需求說明書（含驗收規範）

壹、購案名稱

「會計權責系統」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 117__年 07__月 31__日止。

二、 預算

新台幣待討論__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、 會計權責系統（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、Redhead、Linux、PHP、MySQL、Apache、Python 最新版、FSI Server。

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。

(五) 履約標的須採用響應式網頁設計（RWD），以提供使用者最佳瀏覽畫面。

四、 功能及建置說明

系統	功能模組	具體需求描述
會計系統	傳票模組	傳票製作、送核、覆核、歸檔、列印等完整流程；支援多幣別、自動分錄；提供傳票版面維護與排版設定。
會計系統	營業稅申報	進銷項資料維護、媒體檔產生、申報作業流程、稅檔開關檔；符合臺灣營業稅（401/403）申報規範，支援電子發票整合。
會計系統	所得稅申報	各類所得扣繳、媒體申報檔產生、扣繳憑單列印；各類所得扣繳檢查報表、免申報清冊。

會計系統	資產管理	設備使用費計算、折舊攤銷作業（含耐用年限設定）、資產除帳、帳項轉正；資產維護檔管理與資產編號查詢。
會計系統	投資管理	債券、基金、股權投資之購入、評價、收息、處分之完整作業流程；支援投資損益計算與報表產出。
會計系統	月結關帳	兩階段關帳流程、即時過帳、關帳檢查報表；支援會計項目過帳與試算表產生。
會計系統	報表模組	綜合餘絀表、資產負債表、現金流量表、各類明細表（銀行存款及外幣明細表、計畫收支餘額表等）、定期存款報表；支援報表權限管理與版本鎖定；能夠自行透過操作介面自定義個報表的欄位及計算方式。
發票系統	收入模組	各類收入申請單、退款申請單、收入變更單、應收確認單、銷貨折讓發票作廢、專案退稅單；詳細記錄收入相關資訊包含發票。
發票系統	消費發票及收據	各類發票、各類收據；銷項發票維護，並按照法規規定將發票上傳至主管機關。
發票系統	稅務申報	銷項資料維護、媒體檔產生、分配設定發子發票號碼；符合臺灣營業稅（401/403/零稅率）清單產生，支援電子發票整合。
發票系統	報表模組	合約報表、計畫收款查詢、信用卡收款查詢、發票收據查詢、折讓單查詢等；支援報表權限管理與版本鎖定；能夠自行透過操作介面自定義個報表的欄位及計算方式。
出納系統	收入模組	收款單、收入核銷、收入兌現、異動處理、針對實際銀行存款增加紀錄處理作業用。
出納系統	支出模組	集中付款及指定付款；執行定期付款作業以及外幣付款或是非正常付款日作業用。
出納系統	資金調度模組	管理各銀行帳戶間的資金流動帳戶調撥（同幣別帳戶間轉帳，包含專戶提撥與營運帳戶調撥）、外幣買賣（不同幣別轉換）、定存相關（新承作、到期續作、解約）。
出納系統	投資模組	短期投資的完整生命週期管理，涵蓋定期存款（定存）、公司債、基金／受益憑證三大類別。長期股權投資（股票）之帳務細節由財會管理，出納僅負責保管箱托管／領回
出納系統	保證金模組	對外提供之各類保證金，涵蓋保證金的建立、補登、狀態追蹤及返還／解約作業。
出納系統	保管箱模組	存放於銀行保管箱之各類實體憑證，包括托管登記與領回作業。
出納系統	廠商模組	負責維護本會對外付款對象的基本資訊與銀行帳戶。
出納系統	報表	銀行存款查詢、收入查詢、支出查詢、資金調度作查詢投資買賣查詢、保管品類查詢、保證金類查詢。

中介資料庫	串接模組	傳遞資料給會計、出納、發票系統；反項接受來自會計、出納、發票系統的資料；傳遞資料給舊系統；反項接受。來自舊系統的資料。

詳細功能請參考附件

- 財會系統:詳細內容請查閱【附件一】會計系統設計規格書
- 發票系統:詳細內容請查閱【附件二】發票系統設計規格書
- 出納系統:詳細內容請查閱【附件三】出納系統設計規格書
- 中介系統:詳細內容請查閱【附件四】總表跟關係圖

五、 開發標準

(一) 網站開發規範：

1. 依「**政府網站服務管理規範**」製作維護，網站功能調整、擴增後亦同。
2. 新系統如需整合既有系統之資料，應提供完整之資料移轉及整合機制，將舊系統既有資料依新系統之資料結構及業務需求進行盤點、轉換、清理及匯入。
3. 資料移轉應確保資料之完整性、正確性及一致性，並建立新舊資料欄位之對應關係及轉換規則。對於資料格式、代碼、狀態或欄位定義不一致之情形，應依雙方確認之規則進行轉換。
4. 資料移轉完成後，應執行資料筆數、欄位內容及關聯性之檢核與驗證，並產出移轉結果及異常資料清單。若發生資料遺漏、格式錯誤或移轉失敗等異常情況，應提供適當之錯誤紀錄及補正機制。
5. 涉及個人資料、密碼或其他敏感資料時，應依相關資訊安全規範採取適當之保護措施，於資料傳輸、轉換及儲存過程中避免以明文方式處理。
6. 資料移轉作業應於正式上線前完成測試及驗證，並經業務單位確認資料正確後，始得進行正式資料移轉及系統上線。
7. 但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舊網站。

(二) 資安要求：

1. 如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. 本案如使用之雲端服務涉及提供業務及服務，得標廠商應遵守「雲端服務租用資訊安全要求（附件）」。
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. 會員登入密碼應有檢查機制，確認密碼複雜度（應包含英文大小寫及數字，且密碼長度達十二碼以上）；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。
8. 所有儲存於資料庫的密碼（及敏感資料）必須加以編碼。
9. 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。
10. 得標廠商應協助本會處理及通報資通安全事件。

11. 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。

12. **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核心系統：需提供原始程式碼檢測報告（如 Checkmarx、Micro focus Fortify、Sonar Qube 或由得標廠商建議並經本會請購部門同意之檢測工具）。**

☑**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.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。

(三) 個資要求：

1. 本案開發內容不可完整顯示身份證字號及相關個人資料之資訊。
2. 需過濾含有個人資料之檔案。
3. 個資檔案存取紀錄：
   (1) 留存個資相關之使用者操作及資料變更之軌跡紀錄（包括記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送）。
   (2) 軌跡資料，至少應包含存取者（如電腦名稱、IP、姓名或其他直接或間接得以識別存取者之資訊）、存取日期及時間、執行之動作。
   (3) 後台之最高管理者得查詢各軌跡清單。

六、 上線作業

(一)

☑履約期間內須完成**上線測試**，待本會正式上線時，得標廠商應協助上線相關作業，不因履約、驗收完成而免除責任。

□履約期間內履約標的須能正常運作並**對外正式上線**。

(二) 後續視本會需求配合將履約標的移入指定機房環境。

七、 教育訓練

☑至多 10__場（場次及時數依本會需求調整），讓相關人員確實瞭解履約標的之使用或操作。

八、 法令依據及相關規定

(一) □媒體採購或廣告費申請相關規定：

得標廠商執行本案務必依照「政府機關政策文宣規劃執行注意事項」及預算法第 62 條之 1 規定辦理：

1. 若於平面媒體、廣播媒體、網路媒體（含社群媒體）及電視媒體辦理業務宣導，應明確揭示辦理或贊助機關、單位名稱，若屬政策文宣，應明確標示其為廣告(請得標廠商先與購案聯絡人確認是否屬政策文宣後再執行)；
2. 若辦理活動、說明會、園遊會或發放各式宣導品，應明確揭示辦理或贊助機關、單位名稱。

※違反上述規定者，相關經費不予核銷，如事後遭審計機關剔除經費，亦將辦理經費收回。

(二) 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)。

九、 保固需求

☑有

(一) 保固期間

自本案驗收合格之日起__年內，免費提供履約標的正常操作之必要保固維護及正常操作中發生任何事情之必要改善。

(二) 故障叫修

1. 本案履約標的故障時，得標廠商應於接獲本會通知後___個工作小時內電話回覆，___個工作小時內到場提供維修服務或是遠端登入處理，並於本會通知叫修後___個工作小時內恢復履約標的正常運作。
2. 故障維修每遲延 1 工作小時計罰新台幣__ 元，不足 1 小時以 1 小時計算，連續發生得連續處罰；若經本會認定有特殊原因或有不可抗力情形者，不在此限。
3. 履約標的除錯應於本會通知後 4 日內提出改正時程。

(三) 保固期滿後，延續服務之維護費用另議之，惟其維護費用以不超過開發案經費__ %為限。

(四) 保固期滿時，得標廠商須返還、移交、刪除或銷毀因履行契約而持有之資料，並出具「資料返還、刪除、銷毀聲明書(附件)」提送本會確認。

(五) 請廠商針對 1-4 條款於回饋公告內容，提供能提供的保固條件。

十、 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：

項次	交付項目	交付內容	數量	交付型態	交付期限
1	服務建議書	內容包含但不限於：	1 份	電子檔	決標次日起

		1. 工作計畫內容 2. 工作進度 3. 工作團隊組織與工作分配 4. 經費配置			30 日曆天
2	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」 ※格式請向購案聯絡人索取。 2. 主機資通安全管理要求檢核表(詳附件)	各 1 份	紙本	決標次日起 30 日曆天
3	個資文件	得標廠商簽署之委外廠商個資安全管理措施說明表 （本交付項目及交付期限如與本案其他採購文件牴觸者，以本需求說明書為準） ※格式請向購案聯絡人索取；若需求未涉及蒐集、處理或利用個人資料則免	1 份	紙本	決標次日起 7 日曆天
4	個資文件	得標廠商簽署之委外廠商個資安全管理措施自評表 （本交付項目及交付期限如與本案其他採購文件牴觸者，以本需求說明書為準） ※格式請向購案聯絡人索取；若需求未涉及蒐集、處理或利用個人資料則免	1 份	紙本	決標次日起 14 日曆天
5	完成開發	1. 原始程式碼 2. 設計文件 3. 舊資料轉入	1 式	電子檔	117 年 07 月 01 日
6	教育訓練	課程教材	依實際狀況檢附，若無則免		117 年 07 月 01 日
7	相關手冊	1. 使用者操作手冊 2. 測試報告書 (1) 功能測試報告 (2) 安全性檢測報告 (3) 100 人同時在線之壓力測試報告 (4) 載入時間於 10 秒內之測速證明 3. 開發文件（需包含資料庫欄位說明及 Schema 相關建置資料） 4. 維護手冊 5. 災害復原手冊	1 式	電子檔	同本案 履約期限
8	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
9	非自行開發軟體元件清單	1. 所用之非自行開發軟體、服務、函式庫或其他元件 2. 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	使用非自行開發軟體元件需檢附，若無則免		同本案履約期限

10	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	紙本	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：同購案聯絡人。

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、 本會得要求得標廠商配合出席驗收會議，並做口頭簡報（須視本會需求提供會議文件）。

三、 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。

陸、其他注意事項

一、購案聯絡人：

姓　名：數轉院　洪志偉先生

電　話：(　　) 0953 -551-179

Email：eyasutw@gmail.com

地 址：105412 臺北市松山區精忠里民生東路四段 133 號, 3F

二、發票資料：

抬　頭：財團法人資訊工業策進會

統一編號：05076416

柒、評選規範／審查須知

□詳投標須知之「評選須知」內容；評選項目及建議書撰寫重點如下述。

過半數（不含半數）評選委員評定總分達___分以上，始為合格，方列入名次和之統計與優勝序位之排列。

☑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）**	配分 （審查則免）
		封面、目錄	
1	**執行力與配合度** ● 人力配置規劃	1. 公司簡介（如業務範圍、營運狀況） 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	

	● 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	4. 廠商履約實績：請詳述專案經驗及其成效	
	整體企劃 ● 網站架構之完整性與可行性 ● 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 ●加值服務	5. 說明整體網站設計理念、網站的動線設計 6. 使用者友善及管理人員管理資料維護設計 7. 資訊安全、個資安全及保密之規劃及執行方式 8. 網站測試、教育訓練之規劃及執行方式 9. 說明保固期間之售後服務方式 10.提供時程進度規劃，說明相關工作預定進度、完成時點 11.加值服務說明（請依實際需求撰寫，若無則請將此項刪除）	
2	**經費合理性** ●相關執行費用估算與分配之合理性	12.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） 13.說明保固期滿之維護費用	
	●	14.	

【附件】

委外廠商之資通安全責任事項

一、 委外廠商辦理受託業務之相關程序及環境，應依廠商類型填寫適用之「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，或通過第三方資安驗證，如受託業務涉及提供雲端運算服務(IaaS)者，應提供原廠 ISO 27001、ISO 27017、ISO 27018 或 CSA STAR 等同質性證書或 SOC 2 報告。如委外廠商為國外廠商，或經由代理商委託國外廠商辦理受託業務，具備前述證書、報告或資安相關管理措施者，得免填之。

二、 委外廠商受託業務內容如涉及資通系統委外開發、維護或維運，應辦理「主機資通安全管理要求檢核表」適用之檢核內容，並於該表說明辦理情形，交由本會委外業務負責人確認。

三、 委外廠商應建立資通安全管理制度。

四、 委外廠商(除自然人外)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。

五、 委外廠商專案人員應定期接受資通安全教育訓練。

六、 委外廠商專案人員使用之電腦應安裝防毒軟體，並定期更新病毒碼及執行病毒掃描，電腦作業系統亦應定期更新。

七、 委外廠商應對專案相關資料建立存取管控機制。

八、 經本會同意，委外廠商始得將受託業務分包予第三人並對其資安管理全權負責。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或標準，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。

九、 辦理資通系統開發/維護/維運作業，應依受託業務指定之系統防護需求等級落實「資通系統防護基準控制措施」。

十、 辦理資通系統開發/維護作業，應制定安全軟體開發生命週期程序，並建立資安檢測機制(源碼掃描、應用系統弱點掃描)、原始程式碼備份及版本控管機制，且應用系統開發測試及正式環境應區隔在不同作業環境。

十一、 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。

十二、 辦理資通系統維運作業，如主機所在實體環境由委外廠商提供者，應具備消防設備、備援電力設備、溫溼度監控設備及監視設備，並定期保養與檢查以確保正常運作。

十三、 委外廠商應就受託業務建立資通安全事件通報機制，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、應變、調查及改善等相關處理作業。委外廠商未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。

十四、 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」。

十五、 委外廠商同意本會得於履約期間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委外廠商資通安全管理措施完善性與受託業務之執行情形，

如有稽核發現事項或不符合委託契約資安要求之情形，應於履約期限內完成改善，並提報改善措施執行情形及相關佐證予本會確認。如無法於履約期限內完成改善，委外廠商應說明原因並經本會同意。

十六、 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。

十七、 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。

十八、 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「資通服務駐點人員資通安全同意表」之資通安全相關規定。

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

【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：

☐ 系統主機弱點掃描

☑ 網頁弱點掃描

☑ 滲透測試

☑ 原始碼檢測

☐ 其他_____

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，以符合本會、本會業主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 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；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、資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。

八、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 2,000,000 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_日（或小時），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_小時，以_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_日，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__分鐘內通報本會，並於__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_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__小時（重大資安事件為__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__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	每季統計	每次計＿點		

九、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。

十、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）共通規範辦理，例如「政府機關雲端服務應用資安參考指引」、「政府資訊作業委外安全參考指引」與資通安全有關事項。

十一、 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】

雲端服務租用資訊安全要求

一、 一般資訊安全

(一) 服務供應商應具備 ISO 27001、ISO 27017、ISO 27018 或 CSA STAR 等同質性證書或 SOC 2 報告。

(二) 服務供應商應提供有關雲端服務之各項資通安全能力、政策及服務水準（含服務可用性、資通安全防護、資安事件通報及處理程序、備援機制等）之說明。

(三) 服務供應商應提供身分識別及存取管理（IAM）功能。

(四) 服務供應商應採加密網路協定傳輸資料，如超文字傳輸安全協定（HTTPS）、安全檔案傳輸協定（SFTP）等。

(五) 雲端資料之存取、備份及備援之實體所在地不得位於大陸地區（含香港及澳門地區），且不得跨該等境內傳輸資料。

二、 基礎設施即服務（IaaS）安全

(一) 服務供應商應具備雲端服務相關監控及異常事件告警機制，並提供各項服務日誌查詢及統計報表功能。

(二) 服務供應商應提供防火牆、分散式服務阻斷攻擊（DDoS）防護機制、虛擬私有網路（VPN）服務。

(三) 服務供應商應提供雲端服務資料加密功能。

(四) 服務供應商應提供虛擬機之異動紀錄，例如調整虛擬機記憶體大小、硬碟容量等，並提供檢視紀錄之功能。

(五) 服務供應商應提供虛擬硬碟加密、快照限制或存取控管功能。

(六) 服務供應商應具備虛擬機映像檔、快照及備份刪除機制。

(七) 服務供應商應具備基礎設施之弱點修補作為。

三、 平台即服務（PaaS）安全

(一) 服務供應商應具備平台之弱點修補作為。

(二) 服務供應商應具備資通安全防護機制（如防範入侵或惡意軟體之控制措施等）。

(三) 服務供應商應具備 API Gateway 安全控管機制，以防止濫用及阻斷攻擊。

(四) 服務供應商應提供資料庫加密功能。

(五) 服務供應商應提供系統操作及 API 呼叫之日誌紀錄。

四、 軟體即服務（SaaS）安全

(一) 服務供應商應具備應用服務之弱點修補作為。

(二) 服務供應商應具備資通安全防護機制（如防範入侵或惡意軟體之控制措施等）。

(三) 服務供應商應對於提供之應用程式介面（API）進行安全控管（如 SSL/TLS 憑證、加密傳輸等）。

(四) 服務供應商應提供應用程式介面登入及特權操作日誌（如密碼變更、權限調整）。

【附件】

主機資通安全管理要求檢核表(得標廠商填寫)

委外資通作業名稱：_____ 廠商專案負責人：_____

填表日期：____年____月____日

□ **全部適用**

□ **部分適用(擇一勾選)，原因：(必填)**

□ **實體及環境資訊安全要求事項**

□ **主機資訊安全管理要求事項**

□ **全部不適用，原因：(必填)**

1. 廠商專案負責人應針對檢核內容，分別說明正式或測試環境之辦理情形，並附上佐證資料。 **2. 如委外廠商無相關環境者得免填。**			
必要	檢核內容	檢核結果	
		正式環境	測試環境
1.實體及環境資訊安全要求事項 (主機維運環境由委外廠商提供者適用)			
*	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、電力及通信纜線保護等)		
*	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 服務網路應有一般防火牆防護及過濾控管		

1. 廠商專案負責人應針對檢核內容，分別說明正式或測試環境之辦理情形，並附上佐證資料。 2. 如委外廠商無相關環境者得免填。			
必要	檢核內容	檢核結果	
		正式環境	測試環境
*	1.7 服務網路應有建置偵測機制(IDS)或入侵防禦機制(IPS)		
	1.8 服務網路宜有負載平衡防護及過濾控管		
	1.9 服務網路宜有應用程式防火牆(WAF)防護及過濾控管		
	1.10 服務宜具有資訊安全防護中心(SOC)24小時網路監控及通報機制		
2.主機資訊安全管理要求事項 (主機由委外廠商維運者適用)			
*	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		

1. 廠商專案負責人應針對檢核內容，分別說明正式或測試環境之辦理情形，並附上佐證資料。 **2. 如委外廠商無相關環境者得免填。**			
必要	檢核內容	檢核結果	
		正式環境	測試環境
*	2.6 服務主機特權帳號密碼長度應不低於12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		
*	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 服務主機應使用防毒軟體並即時更新病毒碼		
*	2.10 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 服務主機應定期執行必要之資料與軟體備份及備援作業		
*	2.13 應配置足夠資源並確保服務主機日誌紀錄(包含但不限於作業系統日誌、網站日誌、應用程式日誌、登入日誌等)可保留至少 6 個月		
*	2.14 應確保服務主機可紀錄特定事件(如：帳號登入成功失敗、觸發帳號鎖定等紀錄)		

委外業務負責人確認：_____

【附件】

資通系統防護基準控制措施

資通系統名稱：會計權責系統__　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。
		□	普/中/高	一、已逾期之臨時或緊急帳號應刪除或禁用。
		□	普/中/高	二、資通系統閒置帳號應禁用。
		□	普/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。
		□	中/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。
		□	中/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	□	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。
	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。
		□	普/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。
事件日誌與可歸責性	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。
		□	普/中/高	三、應記錄資通系統管理者帳號所執行之各項功能。

構面	控制措施	必要符合	等級	措施內容
		□	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)。
		□	普/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	資料備份	□	普/中/高	一、訂定資料可容忍損失之時間要求。
		□	普/中/高	二、執行資料備份。
		□	中/高	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。
		□	高	一、應將備份還原，作為營運持續計畫演練之一部分。
		□	高	二、應建立資料異地備份機制。
	系統備援	□	普/中/高	一、訂定資通系統從中斷後至重新恢復服務之最大可容忍時間要求。
		□	中/高	二、應定期測試原服務中斷時，於最大可容忍時間內，由備援設備或其他方式取代並提供服務。
		□	高	應將備援啟動作為營運持續計畫演練之一部分。
識別與鑑別	內部使用者之識別與鑑別	□	普/中/高	資通系統應識別及鑑別使用者，並禁止使用者使用共用帳號。
		□	高	對資通系統之存取採取多因子鑑別技術。

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、使用預設密碼初次登入系統時，應於登入後立即變更。
		□	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；依機關密碼效期規定變更密碼。
		□	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，對外使用者，機關得自行規範辦理。
		□	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。
	鑑別資訊保護	□	普/中/高	資通系統應遮蔽鑑別過程中之資訊。
		□	中/高	資通系統如以密碼進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存。
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。
	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。

構面	控制措施	必要符合	等級	措施內容
	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。
		☐	普/中/高	二、識別並關閉不必要服務及埠口
		☐	普/中/高	三、資通系統不使用預設密碼。
		☐	普/中/高	四、執行系統源碼備份
		☐	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	☐	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。
		☐	普/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	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。
		□	普/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：