

臺灣集中保管結算所股份有限公司
網際網路系統與參加人網路環境第二層防火牆汰換案
規範書

資訊作業部
中華民國 111 年 7 月

目 錄

壹、總則.....	2
貳、廠商資格.....	4
參、採購項目.....	6
肆、採購規格.....	7
伍、交付項目及時程.....	8
陸、驗收及付款方式.....	10
柒、保固與維護.....	12

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「網際網路系統與參加人網路環境第二層防火牆汰換案」（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、本規範書之「肆、採購規格」係對本案購置所須之軟、硬體設備規格，作整體概括性之說明及規範，其所訂定之各項設備性能及須具備之功能應視為最低要求，並提供廠商有義務提供超過最低要求之完整可供運轉設備，並可與現有環境整合運作。
- 四、廠商應依本規範書之「伍、交付項目及時程」完成交付，並至本公司指定之地點安裝並完成功能測試、組態設定與調校、設備所需網路佈線施工等作業，且應與本公司現有環境整合運作。
- 五、廠商應依本規範書「陸、驗收及付款方式」進行驗收手續，另需配合本案設備之上線相關作業，倘有延遲之罰則，悉依合約規定辦理。
- 六、本規範書之「柒、保固與維護」規範廠商應提供之保固與維護服務項目，有與本公司簽訂買賣或維護合約者，以合約內容為準。
- 七、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。
- 八、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。
- 九、倘廠商與協力廠商知悉資通安全事件，應立即通知本公司及採行之補救措施。
- 十、廠商得委由協力廠商協助執行本案之作業，協力廠商須出具原廠授權之證明文件，並註明本案執行之範圍及項目。協力廠商或原廠協助執行作業造成本公司損害時，廠商應對本公司負賠償責任。

- 十一、廠商與協力廠商之資通訊設備，非經本公司同意不得與本公司資訊系統介接。
- 十二、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。
- 十三、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貳仟萬元整（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)廠商與協力廠商不得為經濟部投資審議委員會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委員會網站 <https://www.moeaic.gov.tw/>）。
- (五)廠商與協力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)為本案各項設備之原製造廠商、代理商或經銷商。代理商或經銷商須檢具代理商或經銷商之證明文件，若經銷商之證明文件由代理商出具者，須另檢附其為合法代理商之證明文件。
- (七)廠商與協力廠商（原廠除外）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。
- (八)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。
- (九)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。

(十) 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. Certificated Ethical Hacker (CEH)

2. CompTIA Security+

3. Certified Information Systems Security Professional (CISSP)

4. Fortinet 原廠相關證照

二、廠商於資格審核時，應檢具各項設備之型錄或技術手冊資料，並加蓋公司大小章。

三、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、採購項目

本案採購項目之品名及數量說明如下，其詳細型號或規格請參閱

「肆、採購規格」。

一、Fortinet 防火牆設備：四部。

二、專案服務：乙式。

肆、採購規格

本案採購項目品名之型號或規格如下：

一、Fortinet 防火牆設備：四部，每部規格如下：

- (一) 為硬體式(Appliance)架構，符合標準 19 吋機架式。
- (二) 提供 Firewall Throughput 140 Gbps(含以上)。
- (三) 提供 Concurrent Sessions 為 12,000,000 (含以上)，New Connections per Second 為 750,000 (含以上)。
- (四) 需提供 14 個(含以上) 10/100/1000BaseTX RJ45 介面埠、8 個(含以上)1GE SFP 介面埠、14 個(含以上)10GE SFP+介面埠及 2 個 10/100/1000BaseTX RJ45 管理介面埠。
- (五) 提供原廠 2 個(含)以上電源供應器 Redundant Power Supplies (Hot Swappable)。
- (六) 提供最高達 100,000 個(含)以上的安全策略(Security Policy)。
- (七) 提供 10,000 Concurrent SSL-VPN Users (Tunnel Mode)，SSL-VPN Throughput 11 Gbps。
- (八) 提供 HA 模式：主動與備援模式(Active-Passive)，及雙主動模式(Active-Active)。
- (九) 具備 10 個(含)以上虛擬防火牆功能。
- (十) 提供 20,000 OTP(One Time Password) Token 控管能力。
- (十一) 須具備 IPv4 與 IPv6 防火牆及路由功能。
- (十二) 須支援 RADIUS 帳號驗證服務。
- (十三) 廠商技術須通過 ICSA Firewall 國際第三方實測安全認證，廠商須提供至今仍然有效的證明文件。
- (十四) 須支援日誌(SYSLOG)紀錄服務，可儲存日誌於本機設備，或遠端日誌紀錄系統。

二、專案服務:乙式，規格如下：

- (一)須提供本案新、舊防火牆設備轉置服務，建置地點為本公司主機房與異地備援機房。
- (二)須提供本案建置設備之設備安裝、設定與調校，並確認運行正常。
- (三)須整合本公司現有 SOC 監控管理平台。
- (四)提供本案建置設備之相關網路佈線作業。

伍、交付項目及時程

一、廠商須於簽約後 60 天（含）內完成硬體交付，交付項目如下：

1. Fortinet 防火牆設備四部。

二、本規範書之「參、採購項目」。

三、廠商應提供軟、硬體設備不含惡意程式之承諾書(附件三)。

四、廠商應提供系統安全弱點掃描檢測報告(報告中應列示風險等級之檢出內容及評估說明)。

五、交付設備之使用手冊至少二份(紙本或光碟，若交付文件為光碟，內容需經過本公司掃毒並留存檢測結果證明)。

六、本案之專案計劃書簽約後 30 天（含）內交付、安裝建置文件與操作手冊至少各二份，(紙本或光碟，若交付文件為光碟，內容需經過本公司掃毒並留存檢測結果證明)。

七、本案採購之硬體設備如由外國製造，須檢附進口報單。

八、硬體設備須檢附該產品係為簽約日前一年內生產之出廠證明文件。

九、硬體須檢附原製造廠商或其在臺灣之合法分（子）公司產品保固服務證明書。

十、廠商交付之軟、硬體設備，需留置本公司指定區域 14 天，並通過本公司新進軟、硬體設備檢測作業。

十一、廠商應於簽約後 30 日內提供資訊安全管理計畫(附件四)，經送交本公司審閱後認可。

陸、驗收及付款方式

廠商應於民國 111 年 12 月 15 日（含）前，完成本案「伍、交付項目及時程」所定之服務及交付全部項目，經廠商與本公司系統安全弱點掃描檢測之軟、硬體設備不得有高風險以上項目(經本公司評估屬廠商應修補之資安漏洞)。本公司確認驗收無誤後，一次付款。

柒、保固與維護

- 一、本案之硬體設備保固期間自全案驗收完成次日起為期 4 年。本公司於保固期間內應享有保固維護服務及到場維修，維護時段區分如下：主機房為星期一至星期六之每天 24 小時，異地備援機房為星期一至星期五，以及本公司之彈性上班日（以政府或臺灣證券交易所公告者為準）八時三十分至十七時三十分。

項目如下：

(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」(附件五)，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、 本案驗收階段之系統安全弱點掃描檢測，屬於中風險資安漏洞，經本公司評估屬廠商應修補之資安漏洞，廠商需於本案驗收完成次日起為期一年內完成修補。
- 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。

資訊廠商應遵循之資通安全事項

一、資訊相關設備及帳號之使用與管理規定

(一) 資訊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，本公司得隨時命令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，禁止共用帳號。
4. 廠商人員因業務需要進入本公司資訊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。

二、電腦機房或管制區域進出管理

(一) 資訊系統委外廠商或委外購買人力之派駐人員，負責資訊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)。

三、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，以強化人員資通安全意識，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)資訊系統之規劃，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，以及時發現資通安全事件並有效的因應處理。

四、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。

五、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)資訊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。

廠商應提供下列四項說明（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

承諾書

本公司承諾銷售之網際網路系統與參加人網路環境第二層防火牆汰換案產品，所提供之軟、硬體設備不含惡意程式，若違反上開承諾，本公司願依合約承擔法律責任，特開立此承諾書。

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

資訊安全管理計畫

附件四

廠商應提供下列十六項說明（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、 服務交付方式。
- 五、 交付之軟體與硬體元件來源不得為大陸地區。
- 六、 防範惡意碼與安全漏洞措施。
- 七、 保固期間發現系統或程式弱點之修復方式。
- 八、 服務驗收或稽核服務之管理程序。
- 九、 專案人員應參與機關之資安管理規範與個資法等之教育訓練。
- 十、 專案人員籌組與異動時之規劃。
- 十一、 訂定驗證項目，以鑑定資安服務水準。
- 十二、 資訊安全事件管理。
- 十三、 資訊安全事件之檢討與監督。
- 十四、 服務終止之措施。
- 十五、 所有權與智慧財產之保障。
- 十六、 遵循適法性做法。

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

臺灣集中保管結算所
軟/硬體資訊設備定期保養檢核表

附件五

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	<input type="checkbox"/>	<input type="checkbox"/>
	2-完成設備清潔及外觀檢視	<input type="checkbox"/>	<input type="checkbox"/>
	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	<input type="checkbox"/>	<input type="checkbox"/>
	4-檢查硬體修補程式是否已更新至本公司確認版本	<input type="checkbox"/>	<input type="checkbox"/>
	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	<input type="checkbox"/>	<input type="checkbox"/>
	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	<input type="checkbox"/>	<input type="checkbox"/>
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	<input type="checkbox"/>	<input type="checkbox"/>
	2-檢查軟體修補程式是否已更新至本公司確認版本	<input type="checkbox"/>	<input type="checkbox"/>
	3-檢查軟體設定檔是否正常，並完成調校作業	<input type="checkbox"/>	<input type="checkbox"/>
三、	檢附電腦設備定期保養記錄表及相關文件	<input type="checkbox"/>	<input type="checkbox"/>
備註			

維護廠商名稱：_____ 維護人員章：_____