# 附件

1. 安全功能介面表

| **功能介面**  **TSFI** | **目的**  **Purpose** | **可執行的安全功能需求**  **SFR** | **操作方式**  **Method of Use** | **參數**  **Parameter** | **執行動作**  **Actions** | **錯誤訊息**  **Error Message** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | *基礎型填寫說明：*  *需提供此介面與安全功能相關之參數(內容應與指引文件相符)*  *進階型填寫說明：*  *需提供此介面的所有參數(內容應與指引文件相符)* | *基礎型填寫說明：*  *需提供此介面與SFR的預期動作(內容應與設計文件對應)*  *進階型填寫說明：*  *需提供此介面的所有預期動作，包括非執行SFR的動作(內容應與設計文件對應)* | *基礎型填寫說明：*  *需提供此介面與安全功能相關的錯誤訊息(內容應與指引文件相符)*  *進階型填寫說明：*  *需提供此介面的所有可能的錯誤訊息(內容應與指引文件相符)* |

1. 子系統描述與分類表

| **名稱** | **子系統與SFR之對應** | | | | **行為描述** |
| --- | --- | --- | --- | --- | --- |
| **執行** | **支援** | | **非涉** |
|  |  |  | |  | *填寫說明：*  *需提供子系統行為資料如次：*  *1.TSFI(須與6.2.2.1相符)*  *2.描述與其他子系統之互動*  *3.如為非涉，需敍明與安全功能無關之理由* |
| 範例：  Subsystem XXX |  | 14.可選取之稽核審查 | |  | 1.TSFI: TSFI\_WebGUI, TSFI\_CLI  2.與其他子系統之互動：  (1)向記憶體管理子系統要求一個記憶體區塊  (2)記憶體管理子系統回應所分配之記憶體起始位址 |
|  |  |  | |  |  |
|  |  | |  |  |  |

1. 安全架構描述表

| 項目 | **描述** | | |
| --- | --- | --- | --- |
| 1.安全領域  Security Domain | **安全功能** | **領域說明** | |
| 安全稽核 |  | |
| 密碼支援 |  | |
| 身分認驗證 |  | |
| 資料安全管理 |  | |
| 功能自我保護 |  | |
| 用戶資料保護 |  | |
| 填寫說明 | | 在安全功能操作環境及內部執行限制下，如何區隔所需保護的資料。 | |
| 範例：安全稽核 | | 安全稽核透過TSFI\_GUI來執行，該TSFI同一時間只能執行單一功能之資料處理請求。 | |
| 2.初始程序  Secure Initialization | **相關元件** | **程序說明** | |
|  |  | |
|  |  | |
| 填寫說明 | 操作設備的相關元件/環境 | 提供安全啟動該設備之相關元件起始步驟及安裝程序。 | |
| 範例： | 網路連接 | 1. 從端口標記為 0/ 0（ethernet0 / 0接口）連接一個 RJ- 45電纜到交換機或路由器Trust安全區。  2. 從端口標記為 0/ 1（ethernet0 / 1接口）連接一個 RJ- 45電纜到交換機或路由器中的DMZ安全區。 | |
| 3.自我保護  Self-Protection | **安全功能** | **與外部設備之介面** | **保護機制** |
| 安全稽核 |  |  |
| 身分認驗證 |  |  |
| 密碼支援 |  |  |
| 資料安全管理 |  |  |
| 功能自我保護 |  |  |
| 用戶資料保護 |  |  |
| 填寫說明 | | 安全功能及其介面與外部設備之資料交換動作 | 需檢視介面是否提供實體上或邏輯上的保護機制，諸如：  1.通行碼保護  2.資料傳輸機制  3.特殊執行方式  4.特殊設備需求 |
| 範例：身分認驗證 | | 以網路連結外部弱點資料庫、以TSFI\_WEBGUI介面進行身分認驗證 | 1.應輸入通行碼才能進入介面  2.資料傳輸機制：SSL  3.特殊執行方式：指紋辨識  4.特殊設備需求：指紋辨識器 |
| 4.防止繞道攻擊  Bypass | **安全功能** | **防護機制** | |
| 安全稽核 |  | |
| 身分認驗證 |  | |
| 密碼支援 |  | |
| 資料安全管理 |  | |
| 功能自我保護 |  | |
| 用戶資料保護 |  | |
| 填寫說明 | | 1.列舉繞道攻擊之手法  2.說明防範作法，諸如：進入安全功能的介面如何被保護、執行階段的資料處理如何保護、是否存有其他對外通道及相關防範非法進入之機制等。 | |
| 範例：身分證驗證 | | 以實體封鎖方式，防止利用維護介面繞道身分認證程序。 | |