需求說明書（含驗收規範）

壹、購案名稱

「ITIS 資料建置及 API 串接與轉檔架構維護」採購案

貳、履約期限與預算

一、 履約期限（如遇假日，原則順延至次一工作日，有分階段交付者亦同；惟實際是否順延仍依本會需求為準）

■決標次日起至 114 年 12 月 10 日止。

二、 預算

新台幣 800,000 元整（含稅）。

參、需求說明

一、設計宗旨／風格

設計風格應符合專業、簡潔、易於瀏覽之特點。

二、網站（以下簡稱履約標的）開發環境

(一)作業系統：Windows 2016 Server or Windows 2016 Server R2 SP1 以上相容。

(二)資料庫：Microsoft SQL Server 2016 以上相容。

(三)技術架構：ASP.NET、ASP.NET MVC

三、使用者操作介面

(一) 提供使用者以 WWW 瀏覽器（Browser）軟體連結及查詢履約標的各項服務。

(二) 瀏覽器相容版本應支援 Chrome、Safari、Firefox、Microsoft Edge…瀏覽器環境。

(三) 履約標的須為繁體中文介面，字集定義以 UTF-8 為原則，瀏覽器編碼方式於「自動選取」選項下不得出現亂碼。

(四) 支援行動裝置作業系統 iOS 14、Android 11 以上版本。

四、 需求內容

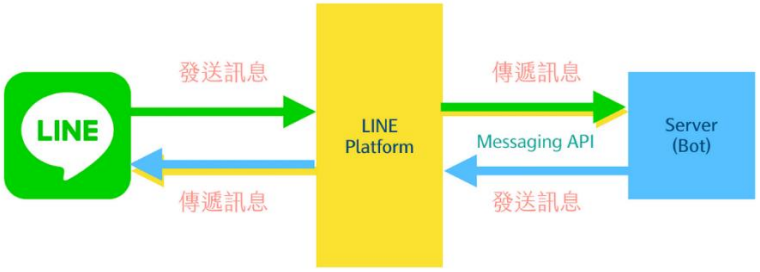
(一)向量資料建立與搜尋

項次	功能項目	功能說明
1	報告段落讀取與前處理	1. 解析報告原始檔案，支援 HTML 格式。 2. 自動濾除無效標籤（如 <script>、<style>）、特殊符號或非內容相關之雜訊。 3. 進行段落切分，保留段落標題、內文與其上下文語境資訊。
2	段落向量化處理	1. 使用語言模型（如 OpenAI Embeddings、LangChain Embedding 等）將每段文字轉換為語意向量。 2. 向量資料內容包含： (1)報告編號與相關 metadata (2)段落標題：便於回顧與理解搜尋結果。 (3)段落文字：實際的段落主體內容。

3	建立向量索引與儲存	1. 使用向量資料庫（chromadb）儲存向量資料。 2. 對所有段落向量進行索引建構，以支援相似度查詢。 3. 每筆向量資料綁定其來源報告編號與報告標題，以利後續查詢回傳。
4	新報告排程處理	1. 系統支援定期排程自動更新，處理新上架的報告。 2. 自動觸發前處理與向量化流程，將新資料納入向量資料庫。
5	查詢 API 設計	1. 提供標準 RESTful API，供用戶提交自然語言查詢並取得相關結果。 2. 系統將使用者輸入的查詢文字轉換為語意向量，並與資料庫中的段落向量進行相似度比對，計算相關性分數。 3. 輸入：自然語言查詢系統處理後，擷取與查詢語意最接近的前 N 筆資料。 4. 輸出：回傳 JSON 格式資料，包含相似度最高的前 N 筆結果。每筆資料可包含報告標題、內容、相似度分數與報告編號等欄位。

(二)其他需求

序	功能項目	功能說明
1	交談對話 API	1. 系統提供一組對話 API，支援用戶以自然語言提問，並獲得具參考依據的智慧回覆。 2. 使用者透過應用端輸入問題後，系統會接收查詢並將其語意向量化，再透過向量比對技術，從資料庫中找出最相關的段落或報告內容。系統接著將這些參考資料提供給語言模型作為上下文，生成語意完整且具有回應性的答案。 3. API 回傳格式為 JSON，內容包含 AI 生成的回覆文字，並可選擇性附上參考報告列表。每筆參考資料包含報告標題與超連結，使用者可點擊連結以檢視完整的原始報告內容。
2	LINE 對話服務與每日新聞推送	1. 使用者透過 LINE 聊天視窗傳送訊息，由 LINE 平台透過 LINE Messaging API 接收並轉發訊息。 2. 後端客服系統串接對話 API，負責接收使用者訊息並回傳對應的回覆內容。 3. 系統每日依排程整理最新產業新聞，轉換為符合 LINE 推播格式的訊息，並透過 Messaging API 發送給群組用戶。 4. 處理 webhook 相關功能，包括訊息接收、回覆與推播通知等作業。

		
3	報告剖析擴充	1. 因應報告格式改版，系統將進行相應調整，支援以下格式變動項目： (1)字體顏色 (2)字型大小 (3)段落間距 (4)排版結構 2. 在現有的報告剖析排程中，新增「標題一完整內容」的擷取功能。系統將擷取每個第一層章節標題（標題一）下的所有段落文字，包含其子標題所屬的內容，並排除圖表說明等非正文資料。 3. 擷取後的內容將進行結構化處理，並儲存至資料庫，供後續查詢與分析使用。
4	PPT 簡報剖析擴充	1. 在現有的簡報剖析排程中，新增「完整內容」的擷取功能。 2. 系統將自動判斷簡報的主要內容範圍，排除首頁、大綱頁與結尾頁，並擷取主要頁面中的所有文字資料。擷取後的內容將進行結構化處理，並儲存至資料庫，以供後續查詢與應用使用。
5	報到 APP 擴充與維護	1. AISP 與 ITIS 報到 APP，系統在回寫學員報到時間的同時，將同步更新「給檔 Flag」欄位。 2. 修正程式錯誤，包括 Crash、UI 異常、資料錯誤等問題。 3. 支援作業系統版本更新（iOS/Android）。 4. 升級第三方套件或 SDK，以維持相容性與功能穩定。 5. 進行硬體相容性測試，確保 APP 可於多款裝置正常運作。 6. UI/UX 微調與優化，提升使用者體驗。

五、 維護需求說明

(一) 技術諮詢服務：有關本案相關之系統問題的技術支援、E-mail詢問、電話協助等，基本時間為星期一至星期五（不含國定假日）上午九點至下午六點，另行約定時間、例假日或有7*24維修條款不在此限。

(二) 維持系統功能不中斷、中斷後之恢復、故障修復，隨時提供遠端連線技術與問題支援服務，若有必要並應親自到場服務，於通知日起24個工作小時內修復或排除問題。

(三) 維護時效：

1. 當系統出現錯誤或功能錯誤時，接獲本會之要求諮詢服務，應於4個工作小時內回應，並協助解決問題進行系統修復、瑕疵與錯誤之修正。若仍無法經由遠端簽入進行修復時，則應提供免費派員修正之維護服務，並於3個工作天內檢修完成。
2. 未依規範時限內完成者，每逾一小時則依契約總價金千分之3計算逾期違約金（不足一小時，以一小時計），直至修復完成並恢復正常運作。除有特殊原因未能於規定時限內完成，並經本會同意且另訂相關時限者除外。

(四) 因法令或作業方式修改，所引起之系統或程式功能之變更、新增之電腦報表、查詢功能等。

(五) 配合本會需求，進行系統局部功能之調整，或新增、修改網頁內容、網頁圖片資料的修改與製作，並提供電子檔等。

(六) 維護期間，系統及各模組需能隨電腦作業系統及網路瀏覽器版本免費升級。或有任何版本更新或異動時，亦需提供免費更新服務。

(七) 本案系統操作中所發生任何異常事項之問題回覆。

(八) 支援系統備援及緊急回復工作，並視本會要求配合執行系統遷移不同伺服主機作業。

(九) 維持本案系統與其他相關系統整合介面之正常運作（含介接作業所需之欄位增修），並需整合舊網站，且不影響舊網站之功能；若有影響，得標廠商應負責修正調整，維持整體網站之正常運作；前述所稱網站均指本案之網站，如專指擴充前系統或網站則稱之為舊系統/網站。

六、 維護管理要求：

(一) 資安要求：

1. 本系統為普級系統，另本購案涉及資通系統之建置、維運，得標廠商應依「資通系統防護基準控制措施」(詳附件)完成指定控制措施(提醒：新開發系統須先進行資通系統防護需求分級)
2. 如需使用雲端運算服務，應依「雲端運算服務資訊安全要求（附件）」執行。
3. 所有資料異動必須提供 Log 記錄供查詢。
4. 須記錄使用者登入之 IP 位址及登入時間。
5. 後台管理者應配合本會密碼政策，如無特殊需求應限制後台管理者登入位址。
6. 檔案下載時應隱藏檔案之實體路徑，避免發生資料外洩事件。
7. 驗證人員登錄之系統，須配合使用可防禦暴力破解攻擊之機制（如：圖形化驗證碼、CAPTCHA、reCAPTCHA 等），登入後須透過 SSL/TLS 加密機制傳輸網頁資料。
8. 會員系統、活動報名系統及驗證人員登錄系統，需配合圖形化驗證碼以降低暴力破解發生機率，登入後需透過 SSL 加密機制傳輸網頁資料。
9. 所有儲存於資料庫的密碼（及敏感資料）必須加以編碼。
10. 得標廠商應遵守本會的資通安全規範及相關資安作業流程標準，於專案執行期間（含保固期間），並應配合本會執行相關資安活動（如：資安稽核、業務持續運作演練、弱點掃描等），並完成中、高風險的修補。
11. 得標廠商應協助本會處理及通報資通安全事件。
12. 原始程式碼、應用程式與安裝包須確保無病毒、無後門且可執行。

13. **安全性檢測：**

(1) 於開發完成及正式上線前，須提供安全性檢測證明：

I. 原始程式碼安全性證明（本會或業主為政府部門之系統／網站／網頁（Web）／模組者必選)

■履約標的為本會議定之非核心系統／網站（Web）／網頁／模組功能者：需提供原始程式碼安全性證明(不限檢測工具)。

II.應用程式弱點掃描報告

履約標的含系統／網頁／網站（Web），需提供最新版 OWASP Top 10 之弱點掃描報告（如 Micro focus Fortify WebInspect, Acunetix, AppScan 或由得標廠商建議並經本會請購部門同意之檢測工具）。

(2) 提供實體主機服務者，不得提供及使用大陸廠牌資通產品；提供實體或虛擬主機服務者，除採下述情形辦理者外，於正式上線前須提供架設主機之安全性檢測證明（如 Nessus 或由得標廠商建議並經本會請購部門同意之檢測工具）：

I. 提供虛擬主機服務者，得以檢附 ISO 27001 及 ISO 27017 認證文件代替安全性檢測證明；若資料處理內容涉及個資者須另提供 ISO 27018 認證文件。

II.架設於 AWS／GCP／Azure 之雲端服務者，免附安全性檢測證明及 ISO 認證文件。

(3) 上述檢測工具由得標廠商負責提供，檢測結果不可含有中、高以上之風險等級，且不因已履約、驗收完成而免除檢測及修復責任。

七、 法令依據及相關規定

(一) 資通安全管理規定：

1. 得標廠商應遵守「委外廠商之資通安全責任事項」(詳附件)。
2. 得標廠商應遵守「委外廠商之資通安全責任特別約定事項」(詳附件)。

八、 保固需求

■無

九、 其他

(一) 商用產品模組

本案若另行採購商用產品模組，須包含該授權書及函式呼叫等開發相關說明文件，且費用包含在契約價款之中。

(二) 商用檔案

本案若另行採購商品圖片、個人著作圖片、音樂...等，須包含該授權書，且費用包含在契約價款之中。

肆、交付說明

一、 交付項目、內容、期限如下：

項目	交付項目	交付內容	數量	交付型態	交付期限

1	資安文件	1. 得標廠商簽署之「委外廠商資通安全管理措施說明表」 2.主機資通安全管理要求檢核表(詳附件)	各 1 份	電子檔	決標次日起 28 日曆天
2	專案系統完成開發	原始程式碼	1 式	電子檔	同本案履約期限
3	相關手冊	1. 測試報告書 (1) 功能測試報告 (2) 安全性檢測報告 2. 開發文件（需包含資料庫欄位說明及 Schema 相關建置資料）	1 式	電子檔	同本案履約期限
4	商用授權書	所用商用產品模組、檔案之授權書或購買證明	依實際狀況檢附，若無則免		同本案履約期限
5	資安文件	1. 資通系統防護基準實施情形廠商自評表 ※格式請向購案聯絡人索取。 2. 資料返還、刪除、銷毀聲明書(詳附件) ※有保固者於保固期滿時交付	各1份	電子檔	同本案履約期限

備註：得標廠商應依本會需求配合調整各階段交付期限，惟不可超過本案履約期限。

二、 交貨地點：台北市大安區敦化南路二段 216 號 19 樓。

三、 得標廠商應依上表提供履約標的，並提供履約通知文件予本會〔購案聯絡人〕確認。

四、 履約通知文件參考格式可至 http://www.iii.org.tw /綜合公告/採購資訊/檔案下載區下載，廠商亦可自訂格式（Email 亦視同履約通知文件，惟內容應足資識別本案）。

五、 履約通知文件僅為通知本會交付全部或部份履約標的，相關驗收事宜另依本會驗收程序辦理，本會驗收合格後方視為履約完成。

伍、驗收規範

一 依本案需求說明書（若購案有服務建議書者亦併同納入）進行數量、內容點收。

二 維護標的可正常運作且無異常狀況，並符合本案需求說明書所規範維護標的之維護服務方式。

三 購案查驗/驗收後，經本會複查證明文件有缺失者，本會得扣除缺失價款外，加計缺失價款 20%計罰懲罰性違約金；若其缺失無明確計算基礎，依契約總價款 20%做為缺失價款，加計懲罰性違約金同前，不因已完成查驗/驗收而受影響。

四 本會得要求得標廠商配合出席參加驗收會議，協助做成果展示及口頭簡報（須提供紙本及電子檔各一份，驗收會議時間本會另行通知）。

五 本會得要求得標廠商依據本會驗收會議意見修訂調整交付項目內容，且應附上意見回覆對照（須提供紙本及電子檔各一份。

陸、其他注意事項

一、 購案聯絡人：

姓　名：產業情報研究所　賴俊銘先生

電　話：(02) 6631-1263

Email：jimmy@iii.org.tw

二、 發票資料：

抬　頭：財團法人資訊工業策進會

統一編號：05076416

柒、審查須知

詳投標須知之「審查須知」內容；審查項目及建議書撰寫重點如下述。

項次	項目	服務建議書撰寫重點 **（請依下列章節序參考製作）**
		封面、目錄
1	**執行力與配合度** ●人力配置規劃 ●執行團隊之相關經驗、學經歷及過去績效 ●計畫執行及管理能力	1. 公司簡介 （1） 業務範圍 （2） 人力、資本額 2. 執行團隊組織與工作分配 3. 專案負責人及執行團隊成員履歷：包含現職、學經歷等 4. 廠商履約實績：請詳述專案經驗及其成效
2	**整體企劃** ●設計理念、使用者友善及管理人員管理及資料維護之便利性 ●執行進度之時程規劃	5. 使用者友善及管理人員管理資料維護設計 6. 資訊安全規劃及執行方式 7. 網站測試、教育訓練之規劃及執行方式 8. 提供時程進度規劃，說明相關工作預定進度、完成時點
3	**經費合理性** ●相關執行費用估算與分配之合理性	9. 於服務建議書詳列報價內容（請參考Excel 附件〔**委外開發報價明細表**〕填寫）

【附件】

委外廠商之資通安全責任事項

一、 辦理受託業務之相關程序及環境，應填寫「委外廠商資通安全管理措施說明表」佐證具備完善之資通安全管理措施，或通過第三方驗證(TAF 認證機構)，如受託業務涉及提供雲端服務者，應提供原廠 ISO 27001 標準認證。

二、 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，負責推動、協調及督導資通安全管理事項。

三、 經本會同意，委外廠商始得將受託業務分包予第三人，委外廠商須要求並監督該第三人應具備與委外廠商同等之資通安全維護措施及標準，並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。

四、 辦理客製化資通系統之開發，若涉及利用非自行開發之系統或資源者，應標示非自行開發之內容與其來源及提供授權證明。

五、 辦理受託業務，違反資通安全相關法令或知悉資通安全事件發生時，應立即通知本會承辦單位及採行必要之補救措施，並應配合本會之資通安全事件通報及相關處理作業。委外廠商未為通知或未配合本會相關處理作業者，應就本會因此所生之一切損害負賠償責任。

六、 委託關係終止或解除時，委外廠商就履行委託契約而持有之資料應返還、移交、刪除或銷毀，並填具「資料返還、刪除、銷毀聲明書」。

七、 委外廠商同意本會得定期或於知悉發生可能影響本案之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

八、 委外廠商受託業務涉及資通訊軟體、硬體或服務等相關事務者，執行本案之團隊成員不得為大陸籍人士，並不得提供及使用大陸廠牌資通產品或服務。

九、 受託業務涉及國家機密時，執行業務之相關人員應接受適任性查核，並受國家機密保護法規定之管制。

委外廠商應確保執行該業務之所屬人員及可能接觸該國家機密之其他人員，無下列事項：

(一) 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

(二) 曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

(三) 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

(四) 招標公告、招標文件或契約所載其他與國家機密保護相關之具體項目。

十、 委外廠商執行受託業務之人員進出本會範圍應受限制。且應遵守本會「資通服務廠商派駐人員資通安全同意表」之資通安全相關規定。

十一、委外廠商駐點人員若要更換或撤離，應填寫「資通服務廠商派駐人員撤離資料表」。

【附件】

委外廠商之資通安全責任特別約定事項

一、委外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，並遵守本會、本會業主之資通安全管理及保密相關規定。此外，本會、本會業主保有依本會與委外廠商同意之適當方式對委外廠商及其分包廠商以派員稽核、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，稽核結果不符合本採購案約定、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，於接獲本會通知後應於期限內完成改善，未依限完成者，依本採購案之契約或履約相關規定「違約罰則」約定計罰逾期違約金。

二、委外廠商執行本採購案應依行政院、本會及本會業主資通安全要求，執行必要之系統設定及修補等改善措施。

三、委外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。涉及利用非委外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，委外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。

如履約項目涉及資通系統且(1)屬本會、本會業主之核心資通系統，或(2)採購金額達新臺幣一千萬元以上，委外廠商交付之軟硬體及文件，應接受本會、本會業主，或本會、本會業主所委託之第三方進行安全性檢測：弱點掃描。

四、委外廠商所提供之服務，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。

五、委外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，以符合甲方對系統品質及資通安全的要求。

六、委外廠商提供服務，如違反資通安全相關法令、知悉本會或自身發生資安事件時，均必須於 1 小時內通報本會，提出緊急應變處置，並配合本會做後續處理；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。

七、委外廠商如有下列情形，應依下列約定負責：

1. 委外廠商未為通知或未配合本會相關處理作業者，應就本會因此所生之一切損害負賠償責任。如造成第三人損失者，亦同。
2. 本會業主為**經濟部產業發展署或數位發展部數位產業署**時，履約期間內委外廠商提供之資訊服務，如有未達本會所定服務水準及績效，除有不可抗力或不可歸責於委外廠商事由外，依本項約定計算違約金。屬遲延性質之損害賠償，且已依本採購案之契約或履約相關規定「違約罰則」約定計罰逾期違約金者，不再依本項計算違約金。但屬遲延性質之項目依本項計算違約金數額較高者，改依本項計算。

   (1) 依本項計算違約金之總額，以新臺幣<u>◯◯</u>元為上限。

   (2) 服務水準及績效違約金計算方式詳下表：

〔表 1-1〕

評估項目	評斷方式	要求基準	違約金計點	是否須符合要求？	每點違約金金額
定期維護	未依契約規定維護	每次統計	每逾○○○，計○點	□是。 □否，本案無資通系統。	依本表計罰之違約金，每點為新臺幣○○○元
故障排除、系統修復	系統中斷時間，不得高於○○○小時	每次統計	每次計○○○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	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○○，計○點	□是。 □否，本案無資通系統。	
	資安事件之通報及應變：自知悉或接獲資安事件通知或即時警示（不滿1小時，以1小時計）	應至遲於30分鐘內通報本會，並於4小時內提供資安事件等級評估、處理應變規劃及建議	1.資安事件每次計○點。每逾○○小時未通報本會計○點。 2.每逾○○小時未提供資安事件等級評估、處理應變規劃及建議計○點。	無論是否有資通系統，如知悉資安事件，均須配合通報。	
	完成損害控制或復原作業之時效（不滿1小時，以1小時計）	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○○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（或協助本會調查處理）	每逾○○日，計○點		

評估項目	評斷方式	要求基準	違約金計點	是否須符合要求？	每點違約金金額
	本會、本會業主資料之機密性及完整性	本會、本會業主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	委外廠商於本契約承接範圍內，因未採取適當防護，致本會、本會業主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	□是。 □否，本案無資通系統。 □不適用，本案資通系統無敏感資料。	
	個人資料之機密性及完整性	資通系統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	委外廠商於本契約承接範圍內，因未採取適當防護，致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		
其他	違反契約約定委外廠商應履行之項目	每季不得超過○次	按超過之次數計算，每超過乙次計○點		

〔表 2-1〕

評估項目	評斷方式	要求基準	違約金計點	每點違約金金額
定期維護	未依契約規定維護	每次統計	每逾○○○，計○點	依本表計罰之違約金，每點為新臺幣○○○元
故障排除、系統修復	經本會通知(不限形式)後，未依契約規定，修復或提供相同系統供本會暫時使用	每次統計	每逾○○○，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	

評 估項目	評斷方式	要求基準	違約金計點	每點違約金金額
資 安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾○○日計○點	
	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 小時內通知本會（或接獲本會通知 1 小時內），並採取適當之應變措施	每逾◯◯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◯◯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（或協助本會調查處理）	每逾◯◯小時計◯點	
	本會、本會業主資料之機密性及完整性	本會、本會業主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	委外廠商於本契約承接範圍內，因未採取適當防護，致本會、本會業主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	本會、本會業主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	委外廠商於本契約承接範圍內，因未採取適當防護，致本會、本會業主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	

評估項目	評斷方式	要求基準	違約金計點	每點違約金金額
出席或主持會議	未出席或主持者	每季統計	按每人每次計○點	
派駐機關服務人員	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	
服務團隊成員	服務團隊成員未依工作計畫（或建議書）滿編，依未滿編之日數計算	每季統計	每日計○點	
	服務團隊成員離任人數（扣除本會要求離任）除以全體成員之異動率，不得高於○○%	每季統計	每逾○○%計○點	
會議決議	累計未依會議決議執行之次數	每季不得超過○次	按超過之次數計算，每次計○點	
	累計未依會議決議應完成期限天數	每季不得超過○○天	按超過之天數計算，每天計○點	
節能減碳	按採購文件規定及委外廠商文件承諾事項，未達成之成效認定	本會於採購文件載明之項目	按未達項目，每項計○點	
其他	違反契約約定委外廠商應履行之項目	每季不得超過○○次	按超過之次數計算，每超過乙次計○點	

八、本採購案履約完畢或提前終止、解除後，委外廠商應刪除或銷毀執行本採購案所持有本會、本會業主之相關資料，或依本會指示返還或移交之，並保留執行紀錄。

九、其餘涉及資通安全事項，由本會及業主視個案實際需要，依國家資通安全研究院（網址：www.nics.nat.gov.tw）或行政院國家資通安全會報技術服務中心（網址：https://www.nccst.nat.gov.tw）共通規範辦理，例如「政府資訊作業委外安全參考指引」與資通安全有關事項。

十、本附件規範與附件「委外廠商之資通安全責任事項」衝突部分，應優先適用本附件。

【附件】

雲端運算服務資訊安全要求

一、 一般資訊安全要求

(一) 服務供應商應通過 ISO 27001 標準認證。

(二) 服務供應商應提供使用者有關雲端服務之各項資通安全能力、政策及服務水準（含資通安全防護）之說明，以評估是否符合需求。

(三) 服務供應商應建立雲端服務備援機制，並宜有明確規定雲端服務復原時間之相關要求。

(四) 服務供應商應使用業界常見之虛擬化平台、虛擬機檔案格式、資料檔案格式，以確保互通性。

(五) 服務供應商應提供雲端服務相關監控服務，例如資訊安全監控中心（SOC）、事件告警，並提供各項服務日誌查詢及統計報表功能。

(六) 服務供應商應有能力提供防火牆、分散式服務阻斷攻擊（DDoS）防護、虛擬私有網路（VPN）服務。

二、 存取安全要求

(一) 服務供應商應提供使用者有關雲端服務加密服務範圍及加密能力之說明，以評估是否符合需求。

(二) 服務供應商應提供使用者於使用雲端服務平台之身分識別及存取管理（IAM）功能，並賦予使用者所需之平台存取權限，允許使用者註冊及退租，且可透過雲端服務保存各項登入及存取紀錄。

(三) 服務供應商應提供使用者於雲端服務平台內設定相關運作人員角色及權限之存取控制功能。

(四) 使用者之權限管理應採權限最小化原則，輔以適當安全控管措施，例如稽核軌跡、網路位址過濾、防火牆，以及使用傳輸層安全協定（TLS）。

(五) 服務供應商應使用標準化網路協定，其涉及敏感性資料之傳遞者，並應使用超文字傳輸安全協定（HTTPS）、安全檔案傳輸協定（SFTP）等加密網路協定。

三、 虛擬化安全要求

(一) 服務供應商應有能力確保虛擬機映像檔之完整性，有關映像檔之異動，例如調整虛擬機記憶體大小、硬碟容量等，應予記錄保存，並提供使用者檢視相關變更紀錄之功能。

(二) 服務供應商應依據使用者需求，提供虛擬機隔離性（isolation）說明；隔離性失效時，並應立即通知使用者。

(三) 服務供應商提供基礎設施即服務（IaaS）服務時，應依使用者需求將涉及敏感性資料之虛擬硬碟進行加密、限制快照或限制授權存取。

(四) 服務供應商於 IaaS 服務終止後，應刪除虛擬機映像檔、快照及備份。

【附件】

主機資通安全管理要求檢核表

委外資通作業名稱：_____ 填表人：_____ 填表日期：____年____月____日

確認	檢核內容	說明
1.實體及環境資訊安全要求事項		
	1.1 具儲存資訊之設備外送維修時，應有安全評估措施	
	1.2 正式服務網段與研發網段應實體隔離	
	1.3 服務主機所在實體環境應設有安全保護措施(例如門禁管理、不斷電(UPS)系統、空調設備、消防設備等)	
	1.4 服務主機所在實體環境應有 1.3 項安全保護措施的定期檢查機制	
	1.5 服務實體主機應定期維護(例如:定期檢視燈號是否有故障…)	
	1.6 正式服務網路應有一般防火牆防護及過濾控管	
	1.7 正式服務網路應有負載平衡防護及過濾控管	
	1.8 正式服務網路應有應用程式防火牆(WAF)防護及過濾控管	
	1.9 正式服務網路應有建置偵測機制(IDS)或入侵防禦機制(IPS)	
	1.10 正式服務應具有資訊安全防護中心(SOC)24 小時網路監控及通報機制(optional)	
2. 主機資訊安全管理要求事項		
	2.1 服務主機應停用主機預設特權帳號，並另設定特權帳號使用	
	2.2 主機設備不使用時，應設有關機、登出、設定密碼之螢幕保護或其他保護控制措施	
	2.3 停用不必要之網路服務(如 RDP)，並定期檢視防火牆策略	
	2.4 主機、系統需維護時，應透過加密管道進行(如 SSH、SSL 等)，並有限制維護來源 IP	
	2.5 服務主機應定期更新主機作業系統修補程式 patch	
	2.6 服務主機特權帳號密碼長度應不低於 9 碼，且由大小寫、數字及符號組成混合	
	2.7 服務主機特權帳號及密碼政策應訂定期限(90 天)或使用次數限定	

確認	檢核內容	說明
	2.8 服務主機系統應定期/不定期檢查各系統之使用者存取權限	
	2.9 正式服務主機應使用防毒軟體並即時更新病毒碼	
	2.10 正式服務主機應定期進行弱點掃瞄及漏洞修補	
	2.11 系統管理人員應持續觀察並分析系統資源使用狀況，包含處理器、記憶體、硬碟容量及其他輸出設備及通信系統之使用狀況	
	2.12 正式服務主機應定期執行必要之資料與軟體備份及備援作業	

系統負責人：_____

測試及正式環境同時適用
正式環境適用

【附件】

資通系統防護基準控制措施

資通系統名稱：ITIS 資料建置及 API 串接與轉檔架構維護資通系統防護需求等級：■普□中□高

□ 全部適用 (依評定之**資通系統防護需求等級**控制措施全部適用)

■ 部分適用 (請於「必要符合」欄位**勾選**所需**控制措施相關功能**)

□ 全部不適用

構面	控制措施	必要符合	等級	措施內容
存取控制	帳號管理	■	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。
		□	中/高	一、已逾期之臨時或緊急帳號應刪除或禁用。
		□	中/高	二、資通系統閒置帳號應禁用。
		□	中/高	三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。
		□	高	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。
		□	高	二、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。
		□	高	三、應依機關規定之情況及條件，使用資通系統。
		□	高	四、監控資通系統帳號，如發現帳號違常使用時回報管理者。
	最小權限	□	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。
	遠端存取	■	普/中/高	一、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。
		■	普/中/高	二、使用者之權限檢查作業應於伺服器端完成。
		■	普/中/高	三、應監控遠端存取機關內部網段或資通系統後臺之連線。
		■	普/中/高	四、應採用加密機制。
		□	中/高	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。
事件日誌與可	紀錄事件	■	普/中/高	一、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。
		■	普/中/高	二、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。

構面	控制措施	必要符合	等級	措施內容
歸責性		■	普/中/高	三、應記錄資通系統管理者帳號所執行之各項功能。
		□	中/高	應定期審查機關所保留資通系統產生之日誌。
	日誌紀錄內容	■	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，採用單一日誌機制，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。
	日誌儲存容量	■	普/中/高	依據日誌儲存需求，配置所需之儲存容量。
	日誌處理失效之回應	■	普/中/高	資通系統於日誌處理失效時，應採取適當之行動。
		□	高	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。
	時戳及校時	■	普/中/高	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)。
		□	中/高	系統內部時鐘應定期與基準時間源進行同步。
	日誌資訊之保護	■	普/中/高	對日誌之存取管理，僅限於有權限之使用者。
		□	中/高	應運用雜湊或其他適當方式之完整性確保機制。
		□	高	定期備份日誌至原系統外之其他實體系統。
營運持續計畫	系統備份	■	普/中/高	一、訂定系統可容忍資料損失之時間要求。
		■	普/中/高	二、執行系統源碼與資料備份。
		□	中/高	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。
		□	高	一、應將備份還原，作為營運持續計畫測試之一部分。
		□	高	二、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。
	系統備援	□	中/高	一、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。
		□	中/高	二、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。
識別與鑑別	內部使用者之識別與鑑別	■	普/中/高	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。
		□	高	對資通系統之存取採取多重認證技術。

構面	控制措施	必要符合	等級	措施內容
	身分驗證管理	■	普/中/高	一、使用預設密碼登入系統時，應於登入後要求立即變更。
		■	普/中/高	二、身分驗證相關資訊不以明文傳輸。
		■	普/中/高	三、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。
		■	普/中/高	四、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。
		■	普/中/高	五、密碼變更時，至少不可以與前五次使用過之密碼相同。
		■	普/中/高	六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。
		□	中/高	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。
		□	中/高	二、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。
	鑑別資訊回饋	■	普/中/高	資通系統應遮蔽鑑別過程中之資訊。
	加密模組鑑別	□	中/高	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。
	非內部使用者之識別與鑑別	■	普/中/高	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)。
系統與服務獲得	系統發展生命週期需求階段	■	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。
	系統發展生命週期設計階段	□	中/高	一、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。
		□	中/高	二、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。

構面	控制措施	必要符合	等級	措施內容
	系統發展生命週期開發階段	■	普/中/高	一、應針對安全需求實作必要控制措施。
		■	普/中/高	二、應注意避免軟體常見漏洞及實作必要控制措施。
		■	普/中/高	三、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。
		□	高	一、執行「源碼掃描」安全檢測。
		□	高	二、系統應具備發生嚴重錯誤時之通知機制。
	系統發展生命週期測試階段	■	普/中/高	執行「弱點掃描」安全檢測。
		□	高	執行「滲透測試」安全檢測。
	系統發展生命週期部署與維運階段	■	普/中/高	一、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。
		■	普/中/高	二、資通系統不使用預設密碼。
		□	中/高	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。
	系統發展生命週期委外階段	■	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。
	獲得程序	□	中/高	開發、測試及正式作業環境應為區隔。
	系統文件	■	普/中/高	應儲存與管理系統發展生命週期之相關文件。
系統與通訊保護	傳輸之機密性與完整性	□	高	一、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。
		□	高	二、使用公開、國際機構驗證且未遭破解之演算法。
		□	高	三、支援演算法最大長度金鑰。
		□	高	四、加密金鑰或憑證應定期更換。
		□	高	五、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。

構面	控制措施	必要符合	等級	措施內容
	資料儲存之安全	□	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。
系統與資訊完整性	漏洞修復	■	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。
		□	中/高	定期確認資通系統相關漏洞修復之狀態。
	資通系統監控	■	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。
		□	中/高	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。
		□	高	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。
	軟體及資訊完整性	□	中/高	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。
		□	中/高	二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。
		□	中/高	三、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。
		□	高	應定期執行軟體與資訊完整性檢查。

【附件】

資料返還、刪除、銷毀聲明書

填寫日期： 年 月 日

購案/委外資通作業名稱（下稱本案）		廠商名稱(下稱立書人)	(請加蓋廠商印鑑)
		立書人之負責人	(請加蓋負責人印鑑)

立書人因執行本案所持有之本案相關資料（包括但不限於開發需求規格書、原始碼、執行碼或程式等，詳如下表所列）及其影本、複製本或備份予以返還、刪除或銷毀，且將嚴格監督並確認立書人及其參與本案的相關人員（包括但不限於勞工、派遣人員、受任人或分包廠商等）未以任何形式為資料之私自留存、使用、竄改或洩漏，亦不得為自身或第三人的利益而使用。

立書人及其參與本案之相關人員若發生將資料私自留存、使用、竄改或洩漏等不利於 貴會的行為，立書人同意配合 貴會進行必要之查證行為及提供 貴會所需之協助，如經查證屬實，立書人願支付本案價金總額 20 %之懲罰性違約金及賠償 貴會所受之一切損害，並負一切法律責任，絕無異議。

編號	資料名稱	數量	檔案類型	執行方式
範例	需求/設計規格書	1	■電子檔案 ■實體檔案	■已返還 ■已刪除 ■已銷毀
範例	程式原始碼	1	■電子檔案 ■實體檔案	■已返還 ■已刪除 ■已銷毀
1.			□電子檔案 □實體檔案	□已返還 □已刪除 □已銷毀
2.			□電子檔案 □實體檔案	□已返還 □已刪除 □已銷毀

備註：表格不敷使用，請自行增加。

(資策會)點收人簽名：	(資策會)點收日期：