需求說明書（含驗收規範）

壹、購案名稱

「114 年台灣智慧財產管理制度(TIPS)網站雲端環境建置與部署」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 7 月 18 日止。

二、 預算

新台幣 320,816 元整（含稅）。

參、需求說明

一、 現有服務架構

(一) Web Server：

1. Windows Server 2016(Hyper-V VM)
2. CPU 20 core / 16G Ram
3. 程式語言使用 Classic ASP 開發
4. 儲存空間約 200GB，本機備份資料約 450GB
5. 每週回傳備份資料一次，約 42G

(二) Database Server：

1. Windows Server 2019(Hyper-V VM)
2. CPU 20 core / 16G Ram
3. 資料庫 SQL Server 2019
4. 儲存空間約 50GB，資料庫約 5GB，本機備份資料約 150GB
5. 每週回傳備份資料一次，約 500MB

二、工作項目及功能說明：

(一) AWS 環境 （由本會會級供應商提供）:

1.區域需為臺灣
2.訂閱開啟/權限指派
3.AWS 基礎網路環境 (VPC、Subnet、Route Table、IGW、Security group、NAT)
4.EC2*1、RDS for SQL server*1
5.WAF、ALB*1、Network Firewall(內對外)
6.S3
7.其他所有監控 Cloudwatch + log
8.AWS Backup

(二) 工作項目：

項次	需求項目	詳細內容
1.	顧問與諮詢	● 架構分析 ● 環境評估 ● 需求確認

		● 雲端相關技術顧問與諮詢
2.	服務搬遷作業	● 將現有服務架構部署 ● AWS Application Migration Service (MGN) set up 總數：2 台 ● SQL 資料庫搬遷 (含搬遷評估) ● 檔案由地面 Storage 搬至 S3 ● 將強化企業智慧財產經營管理計畫之 ● TIPS 台灣智慧財產管理制度網站前後台整體搬遷至 AWS 運作
3.	測試工作	● 系統正確性測試 ● 連線測
4.	系統正式搬遷/切換	● 環境重新部署 ● 服務切換
5.	移交	● 管理權限移交

三、 維護管理

(一) 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. 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. **安全性檢測：**

(1) 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。

(2) 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。

四、 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指定機房環境。

五、 教育訓練

■至多 1 場，每場至少兩小時（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（內容須包括本案環境說明）。

六、 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)。

七、 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	環境交付說明文件	依「參、需求說明－工作項目」提供	1 式	電子檔	同本案履約期限
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	同本案履約期限
3	教育訓練	課程教材	1 式	電子檔	同本案履約期限
4	資安文件	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	1份	紙本	同本案履約期限
5	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

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： 台北市敦化南路二段 216 號 22 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、 廠商特定資格

投標廠商或其受雇人、從業人員具有專門技能之證明：

投標廠商需於 ■投標	須檢具 1 名具備 AWS 雲端機房架構師專業證照（AWS Certified Solutions Architect – Professional）文件影本。 ■員工在職證明。 ■如該原廠證照有效期規定，則需在效期內。

二、 購案聯絡人：

姓　名：科法所　黃偵哲先生

電　話：（02）6631-1154

Email：jim611@iii.org.tw

三、 發票資料：

抬　頭：財團法人資訊工業策進會

統一編號：05076416

【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<u>24 小時</u>，計<u>1</u>點	■是。	依本表計罰之違約

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
故障排除、系統修復	系統中斷時間，不得高於24小時	每次統計	每次計1點	□否，本案無資通系統。	金，每點為新臺幣伍仟元
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99.5%	每季統計	每不足1%，計1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4小時	每逾1工作小時，計0.5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1日，計1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1點。每逾1小時未通報本會計1點。 2.每逾1小時未提供資安事件等級評估、處理應變規劃及建議計1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24小時，計1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1日，計1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，按次計1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0.5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1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	
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	

評估項目	評斷方式	要求基準	違約金計點	每點違約金金額
	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	
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	

評估項目	評斷方式	要求基準	違約金計點	每點違約金金額
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】

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：