附表 通訊及傳播領域控制系統資通安全防護基準

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、應依規定之情況及條件，使用系統。 二、監控系統帳號，如發現帳號違常使用時，回報管理者。 三、等級「中」之所有控制措施。	一、應定義各系統之閒置時間或可使用期限與系統之使用情況及條件。 二、逾越所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。 三、等級「普」之所有控制措施。	一、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。 二、已逾期之臨時或緊急帳號應刪除或禁用。 三、系統閒置帳號應禁用。 四、定期審核系統帳號之申請、建立、修改、啟用、停用及刪除。
	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。		
	遠端存取	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、應監控遠端存取內部網段或控制系統後臺之連線。 三、應採用加密機制。 四、遠端存取之來源應為已預先定義及管理之存取控制點。 五、遠端存取應採用多因子鑑別機制。		
	本地端存取	內外部設備或可攜式媒體於本地端連接至系統前，均應先取得授權，並應執行掃毒或其他必要之安全檢測。		
事件日誌及可歸責性	記錄事件	一、應定期審查所保留系統產生之日誌。 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。 二、確保系統有記錄特定事件之功能，並決定應記錄之特定系統事件。 三、應記錄系統管理者帳號所執行之功能。但傳播領域系統不具備此

				記錄功能時，不在此限。
	日誌紀錄內容	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，並應依法規及資通安全政策要求納入其他相關資訊。		
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。		
	日誌處理失效之回應	一、規定需要即時通報之日誌處理失效事件發生時，系統應於規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	系統於日誌處理失效時，應採取適當之行動。	
	時戳及校時	一、系統應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（UTC）或格林威治標準時間（GMT）。 二、系統內部時鐘應定期與基準時間源進行同步。		
	日誌資訊之保護	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、應運用適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對日誌之存取管理，僅限於有權限之使用者。
營運持續計畫	資料備份	一、應將備份還原，作為營運持續計畫演練之一部分。 二、應建立資料異地備份機制。 三、應將重大災害或其他須進行資料銷毀或轉移之極端狀況，作為營運持續計畫演練之一部分。 四、等級「中」之所有控制措施。	一、應定期測試備份資料，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定資料可容忍損失之時間要求。 二、執行資料備份。
	系統備援	一、應將備援啟動作為營運持續計畫演練之一部分，並將電力、機房、人員及備援設備可用性納入	一、應定期測試原服務中斷時，於最大可容忍中斷時間內，由備援設備或其他方式取代並提供服務。	訂定系統從中斷後至重新恢復服務之最大可容忍中斷時間要求。

		考量。 二、應將重大災害或其他須進行系統銷毀或轉移之極端狀況，作為營運持續計畫演練之一部分。 三、等級「中」之所有控制措施。	二、等級「普」之所有控制措施。	
	安全模式	系統偵測到異常或進入不可信任狀態時，應進入限制性操作模式、保護性停機或僅保留基本運作能力。但系統不具備限制性操作模式、保護性停機或僅保留基本運作能力功能者，不在此限。	無要求。	無要求。
識別及鑑別	使用者之識別及鑑別	一、工程邏輯修改或保護參數變更等高風險操作，應採取多因子鑑別或第二階段確認機制。 二、應禁止匿名裝置連線，並實施設備白名單機制。 三、等級「普」之所有控制措施。		系統應識別及鑑別使用者，並禁止使用者使用共用帳號。但有其他輔助管控機制（如門禁管控、錄影監視、工單系統或排班制度等），不在此限。
	身分驗證管理	一、使用預設密碼初次登入系統時，應於登入後立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，應訂定帳號登入進行身分驗證失敗達五次後，不允許該帳號繼續嘗試登入之時間限制。但用於保護性停機之帳號，或具替代身分驗證失敗機制之控制措施者，不在此限。 四、使用密碼進行驗證時，應強制最低密碼複雜度，並依密碼效期規定變更密碼。 五、密碼變更時，至少不可以與前三次使用過之密碼相同。但具替代密碼重複使用限制機制之控制措施者，不在此限。		
	鑑別資訊保護	一、系統如以密碼進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存。但傳播領域系統無法以雜湊或其他適當方式處理後儲存密碼者，不在此限。 二、等級「普」之所有控制措施。		系統應遮蔽鑑別過程中之資訊。
系	系統發展	針對系統安全需求（含機密性、可用性、完整性）進行確認。		

統及服務獲得	生命週期需求階段			
	系統發展生命週期設計階段	一、根據系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		無要求。
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、系統應具備發生嚴重錯誤時之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、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	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署及維運階段	一、於系統發展生命週期之維運階段，應執行版本控制及變更管理。 二、等級「普」之所有控制措施。		一、於部署環境中應針對相關資通安全威脅，進行更新及修補。 二、識別並關閉不必要服務及埠口。 三、系統不使用預設密碼。 四、執行系統源碼備份。
	系統發展生命週期委外階段	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。		
	獲得程序	識別系統使用之第三方軟體、服務、函式庫或其他元件。		
	操作及營運文件	一、應建立系統操作及營運相關管理文件。 二、應留存至少六個月之操作及維護紀錄，並定期審查。		
	安全措施文件	一、應建立系統安全防護措施管理文件，並留存至少六個月之相關紀錄。 二、應定期確認及更新上述文件紀錄之完整性。		
系統及通	傳輸之機密性及完整性	一、系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變	無要求。	無要求。

訊保護		更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、系統應使用公開、國際機構驗證且未遭破解之演算法。但傳播領域系統不具備演算法功能時，不在此限。		
	資料儲存之安全	系統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。	無要求。	無要求。
系統及資訊完整性	漏洞修復	一、定期確認系統相關漏洞修復之狀態及替代控制措施之實施情形。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，並定期更新。系統漏洞如無法修補，須實施替代控制措施（如加強網路區隔、限制可存取來源、強化監測及縮減可執行功能等）。
	系統監控	一、應監控系統，以偵測攻擊及未授權之連線。 二、應建立異常告警及通報機制，並留存至少六個月之相關紀錄。 三、等級「普」之所有控制措施。		發現系統有被入侵跡象時，應通報特定人員。
	軟體及資訊完整性	發現違反資訊完整性時，系統應實施指定之安全保護措施。		
實體環境防護	實體進出管制	一、機房及系統控制室除設置、維護、監督或其他營運必要之目的外，禁止任何人進入。 二、應建立紀錄機制，紀錄內容應包含進出人員姓名及其所屬機關（構）、進出時間、進入目的及進出物品。		
	實體隔離	機房及系統控制室應以實體隔離方式設置，並具備獨立出入口。		
	實體環境監測	一、機房及系統控制室之出入口，應設置全天候入侵告警與錄影監控之門禁安全管理系統，入侵告警與錄影監控紀錄至少應保存六個月。 二、機房及系統控制室應監測電力資源供應情形。		
組態管理	變更流程及紀錄	一、應建立變更流程，包含需求提出、風險評估、測試驗證、核准、實施及回復方案等完整步驟。 二、應留存變更紀錄，包含變更內容、時間、執行人員、原因及核准人，以確保所有異動均有跡可循。		

		三、應定期審查變更紀錄。		
網路架構	邊界防護配置及隔離	一、應建立控制系統網路邊界監控機制並定期監控，有異常狀況應向管理者回報。 二、控制系統網路應與一般資通系統網路環境予以區隔（如設立防火牆等）。 三、等級「中」之所有控制措施。	一、應建立安全防護網路架構，並區隔控制系統網路邊界，採取網路存取管控機制。 二、等級「普」之所有控制措施。	應執行最小通道原則，僅開放系統運作所必須之連線路徑。
組織管理	供應商管理	一、應將相關法規及資通安全政策納入委外契約。 二、應要求委外廠商及人員簽署保密文件。		
	職務區隔	應落實權責分工，避免申請人與核准人為同一人之情形。		
	環境管理	應建立環境管理機制，包含消防、保全、電力及相關設施管理。		
	維運管理	應建立維運管理機制，包含員工維運或協力廠商維護機房設備等管理。		
	紀錄管理	應建立紀錄管理機制，包含門禁管理、環境管理及維運管理等紀錄。		