

經濟部能源及水資源領域工業控制系統防護基準第一點附表修正案對照表

修正規定					現行規定					說明
附表 能源及水資源領域工業控制系統防護基準					附表 能源及水資源領域工業控制系統防護基準					配合一百一十年八月二十三日修正發布之資通安全責任等級分級辦法第十一條附表十資通系統防護基準(以下簡稱附表十)之修正，爰參酌該附表之修正原則，修正本附表，說明如下： 一、存取控制構面： （一）帳號管理之高級控制措施：增訂第一點明定應定義各系統之閒置時間或可使用期限與使用情況及條件。現行控制措施內容第一點及第二點酌作文字修正，並與現行第三點及第四點配合前開增訂規定遞移為第二點至第五點。 （二）帳號管理之中級及普級控制措施：酌作文字
控制措施		系統防護需求分級			控制措施		系統防護需求分級			
構面	措施內容	高	中	普	構面	措施內容	高	中	普	
存取控制	帳號管理	一、應定義各系統之閒置時間或可使用期限與使用情況及條件。 二、逾越許可之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。 三、應依規定之情況及條件使用系統。 四、監控帳號異常使用情況並回報管理者。 五、等級「中」之所有控制	一、已逾期之臨時或緊急帳號予以刪除或禁用。 二、應禁用閒置帳號。 三、定期審核帳號之申請、建立、修改、啟用、停用及刪除作業。 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、建立、修改、啟用、停用及刪除程序。	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，使用資通系統。 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	採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存				無要求。			

	措施。		
	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、遠端存取來源應為預先定義及管理之存取控制點。 二、等級「普」之所有控制措施。	一、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。 二、應監控遠端存取工控網路或工控系統之連線。 三、應採用加密機制。
	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。
	事件日誌與可	一、應定期審查保留之日誌。 二、等級「普」之所有控制措施。	一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。

	限	取。	
	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。
	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。	

稽核與可歸責性	稽核	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。
---------	----	---------------------------

修正。

(三)遠端存取之普級控制措施：為強化監控範圍之類型(工控網路或工控系統)，將現行高級及中級控制措施第一點及第二點酌作修正移至普級控制措施第二點及第三點。現行高級及中級控制措施第三點及第四點遞移為第一點及第二點。

二、稽核與可歸責性構面：

(一)參照附表十修正原則，將相關規定之「稽核」屬名詞者修正為「日誌」，屬動詞者修正為「記錄」，爰將構面「稽核與可歸責性」修正為「事件日誌與可歸責性」，各措施內容名稱分別修正為「記錄事件」、「日誌

歸責性			二、確保有記錄特定事件之功能，並決定應記錄之特定事件。					紀錄內容」、「事件日誌與可歸責性」、「日誌儲存容量」、「日誌處理失效之回應」及「日誌資訊之防護」。 (二) 記錄事件之高級及中級控制措施：第一點酌作文字修正。 (三) 記錄事件之普級控制措施：修正第一點及第二點，以明確日誌記錄時間週期、留存時間及相關用詞，並明定保留日誌至少六個月。 (四) 為使用詞一致，修正日誌紀錄內容之高級、中級及普級控制措施、日誌儲存容量之高級、中級及普級控制措施、日誌處理失效之回應之高級、中級及普級控制措施、時戳及校時之普級控制措施及日誌資訊
	日誌紀錄內容	日誌應包含事件類型、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。	
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。			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)。	
	日誌處理失效之回應	一、規定需即時通報之日誌處理失效事件發生時，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。	日誌處理失效時，應採取適當之行動。		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。
	時戳及校	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日誌所需時戳，並可以對應到世界協調時間		營運持	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。	無要求。

	時			(UTC)或格林威治標準時間(GMT)。	續計畫		二、定期進行電源供應備援機制測試。		之防護之中級及普級控制措施之文字，將「稽核紀錄」修正為「日誌」。
	日誌資訊之防護	一、定期備份日誌至原系統外之其他實體系統。 二、等級「中」之所有控制措施。	一、應防護日誌之完整性。 二、等級「普」之所有控制措施。	對日誌之存取管理，僅限於有權之使用者。		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。	
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演練。		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。		(五)日誌資訊之防護之高級控制措施：修正第一點，明定日誌紀錄應備份至不同實體系統。 三、營運持續計畫構面：
	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演練。		無要求。		身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、等級「普」之所有控制措施。	一、使用預設密碼登入時，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	
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。							
	身分鑑別管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、等級「普」之所有控制措施。		一、使用預設密碼登入時，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					

系統與通訊防護			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、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之期效限制。 五、訂定密碼變更時，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。			
	資料儲存安全	<u>重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。</u>	無要求。	無要求。	
傳輸	於資訊傳遞過程中採用加密機	無要求。	無要求。		

系統與通訊防護			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。		
	資料儲存安全	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實體保護措施者，不在此限。	無要求。	無要求。	
系統操作、營運	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。			

密碼最少變更字元數功能，而國內能源及水資源工業控制系統採用 Windows 作業系統之比例較高)，爰修正第四點及刪除「強制新密碼最少變更字元數」，並酌修第五點。
五、系統與通訊防護構面： 資料儲存之安全之高級控制措施：考量儲存作業多元性，將現行第一點及第二點規定合併修正，並明定需保護資訊。
六、系統與資訊完整性構面： 為使規範文義更為明確，將「系統日誌資訊留存」修正為「操作與維護日誌資訊留存」，並配合修正高級、中級及普級之控制措施內容文字。
七、其餘構面及控制措施內容未修

	之機密性與完整性	制。但傳輸過程中有替代之實體保護措施者，不在此限。			與服務獲得	運及運作限制文件	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。	正。
系統與服務獲得	操作、營運及運作限制文件	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。 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。	
	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、 建立入侵偵測機制，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	日常	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。	

系統與資訊完整性	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、 建立入侵偵測機制，包含即時告警與記錄。 三、 建立外部人員陪同與記錄機制。	
	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。	
	操作與維護日誌資訊留存	建立操作與維護日誌資訊留存機制，包含相關日誌資訊備份、保存。	
	系統監控工具/技術導入	導入系統營運監控工具/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。
與資訊完整性	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。	
	系統監控工具/技術導入	導入系統營運監控工具/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	報		
		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。
		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。
		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。	

			合約。 二、留存相關委 外服務紀錄。		
--	--	--	--------------------------	--	--