「000系統」資通系統防護基準表(普)

系統防護需求分級控制措施		措施內容	執行作法	是否已完成控制措施	現況說明	備註
構面	措施內容					
存取控制	帳號管理	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。		否		
	遠端存取	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。				
		使用者之權限檢查作業應於伺服器端完成。				
		應監控遠端存取機關內部網段或資通系統後台之連線。				
		應採用加密機制。				
	記錄事件	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。				
		確保資通系統有記錄特定事件(如更改密碼、登錄失敗、資通系統存取失敗)之功能，並決定應記錄之特定資通系統事件。				
		應記錄資通系統管理者帳號所執行之各項功能。				

事件日誌與可歸責性	日誌紀錄內容	資通系統產生之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，並採用單一日誌紀錄機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。				
	日誌儲存容量	依據日誌紀錄儲存需求，配置稽核紀錄所需之儲存容量。				
	日誌處理失效之回應	資通系統應於日誌處理失效(如儲存容量不足)時，應採取適當之行動(如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等)。				
	時戳及校時	資通系統應使用系統內部時鐘產生日誌紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。				
	日誌資訊之保護	對日誌紀錄之存取管理，僅限於有權限之使用者。				
營運持續計畫	系統備份	訂定系統可容忍資料損失之時間要求。				
		執行系統源碼與資料備份。				
	內部使用者之識別與鑑別	資訊系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)功能，禁止使用共用帳號。				
		使用預設密碼登入系統時，應於登入後要求立即變更。				
		身分驗證相關資訊不以明文傳輸。				

識別與鑑別	身分驗證管理	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。				
		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 之效期限制。(非內部使用者，可依機關自行規範辦理。)				
		密碼變更時，至少不可以與前三次使用過之密碼相同。(非內部使用者，可依機關自行規範辦理。)				
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。				
	非內部使用者之識別與鑑別	資通系統應識別及鑑非機關使用者(或代表機關使用者行為之程序)。				
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。				
	系統發展生命週期開發階段	應針對安全需求實作必要控制措施。				
		應注意避免軟體常見漏洞及實作必要控制措施。				
		發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。				
	系統發展生命週期測試階段	執行「弱點掃描」安全檢測。				
	系統發展生命週期部署與維運階段	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。				
		資通系統不使用預設密碼。				

	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。				
	系統文件	應儲存與管理系統發展生命週期之相關文件。				
系統與資訊完整性	漏洞修復	系統之漏洞修復應測試有效性及潛在影響，並定期更新。				
	資通系統監控	發現資通系統有被入侵跡象時，應通報機關特定人員。				