特權帳號管理與支援系統規格

壹、 設備採購通則要求

一、 本案採購之各類設備均需符合標準 19 吋機架規範，適用於本會機房安裝環境。

二、 簽約日次一日起 30 個日曆天交貨，簽約日次一日起 60 個日曆天完成安裝。逾期每日罰款合約總價千分之二。

三、 本案採購之所有軟硬體皆須提供原廠新品證明、原廠連帶保固證明、軟體合法授權證明、原廠三年保固證明，所提供之軟硬體不得為已停產之產品。所提供之文件完整列出品名及數量。

四、 本案採購廠商提供之設備，需為國內製造之產品或國內廠商自行進口之國外廠商製造產品，但不可為中國大陸製造之產品，國外廠商於大陸地區製造除外，需提供原廠證明文件。

五、 須提供該設備相關完整功能所有的 License 安裝於設備上並需提供原廠證明文件，證明為合法 License 授權。

貳、 特權帳號行為管控系統設備規格

1. 作業系統平台須具備安全固化(Harden)設計，避免 Root 權限及系統後門漏洞的風險，並符合 Common Criteria Evaluation Assurance Level 2 (EAL2)認證。
2. 提供標準 19 英吋 1U 機架式之硬體設備。
3. 須提供線上儀表板化監控畫面，提供系統管理者檢視授權使用狀態、

目前登入系統人數、系統效能狀態及最新紀錄訊息等資訊。

4. 提供經授權之管理員可以即時中斷主機連線之違規操作。

5. 系統支援特權管理使用者同時連線數 1000(含)以上，本專案需提供 500(含)以上授權。

6. 系統支援特權管理容許主機管理數 500(含)以上，本專案需提供 130(含)以上授權。

7. 支援 Master/Slave 等系統備援功能，系統狀態能自動同步，並使用 Virtual IP 技術當 Master 失效時，Slave 自動轉換為 Master 保持管理連線不中斷。

8. 提供多台 Active/Active 系統備援功能，搭配本會既有的負載平衡交換器，達到異地備援機制。

9. 提供帳號自動密碼變更管理功能，帳號管控平台可提供 :

   9.1)網路設備廠牌: BROCADE / CISCO / FORTINET / Juniper / Paloalto

   9.2)系統設備廠牌: Linux / Windows / VMWARE

   9.3)資料庫廠牌: MySQL / MS-SQL

   9.4) 其他系統均提供客制化

10. Windows Server 提供安裝 Agent 與不須安裝 Agent 方式整合。

11. 提供 Agent 架構時被控主機不須提供任何帳號密碼即可自動發現／

下載所有管理帳號。

12. 提供 SSH 密鑰交換認證(Public Key Authentication)的使用方式，系統不須打密碼即自動發現／下載所有管理帳號。

13. 自動密碼變更提供歷史密碼不重複，密碼強度可依政策自行定義，包含：

13.1) 文數字符號組合

13.2) 可排除特殊字元

13.3) 密碼長度

14. 設備須提供加密 USB 介面密碼備存裝置與解密 USB 介面密碼解密裝置，系統變更特權帳號密碼時同時備份所有特權帳號密碼清單到加密 USB 介面密碼備存裝置上，並可在系統儀表板上隨時監控，當設備主機失效時，可利用加密 USB 介面密碼備存裝置與解密 USB 介面密碼解密裝置，將特權帳號密碼解密至新的外部主機上。

15. 基於使用者/管理者帳號及權限管理功能需求，使用者/管理者帳號除了本系統自建外，並且可提供與外部的帳號系統，如 AD/LDAP 等整合搭配。

16. 提供智慧型單一登入功能，能自動啟動用戶端電腦所需之管理工具，自動控制登入， 無需使用者輸入密碼。

17. 單一登入可整合 OTP 認證，達到二階段認證防護。

18. 提供自動輸入二次密碼，如 Linux / Unix 的 su 指令，Cisco 的 en 指令等。

19. 系統提供整合 OTP 認證確認自動輸入二次密碼。

20. 提供多因數認證(Multi-factor Authentication)功能，內建並提供以下機制：Mobile OTP

21. Mobile OTP 須與特權管理系統為同一廠牌並支援以下平台：Android、Apple IOS，本專案需提供 10 套含(以上)授權。

22. 提供依角色定義設定帳號權限，角色定義可自行新增、修改及刪除。

23. 系統記錄提供.xls 格式下載功能，可連線下載儲存。

24. 提供 Syslog 系統日誌功能，可將 Log 紀錄指定儲存於外部的 Syslog Server 或 SIEM 系統。

25. 帳號申請提供電子化申請授權流程，同一主機可提供多人同時申請特權帳號登入，並提供以下申請資訊欄位審核：

    25.1) 帳號權限

    25.2) 姓名

    25.3) 公司名稱

    25.4) 部門

    25.5) 職位

    25.6) 公司電話

25.7） 行動電話

25.8） E-Mail

25.9） 其他補充

25.10） 所需存取日期範圍、時間範圍、每週(天)等，並可設定申請使用時間上限值

26. 提供 Excel 匯出及匯入系統設定，如 Policy（政策）建立、帳號資訊建立與受管理主機清單建立等。

27. 電子化申請授權流程提供多階層核可，審核人員提供修改申請人帳號權限、所需存取時間等要求，並需階層全部核可後，申請人方可進行連線存取。

28. 可提供多階段單一登入(Multi-Step Single Sign ON)功能，提供整合 Mobile OTP 多階段認證存取。

29. 提供Share Account 管理,能分辨被控主機多人連線並共用帳號時，區分並管理不同申請帳號人之權限

30. 可檢視「受管理設備」之歷史連線操作歷程記錄，並可提供以下單一或多個條件搜尋：

30.1） 主機名稱

30.2） 主機 IP

30.3） 使用者 IP

30.4） 登入帳號

30.5） 指令

30.6） 日期

30.7） 狀態

31. 需提供以黑名單(Blacklist)或白名單(Whitelist)方式設定指令過濾功能，並支援以下控制協定：

31.1） SSH

31.2） TELNET

31.3） FTP

31.4） SFTP

32. 符合違規指令過濾條件時，提供以下動作：

32.1） 阻擋

32.2） OTP 要求

32.3） 再次確認

32.4） 發送 EMAIL 通知系統管理者。

33. 提供即時側錄功能，可於管理介面上直接觀看即時連線及控制中斷連線。

34. 提供管理者阻斷線上之遠端桌面 RDP、SSH、Telnet 等連線。

35. 側錄內容可直接於 Web 管理介面上直接觀看，可下載至本地端。

36. 側錄內容可提供以下類別：

36.1） SSH

36.2） TELNET

36.3） FTP

36.4） SFTP

36.5） RDP

36.6） HTTP / HTTPS

36.7） Application / Program

37. 提供連線側錄時記錄鍵盤輸入。

38. 連線側錄搜尋方式，可依照特定字串或輸入指令尋找。

39. 具備完整使用者操作記錄(Log)功能，包含：

39.1) 使用者存取過那些帳號密碼。

39.2) 密碼何時被修改。

39.3) 申請理由、授權原因。

40. 提供匯出報表為 PDF、XLS、DOCX、PPTX 格式。

41. 提供資料庫應用程式之密碼變更及提取。

42. 提供完整 API 以供使用者整合現有系統

參、 教育訓練

系統安裝完成後，即可進行全單位教育訓練，並於付款前完成。立約商準備教育訓練計畫，並提供原廠或原廠教育訓練合格證教師在指定之時間及地點進行教育訓練課程，課程至少提供 16 小時(含)以上之專業訓練，並得視使用單位需要延長，惟課程總天數以 30 天為上限，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，教育訓練課程內容，必須包括系統操作與維護。不限上課時間、梯次。

配合上述之需求，立約商須提供完整之使用者及管理者教育訓練計畫。

驗收前，立約商應製作全系統中文操作手冊，作為驗收項目之一。