公共電視文化事業基金會

特權帳號安控稽核系統

徵求文件

Request for Proposal

中華民國 113 年 8 月

目　　錄

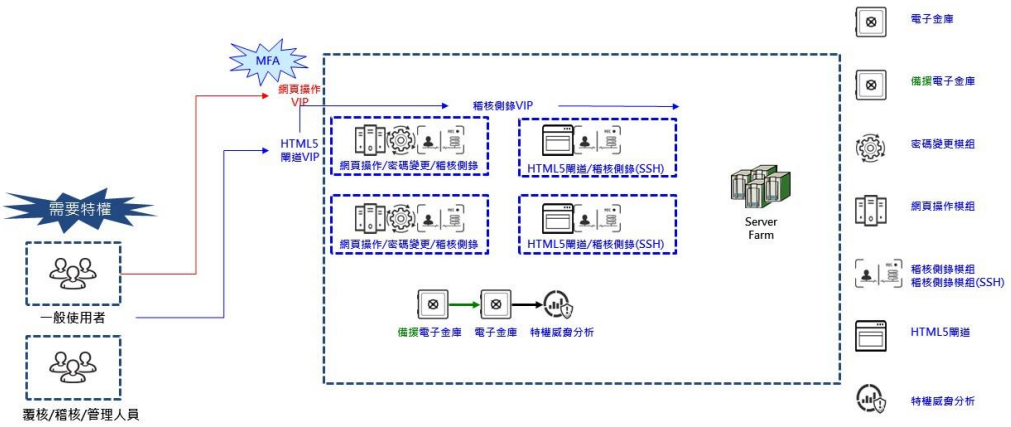
壹、 專案說明

一、 專案目標

為管理和監控企業內部的特權帳號，防止未經授權的存取，並提升整體資訊安全性及合規性，規劃採購特權帳號管理系統。

二、 可交付成果

建置及設定前端主機一座、電子金庫一座及備援電子金庫一座於本會所轄之指定場所集中管理本會資訊部管轄之特權帳號，如作業系統、應用系統、資料庫、硬體設備最高管理者權限、排程服務啟動帳號、委外廠商連線帳號等，並針對申請紀錄留存核准軌跡，於使用期間紀錄連線軌跡包含登入登出留存及錄影紀錄，並可依本會管理需求設定排程產出管理報表。



三、 預期成果

本會資訊部持有之特權帳號落實使用者在適當的時間安全存取適當的資源，以防止未經授權的存取和數據洩漏。確保特權帳號的使用符合企業的安全政策。提供有效的審計和監控機制，便於追蹤和管理特權帳號的使用情況。

貳、 系統功能需求 (授權 3 年)

一、 系統架構與管理功能

1. 提供本單位 10 個(含)以上使用者連線登入特權帳號安控稽核系統授權並內含多重要素驗證(MFA)機制。
2. 系統須提供密碼管理、稽核側錄與威脅分析功能，能分析識別可疑特權帳號登入行為與敏感動作。
3. 多重要素驗證(MFA)機制，系統須至少包含行動 APP 驗證碼、QR Code 碼、電子郵件驗證碼、人臉辨識、指紋辨識，並提供行動 APP 安裝在 Android、iOS 行動裝置。
4. 系統須經過 Gartner 評比 Privileged Access Manager 為領導象限品牌。
5. 系統架構須具備中央儲存伺服器，所有存放在系統中的檔案須為加密檔案，並符合 FIPS 140-2 安全需求規範。
6. 系統架構須具備災難復原 DR(Disaster Recovery)機制，可於中央儲存伺服器停止運作時自動連線至備援系統，不會影響日常運作。
7. 系統須支援全域政策，統一定義密碼檢查與變更週期，亦可依受管理主機系統設定例外政策。
8. 系統須支援使用者登入系統後僅顯示被授權登入的受管理主機系統。
9. 系統需支援分段式密碼存取方式，依使用者權限只能看到前段或後段密碼。
10. 系統需支援密碼設定不顯示功能(密碼不揭露)，僅允許使用者代登入受主機系統。
11. 系統須支援一層或階層覆核流程機制，至少一位或二位以上人員核可後，並可同時採用批次方式進行大量的申請使用與核准請求。
12. 系統須支援登入 Web 圖形化(GUI)操作介面與行動 APP 簽核。
13. 系統須支援預先申請密碼使用區間，如: 下班後或假日作業，待覆核後，僅能在申請使用區間作業。
14. 系統須支援密碼版本控管功能，當需要使用舊版本密碼時可由被授權使用者取得，例如受管理系統被備份檔還原後。
15. 系統須支援受管理設備帳號密碼批次或一次上傳功能。
16. 系統須支援 SSH Key 管理功能。
17. 系統須支援內建電子郵件(Email)事件通知引擎，並支援提供變數允許管理者自訂郵件範本內容。

18. 系統須支援 Web 圖形化(GUI)統一管理與使用者操作介面，並至少支援英文、繁體中文。
19. 系統須至少於線上保留一年報表、影片、稽核紀錄等資料，以供隨時調閱稽查。
20. 系統須支援透過 syslog 轉送至本單位現有 SOC 資安監控平台。

二、 密碼管理功能

1. 系統密碼管理功能，必須以不安裝代理程式(Agent-less) 方式，且不須因密碼變更機制而必須額外新增帳號執行。
2. 系統須支援至少可自動控管本會資訊部管轄之主機系統特權帳號，包含但不限於：

   (1) Linux Server
   (2) Windows Server (本機與網域帳號)
   (3) VMWare ESXi
   (4) VMware vCenter

3. 系統須支援至少可自動控管本會資訊部管轄之資料庫特權帳號，包含但不限於：

   (1) SQL Server、My SQL

4. 系統須支援至少可自動控管本會資訊部管轄之網路&資安設備特權帳號，包含但不限於：

   (1) Switch
   (2) CheckPoint Firewall
   (3) Palo Alto Firewall
   (4) F5 WAF
   (5) DNS Controller

5. 系統須支援管理 Windows 服務啟動帳號與排程工作的密碼。
6. 系統須支援管理儲存於一般 TXT 文件(Plain Text)、INI 檔案、XML 檔案中的密碼。

7. 系統須支援提供定期自動更改密碼功能，密碼複雜度可依本單位政策定義。
8. 系統須支援密碼依需求限制於特定時間變更，如：04:00~06:00。
9. 系統須支援自動檢查受管理主機系統上的特權密碼是否與系統相同，若不一致可主動發出電子郵件警告通知管理者，並可於兩者密碼不同時自動重置密碼，使受管理設備密碼與系統相同。
10. 系統須支援一次性密碼(One-Time Password)功能，經授權取得密碼後，可依政策規定，在一定時間後自動更新密碼。
11. 系統須支援將受管理主機系統帳號設定為統一密碼內容群組，一次性變更相同密碼。

三、 稽核側錄報表與威脅分析功能

1. 系統稽核側錄功能，必須以不安裝代理程式(Agent-less)方式執行。
2. 系統需支援至少側錄下列本會資訊部常用通訊協定或軟體：

   - SSH
   - Remote Desktop
   - SQL Server Management Studio (SSMS)
   - CheckPoint SmartCosloe
   - HTTPS

3. 系統須支援連續錄影(非操作鍵盤滑鼠才開始錄影)，並將側錄影片自動壓縮加密儲存於中央儲存伺服器。
4. 系統須支援線上即時監看，經授權的使用者可即時監看或中斷操作過程，並可與原始使用者同時操作受管理主機系統。
5. 系統須支援 Web 圖形化(GUI)介面直接播放側錄檔案、亦可將側錄檔案下載在本機播放。
6. 系統須支援依本會資安政策要求，暫停(Suspend)外部廠商使用者可執行的 Linux 指令(如：adduser、rm)與 Windows 動作(如：新增帳號、遠端桌面) ，並能夠即時透過電子郵件警示。
7. 系統須支援提供完整使用者操作與密碼使用等稽核紀錄功能，並可直接登入 Web 圖形化(GUI)介面進行查詢。
8. 系統須支援指令搜尋功能，可輸入關鍵字快速查詢操作過或違反政策的指令。

9. 系統須支援提供即時安全事件風險儀表板，至少包含風險評分、發生時間、事件數量、帳號名稱、主機名稱等。
10. 系統須支援報表排程寄送與手動產出，並至少包含下列類型報表：

- 特權帳號納管狀況報表
- 特權帳號密碼變更合規性報表
- 特權帳號授權使用報表
- 活動日誌報表，如:使用者存取過哪些密碼、密碼何時被修改、申請理由、授權原因等。

參、 產品建置導入、教育訓練及技術維護

1. 雙方應針對本專案各項交付工作規劃時程，及所需之相關本會資訊取得共識。
2. 廠商應同意配合本會之採購作業要點協助本會承辦人員提供必要之資訊及說明文件。
3. 廠商應充分配合本專案各項交付項目之時程進行階段確認及查驗流程。
4. 廠商應於完成各階段交付工作後，備妥各階段相關文件通知本會辦理驗收，並派員配合本會進行確認及驗收程序。
5. 各階段工作驗收後提供驗收文件，始得由本會承辦人員依本會採購作業要點辦理請款。
6. 本案進行期間廠商至少應提供每周進度報告，以確保執行品質。
7. 設備或環境建置完成，廠商應製作驗收報告，內容至少須包括系統組態設定、報表設定等，作為驗收項目之一。
8. 設備或環境準備完成，即可進行教育訓練，教育訓練至少辦理兩梯次，內容至少必須包括設定、維運操作及簡易障礙排除。
9. 廠商準備教育訓練計劃及簽到表，提供合格教師在公共電視指定之時間、地點及受訓人員數進行教育訓練課程，並視需要延長或增加梯次。
10. 教育訓練師資及其他相關衍生之所有費用由廠商自行負擔。
11. 技術維護內容：

- 廠商於合約期間需於本會上班時間周一至五上午九點至下午六點提供維護，使其能經常保持良好而可用之狀況，維護標的故障時，須負責修復至正常運作。發現維護標的有故障致不能運作時，得隨時在服務時間內

以電話通知廠商維修。

- 遇有緊急情況時，廠商接獲通知後，於上班時間四小時內到機關服務或須提供緩解方案。
- 如本會要求之服務時間係辦公時間以外者, 廠商仍應盡力提供修護服務。
- 維護範圍以本合約維護標的物在甲方正常使用下所致之損壞為限，軟體維護包括軟體正常功能之維持（但除錯程式除外）
- 不包括事項：
  - 設備損毀係因本會移機意外事件疏忽或使用錯誤。
  - 設備損毀係因受天災(水災、火災、地震、雷擊等)、非可歸責於乙方之人為故意破壞及人為之疏忽所致

12. 本案工作項目及辦理期程：

工作項目	預估天數	預計工作內容	交付文件
啟動會議	簽約後14個日曆天內	確認雙方配合事項及時程安排細節	工作計劃書
軟體授權交付	工作計劃書核定後14個日曆天內	軟體授權交付	1. 啟動會議簡報或記錄 2. 軟體原廠授權證明
軟體設定	軟體授權交付後30個日曆天內	本案採購之主要程式及管理所需之報表設定	1.設定紀錄及報告書 2.保固證明書
教育訓練	軟體設定完成後	針對本案採購進行必要維運及使用之教育訓練	教育訓練紀錄 操作說明書等
完成技術維護	軟體設定後一年	確認本案各項作業完成，本會資訊部完備程序後進行請款	技術維護紀錄

13. 本案付款方式：

- 第一期：廠商完成軟體授權交付及設定，經本會驗收通過後，撥付契約總價 70%。
- 第二期：廠商完成教育訓練及技術維護，經本會驗收通過後，撥付契約總價 30%。

肆、 組織成員基本要求

1. 廠商公司履約應遵循中華民國相關法令法規。
2. 廠商公司有三年內可受公評之業界相關本系統導入及維護之經驗與實例。
3. 廠商公司或專案負責成員持有資安或服務相關認證，如 ISO27001、ISO20000 尤佳。
4. 提供本會一位專屬服務窗口，須為廠商公司任職兩年以上之正式員工。
5. 提供本會至少一位專屬維運工程師。

伍、 責任規範

1. 廠商於專案履約期間應維持產品銷售商之資格有效。
2. 廠商於專案履約期間應遵循法律之規定及應負之保密責任。
3. 廠商因業務需求存取本會之資訊處理設施或資訊，應遵守資通安全相關規定。相關人員涉及資產完整性與機密性之資訊安全管理範圍者，廠商並應要求相關人員簽署保密切結書，併同工作計劃書提交。
4. 專案履約期間如相關人員異動，應於人員到任前提交，並於次年度專案工作計劃書更新版本進行更新。
5. 駐點或進入本會之工作人員並應依資安規範進行報到與權限申請作業。
6. 廠商提供或援用之軟體，應為經合法授權之軟體。
7. 本會得要求廠商出具原廠保證書或簽署聲明文件等，以確保廠商所提供之軟體、硬體及自行開發之程式確實符合其所宣稱之標準。
8. 本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品，服務如涉及使用雲端工具，應確保機關利用服務之所屬一切資料存取、備份、及備援之實體所在地，應為我國管轄權所及之境內。
9. 本案履約合約有效期間，廠商應提供本案相關原廠安全性修補資訊、程式或韌體等，並提供相關技術支援。
10. 本建議徵求說明書未盡事宜，如保固、轉分包、爭議處理或其他商業條款

等，以履約合約為準。

陸、 計劃書撰寫格式

1. 投標廠商應依本案招標規範內容與規定項目備妥相關資料製作「計劃書」一式三份附於「規格標」內供審核。
2. 計劃書製作格式如下：

   - 格式：主要內容為 A4 紙直式橫書，並加註目錄及頁碼，如有進度表、配置圖等相關內容時，可改用其他規格摺疊為 A4 大小。
   - 封面：財團法人公共電視文化事業基金會，【特權帳號安控稽核系統】計劃書。
   - 裝訂：左側裝訂（即書本形式）。
   - 色彩：彩色或黑白印刷不拘，以能表現內容為原則。

3. 依本規範之各項規格及相關證明文件，投標廠商應檢附製造廠型錄並於其規格型錄上以螢光色筆劃出所報規格並註明招標文件所要求規格之項次，以便審核。