

附表 能源及水資源領域工業控制系統防護基準

| 控制措施 | | 系統防護需求分級 | | |
|--------|-----------|--|---|--|
| 構面 | 措施內容 | 高 | 中 | 普 |
| 存取控制 | 帳號管理 | 一、逾越預期閒置時間或可使用期限時，系統應自動將使用者登出。但操作過程中有替代之監管措施者，不在此限。 二、應依機關規定之情況及條件使用系統。 三、監控帳號異常使用情況並回報管理者。 四、等級「中」之所有控制措施。 | 一、已逾期之臨時或緊急帳號應予以刪除或禁用。 二、應禁用閒置帳號。 三、定期審核帳號之建立、修改、啟用、禁用及刪除作業。 四、等級「普」之所有控制措施。 | 建立帳號管理機制，包含帳號之申請、開通、停用及刪除程序。 |
| | 最小權限 | 採最小權限原則，僅允許使用者（或代表使用者行為之程序）依任務及業務功能，完成指派任務所需之授權存取。 | | 無要求。 |
| | 遠端存取 | 一、應監控遠端連線。 二、應採用加密機制。 三、遠端存取來源應為預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。 | | 對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。 |
| | 網路架構配置與隔離 | 一、建立工控網路邊界監控機制，定期檢視並回報異常狀況予管理者。 二、等級「中」之所有控制措施。 | 一、區隔工控網路邊界，採取網路存取管控機制。 二、等級「普」之所有控制措施。 | 建立安全防護網路架構，管控網際網路連線存取。 |
| 稽核與歸責性 | 稽核事件 | 一、應定期審查稽核事件。 二、等級「普」之所有控制措施。 | | 一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、確保有稽核特定事件之功 |

| 控制措施 | | 系統防護需求分級 | | |
|--------|-------------|---|---|-----------------------|
| 構面 | 措施內容 | 高 | 中 | 普 |
| | | | | 能，並決定應稽核之特定事件。 |
| | 稽核紀錄內容 | 稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用日誌紀錄機制。 | | |
| | 稽核儲存容量 | 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。 | | |
| | 稽核處理失效之回應 | 一、規定需即時通報之稽核失效事件發生時，系統應於規定時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。 | 稽核處理失效時，應採取適當之行動。 | |
| | 時戳及校時 | 一、系統內部時鐘應具備定期同步機制。 二、等級「普」之所有控制措施。 | 使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。 | |
| | 稽核資訊之防護 | 一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。 | 一、應防護稽核資訊之完整性。 二、等級「普」之所有控制措施。 | 對稽核紀錄之存取管理，僅限於有權之使用者。 |
| 營運持續計畫 | 電源供應備援 | 一、考量廠(場)站營運之需求，規劃至少包含核心業務相關重要系統、設備在內之電源供應備援機制。 二、定期進行電源供應備援機制測試。 | 無要求。 | |
| | 通訊線路備援 | 一、考量廠(場)站營運之需求，規劃至少包含核心業務相關重要系統、設備在內之通訊線路備援機制。 二、定期進行通訊線路備援機制測試。 | 無要求。 | |
| 識別與鑑別 | 內部使用者之識別與鑑別 | 系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能，禁止使用共用帳號；但操作過程中有替代之監管措施者，不在此限。 | | |
| | 身分鑑別 | 一、身分驗證機制應防範自動化程式之 | 一、使用預設密碼 | |

| 控制措施 | | 系統防護需求分級 | | |
|---------|------------|--|------|--|
| 構面 | 措施內容 | 高 | 中 | 普 |
| | 管理 | 登入或密碼更換嘗試。 二、等級「普」之所有控制措施。 | | 登入時，應於登入後要求立即變更。 二、身分鑑別相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，訂定帳號登入進行身分鑑別失敗次數，以及不允許該帳號繼續嘗試登入之時間。但操作過程中有替代之監管措施者，不在此限。 四、基於密碼之鑑別強制最低密碼複雜度；強制新密碼最少變更字元數；強制密碼最短及最長之期效限制。 五、訂定更換密碼時，異於使用過密碼相同之次數。 |
| | 鑑別資訊回饋 | 應遮蔽鑑別過程中之資訊。 | | |
| 系統與通訊防護 | 資料儲存之安全 | 一、靜置資訊應予以防護。 二、機密資訊應加密儲存。 | 無要求。 | 無要求。 |
| | 傳輸之機密性與完整性 | 於資訊傳遞過程中採用加密機制。但傳輸過程中有替代之保護措施者，不在此限。 | 無要求。 | 無要求。 |
| 系統與服 | 操作、營運及運作限 | 一、建立系統、設備操作與營運相關管理文件。 二、建立系統、設備運作限制之文件紀錄。 | | |

| 控制措施 | | 系統防護需求分級 | | |
|----------|-------------|--|---|-----------------------|
| 構面 | 措施內容 | 高 | 中 | 普 |
| 業務獲得 | 制文件 | 三、指派負責人員管理上述文件內容品質與完整，並妥善留存。 | | |
| | 安全措施文件 | 一、建立系統、設備安全防護措施之文件紀錄。 二、指派負責人員確保上述文件紀錄和實際狀態之一致性，並妥善留存。 | | 無要求。 |
| 實體與環境防護 | 實體存取授權 | 建立設施實體存取授權之人員清單，並定期或遇人員異動時進行更新。 | | |
| | 實體隔離與設備進出管控 | 一、建立設施所在區域之實體隔離機制。 二、建立設備進出/維護申請之流程，並留存紀錄。 | | |
| | 實體監視與偵測 | 一、於重要位置處架設監視設備，並留存監視紀錄。 二、建立實體偵測機制，包含即時告警與記錄。 三、建立外部人員陪同與記錄機制。 | | |
| 系統與資訊完整性 | 日常操作與查檢紀錄 | 一、建立日常操作與查檢機制，並形成作業參照文件。 二、留存日常操作與查檢紀錄。 | | |
| | 系統日誌資訊留存 | 建立日誌資訊留存機制，包含日誌資訊備份、保存。 | | |
| | 系統監測工具/技術導入 | 導入系統營運監測工具/技術。 | | 無要求。 |
| | 系統異常告警與通報 | 一、建立異常告警與通報機制。 二、留存異常告警與通報紀錄。 | | |
| | 系統、設備漏洞評估 | 一、進行系統、設備之漏洞影響性評估，並留存相關紀錄，作為後續修補/更新規劃之依據。 二、等級「普」之所有控制措施。 | | 蒐集、掌握既有/新進系統、設備之漏洞資訊。 |
| | 漏洞修補 | 一、評估已掌握之漏洞資訊，進行修補時程之規劃。 二、修補作業完成後，進行漏洞修補驗證作業，留存相關紀錄。 | | |
| | 故障預防 | 依據設備之保固或生命週期，建立故障預防機制。 | | 無要求。 |
| 組態管理 | 系統、設備變更管控 | 一、建立變更作業規劃及管控流程。 二、相關變更作業皆有管理階層核准確認。 三、指派負責人員執行變更作業，並留存相關紀錄。 | | |
| | 變更作業測試 | 一、建立系統、設備變更作業之測試與驗證流程。 二、留存變更作業測試相關紀錄。 | | 無要求。 |

| 控制措施 | | 系統防護需求分級 | | |
|------|-----------|--|---|--|
| 構面 | 措施內容 | 高 | 中 | 普 |
| | 變更作業紀錄 | 建立系統、設備變更作業之紀錄，留存變更前後之相關資訊。 | | |
| 組織管理 | 委外資安規範與要求 | 規劃與要求委外作業必要資安辦理事項及管控措施，並列入履約項目當中。 | | |
| | 服務安全管理 | 一、訂定委外廠商遠端維護、到點服務及人員駐點等服務項目之管控程序。 二、等級「普」之所有控制措施。 | | 一、依委外業務之需求，要求委外廠商/人員簽署保密合約。 二、留存相關委外服務紀錄。 |