成本拆解、四年期技術發展藍圖、商業模式等。 (9)教學說明文件：提供系統操作說明、訓練時數或其他教育訓練方式，確保院內人員與合作企業能上手使用。
11	量化驗收指標	(1)根據專案需求應提出可驗證知識庫成效之量化指標，根據驗證題組，以當前匯入知識的回答題目範圍為例，可以達到 8 成以上「有效回答率」；其中「有效回答」係指系統可提供與題意相關之回答，且能正

項次	項目	說明
		確呈現至少一項可追溯之知識來源。另得輔以檢索結果、來源正確性及使用者回饋等指標進行評估。 (2)有效回答應至少符合下列條件： 1.回答內容與題目需求具實質關聯 2.回答主要內容未明顯偏離知識來源； 3.至少提供一項可供追溯之來源文件或知識單元 (3)於評測報告中以有效回答為基礎，評估並揭露「來源可追溯率、正確拒答率（幻覺控制）」等指標。 * 實際題組、評測方式及有效回答判定標準，於需求確認階段由本計畫共同確認。 * 來源可追溯率為評估「有效回答」結果有沒有附加知識依據的比率。 * 正確拒答率為資訊不足時是否能適當提示或拒答作為評估依據。
12	資訊安全需求	(1)本案依循資通安全法及本計畫資通訊安全政策作為系統開發之整體安全與委外管理之規範，對於處理機敏資料之資訊應用系統，應提出完整安全機制管控規劃，同時參照資通系統管理暨自我檢核表內之項目（等級中之管控措施），進行資料保護與相關系統安全控制措施，以確保資料之機密性、完整性、可用性、法尊依循性，完整地保護各項交易不被盜取、竊改，並杜絕發生系統被入侵之行為。 (2)本案須於驗收前執行至少一次弱點掃描，並完成中等級(含)以上之漏洞修復。 (3)廠商需依本計畫安全需求對於所開發之系統、參與人

項次	項目	說明
		員及程式執行系統安全檢查作業。本計畫亦得對廠商內部涉及本案人員、設施與作業管理程序等，進行不定期資安稽核作業。如有發現違反本計畫資安之事實者，本計畫得依相關法令對廠商提出賠償要求並追究相關法律責任。 (4) 本案廠商所使用之技術與相關工具，以不更動本計畫現有系統運作環境為原則，經本計畫同意後採用。 (5) 系統軟、硬體設備之安全漏洞，廠商於履約期間須進行修補防護，必要時需配合修改所開發程式及更新提升系統軟體版本。本系統之網站應用程式，廠商應提出本案系統防護最新 OWASP TOP 10 證明，並列入「系統資安檢測報告書」內，廠商並應就測試之方式及所採用之工具（原則上應使用商用軟體，若所採用之工具非商用軟體，廠商應於系統資安檢測報告書中詳細敘明）進行說明。 (6) 廠商已通過資通安全管理、隱私資訊管理相關國際驗證如 ISO27001、ISO27701 等，證明廠商於本案系統發展及維運期間具有良好資通安全及隱私資訊管理能力為佳。 (7) 廠商須配置 1 名(含)以上資安人員，並具有資安證照，證照以數位發展部資通安全署最新資通安全專業證照清單內為限。 (8) 本計畫已導入資訊安全管理系統規範，本案需遵循 ISO 27001 規範，並不定期接受上級單位進行稽核，以及第三方驗證及審查，以維持本計畫 ISO 27001 有效性。驗證期間如需廠商配合辦理之事項，廠商應

項次	項目	說明
		配合之，如有衍生相關費用，廠商應自行吸收。 (9) 廠商至本計畫洽公、開會及測試資料等公務時，均不得使用有資安疑慮之大陸廠牌筆電（筆電需安裝最新及有效之防毒軟體）及手機等相關連網設備且不得與公務網路介接。 (10) 專案人員需為建議書內所列人選，不得為陸籍人士，並以本國籍為優先，且未經本計畫同意不得任意更換人選；本案執行期間，專案經理及專案成員之更換，除離職外需經本計畫同意或本計畫提出更換之要求時始得更換，且為利工作交接，既有人員與接手人員必須有 14 個日曆天以上之交接與並行作業期間，另成員更換時亦需符合專長人員資格規定，並檢附相關文件（至少含學經歷、專業證照、勞保投保證明等）通知。

*** 注意事項**

1. 本專案所列功能需求為系統建置基本需求，實際功能細節、操作流程、欄位內容、權限設定及畫面呈現，得於執行期間經需求訪談及討論後調整確認，並以最終核定之系統需求規格書（SRS）為準。
2. 資料轉移：本專案涉及資料作業，得標廠商應配合辦理資料盤點、欄位對應、資料轉換、匯入及驗證等相關工作，並於需求訪談階段提出資料訓練規劃，經本計畫確認後執行。廠商應確保移轉資料之完整性與正確性，於系統正式上線前完成資料移轉測試及驗證，並提供相關紀錄與報告，以利後續查核及系統維運。

7、 比稿項目

投標廠商之比稿項目建議包含但不限於下列各項：

- (1) 知識工程與 AI 調教能力
- (2) 專案管理與時程掌握
- (3) 團隊經驗與類似實績

「設計導向 AI 知識基礎建置及驗證」

資通系統管理暨自我檢核表

☐ 本系統(網站)尚未建置系統(網站)，預計 年 月 日上線。 ☐ 本系統(網站)為後續維護之系統(網站)。							
一、資通系統防護基準自評表							
檢查項目					計畫執行單位自行查驗（請計畫執行單位填寫說明，並勾選是否符合）		
主項目	次項目	系統防護需求	普	中	高	說明現有控制措施（廠商填寫欄）	符合性評估（每題皆須勾選）
1.存取控制	1.1 帳號管理	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。(應說明不使用身分證字號為帳號名稱)	★	★	★	（請廠商說明帳號註冊與審查程序）	☐ 符合 ☐ 不符合
	1.2 帳號管理	已逾期之臨時或緊急帳號應刪除或禁用。		★	★	（請廠商說明臨時帳號禁用機制）	☐ 符合 ☐ 不符合 ☐ 不適用
	1.3 帳號管理	資通系統閒置帳號應禁用。		★	★	（請廠商說明閒置帳號清理機制與定義天數）	☐ 符合 ☐ 不符合 ☐ 不適用

	1.4 帳號管理	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。(應說明週期，並以不超過半年為宜，須檢附審查紀錄)		★	★	(請廠商說明定期審核帳號之週期與作法)	☐ 符合 ☐ 不符合 ☐ 不適用
	1.5 帳號管理	機關應定義各系統之間置時間或可使用期限與資通系統之使用情況及條件。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	1.6 帳號管理	逾越機關所許可之間置時間或可使用期限時，系統應自動將使用者登出。(說明系統登出時間)			★		☐ 符合 ☐ 不符合 ☐ 不適用
	1.7 帳號管理	應依機關規定之情況及條件，使用資通系統。(說明機關規定，包含組態)			★		☐ 符合 ☐ 不符合 ☐ 不適用
	1.8 帳號管理	監控資通系統帳號，如發現帳號違常使用時回報管理者。(應設定特殊權限的嚴格管理措施)			★		☐ 符合 ☐ 不符合 ☐ 不適用

	1.9 最小權限	採最小權限原則，僅允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取。(範圍:運行於作業系統上之網站及資料庫相關應用程式[非使用作業系統最高權限帳號啟動])		★	★	(請廠商說明應用程式與資料庫帳號權限控管方式)	☐ 符合 ☐ 不符合 ☐ 不適用
	1.10 遠端存取	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。	★	★	★	(請廠商說明遠端管理/維運之授權與連線控管，如 IP 白名單、VPN 等)	☐ 符合 ☐ 不符合
	1.11 遠端存取	使用者之權限檢查作業應於伺服器端完成。	★	★	★	(請廠商說明伺服器端權限驗證與防範越權存取之機制)	☐ 符合 ☐ 不符合
	1.12 遠端存取	應監控遠端存取機關內部網段或資通系統後臺之連線。	★	★	★	(請廠商說明後台連線監控與日誌記錄方式)	☐ 符合 ☐ 不符合
	1.13 遠端存取	應採用加密機制。	★	★	★	(請廠商說明遠端存取與傳輸加密機制)	☐ 符合 ☐ 不符合
	1.14 遠端存取	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。		★	★	(請廠商說明維運端之遠端存取控制點管理)	☐ 符合 ☐ 不符合 ☐ 不適用

2.事件日誌與可歸責性	2.1 記錄事件	訂定日誌之記錄時間週期及紀錄留存政策，並保留日誌至少六個月。(應保留以下 4 種 Log) 1.作業系統日誌(OS event log) 2.網站日誌(Web log) 3.應用程式日誌(AP log) 4.登入日誌(Logon log)	★	★	★	(請廠商說明四類日誌留存至少六個月之空間配置與政策)	☐ 符合 ☐ 不符合
	2.2 記錄事件	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。(如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及等)	★	★	★	(請廠商說明系統記錄特定敏感事件之範圍與功能)	☐ 符合 ☐ 不符合
	2.3 記錄事件	應記錄資通系統管理者帳號所執行之各項功能。(如：帳號登出入、密碼變更、存取權限異動等)	★	★	★	(請廠商說明管理者最高權限之稽核日誌 Audit Log 控管機制)	☐ 符合 ☐ 不符合
	2.4 記錄事件	應定期審查機關所保留資通系統產生之日誌。(應說明週期，並以不超過每週為宜。)		★	★	(請廠商說明定期主動審查 / 分析日誌之週期與方式)	☐ 符合 ☐ 不符合 ☐ 不適用

	2.5 日誌紀錄內容	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，採用單一日誌機制，確保輸出格式的一致性，並應依資通安全政策及法規要求納入其他相關資訊。	★	★	★	請廠商說明通用日誌格式與集中管理之輸出機制)	☐ 符合 ☐ 不符合
	2.6 日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。(應配置最少 6 個月之儲存容量)	★	★	★	(請廠商說明主機日誌儲存空間規劃與容量告警機制)	☐ 符合 ☐ 不符合
	2.7 日誌處理失效之回應	資通系統於日誌處理失效時，應採取適當之行動。(如：儲存容量空間不足，選擇進行封存，不要覆寫日誌資料)	★	★	★	(請廠商說明當日誌空間將滿或失效時之自動封存 / 告警機制)	☐ 符合 ☐ 不符合
	2.8 日誌處理失效之回應	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。(特定人員：系統相關人員)			★		☐ 符合 ☐ 不符合 ☐ 不適用

	2.9 時戳及校時	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	★	★	★	(請廠商說明內部系統時鐘與日誌時戳對齊世界標準時間之作法)	☐ 符合 ☐ 不符合
	2.10 時戳及校時	系統內部時鐘應定期與基準時間源進行同步。(應說明週期，並以不超過每週為宜。)		★	★	(請廠商說明校時工具及同步週期)	☐ 符合 ☐ 不符合 ☐ 不適用
	2.11 日誌資訊之保護	對日誌之存取管理，僅限於有權限之使用者。	★	★	★	(請廠商說明限制日誌查閱、下載與刪除之帳號與權限管控機制)	☐ 符合 ☐ 不符合
	2.12 日誌資訊之保護	應運用雜湊或其他適當方式之完整性確保機制。		★	★	(請廠商說明防止日誌遭竄改之完整性驗證或儲存防護機制)	☐ 符合 ☐ 不符合 ☐ 不適用
	2.13 日誌資訊之保護	定期備份日誌至原系統外之其他實體系統。(應說明週期，並以不超過每週為宜。)			★		☐ 符合 ☐ 不符合 ☐ 不適用
3.營運持續計畫	3.1 系統備份	訂定系統可容忍資料損失之時間要求。	★	★	★	(應承諾最大 RPO 時間為 24 小時，並說明備份頻率)	☐ 符合 ☐ 不符合
	3.2 系統備份	執行系統源碼與資料備份。	★	★	★	(請廠商說明系統原始碼與資料庫定期備份之排程與機制)	☐ 符合 ☐ 不符合

	3.3 系統備份	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。(應說明週期，並以不超過每季為宜。)		★	★	(請廠商說明每季定期執行備份資訊有效性檢驗與記錄之作法)	☐ 符合 ☐ 不符合 ☐ 不適用
	3.4 系統備份	應將備份還原，作為營運持續計畫測試之一部分。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	3.5 系統備份	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	3.6 系統備援	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。(須與當年核定之最大可容忍中斷時間相同)		★	★	(應承諾復原時間目標 $RTO \leq 12$ 小時，並說明復原評估)	☐ 符合 ☐ 不符合 ☐ 不適用
	3.7 系統備援	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。		★	★	(請廠商說明高可用性機房架構或備援設備迅速回復服務之機制)	☐ 符合 ☐ 不符合 ☐ 不適用
4.識別與鑑別	4.1 內部使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	★	★	★	識別方式： ☐ 帳號 ☐ 憑證 ☐ 其他 鑑別方式： ☐ 密碼 ☐ PIN 碼 ☐ 其他	☐ 符合 ☐ 不符合

	4.2 內部使用者之識別與鑑別	對資通系統之存取採取多重認證技術。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	4.3 身分驗證管理	使用預設密碼登入系統時，應於登入後要求立即變更。 (建議透過系統機制要求使用者登入後立即變更密碼)	★	★	★	(請廠商說明系統如何強制首次登入變更預設密碼或由使用者自訂)	☐ 符合 ☐ 不符合
	4.4 身分驗證管理	身分驗證相關資訊不以明文傳輸。	★	★	★	(請廠商說明身分驗證資料、密碼之隱碼加密傳輸與雜湊儲存演算法)	☐ 符合 ☐ 不符合
	4.5 身分驗證管理	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。	★	★	★	(請廠商說明登入失敗鎖定機制之次數與鎖定時間限制)	☐ 符合 ☐ 不符合
	4.6 身分驗證管理	使用密碼進行驗證時，應強制最低密碼複雜度;強制密碼最短及最長之效期限制。(密碼不少於12碼，且由大小寫、數字及符號組成混合，且需在一定期間[1~90天]內變更)	★	★	★	(請廠商說明密碼複雜度原則、最長 90 天與最短 1 天之效期限制組態)	☐ 符合 ☐ 不符合
	4.7 身分驗證管理	密碼變更時，至少不可以與前三次使用過之密碼相同。	★	★	★	(請廠商說明系統防止重複使用歷史密碼之限制機制)	☐ 符合 ☐ 不符合

	4.8 身分驗證管理	對非內部使用者，可依機關自行規範密碼設定強度、效期與密碼不重複次數。	★	★	★	(請廠商說明對外部廠商 / 公眾使用者帳號之密碼安全強度規範)	☐ 符合 ☐ 不符合
	4.9 身分驗證管理	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。(應有 captcha 等相關機制，請提供佐證)		★	★	(請廠商說明防範機器人自動化惡意登入之防護機制並檢附佐證)	☐ 符合 ☐ 不符合 ☐ 不適用
	4.10 身分驗證管理	密碼重設機制對使用者新身分確認後，發送一次性及具有時效性符記。		★	★	(請廠商說明密碼重設流程之安全性與一次性符記時效限制)	☐ 符合 ☐ 不符合 ☐ 不適用
	4.11 鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。(如：以*取代真實輸入字元)	★	★	★	(請廠商說明密碼輸入欄位之遮蔽處理)	☐ 符合 ☐ 不符合
	4.12 加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。		★	★	(請廠商說明資料庫儲存密碼之單向雜湊演算法與加鹽 Salt 機制)	☐ 符合 ☐ 不符合 ☐ 不適用
	4.13 非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	★	★	★	識別方式： ☐ 帳號 ☐ 憑證 ☐ 其他 鑑別方式： ☐ 密碼 ☐ PIN 碼 ☐ 其他	☐ 符合 ☐ 不符合
5.系統與服務獲得	5.1 系統發展生命週期需求階段	針對系統安全需求(含機密性、可用性、完整性)，進行確認。	★	★	★	(請廠商說明如何透過安全評估機制確認平台三項安全構面)	☐ 符合 ☐ 不符合

	5.2 系統發展生命週期設計階段	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。		★	★	(請廠商說明設計階段執行威脅識別與專案風險評估之規劃)	☐ 符合 ☐ 不符合 ☐ 不適用
	5.3 系統發展生命週期設計階段	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。		★	★	(請廠商說明如何將風險評估結果回饋至後續開發之安全修正)	☐ 符合 ☐ 不符合 ☐ 不適用

	5.4 系統發展生命週期開發階段	應針對安全需求實作必要控制措施。 (系統發展生命週期皆適用) 主機使用之防毒軟體及版本。 定期更新主機 patch。(應說明週期，並以不超過每月為宜。) 網路具有防火牆防護。 網路或主機具有入侵偵測機制 (IDS)。 網路或主機是否具有入侵防禦機制 (IPS)。 網站是否設有反弱點防護機制(網站漏洞修補前之替代性防護機制)？ 資安防護設備(如防火牆、入侵防禦機制等)是否設有偵測與告警機制，並有專人定期檢視？(應說明週期，並以不超過每週為宜。) 存放資通訊設備區域是否設有安全保護措施(例如門禁管理、不斷電(UPS)系	★	★	★	(請廠商逐項填寫 1~13 項雲端主機/網路資安防護設備之軟硬體名稱、版本與更新週期)	(1~13 項控制措施皆須符合才可勾符合) ☐符合 ☐不符合
--	------------------	--	---	---	---	--	---

		統、空調設備、消防設備等)？ 對具儲存資訊之設備外送維修時，是否具有安全評估措施？(例：備份資料後，將外送設備的資料抹除後再送修。) 是否具有資訊安全防護中心(SOC)24小時網路監控及通報機制？ 機房是否有 24 小時操作人員輪值？					
--	--	---	--	--	--	--	--

	5.5 系統發展生命週期開發階段	應注意避免軟體常見漏洞及實作必要控制措施。	★	★	★	(請廠商說明軟體開發如何遵循 OWASP Top 10 或安全程式碼規範)	☐ 符合 ☐ 不符合
	5.6 系統發展生命週期開發階段	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。	★	★	★	(請廠商說明例外處理機制，避免在前端暴露底層除錯或資料庫語句)	☐ 符合 ☐ 不符合
	5.7 系統發展生命週期開發階段	執行「源碼掃描」安全檢測。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	5.8 系統發展生命週期開發階段	系統應具備發生嚴重錯誤時之通知機制。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	5.9 系統發展生命週期測試階段	執行「弱點掃描」安全檢測。 (1.系統發展生命週期皆適用。 2.範圍為網頁、主機、網路系統且需涵蓋 OWASP 最新 TOP 10 中指出的網頁應用程式常見弱點的檢測。 3.修補掃描結果各等級之弱點，並應再次確認已無弱點。)	★	★	★	(請廠商說明預計使用之弱掃工具、執行廠商、並承諾上線前完成所有風險修補)	☐ 符合 ☐ 不符合

	5.10 系統發展生命週期測試階段	執行「滲透測試」安全檢測。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	5.11 系統發展生命週期部署與維運階段	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	★	★	★	(請廠商說明上線組態檢視、關閉無效 Port 與正面表列開啟 Port 之清單)	☐ 符合 ☐ 不符合
	5.12 系統發展生命週期部署與維運階段	資通系統不使用預設密碼。	★	★	★	(請廠商承諾所有託管基礎設施、資料庫及管理帳號絕不使用預設密碼)	☐ 符合 ☐ 不符合
	5.13 系統發展生命週期部署與維運階段	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。 (原始程式庫新增、修改、修改存取是否有控制措施並留有稽核日誌記錄存取行為)			★	★	☐ 符合 ☐ 不符合 ☐ 不適用
	5.14 系統發展生命週期委外階段	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。	★	★	★	(請廠商說明如何配合本案契約規範，將安全需求貫徹至開發生命週期)	☐ 符合 ☐ 不符合
	5.15 獲得程序	開發、測試及正式作業環境應為區隔。		★	★	(請廠商說明開發、測試、正式環境之實體區隔或邏輯隔離部署架構)	☐ 符合 ☐ 不符合 ☐ 不適用

	5.16 系統文件	應儲存與管理系統發展生命週期之相關文件。(應以書面或電子化形式保存，並被納入管理程序)	★	★	★	(請廠商說明系統需求書、規格書、測試報告等技術文件之儲存與管理方式)	☐ 符合 ☐ 不符合
6.系統與通訊保護	6.1 傳輸之機密性與完整性	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。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	6.2 傳輸之機密性與完整性	使用公開、國際機構驗證且未遭破解之演算法。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	6.3 傳輸之機密性與完整性	支援演算法最大長度金鑰。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	6.4 傳輸之機密性與完整性	加密金鑰或憑證應定期更換。(應說明檢查週期，並以不超過每季為宜。)			★		☐ 符合 ☐ 不符合 ☐ 不適用
	6.5 傳輸之機密性與完整性	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。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	6.6 資料儲存之安全	資通系統重要組態設定檔案及其他相關具保護需求之資訊應加密或以其他適當方式儲存。			★		☐ 符合 ☐ 不符合 ☐ 不適用

7.系統與 資訊完整 性	7.1 漏洞修 復	系統之漏洞修復應 測試有效性及潛在 影響，並定期更 新。（應說明週 期，並以不超過每 月為宜，須檢附測 試佐證）	★	★	★	（請廠商說明每月元 件、軟體套件之安全漏 洞關注與環境測試更新 程序）	☐ 符合 ☐ 不符合
	7.2 漏洞修 復	定期確認資通系統 相關漏洞修復之狀 態。（應說明週 期，並以不超過每 週為宜。）		★	★	（請廠商說明每週主動 清查、確認 OS 或應用 軟體漏洞更新狀態之機 制）	☐ 符合 ☐ 不符合 ☐ 不適用
	7.3 資通系 統監控	發現資通系統有被 入侵跡象時，應通 報機關特定人員。 (特定人員:系統相關 人員)	★	★	★	（請廠商承諾發生資安 事件時之即時通報窗 口、1 小時內通報產發 署與緊急應變機制）	☐ 符合 ☐ 不符合
	7.4 資通系 統監控	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。		★	★	（請廠商說明進出通信 流量監控、異常連線偵 測與即時告警通知之工 具）	☐ 符合 ☐ 不符合 ☐ 不適用
	7.5 資通系 統監控	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。			★		☐ 符合 ☐ 不符合 ☐ 不適用
	7.6 軟體及 資訊完整 性	使用完整性驗證工 具，以偵測未授權 變更特定軟體及資 訊。		★	★	（請廠商說明如何透過 檔案完整性監控、防毒 軟體定時檢查以防止惡 意竄改）	☐ 符合 ☐ 不符合 ☐ 不適用

	7.7 軟體及 資訊完整性	使用者輸入資料合法性檢查應置放於應用系統伺服器端。		★	★	(請廠商說明伺服器端如何利用正規表示式或白名單驗證輸入欄位之合法性)	☐ 符合 ☐ 不符合 ☐ 不適用
	7.8 軟體及 資訊完整性	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。		★	★	(請廠商說明當偵測到資料庫或檔案遭破壞竄改時之緊急隔離與還原應變處置)	☐ 符合 ☐ 不符合 ☐ 不適用
	7.9 軟體及 資訊完整性	應定期執行軟體與資訊完整性檢查。 (應說明週期，並以不超過每季為宜。)			★		☐ 符合 ☐ 不符合 ☐ 不適用

單位名稱：

單位負責人或代表人：

地址：

統一編號：