工研院綠能所採購規範書

購案名稱：自動需量反應管理平台資安優化程式設計

一、工作項目：

1. 依 OWASP TOP 10:2025 之以下項目進行平台功能資安優化
2. Broken Access Control 存取控制漏洞函式設計
3. Cryptographic Failures 加密機制強化函式設計
4. Authentication Failures 身份驗證管理函式設計
5. Logging & Alerting Failures 日誌記錄與告警管理函式設計
6. Mishandling of Exceptional Conditions 特殊情況處理函式設計
7. 須提供 6 小時內除錯及至台電大樓現場本地端修正服務
8. 因應資安及時程需求，廠商須具備台電正式系統開發經驗(須提供相關實績證明)
9. 提供 C 語言程式碼

二、軟體 / 規格 / 要求

- Broken Access Control 存取控制漏洞
  - ✓ reCAPTCHA 機器人攻擊防堵功能
  - ✓ 遠端連線設定與連線存取紀錄，限制存取連線之行為並留存具時間戳記之紀錄
  - ✓ 遠端存取相關來源與連線授權紀錄，防止非授權來源 IP 進行連線
  - ✓ 遠端存取相關設定與授權紀錄，防止非授權帳戶進行遠端存取
  - ✓ 帳戶存取權限管理功能
- Cryptographic Failures 加密機制
  - ✓ 用戶個資資料庫儲存加密機制(PQC 加密+AES 加密混合型)
  - ✓ 資料加密後雜湊演算法(複雜度高於 SHA256)
  - ✓ HASH 雜湊演算法加鹽機制
  - ✓ 資料編解碼演算法(BASE64)
  - ✓ 憑證簽章函式功能
  - ✓ 金鑰管理介面函式
- Authentication Failures 身份驗證管理
  - ✓ 管理帳戶鎖定設定，帳戶密碼錯誤鎖定次數功能
  - ✓ 管理帳戶鎖定設定，帳戶密碼錯誤鎖定時間功能

- ✓ 管理帳戶密碼設定，密碼複雜度(英數字、大小寫、特殊符號)原則功能
- ✓ 管理帳戶密碼設定，密碼長度原則
- ✓ 管理帳戶密碼設定，密碼最長有效期限原則

■ Logging & Alerting Failures 日誌記錄與告警管理

- ✓ 帳戶異動稽核紀錄設定結果、留存內容及管理
- ✓ 帳戶登入/登出稽核紀錄設定結果、留存內容及管理
- ✓ 資料庫結構異動稽核紀錄設定結果、留存內容及管理，包含:資料庫結構新增/刪除/修改之稽核功能
- ✓ 資料庫稽核紀錄之存取控制與保存紀錄
- ✓ 稽核紀錄分析規則設定、分析紀錄或報告，針對異常事件處理分類

■ Mishandling of Exceptional Conditions 特殊情況處理

- ✓ 資料庫備份加密
- ✓ 資料庫異地備份排程管理
- ✓ 通訊連線異常告警記錄與通報處理(SMS、Email)

三、結案驗收：

結案驗收時按上述規格辦理，交付成果之內容經請購單位確認各項功能，始能完成驗收。