

# 需求說明書（含驗收規範）

## 壹、購案名稱

「次世代通訊 PMO 中英文網站」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 3 個月內完成。

二、預算

新台幣 100 萬元整（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，亦須符合國家科學及技術委員會（以下簡稱國科會）科技辦公室需求。

二、網站（以下簡稱履約標的）開發環境

（一）作業系統：Windows Server 2019 STD，AP Server：IIS 10.0。

（二）資料庫：Microsoft SQL Server 2019。

（三）開發平台：IIS 10.0 以上相容。

（四）技術架構：SP.NET 等，開發工具：Visual Studio，使用框架：.NET Framework。

（五）符合國科會雲端主機管理：相關網站須架構於國科會之科技辦公室專用網站之虛擬主機內。

（六）符合國科會主機安全防護系統：國科會網路另有防火牆及入侵偵測防護機制，廠商須配合國科會完成相關安全防護設定。

（七）網站內容管理須符合國科會科技辦公室專用網站之後台管理系統規格。

三、使用者操作介面

（一）提供使用者以個人電腦之 WWW 瀏覽器（Browser）軟體連結及查詢本網站各項服務。

（二）瀏覽器版本應支援 ■ Microsoft Internet Explorer 8 版（含）以上、■ chrome、■ safari 及 ■ Firefox... 瀏覽器環境。

（三）所有應用系統均須為繁體中文介面，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）用戶端行動通訊作業系統，必須支援行動裝置之 OS 為 iOS 14、Android 11 以上版本皆可。

（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、網站功能及建置說明

（一）視覺設計：

需求功能	說明
首頁設計	首頁設計，整體風格制定及修改 Logo 設計。首頁設計，整體網站風格制定(含履約標的 Logo 置入網站配置設計)，置入履約標的網站的 Favicon，在瀏覽器及即時通訊軟體內皆可呈現該 Favicon。
內頁設計	網站內頁、版型設計須根據響應式網頁設計(RWD)規劃提供對應風格設計稿，經確認後才開始進行切版與 CSS 實作。
視覺設計規格書	依國科會科技辦公室提供的網站示意圖樣、國科會全球資訊網的樣式及輪播機制設計，包含以下 1. 主視覺 Layout 設計。 2. 內頁視覺 Layout 設計。 3. 首頁與內頁採用響應式網頁設計(RWD)。 4. 無障礙空間規劃。 5. 提供所有頁面樣式規劃及 Frontend 原始碼。

(二) 網站前／後台功能：

需求功能	說明
共通	
上稿管理功能	1. 提供如「純文字編輯、HTML 編輯、附件上傳、圖片上傳、插入影音檔」等功能供網站維護人員可於後台進行網頁編輯。 2. 後台可依不同類別提供檔案上傳、新增、編輯、修改、刪除並提供下載。 3. 依據國科會科技辦公室專用網站共通平台管理系統辦理。
相關連結	超連結外部網站，依據國科會科技辦公室專用網站共通平台管理系統辦理。
流量統計	1. 網頁瀏覽次數統計。 2. 檔案下載次數統計。 3. Banner 點擊次數統計。 4. 依據國科會科技辦公室專用網站共通平台管理系統辦理。
架構管理	可設定架構，新增、移動或刪除單元，依據國科會科技辦公室專用網站共通平台管理系統辦理。
權限控管	可群組設定，其權限區分為： 1. 最高管理者：可設定一般管理者各單元之瀏覽及維護權限。 2. 一般管理者：維護權限細分為新增資料、瀏覽資料、修改資料、刪除資料等。 3. 依據國科會科技辦公室專用網站共通平台管理系統辦理。
操作紀錄管理	包含使用者登入紀錄及維護資料之新增、修改、刪除及相關操作紀錄。

(三) 網站/系統/平台功能項目

需求功能	功能說明
隱私權聲明	首頁置放隱私權聲明內容
語系選擇	中文繁體

<p>關於次世代通訊 科技發展方案</p>	<ul style="list-style-type: none"> <li>● 提供「次世代通訊科技發展方案」、「次世代通訊推動辦公室」區塊。</li> <li>● 可設定網站架構，新增、移動網站單元。</li> <li>● 可自行編輯網頁內容。具備多圖上傳功能，可自動產生縮圖，圖片插入網頁畫面中使用時可選擇要插入小圖、大圖或是點小圖彈出大圖的圖片組合。</li> <li>● 可由後台發佈網站訊息 每則訊息可填寫資料如下： <ol style="list-style-type: none"> <li>1. 標題文字</li> <li>2. 內文 (html 編輯器)</li> <li>3. 相關網址連結設定</li> <li>4. 具備多圖上傳功能，可自動產生縮圖</li> </ol> </li> <li>● 嵌入不限數量之 YouTube 影片。</li> <li>● 網頁中連結至其他格式之文件，依照使用者瀏覽習慣自行決定下載或在瀏覽器內直接觀看，勿使用類似 Content-Disposition: attachment; filename="image.jpg"或 Content-Disposition: attachment; filename="document.pdf"之 header</li> </ul>
<p>最新消息</p>	<ul style="list-style-type: none"> <li>● 提供「新聞消息」、「活動訊息」、「政策訊息」區塊。</li> <li>● 可設定網站架構，新增、移動網站單元。</li> <li>● 可自行編輯網頁內容。具備多圖上傳功能，可自動產生縮圖，圖片插入網頁畫面中使用時可選擇要插入小圖、大圖或是點小圖彈出大圖的圖片組合。</li> <li>● 可由後台發佈網站訊息每則訊息可填寫資料如下： <ol style="list-style-type: none"> <li>1. 標題文字</li> <li>2. 內文 (html 編輯器)</li> <li>3. 相關網址連結設定</li> <li>4. 具備多圖上傳功能，可自動產生縮圖。</li> </ol> </li> <li>● 嵌入不限數量之 YouTube 影片。</li> <li>● 網頁中連結至其他格式之文件，依照使用者瀏覽習慣自行決定下載或在瀏覽器內直接觀看，勿使用類似 Content-Disposition: attachment; filename="image.jpg"或 Content-Disposition: attachment; filename="document.pdf"之 header</li> </ul>
<p>方案推動成果</p>	<ul style="list-style-type: none"> <li>● 提供「促進關鍵應用服務落地"成果"」、「建構實驗網加速技術研發與試煉"成果"」、「強化產業生態系跨部門協作"成果"」區塊。</li> <li>● 可設定網站架構，新增、移動網站單元。</li> <li>● 可自行編輯網頁內容。具備多圖上傳功能，可自動產生縮圖，圖片插入網頁畫面中使用時可選擇要插入小圖、大圖或是點小圖彈出大圖的圖片組合。</li> <li>● 可由後台發佈網站訊息 每則訊息可填寫資料如下： <ol style="list-style-type: none"> <li>1. 標題文字</li> <li>2. 內文 (html 編輯器)</li> <li>3. 相關網址連結設定</li> <li>4. 具備多圖上傳功能，可自動產生縮圖</li> </ol> </li> <li>● 嵌入不限數量之 YouTube 影片。</li> <li>● 網頁中連結至其他格式之文件，依照使用者瀏覽習慣自行決定下載或在瀏覽器內直接觀看，勿使用類似 Content-Disposition: attachment; filename="image.jpg"或 Content-Disposition: attachment;</li> </ul>

	filename="document.pdf"之 header
相關連結	可新增連結到外部網站的主選單項目，可將多個網站串連。
網站導覽	依據國科會全球資訊網網站版型與內容管理規範規範製作。
檔案下載	檔案可分自行分類別，每個類別下可自行上傳不限數量的檔案供人下載。
網站流量統計	1. 網頁瀏覽次數統計 2. 檔案下載次數統計 3. 活動瀏覽人次統計 4. Banner/檔案點擊次數統計
搜尋檢索	1. 全文檢索：使用 Google Search 站內檢索。 2. 進階檢索：廠商、產品（特定資料庫）關鍵字查詢。
網站架構管理	可設定網站架構，新增、移動或刪除網站單元。
網站頁面維護模組	提供網頁編輯模組如「純文字編輯、HTML 編輯、附件上傳、圖片上傳、插入影音檔」等功能供網站維護人員可於後端進行網頁編輯。
操作紀錄管理	包含登入紀錄及維護資料之新增、修改、刪除相關操作紀錄
備份機制	依國科會資訊安全管理規範之資料庫定期備份排程，資料庫可透過排程，定期將資料庫備份並匯出至指定目錄存放

- 所有功能皆需符合
  - (1) 網站無障礙（包含無障礙檢測）：「無障礙網頁開發規範」及「政府網站無障礙化作業規定」：符合 AA 等級（含）以上，並張貼等級標章。
  - (2) 依「政府網站版型與內容管理規範」製作維護。
  - (3) 需整合舊網站/系統之功能，不影響舊網站/系統之功能；若有影響，廠商應負責修正調整，維持整體網站/系統之正常運作。
  - (4) 網站應符合國科會網站管理規範之要求，功能調整、擴增後之網站整體亦同。
- 以上所稱系統或網站均指本案之系統或網站，如專指擴充前系統或網站則稱舊系統、舊網站。

## 五、網站開發標準

### (一) 網站開發規範：

1. 依國科會科技辦公室網站版型與內容管理規範規範製作。
2. 「網站無障礙規範（最新版）」及「政府網站無障礙化作業規定」（包含無障礙檢測）：符合 AA 優先等級（含）以上，保固期間內本會因申請作業需補件或做相關調整，得標廠商須配合修正，不因已履約、驗收完成而免除修正責任；申請通過之後，須代為張貼等級標章。

### (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. 所有資料異動必須提供 Log 記錄供查詢。
3. 系統須記錄使用者登入之 IP 位址及登入時間。
4. 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。
5. 所有儲存於資料庫的密碼（及敏感資料）必須加以編碼。
6. 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。

7. 得標廠商應協助本會處理及通報資通安全事件。
8. 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。
9. 全網站開發須防護 SQL Injection、Cross-Site Scripting、Session Hijacking 及其他網路常見攻擊法。

**10. 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. 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），網站及原始程式碼須通過具備檢測本年度 OWASP Top 10 網站弱點之掃描工具檢測，修復中（高）風險以上弱點，並提供檢測報告。

(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。

**六、上線作業**

- (一) 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國科會機房環境。

**七、教育訓練**

1. 訓練目標：讓國科會科技辦公室相關人員確實瞭解平台操作。
2. 訓練課程：包含有系統操作及維護訓練，確保使用單位國科會科技辦公室能夠完整掌握系統操作與擁有操作說明的書面手冊。
3. 內部教育訓練

對象	課程名稱	人次	小時	場次	總時數	教材
本案網站相關人員	系統操作及維護訓練課程	1人	2小時	1	2小時	提供 <input checked="" type="checkbox"/> 電子檔

**八、法令依據及相關規定**

- (一) 智慧財產權之歸屬：

得標廠商交付項目之智慧財產權歸屬本會所有。得標廠商依本契約所提出之履約標的若有使用或涉及他人之智慧財產權，得標廠商應負責使本會及業主就前述智慧財產權在本契約履約目的範圍內取得永久無償、不限時間、次數、方式、地域之任何使用或行使之授權。如涉有權利爭議糾紛，應由得標廠商完全負責，概與本會無涉。

(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

(一) 保固期間

自本案驗收合格之日起1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. 本案網站系統故障時，得標廠商應於接獲本會通知後2個工作小時內電話回覆，4個工作小時內到場提供維修服務，並於本會通知叫修後8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180元，不足1小時以1小時計算，連續發生得連續處罰，上限為本案總價金30%；若經本會認定有特殊原因或有不可抗力情形者，不在此限。

(三) 程式除錯應依據國科會全球資訊網的相關規定辦理。

(四) 延續服務：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10%為限。

(五) 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。

十、其他

(一) 產品授權書

本案若另行採購之商用產品模組，需包含所用商用產品模組之授權書，且費用包含在總預算之中。

(二) 商用檔案購買授權書

本案若另行採購之商品圖片、個人著作圖片、音樂...等，需包含所用商用圖片、個人著作圖片、音樂...等之授權書，且費用包含在總預算之中。

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. 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	1份	電子檔	決標次日起 5個工作天內

2	資安文件	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。	1 份	紙本	決標次日起 5 個工作天
3	完成網站設計開發	1. 網頁程式原始碼 2. 網頁設計檔	1 式	電子檔	115 年 4 月 13 日
4	教育訓練	1. 學員簽到表 2. 課程資料	各 1 份	紙本及 電子檔	115 年 4 月 17 日
5	系統相關手冊	1. 系統測試計畫書 2. 系統開發文件（需包含資料庫欄位說明及 Schema 相關建置資料） 3. 使用者操作手冊 4. 測試報告書（含 SQL Injection 等安全漏洞檢測） (1) 功能測試報告 (2) 安全性檢測報告 5. 系統維護手冊 6. 系統災害復原手冊	1 式	電子檔	同本案履約期限
6	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
7	其他	無障礙標章申請資料	1 式	電子檔	同本案履約期限
8	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：台北市大安區和平東路 2 段 106 號 5 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、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：產業情報研究所 吳冠漩小姐  
電話：(02)2737-7789  
Email：[carolwu@iii.org.tw](mailto:carolwu@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	<b>執行力與配合度</b> <ul style="list-style-type: none"><li>●人力配置規劃</li><li>●執行團隊之相關經驗、學經歷及過去績效</li><li>●計畫執行及管理能力</li></ul>	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 4. 廠商履約實績：請詳述專案經驗及其成效
2	<b>整體企劃</b> <ul style="list-style-type: none"><li>●網站架構之完整性與可行性</li><li>●設計理念及管理人員管理及資料維護之便利性</li><li>●執行進度之時程規劃</li></ul>	5. 說明整體網站設計理念、網站的動線設計 6. 資訊安全及保密之規劃及執行方式 7. 網站測試、教育訓練之規劃及執行方式 8. 說明保固期間之售後服務方式 9. 提供時程進度規劃，說明相關工作預定進度、完成時點
3	<b>經費合理性</b> <ul style="list-style-type: none"><li>●相關執行費用估算與分配之合理性</li></ul>	10.於服務建議書詳列報價內容(請參考Excel附件〔 <b>委外開發報價明細表</b> 〕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】

資通系統防護基準控制措施

資通系統名稱：次世代通訊 PMO 中英文網站 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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	中/高	一、已逾期之臨時或緊急帳號應刪除或禁用。
		<input checked="" type="checkbox"/>	中/高	二、資通系統閒置帳號應禁用。
		<input checked="" type="checkbox"/>	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。
		<input type="checkbox"/>	高	一、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。
		<input type="checkbox"/>	高	二、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。
		<input type="checkbox"/>	高	三、應依機關規定之情況及條件，使用資通系統。
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	普/中/高	二、使用者之權限檢查作業應於伺服器端完成。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	普/中/高	四、應採用加密機制。
<input checked="" type="checkbox"/>		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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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		<input checked="" type="checkbox"/>	普/中/高	三、應記錄資通系統管理者帳號所執行之各項功能。	
		<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	普/中/高	資通系統於日誌處理失效時，應採取適當之行動。	
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	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)。	
		<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	普/中/高	對日誌之存取管理，僅限於有權限之使用者。	
		<input checked="" type="checkbox"/>	中/高	應運用雜湊或其他適當方式之完整性確保機制。	
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	普/中/高	一、訂定系統可容忍資料損失之時間要求。
			<input checked="" type="checkbox"/>	普/中/高	二、執行系統源碼與資料備份。
<input checked="" type="checkbox"/>			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。	
<input type="checkbox"/>			高	一、應將備份還原，作為營運持續計畫測試之一部分。	
<input type="checkbox"/>			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		<input checked="" type="checkbox"/>	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。	
	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。	
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	普/中/高	二、身分驗證相關資訊不以明文傳輸。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	普/中/高	資通系統應遮蔽鑑別過程中之資訊。
	加密模組鑑別	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
	系統發展生命週期設計階段	<input checked="" type="checkbox"/>	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	系統發展生命週期開發階段	<input checked="" type="checkbox"/>	普/中/高	一、應針對安全需求實作必要控制措施。
		<input checked="" type="checkbox"/>	普/中/高	二、應注意避免軟體常見漏洞及實作必要控制措施。
		<input checked="" type="checkbox"/>	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。
		<input type="checkbox"/>	高	一、執行「源碼掃描」安全檢測。
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	普/中/高	執行「弱點掃描」安全檢測。
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	普/中/高	二、資通系統不使用預設密碼。
		<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	中/高	開發、測試及正式作業環境應為區隔。
	系統文件	<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	高
<input type="checkbox"/>			高	二、使用公開、國際機構驗證且未遭破解之演算法。
<input type="checkbox"/>			高	三、支援演算法最大長度金鑰。
<input type="checkbox"/>			高	四、加密金鑰或憑證應定期更換。
<input type="checkbox"/>			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	<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
		<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
		<input checked="" type="checkbox"/>	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。
<input type="checkbox"/>		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)		
<p>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。</p> <p>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 <u>20</u> % 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。</p>				
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	<input checked="" type="checkbox"/> 電子檔案 <input checked="" type="checkbox"/> 實體檔案	<input checked="" type="checkbox"/> 已返還 <input checked="" type="checkbox"/> 已刪除 <input checked="" type="checkbox"/> 已銷毀
範例	程式原始碼	1	<input checked="" type="checkbox"/> 電子檔案 <input checked="" type="checkbox"/> 實體檔案	<input checked="" type="checkbox"/> 已返還 <input checked="" type="checkbox"/> 已刪除 <input checked="" type="checkbox"/> 已銷毀
1.			<input type="checkbox"/> 電子檔案 <input type="checkbox"/> 實體檔案	<input type="checkbox"/> 已返還 <input type="checkbox"/> 已刪除 <input type="checkbox"/> 已銷毀
2.			<input type="checkbox"/> 電子檔案 <input type="checkbox"/> 實體檔案	<input type="checkbox"/> 已返還 <input type="checkbox"/> 已刪除 <input type="checkbox"/> 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：	