臺灣集中保管結算所股份有限公司

第二層 Fortigate 防火牆維護案

規範書

資訊作業部

中華民國 115 年 10 月

目　錄

壹、總則 2

貳、廠商資格 3

參、維護標的 5

肆、付款方式 6

伍、維護服務 7

壹、總則

一、 本規範書係為臺灣集中保管結算所股份有限公司（以下簡稱本公司）「第二層 Fortigate 防火牆維護案」（以下簡稱本案）而制訂。

二、為確保廠商有履行合約及提供完善服務之能力，廠商必須符合本規範書「貳、廠商資格」所訂之各項資格條件。

三、本案係對本規範書「參、維護標的」所列之標的提供維護服務，本公司得於一個月前以書面通知廠商後，終止一部或全部標的之維護服務。

四、本規範書「伍、維護服務」係對本案相關標的維護服務所訂定之最低要求。

五、廠商須至本公司指定之地點進行相關標的維護服務。

六、本案經履約完成、終止或解除時，廠商應返還、移交、刪除或銷毀履行本案而持有之資料，且不得有拷貝、複製或備份持有之行為，並要求受任人、受僱人、代理人及其他相關人員共同遵守。

七、廠商應遵守個人資料保護法、營業秘密法、資通安全管理法、本公司訂定之「資訊廠商應遵循之資通安全事項」(附件一)及本公司提供之相關作業規定;廠商參與人員均應受過適當之資通安全教育訓練。本公司認有必要時，得要求廠商派員參與本公司所舉辦之相關課程。

八、倘廠商知悉資通安全事件，應於 1 小時內通知本公司及採行之補救措施。

九、廠商不得將本案之權利義務轉讓，亦不得將本案之全部或一部轉包或分包予任何第三人。

十、廠商之資通訊設備，非經本公司同意不得與本公司資訊系統介接。

十一、本案廠商不得為主管機關核定生產、研發、製造或提供危害國家資通安全產品之廠商，廠商亦不得提供或使用危害國家資通安全之廠商產品;另本案之參與人員均不得為大陸地區人民，並於受託業務範圍內，不得使用中國大陸廠牌資通訊產品(含硬體、軟體及服務) 作業。

十二、對本規範書內容若有疑義，以本公司解釋為主。

貳、廠商資格

一、廠商須符合下列各項資格條件：

(一)實收資本額須為新台幣 1,500 萬元整(含)以上。

(二)在臺灣之成立時間至少達三年以上。

(三)領有權責機關發給之：

1. 經濟部公司登記證明書或公司變更（設立）登記表或法人登記證明文件或商業登記證明文件。

2.最近一期有效之營業稅或綜合所得稅或機關所得稅納稅證明。

3.票據交換機構或銀行於資格證明文件繳交截止日前一個月內所出具之非拒絕往來戶且最近一年無退票記錄證明。

(四)廠商不得為經濟部投資審議司公告之陸資資訊服務業者（陸資投資資訊產業事業清冊公開於經濟部投資審議司網站 https://www.moea.gov.tw/Mns/dir/home/Home.aspx）。

(五)廠商不得為政府電子採購網公告之拒絕往來廠商（拒絕往來廠商名單公開於政府電子採購網站(https://web.pcc.gov.tw)。

(六)廠商應提出資通安全管理措施自我說明（附件二）或通過我國標準法主管機關委託機構認證之機構出具之有效驗證報告，證明具備完善之資通安全管理措施。

(七)廠商應配置至少一員經適當之資格訓練或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。

(八)廠商須提示其參與人員名單及其有效之資通安全證照或最近一年內參與資通安全訓練課程證明之一項，並由本公司檢核其勞工保險或在職證明文件，廠商如需更換本案參與人員時，應事先向本公司提出接替人員名單及其符合本規範書規定文件，供本公司審核同意後始得更換。

(九)廠商須提示其參與人員下列有效之專業技能證明文件(正本或與正本相符之影本)之任一項，合計一員，擁有多張證照之人員可重複配置，廠商如需更換本案參與人員時，應事先向本公司提出接替人員名單及

其符合本規範書規定文件，供本公司審核同意後始得更換。

1. Fortinet 原廠相關證照

(十)廠商最近二年內未發生資通安全事件者，應出具未發生資通安全事件之**切結**。廠商最近二年內曾發生資通安全事件者，應出具書面說明，內容涵蓋資通安全事件通報、調查、處理、改善措施辦理情形，以及**切結**各項作業均依法規法令與公司程序規定辦理，相關風險並已排除等事項；改善措施尚未完成者，廠商應增列說明對本案履約之影響。

前述廠商出具之切結文件需通過本公司審核，方可參與本案。

二、廠商所提資料、文件，如經證實係偽造、變造或不實者，本公司除得依法處理外，並取消廠商之承攬資格。

參、維護標的

本案維護標的詳如「第二層 Fortigate 防火牆維護案設備維護清單」(附件三)。

肆、付款方式

一、 自簽約日起，每季付款一次。

二、 當季倘有新增或因終止而減少維護標的者，則依各該標的之實際維護日數比例增減計算該季之維護費用。

三、 廠商每季季末須檢附經本公司人員簽名驗收之相關維護保養記錄，向本公司申請付款。

伍、維護服務

一、 本案各維護標的之維護時段,詳如「第二層 Fortigate 防火牆維護案」（附件三),廠商應於維護期間內提供下列服務：

(一)故障維護服務：

1. 廠商應備有行動電話以供本公司聯絡，且須確保可即時聯絡維護人員。
2. 本公司於維護時段內享有異常或故障維修服務之權利。所稱維護時段,係指本公司通知廠商之時間,廠商修復之時間,則不以維護時段為限，亦即本公司得於維護時段內隨時通知廠商進行故障維修，廠商進行故障維修倘超逾維護時段，應繼續進行至修復時為止，且不得另行計費。
3. 本案硬體設備發生異常或故障時，本公司得於維護時段內通知廠商,廠商應於接獲本公司通知後 2 小時內到達本公司指定地點(倘維修地點在本公司異地備援機房者,廠商應於接獲本公司通知後 4 小時內到達），並於到達後 4 小時內修復，倘評估無法於 4 小時內修復者，應立即提供同等（或較優）設備免費供本公司使用。廠商應於修復完成後將維護標的返還本公司，並將異常或故障發生原因以書面告知本公司。如維護標的無法修復或原廠不再提供維修服務時,廠商應提供同等設備(其相關配備及條件與原維護標的相同或較優)並移轉所有權予本公司,以取代原維護標的物之修復及返還，惟因不可抗力或可歸責於本公司之事由致標的物無法即時回復正常運作，延誤之時數應予扣除。

(二)系統調校服務：

廠商依本公司系統實際環境需求,以書面或電子郵件提出系統調校建議，經本公司同意後，廠商須依本公司指定時間(不以維護時段為限)到達辦理系統調校服務。

(三)安裝修補程式服務(系統安全要求)

廠商每季應主動以書面或電子郵件提出安裝修補程式評估,經本公司

同意後，廠商須於本公司指定時間(不以維護時段為限)到達辦理安裝修補程式服務。

(四)問題諮詢服務

廠商於維護時段內接獲本公司通知後，須提供本案標的相關問題諮詢服務及處理。

(五)定期保養服務

廠商應每季至少對本案標的提供一次定期保養服務，服務內容詳如「軟/硬體資訊設備定期保養檢核表」(附件四)，並檢附本案參與人員名單。

二、 廠商應配合本公司事先通知每年最多各 3 次之「系統演練測試作業」及「硬體故障報修作業程序演練」，依本公司指定時間（不以維護時段為限）指派維護人員配合到場待命，免費提供必要之協助及解決相關軟硬體問題之支援服務。

三、 廠商應於簽約後 30 日內提供資訊安全管理計畫(附件五)，經送交本公司審閱後認可。

四、 廠商未能履行前述任一條款規定之情事者，本公司有權按合約規定計罰違約金及請求損害賠償。

五、 本公司得要求廠商於維護時段外提供故障維護及系統調校服務，服務費用每小時以新台幣 3,000 元為上限，超過 4 小時部份以 8 折計價，服務時間自廠商派員到達本公司時起算，費用包含所有與計時維護服務相關之車資、工資、零件、運費、稅捐等相關費用。

臺灣集中保管結算所股份有限公司

附件一

資訊廠商應遵循之資通安全事項

一、廠商發生資通安全事件(以下稱資安事件)涉及本公司委託業務範圍時，應於知悉資安事件後1小時內通知本公司事件發生過程與評估影響範圍，本公司於接獲通知時應判定資安事件等級與告知廠商，廠商並應採取適當之應變措施與辦理下列事項：

(一)一、二級資安事件應於知悉後七十二小時內，完成損害控制或復原作業，並通知本公司。

(二)三、四級資安事件應於知悉後三十六小時內，完成損害控制或復原作業，並通知本公司。

(三)完成損害控制或復原作業後，應於1個月內完成調查、處理及改善報告提供本公司。

二、廠商於公開資訊觀測站發布發生資安事件，應於發布當日通知本公司。

三、本公司委託業務之相關資訊(包含但不限於規範書、程式碼、元件與專案文件)應妥善保管，並僅提供專案團隊人員於執行本公司委託業務時使用，惟經本公司同意者不在此限;本公司委託業務之相關文件或其內容,如遭洩漏或不當使用，應比照資安事件啟動通報與應變機制。

四、處理本公司委託業務範圍時，廠商應遵守下列事項：

(一)資通安全管理法、資通安全管理法施行細則、個人資料保護法、個人資料保護法施行細則及ISO/CNS 27001之規範。

(二)實施資通安全認知宣導與教育訓練，應涵蓋社交工程與本「資訊廠商應遵循之資通安全事項」要求內容，以強化人員資通安全意識、降低誤觸社交工程之機率，與瞭解自身資通安全權責。

(三)制訂適當之安全管控措施，避免未經授權之存取、防範系統遭受破壞，以及確保業務資料之機密性、完整性及可用性。

(四)資通系統之規劃，應考量安全需求，並於設計、測試、變更與維護各階段，採取適當之安全管控措施。

(五)建立監控、通報與應變機制，以及時發現資安事件並有效的因應處理。

(六)涉及本公司委託業務之程式碼、元件與資料夾名稱等，不得使用可直接識別本公司之文字(如集保、TDCC 等)、圖像/符號(如集保 LOGO)、影音等，惟經本公司同意者(如應用系統功能擴充沿用舊有元件、專案文件等)，不在此限。

(七)使用公用雲執行本公司之委託業務時，應檢附公用雲相關安全設定(如權限最小化)說明文件，並取得本公司書面同意，方可使用。

(八)與委託業務相關之開發環境，定期辦理安全性檢測，檢測發現之高風險以上之弱點項目，應研議因應措施與持續追蹤改善。

(九)禁止使用大陸廠牌資通訊產品[含軟體、硬體及服務(含生成式 AI 程式如：Deepseek 等)]。

(十)使用人工智慧(AI)應遵循事項：

1.使用生成式 AI、代理式 AI（Agentic AI）或其他任何人工智慧（AI）技術、模型、系統或服務(以下稱 AI 工具)執行本公司之委託業務時，應取得本公司書面同意，方可使用，並不得向 AI 工具提供本案涉及應保密、個人及未經本公司同意公開之資訊，亦不得向 AI 工具詢問可能涉及本案機敏或個人資料之事項，其經 AI 工具產製之履約標的及相關文件，廠商應予以標明或揭露。

2.廠商不得直接將人工智慧(AI)之原始產出作為履約標的交付本公司。廠商使用 AI 工具輔助製作或產出交付物時，須建立完善之人為審查（Human-in-the-Loop）與驗證機制，對 AI 產出進行實質檢視、校對與修改，確保內容無虛構錯誤、侵犯他人智慧財產權、洩漏機密或違反法令之情事。廠商對於所有交付之履約標的，無論是否涉及 AI 輔助，仍須負完全之正確性、合法性、智慧財產權擔保及品質保證責任。

五、若有公司組織調整、業務重大異動等(如:團隊變更)，於得知異動執行前主動通知本公司。

六、資訊相關設備及帳號之使用與管理規定

(一)資通系統委外廠商或委外購買人力之派駐人員

1. 應使用本公司所提供之電腦設備與各項資源，且不得移作與專案無關之用途。

2. 本公司得派員進行電腦病毒、系統弱點、後門程式偵測等相關安全檢查工作，以維護系統作業安全，如發現有或評估可能發生影響資通安全之情事時，本公司得隨時要求廠商停止作業或撤出本公司。

(二)所有委外廠商人員

1. 不得使用中國大陸元件，且使用開源軟體或第三方元件應先取得本公司同意。

2. 廠商未遵守相關規定而導致本公司設備遺失、毀損或有損及本公司權益之情事，廠商應負賠償之責。

3. 倘持有本公司帳號，帳號持有人應盡妥善保管帳號密碼之責，帳號僅限於該帳號持有人本人使用，亦不得使用非本人帳號。如帳號密碼有外洩疑慮或懷疑遭受未經授權存取，除儘速更換密碼外，並應立即通知本公司。

4. 廠商人員因業務需要進入本公司資通系統執行各項維護作業時，應由本公司持有該系統帳號權限之主辦組陪同人員登入系統，並由廠商人員從旁協助進行維護作業。

5. 廠商人員使用之資訊設備(含伺服器、個人電腦、筆記型/平板電腦等)，倘涉及本公司委託業務時，應辦理下列事項：

(1) 建置防毒機制與適時更新病毒碼，並適時進行病毒掃瞄。

(2) 適時執行作業系統及軟體版本更新作業，與版本修補作業。

(3) 電腦設備應有帳密及螢幕保護機制，以避免資料外洩。

(4) 可攜式電腦設備(筆記型/平板電腦、USB…等)應有適當之保護機制，避免遭非設備持有人員開啟。

七、電腦機房或管制區域進出管理

(一)資**通**系統委外廠商或委外購買人力之派駐人員，負責資**通**系統開發與維護之派駐人員，應於本公司指定之廠商測試區進行作業；負責辦公室自動化設備安裝與維護之派駐人員，應於本公司同仁陪同下，於指定之工作時間及場所進行作業。

(二)需先經由權責部門組級以上主管核准，填寫「電腦機房進出登記簿」或「管制區域人員進出/使用登記簿」後，始得由相關授權人員陪同進入本公司管制區域；惟因應緊急事故處理時，得先填寫前揭登記簿後進入，事後再由權責部門組級以上主管於登記簿補行簽章。

(三)本公司電腦機房或管制區域作業區內禁止將行動電話及具攝錄功能之設備攜出(入)，因業務所需之電腦相關設備，於攜出（入）電腦機房或管制區域前，須獲得權責部門組級主管核准，並於「電腦機房資訊設備進出申請單」或「管制區域人員進出/使用登記簿」中的備註欄位詳細註明後，始可准許攜出（入）。

八、其他

(一)進入本公司前，應至警衛執勤處辦理換證事宜，用以刷卡進出指定作業場所，臨時證遺失或毀損應向本公司主辦部門申請補發，並繳交補發費用。

(二)資**通**系統委外廠商或委外購買人力之派駐人員進駐廠商測試區，應先完成「保密同意書」（公司版）、「保密同意書」（員工版）、「測試區廠商派駐人員專用」之告知聲明。

(三)本公司管制區域內不得攜入或存放具磁性、放射性、易燃性、易爆性等非工作需要物品，且禁止與處理電腦業務無關之一切行為，本公司購置之各類電腦設備，非經核准，不得攜出本公司。

(四)軟、硬體交付項目需經主辦單位檢測不含惡意程式(如後門或木馬程式等)，或由廠商提供不含惡意程式之掃描報告或承諾書。

(五)應確實了解並遵守本公司資通安全政策(請參考本公司官網)及本公司提供之相關作業規定。

(六)應配合本公司通知，並依本公司規定方式辦理資通安全自評作業。

資通安全管理措施自我說明　　附件二

廠商應提供下列各項說明（如有佐證資料需檢附）:

一、 資安事件之預防、通報及應變辦法。(例如：訂定緊急應變、通報程序或其他相關管理機制)

二、 資通安全稽核機制。(例如：內部稽核計劃或其他相關稽核機制)

三、 資通安全教育訓練。(例如：最近一年一般使用者及主管內、外部課程訓練紀錄等)

四、 資通安全技術面防護。(例如：帳號管控、防毒軟體、網路防火牆、電子郵件過濾機制或其他相關防護機制)

此致

臺灣集中保管結算所股份有限公司

公　　司：

負 責 人：

統一編號：

地　　址：

電　　話：

中華民國　　年　　月　　日

臺灣集中保管結算所

附件三

第二層 Fortigate 防火牆維護案設備維護清單

編號	資訊系統/設備標的	機型機號	數量	維護開始日期	維護結束日期	維護時段	備註
1	Fortigate 1801F 防火牆	FG181FTK22900459	1	115/12/6	117/12/5	星期一至星期六，每日 24 小時	位於營運機房(板橋機房)
2	Fortigate 1801F 防火牆	FG181FTK21902096	1	115/12/6	117/12/5	星期一至星期六，每日 24 小時	位於營運機房(板橋機房)
3	Fortigate 1801F 防火牆	FG181FTK21902783	1	115/12/6	117/12/5	星期一至星期五，以及本公司之彈性上班日八時三十分至十七時三十分	位於異地備援機房(竹北機房)
4	Fortigate 1801F 防火牆	FG181FTK22900422	1	115/12/6	117/12/5	星期一至星期五，以及本公司之彈性上班日八時三十分至十七時三十分	位於異地備援機房(竹北機房)

註：本清單中設備歸屬機房位置將會依本公司需求調撥而改變。

臺灣集中保管結算所

附件四

軟/硬體資訊設備定期保養檢核表

合約編號：　　合約名稱：

檢核項目	檢查內容	檢核結果	
		正常/(是)	異常/(否)
一、	檢視硬體設備整體運作是否正常		
	1-檢查硬體暨週邊設備之電源、燈號是否正常	□	□
	2-完成設備清潔及外觀檢視	□	□
	3-檢查硬體之異常記錄檔，並完成調校作業以排除異常狀況	□	□
	4-檢查硬體修補程式是否已更新至本公司確認版本	□	□
	5-檢查系統資源(設定檔、檔案系統、硬碟)配置是否運作正常，並完成調校作業	□	□
	6-檢查異常狀況解析資料檔之資源配置是否運作正常，並完成調校作業	□	□
二、	檢視軟體設備整體運作是否正常		
	1-檢查軟體之異常紀錄檔，並完成調校作業以排除異常狀況	□	□
	2-檢查軟體修補程式是已更新至本公司確認版本	□	□
	3-檢查軟體設定檔是否正常，並完成調校作業	□	□
三、	檢附電腦設備定期保養記錄表及相關文件	□	□
備註			

維護廠商名稱：_____　　維護人員簽章:_____

資訊安全管理計畫

附件五

廠商應提供下列十七項說明（如有佐證資料需檢附）：

一、 與機關資安相關之協調作業。

二、 作業人員職務的區隔。

三、 系統運作程序與方式。

四、 由第三者執行查核與驗證相關之配合作業。

五、 系統存取控制之安全。

六、 作業變更管理。

七、 服務交付方式。

八、 資料被查詢與異動之軌跡紀錄。

九、 防範惡意碼與安全漏洞措施。

十、 後門程式清理。

十一、 系統維運期間之定期系統弱點掃描服務措施。

十二、 委外媒體的處理措施。

十三、 資訊安全事件管理。

十四、 資訊安全事件之檢討與監督。

十五、 服務終止之措施。

十六、 所有權與智慧財產之保障。

十七、 遵循適法性作法

此致

臺灣集中保管結算所股份有限公司

公　　司：

負 責 人：

統一編號：

地　　址：

電　　話：

中華民國　　年　　月　　日