

中南部新聞中心防火牆招標規範

因中南部新聞中心為重要新聞分部，為避免防火牆單點故障問題，導致影響到新聞正常製播維運，故於現有 CheckPoint 設備架構下增購防火牆設備，以完善相互備援機制。

一、 設備規格

A. 每台防火牆規格如下: (共計採購兩台: 台中、高雄各一台)

- 1.1. 獨立主機採硬體式設備(Hardware Appliance)架構本身提供 5 埠(含)以上 1GE RJ45 高速網路連接介面，同時具備 1 埠專屬管理介面。
- 1.2. 系統同時連線數至少須達 4 百萬個(含)以上，以及每秒新增連線數須達 60,000 個(含)以上。
- 1.3. 當防火牆、應用程式控制、入侵防護功能、惡意程式阻絕防護開啟的狀態下，整體處理效能 Throughput 須達 1.5 Gbps (含) 以上。
- 1.4. 支援網路設備 HA (High Availability): Active-Active / Active-Passive 等備援功能，並支援與既有防火牆整合，使單機發生故障無法運作時備援設備接續運作。
- 1.5. 投標產品設備品牌須為 Gartner Report Network Firewalls 魔術象限領導者。
- 1.6. 得標廠商須提供資安功能防護訂閱授權，須包含入侵防護、應用程式管控、進階惡意程式防護、垃圾郵件過濾、網頁過濾功能、雲端沙箱等。
- 1.7. 特徵資料庫(Signature Database)需能透過網路更新，須提供三年(含)以上保固，並於保固期內免費提供特徵資料庫更新服務。
- 1.8. 須與既有防火牆集中化管理平台整合，並提供現有管理機足夠管控設備之 GW License。

B. 每台 L2 網路交換器規格如下: (共計採購四台: 台中、高雄各兩台)

- 1.9. 具備 8 埠(含)以上 100M/1G BaseT 乙太網路埠。
- 1.10. 須提供三年(含)以上保固。

二、 其他

- 2.1 得標商負責所有與本案相關設備(包含本單位現有設備)的安裝設定，並須整合現有台中高雄新聞中心防火牆設備為互為自動備援模式。如有任何費用產生，由得標廠商支付。
- 2.2 本案所有新購之軟硬體產品須提供原廠或原廠授權代理商之新品證明。
- 2.3 交貨地點:公共電視台中新聞中心及高雄新聞中心。

三、 履約期限

- 3.1 立約商應於簽約日次日起 90 日曆天內完成交貨、安裝、測試並報請驗收。逾期每遲延一日，應分別按契約總價千分之一逐日計課逾期違約金，上限為契約總價百分之二十。

四、 保固與維護

- 4.1 立約商於全案驗收合格日起保固三年。保固期間內免費負責標的物之維修、保養換件等維護工作及正常使用狀況下發生故障免費修理與更換非消耗性零組件。若標的物在保固期間內軟硬體有缺點(BUG)，立約商應負責維修或更新改善，並不得索取任何費用。
- 4.2 立約商應於驗收後提供原廠或原廠授權代理商連帶保固三年切結書。
- 4.3 本案自驗收合格日之次日起，立約商提供軟硬體三年 7*24 保固與維護，須於 2 小時內提供電話除錯服務，叫修後 4 小時內到府服務，如無法於 24 小時內修復完畢，立約商須無條件提供相容同等級以上之備品。
- 4.4 若立約商未依上述時限排除故障，又無替代故障設備之措施時，每逾一日按契約價金總額千分之二計算逾期違約金，本會得逕自保固保證金扣抵，並連續處罰至故障完全排除為止。
- 4.5 保固期間內系統有任何異常，包含硬體損壞與軟體不正常運作，立約商需提供免費維修及更換料件服務。
- 4.6 保固期內，倘公視基金會因業務需要，需進行設備關機、移機等工作，立約商應無條件派員技術配合處理，因異動產生之材料費用，由本會負擔。
- 4.7 除特別註明不同保固時間之項目外，立約商需在保固期間內提供免費負責標的物之維修、保養換件等之維護工作，及在正常操作情況下發生故障免費修理與更換零組件。若標的物在保固期間內軟硬體有缺點(BUG)，立約商應負責維修或更新改善，並不得索取任何費用。
- 4.8 全系統操作手冊廠商應不定期無償更新。

五、 驗收

- 5.1 原廠或原廠授權代理商之新品證明，如係進口貨應另附海關進口證明文件。
- 5.2 提供所有軟硬體設備 3 年之立約商保固與維護之保固切結書及原廠或原廠授權代理商保固證明書。該切結書及證明書必須隨附購案中各項電腦系統軟硬體之個別廠商證明文件作為附件。
- 5.3 依本會需求及本規範規定之手冊及電子檔。

六、 其他規範事項

6.1 得標廠商資格:

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件：

- (一) 凡在政府機關登記合格，且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案服務人員不得為陸籍人士。
- (二) 本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他經銷商執行。

6.2 業務保密安全責任:

- (一) 得標廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽定保密協議書。
- (二) 得標廠商對特別以文字標示或口頭明示為機密資料者，非經本會書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，得標廠商應負完全責任。
- (三) 得標廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由得標廠商自訂)。
- (四) 契約終止時，得標廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本會或經本會同意後銷毀。
- (五) 履約期間造成保密及安全事件，得歸咎於得標廠商之責任時，得標廠商應負所有法律及賠償責任。
- (六) 本會對得標廠商保留實地稽核權，以確保得標廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

6.3 配合事項:

- (一) 得標廠商須無償配合提供：本會災難演練、主管機關或行政院災防演習之遠端技術協助或諮詢服務。
- (二) 需無償配合本會依 ISO 27001 之指定的第三方外部稽核或查核，進行實地或書面訪查作業，如有違反資通安全法規情事依合約條款處理，並不得續約。
- (三) 廠商應遵守行政院所頒訂之各項資訊安全規範及標準，並遵守機關資訊安全管理及保密相關規定。此外機關保有對廠商執行稽核的權利。
- (四) 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)，並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。
- (五) 廠商提供服務，如發生資安事件時，必須通報機關，提出緊急

- 應變處置，並配合機關做後續處理。
- (六) 基於法令及合約需求，本會得要求實施定期或不定期稽查，以監督專案內各項安全管理執行情形。
 - (七) 契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄。

七、 教育訓練(免費提供):

設備安裝完成後，即可進行教育訓練，課程內容必須包括系統操作與維護，並於報請驗收前完成。立約商準備教育訓練計畫，並提供合格教師在指定之時間及地點進行教育訓練課程，課程至少 4 小時以上之專業訓練，並得視使用單位需要延長及增加梯次，立約商並不得另外要求收費。師資人員及其他相關衍生性之所有費用皆由立約商自行負擔。