嘉義市政府 Chiayi City Government

資訊安全教育訓練

BCCS 漢昕科技 資訊安全管理顧問：呂瑋原

代理通路顧問服務教育訓練資安稽核

大綱

- 依據
- 資通系統防護需求分級原則
- 資通系統防護基準說明

依據

資通系統防護需求分級原則

資通系統防護基準說明

依據

- 資通安全責任等級分級辦法108.8.26
- 資通安全責任等級A/B/C級之公務機關應辦事項
- 附表九資通系統防護需求分級原則
- 附表十資通系統防護基準

A級

- 各機關有下列情形之一者，其資通安全責任等級為A級：

1. 業務涉及國家機密。
2. 業務涉及外交、國防或國土安全事項。
3. 業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。
4. 業務涉及全國性民眾或公務員個人資料檔案之持有。
5. 屬公務機關，且業務涉及全國性之關鍵基礎設施事項。
6. 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。
7. 屬公立醫學中心。

B級

- 各機關有下列情形之一者，其資通安全責任等級為B級：

1. 業務涉及公務機關捐助、資助或研發之**敏感科學技術資訊**之安全維護及管理。
2. 業務涉及**區域性**、**地區性**民眾服務或跨公務機關共用性資通系統之維運。
3. 業務涉及**區域性**或**地區性**民眾個人資料檔案之持有。
4. 業務涉及**中央二級機關**及**所屬各級機關（構）共用性資通系統**之維運
5. 屬公務機關，且業務涉及**區域性**或**地區性**之**關鍵基礎設施**事項。
6. 屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將**產生嚴重影響**。
7. 屬**公立區域醫院**或**地區醫院**。

C級

- 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

做什麼呢？

- 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**，
    - 附表九完成**資通系統分級**
    - 附表十之**控制措施**
  - 其後應**每年**至少**檢視一次**資通系統分級妥適性

有什麼不同

「政府機關（構）資通安全責任等級分級作業規定」

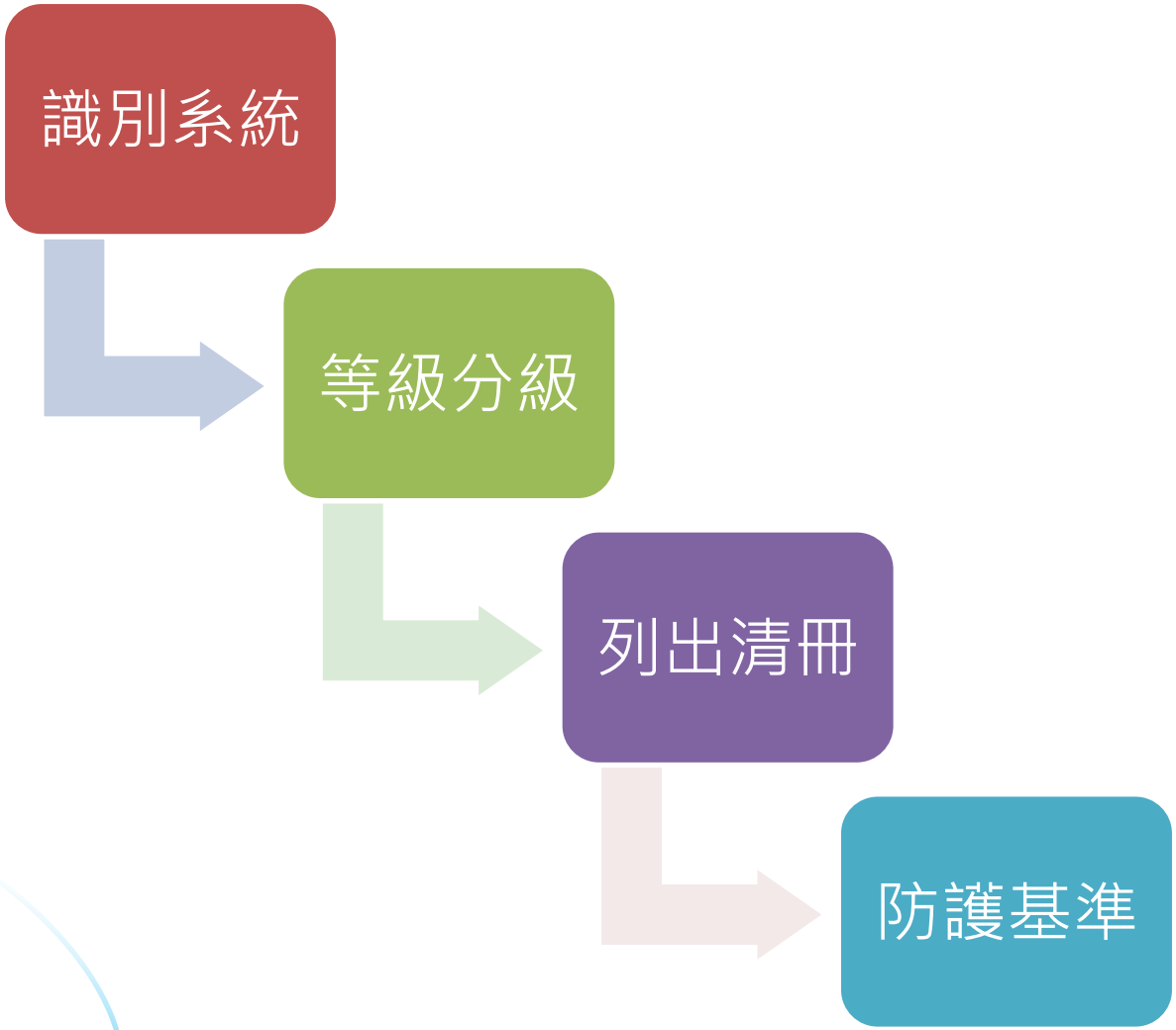
「資訊系統分級與資安防護基準作業規定」

「國家資通安全通報應變作業綱要」

108年3月5日起
停止適用

- 依據
- 資通系統防護需求分級原則
- 資通系統防護基準說明

流程



資通系統

資通系統

- 指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

資通服務

- 指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

資通安全

- 指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

舊的規定

- 資訊系統分級與資安防護基準作業規定

行政院國家資通安全會報

中華民國 104 年 7 月修正

- **套裝軟體**、**作業系統**或**防毒系統**、**防火牆系統**、**入侵偵測/防禦系統**、**弱點掃瞄系統**、**網頁/郵件內容過濾系統**等屬資安防護處理相關控制措施，均**不需**進行資訊系統分級。

問題來了~

- 新的規定中
  - 「網路管理系統」要不要列入？

分級面向

機密性

- 個人或團體的訊息不為其他不應獲得者獲得。

完整性

- 在傳輸、儲存資訊或資料的過程中，確保資訊或資料不被未授權的篡改或在篡改後能夠被迅速發現。

可用性

- 讓資訊可供已獲授權人士在需要時可以取用。

法律遵循性

- 符合相關法規要求

分級等級

高	非常嚴重或災難性之影響。
中	產生嚴重之影響。
普	產生有限之影響。

機密性

普

- 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。

中

- 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。

高

- 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

普

- 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。

中

- 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。

高

- 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

普

- 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。

中

- 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。

高

- 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

普

- 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**。

中

- 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**。

高

- 其他資通系統設置或運作於法令有相關規範之情形。

做做看

全球資訊網	電子公文系統
機密性	機密性
• 普	• 中
完整性	完整性
• 中	• 中
可用性	可用性
• 普	• 普
法律遵循性	法律遵循性
• 普	• 普

依據

資通系統防護需求分級原則

資通系統防護基準說明

防護基準

存取控制(AccessControl)-3
稽核與可歸責性(AuditandAccountability)-6
營運持續計畫(ContingencyPlanning)-2
識別與鑑別(IdentificationandAuthentication)-5
系統與服務獲得(SystemandServicesAcquisition)-8
系統與通訊保護(SystemandCommunicationsProtection)-2
系統與資訊完整性(SystemandInformationIntegrity)-3

存取控制(AccessControl)-1

控制措施	安全等級		
	普	中	高
存取控制(AccessControl)			
帳號管理(AccountManagement)	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。	1. 執行等級「普」之所有控制措施。 2. 資通系統已逾期之臨時或緊急帳號應刪除或禁用。 3. 應禁用資通系統閒置帳號。 4. 應定期審核資通系統帳號之建立、修改、啟用、禁用及刪除動作。	1. 執行等級「中」之所有控制措施。 2. 當逾越機關所規定之預期閒置時間或可使用期限時，系統應自動將使用者登出。 3. 資通系統應依照機關所規定之情況及條件(如上班時間或指定IP來源)，使用資通系統 4. 監控資通系統帳號，如發現帳號違常使用時回報管理者。

存取控制(AccessControl)-2

控制措施	安全等級		
	普	中	高
存取控制(AccessControl)			
最小權限	--	1. 採用最小權限原則，只允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取。 2. ~~應稽核資通系統管理者帳號所執行之各項功能。~~	執行等級「中」之所有控制措施。

存取控制(AccessControl)-3

控制措施	安全等級		
	普	中	高
存取控制(AccessControl)			
遠端存取	對於每一種允許之遠端存取類型，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。	1. 執行等級「普」之所有控制措施。 2. 應監控資通系統遠端連線。 3. 資通系統應實作加密機制來保護遠端存取連線的機密性。 4. 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。 ~~5. 依維運需求，授權透過遠端執行特定之功能及存取相關資訊~~	執行等級「中」之所有控制措施。

稽核與可歸責性-1

控制措施	安全等級		
	普	中	高
稽核與可歸責性			
稽核事件	1. 依律定之時間週期及紀錄留存政策，保留稽核紀錄，並滿足法規要求 2. 確保資通系統有稽核特定事件(如更改密碼、登錄失敗、資通系統存取失敗)之功能，並應決定應稽核之特定資通系統事件 3. 應稽核資通系統管理者帳號所執行之各項功能。	1. 執行等級「普」之所有控制措施。 2. 定期審查稽核事件	執行等級「中」之所有控制措施。

稽核與可歸責性-2

控制措施	安全等級		
	普	中	高
稽核與可歸責性			
稽核紀錄內容	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。	1. 執行等級「普」之所有控制措施。 2. 資通系統產生的稽核紀錄，依需求納入其他相關資訊	執行等級「中」之所有控制措施。

稽核與可歸責性-3

控制措施	安全等級		
	普	中	高
稽核與可歸責性			
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	執行等級「普」之所有控制措施。	執行等級「中」之所有控制措施。

稽核與可歸責性-4

控制措施	安全等級		
	普	中	高
稽核與可歸責性			
稽核處理失效之回應	資通系統在稽核處理失效(如儲存容量不足)之情況下，採取適當之行動，例如：關閉資通系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等	執行等級「普」之所有控制措施。	1. 執行等級「中」之所有控制措施。 2. 當機關規定需要即時通報的稽核失效事件發生時，資通系統應在機關規定之時效內，對機關特定之人員提出告警。

稽核與可歸責性-5

控制措施	安全等級		
	普	中	高
稽核與可歸責性			
時戳	資通系統使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)	1. 執行等級「普」之所有控制措施。 2. 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。	執行等級「中」之所有控制措施。

稽核與可歸責性-6

控制措施	安全等級		
	普	中	高
稽核與可歸責性			
稽核資訊之保護	對稽核紀錄之存取管理，僅限於有權限之使用者	1. 執行等級「普」之所有控制措施。 2. 應運用雜湊或其他適當方式之完整性確保機制。	1. 執行等級「中」之所有控制措施。 2. 定期備份稽核紀錄到與原稽核系統不同之實體系統(如Log伺服器)

營運持續計畫-1

控制措施	安全等級		
	普	中	高
營運持續計畫			
資通系統備份	1. 訂定系統可容忍資料損失之時間要求。 2. 執行系統源碼與資料備份。	1. 執行等級「普」之所有控制措施。 2. 應定期測試備份資訊來驗證備份媒體之可靠性及資訊之完整性。	1. 執行等級「中」之所有控制措施。 2. 應將備份還原，做為營運持續計畫測試之一部分。 3. 應在與運作系統不同地點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拷貝。

營運持續計畫-2

控制措施	安全等級		
	普	中	高
營運持續計畫			
資通系統備援	--	1. 訂定資訊系統從中斷後至重新恢復服務之可容忍時間要求 2. 當原服務中斷，由備援設備取代提供服務	執行等級「中」之所有控制措施。

識別與鑑別-1

控制措施	安全等級		
	普	中	高
識別與鑑別			
內部使用者之識別與鑑別	資訊系統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)，不應有禁止使用共用帳號之行為。	執行等級「普」之所有控制措施。	1. 執行等級「中」之所有控制措施。 2. 對帳號之網路或本機存取採取多重認證技術。

識別與鑑別-2

控制措施	安全等級		
	普	中	高
識別與鑑別			
身分驗證管理	1. 使用預設密碼登入系統時，應於登入後要求立即變更。 2. 身分驗證相關資訊不以明文傳輸。 3. 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。 4. 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制。 5. 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。 6. 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。	1. 執行等級「普」之所有控制措施。 2. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 3. 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。	執行等級「中」之所有控制措施。

識別與鑑別-3

控制措施	安全等級		
	普	中	高
識別與鑑別			
鑑別資訊回饋	資通系統遮蔽在鑑別過程中之資訊(如通行碼)，以防止未授權之使用者可能之窺探/使用。	執行等級「普」之所有控制措施。	執行等級「中」之所有控制措施。

識別與鑑別-4

控制措施	安全等級		
	普	中	高
識別與鑑別			
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。 ~~資訊系統若以通行碼進行鑑別時，該通行碼加密儲存與處理。~~	執行等級「中」之所有控制措施。

識別與鑑別-5

控制措施	安全等級		
	普	中	高
識別與鑑別			
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)。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。

系統與服務獲得-1

控制措施	安全等級		
	普	中	高
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。	執行等級「普」之所有控制措施。	執行等級「中」之所有控制措施。

系統與服務獲得-2

控制措施	安全等級		
	普	中	高
系統與服務獲得			
系統發展生命週期設計階段	--	1. 應根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估。 2. 將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。	執行等級「中」之所有控制措施。

系統與服務獲得-3

控制措施	安全等級		
	普	中	高
系統與服務獲得			
系統發展生命週期開發階段	1. 應針對安全需求實作必要控制措施。 2. 應注意避免軟體常見漏洞(如OWASPTOP10)及實作必要控制措施。 3. 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。	執行等級「普」之所有控制措施。	1. 執行「源碼掃描」安全檢測。 2. 具備系統嚴重錯誤之通知機制。 3. 等級「中」及「普」之所有控制措施。

系統與服務獲得-4

控制措施	安全等級		
	普	中	高
系統與服務獲得			
系統發展生命週期測試階段	執行「弱點掃描」安全檢測。	執行等級「普」之所有控制措施。	1. 執行等級「中」之所有控制措施。 2. 執行「滲透測試」安全檢測。

系統與服務獲得-5

控制措施	安全等級		
	普	中	高
系統與服務獲得			
系統發展生命週期部署與維運階段	1. 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。 2. 資通系統相關軟體，不使用預設密碼。	1. 執行等級「普」之所有控制措施。 2. 在系統發展生命週期之維運階段需要注重版本控制與變更管理。	執行等級「中」之所有控制措施。

系統與服務獲得-6

控制措施	安全等級		
	普	中	高
系統與服務獲得			
系統發展生命週期委外階段	資訊系統開發若委外服務應將系統發展生命週期各階段依安全等級將安全需求(含機密性、可用性、完整性)納入委外合約。	執行等級「普」之所有控制措施。	執行等級「中」之所有控制措施。

系統與服務獲得-7

控制措施	安全等級		
	普	中	高
系統與服務獲得			
獲得程序	--	開發、測試以及正式作業環境應作區隔。	執行等級「中」之所有控制措施。

系統與服務獲得-8

控制措施	安全等級		
	普	中	高
系統與服務獲得			
資訊系統文件	應儲存與管理系統發展生命週期之相關文件。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。

系統與通訊保護-1

控制措施	安全等級		
	普	中	高
系統與通訊保護			
傳輸之機密性與完整性	--	--	1. 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。 2. 使用公開、國際機構驗證且未遭破解之演算法。 3. 支援演算法最大長度金鑰。 4. 加密金鑰或憑證週期性更換。 5. 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。

系統與通訊保護-2（特別）

控制措施	安全等級		
	普	中	高
系統與通訊保護			
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

系統與資訊完整性-1

控制措施	安全等級		
	普	中	高
系統與資訊完整性			
漏洞修復	系統的漏洞修復應測試有效性及潛在影響，並依律定之時間週期更新。	1. 執行等級「普」之所有控制措施。 2. 定期確認資訊系統相關漏洞修復之狀態。	1. 執行等級「普」之所有控制措施。 2. 定期確認資訊系統相關漏洞修復之狀態。

系統與資訊完整性-2

控制措施	安全等級		
	普	中	高
系統與資訊完整性			
資訊系統監控	發現資訊系統有被入侵跡象時，應通報機關特定人員。	1. 執行等級「普」之所有控制措施。 2. 監控資訊系統，以偵測攻擊和未授權之連線，並識別資訊系統之未授權使用。	1. 執行等級「中」之所有控制措施。 2. 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。

系統與資訊完整性-3

控制措施	安全等級		
	普	中	高
系統與資訊完整性			
軟體及資訊完整性	--	1. 使用完整性驗證工具以偵測未授權變更特定軟體及資訊。 2. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。 3. 當發現違反完整性時，資訊系統應實施機關指定之安全保護措施。	1. 執行等級「中」之所有控制措施。 2. 應定期執行軟體和資訊完整性檢查。

ThankYou

感謝聆聽請指教