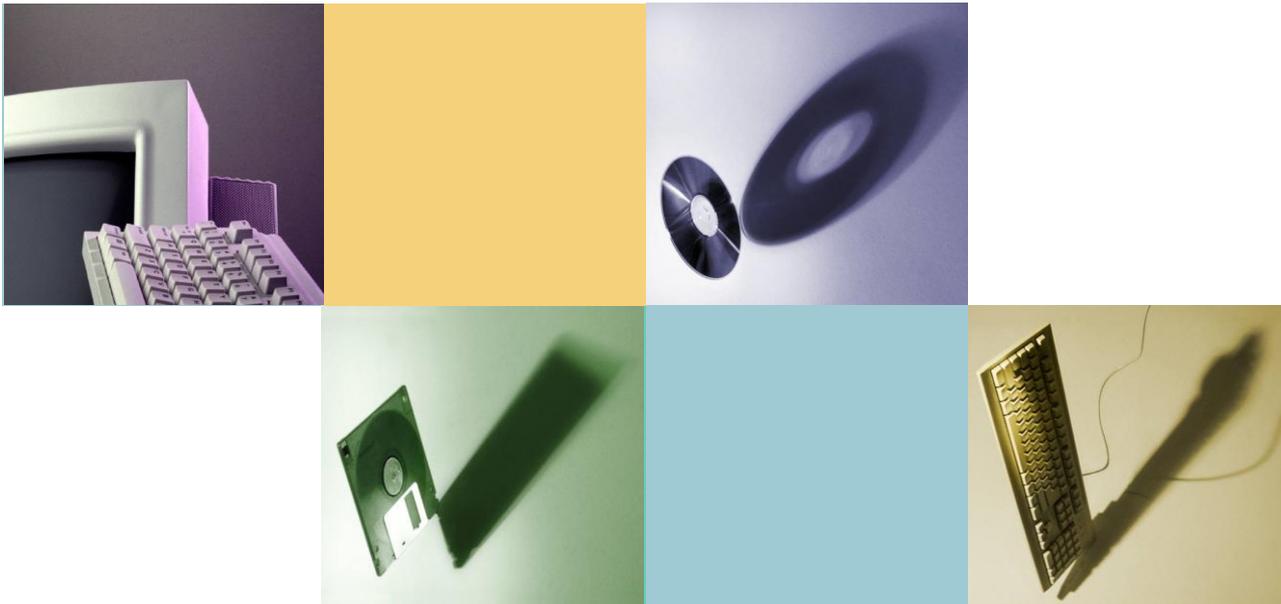


資通安全責任等級暨 資通系統防護基準介紹



Wednesday, Aug 19 2020

資通安全責任等級

- 是C還是D？「資通安全責任等級分級辦法」規定
 - 第六條 各機關維運自行或委外開發之資通系統者，其資通安全責任等級為C級。
 - 第七條 各機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為D級。
- 資通安全責任等級C與D的差別
 - 管理面：C級需進行資通系統分級及防護基準、導入ISMS、配置1位資安專責人員、資通安全內部稽核及業務持續運作演練。D級則完全不用。
 - 技術面：C級需進行安全性檢測、資通安全健診及資通安全防護。D級僅需進行資通安全防護。
 - 認知與訓練：C級每年至少一名人員接受12小時以上之資通安全專業課程訓練或資通安全職能訓練，資通安全專責人員應持有1張以上資通安全專業證照及職能評量證書，並持續維持證照(書)之有效性。C級其餘一般使用者及主管和D級機關人員每年接受3小時以上之一般資通安全教育訓練。



C級之公務機關應辦事項(管理面)

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。



C級之公務機關應辦事項(技術面)

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	



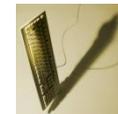
C級之公務機關應辦事項(認知與訓練)

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少一名人員接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	資通安全專職人員總計應持有一張以上。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有一張以上，並持續維持證書之有效性。

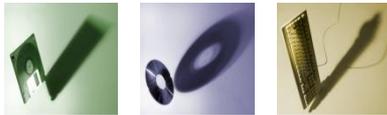


D級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。



資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。 

資通系統防護基準(存取控制)

防護需求 等級		高	中	普
存取控制	帳號管理	<ul style="list-style-type: none"> 一 逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二 應依機關規定之情況及條件，使用資通系統。 三 監控資通系統帳號如發現帳號違常使用時回報管理者。 四 等級「中」之所有控制措施。 	<ul style="list-style-type: none"> 一 已逾期之臨時或緊急帳號應刪除或禁用。 二 資通系統閒置帳號應禁用。 三 定期審核資通系統帳號之建立、修改啟用、禁用及刪除等級「普」之所有控制措施。 四 	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。
	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）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	<ul style="list-style-type: none"> 一 應監控資通系統遠端連線。 二 資通系統應採用加密機制。 三 資通系統遠端存取之來源應為機關已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，使用者之權限檢查作業應於伺服器端完成。	

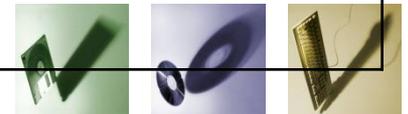
資通系統防護基準(稽核與可歸責性)

防護需求 等級		高	中	普
稽核與可 歸責性	稽核事件	<ul style="list-style-type: none"> 一 應定期審查稽核事件。 二 等級「普」之所有控制措施。 		<ul style="list-style-type: none"> 一 依規定時間週期及紀錄留存政策，保留稽核紀錄。 二 確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 三 應稽核資通系統管理者帳號所執行之各項功能。
	稽核紀錄 內容	<ul style="list-style-type: none"> 一 資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二 等級「普」之所有控制措施。 		資通系統產生之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，並採用單一日誌紀錄機制，確保輸出格式之一致性。
	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。		



資通系統防護基準(稽核與可歸責性)

防護需求等級		高	中	普	
					控制措施
構面	措施內容				
稽核與可歸責性	稽核處理失效之回應	一 機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二 等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。		
	時戳及校時	一 系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 二 等級「普」之所有控制措施。	資通系統應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)。		
	稽核資訊之保護	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 應運用雜湊或其他適當方式之完整性確保機制。 二 等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。	



資通系統防護基準(營運持續計畫)

防護需求 等級		高	中	普
構面	措施內容			
營運持續 計畫	系統備份	<ul style="list-style-type: none"> 一 應將備份還原，作為營運持續計畫測試之一部分。 二 應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。 三 等級「中」之所有控制措施。 	<ul style="list-style-type: none"> 一 應定期測試備份資訊，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。 	<ul style="list-style-type: none"> 一 訂定系統可容忍資料損失之時間要求。 二 執行系統源碼與資料備份。
	系統備援	<ul style="list-style-type: none"> 一 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二 原服務中斷時，於可容忍時間內，由備援設備取代提供服務。 		無要求。



資通系統防護基準(識別與鑑別)

防護需求 等級		高	中	普
構面	措施內容			
識別與鑑別	身分驗證管理	<ul style="list-style-type: none"> 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 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三 等級「普」之所有控制措施。 		<ul style="list-style-type: none"> 一 使用預設密碼登入系統時，應於登入後要求立即變更。 二 身分驗證相關資訊不以明文傳輸。 三 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，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。 四 基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 五 第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。

資通系統防護基準(識別與鑑別)

防護需求 等級		控制措施		
		高	中	普
構面	措施內容			
識別與鑑別	內部使用者之識別與鑑別	一 對帳號之網路或本機存取採取多重認證技術。 二 等級「中」及「普」之所有控制措施。	資通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)之功能，禁止使用共用帳號。	
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。	
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。		



資通系統防護基準(系統與服務獲得)

防護需求等級		高	中	普
構面	措施內容			
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。		
	系統發展生命週期設計階段	<ul style="list-style-type: none"> 一 根據系統功能與要求，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	<ul style="list-style-type: none"> 一 執行「源碼掃描」安全檢測。 二 具備系統嚴重錯誤之通知機制。 三 等級「中」及「普」之所有控制措施。 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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。	



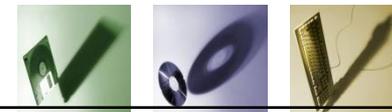
資通系統防護基準(系統與服務獲得)

防護需求 等級		高	中	普
系統與服 務獲得	系統發展 生命週期 部署與維 運階段	<ul style="list-style-type: none"> 一 於系統發展生命週期之維運階段，須注意版本控制與變更管理。 二 等級「普」之所有控制措施。 		<ul style="list-style-type: none"> 一 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。 二 資通系統相關軟體，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。		
	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。		



資通系統防護基準(系統與通訊保護)

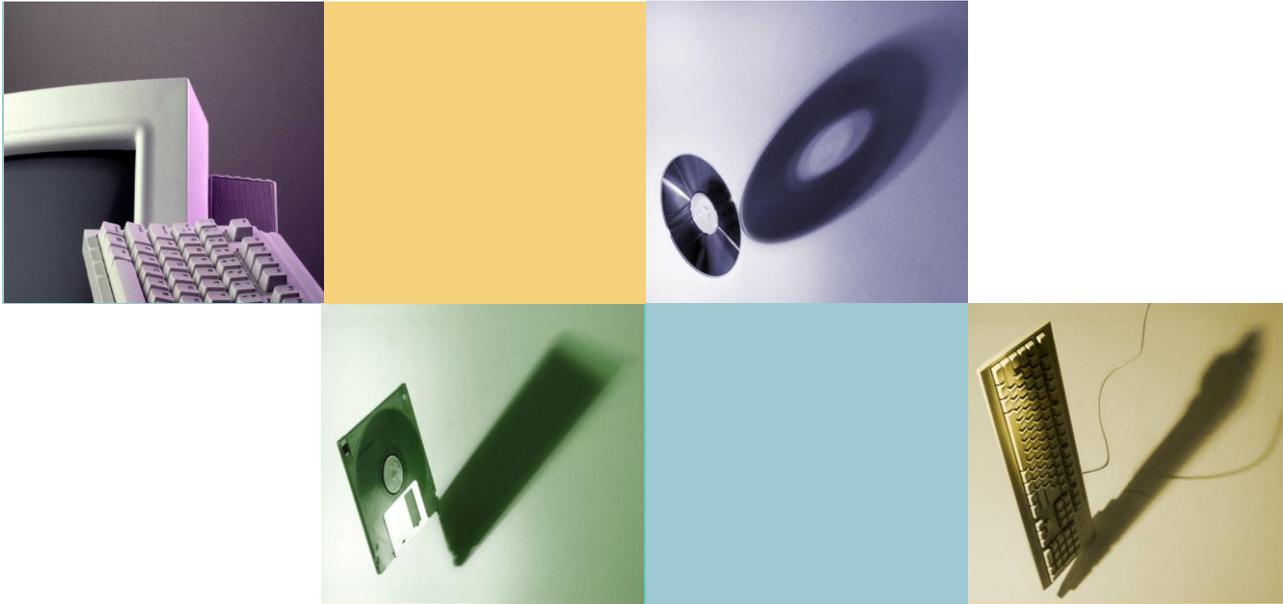
防護需求等級		高	中	普
構面	措施內容			
系統與通訊保護	傳輸之機密性與完整性	一 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二 使用公開、國際機構驗證且未遭破解之演算法。 三 支援演算法最大長度金鑰。 四 加密金鑰或憑證週期性更換。 五 伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	無要求。	無要求。
	資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。



資通系統防護基準(系統與資訊完整性)

防護需求等級		高	中	普
構面	措施內容			
系統與資訊完整性	漏洞修復	<ul style="list-style-type: none"> 一 定期確認資通系統相關漏洞修復之狀態。 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。
	資通系統監控	<ul style="list-style-type: none"> 一 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二 等級「中」之所有控制措施。 	<ul style="list-style-type: none"> 一 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二 等級「普」之所有控制措施。 	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	<ul style="list-style-type: none"> 一 應定期執行軟體與資訊完整性檢查。 二 等級「中」之所有控制措施。 	<ul style="list-style-type: none"> 一 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二 使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三 發現違反完整性時，資通系統應實施機關指定之安全保護措施。 	無要求。





THANKS !