校園資通安全維護計畫

鍾沛原 專案經理

成大資通安全研究與教學中心

2020/11/10

大綱

- 應辦事項與防護基準
- 校園資通安全維護計畫說明
- 結論

應辦事項與防護基準

資通安全責任等分級

本校是C還是D？還是可以只要D?

- 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。

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 或 ISO 27001 等資訊安全管理系統標準、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。

- 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。

資通安全管理法常見問題

資通安全管理法常見問題

日期：109-09-25　　資料來源：資通安全處

資通安全管理法FAQ_1090821版已更新移除
資通安全管理法FAQ_1090611版已更新移除
資通安全管理法FAQ_1090511版已更新移除
資通安全管理法FAQ_1090302版已更新移除
資通安全管理法FAQ_1090213版已更新移除
資通安全管理法FAQ_1080903版已更新移除

資通安全管理法FAQ_1090925 PDF

2.7. 只有一個官網算不算C級機關？	官網如係屬機關自行或委外開發之資通系統，則符合資通安全責任等級第6條C級機關之條件，機關之資安責任等級即為C級。 建議類此機關，宜積極進行資通系統向上集中，減少機關維運負擔，連帶調降機關資通安全責任等級。
2.8. 內部不對外的網站，算不算自行或委外開發之資通系統?	內部不對外的網站，如屬自行或委外開發之資通系統，即符合資通安全責任等級第6條C級機關之條件，機關之資安責任等級即為C級。

持續滾動式調整的資安法

- 資通系統分級及防護基準(C級單位)

	舊	新
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。	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；並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。

持續滾動式調整的資安法(cont.)

- ISMS導入與公正第三方驗證(以B級單位為例)

舊

資訊安全管理系統之導入及通過公正第三方之驗證	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，於三年內完成公正第三方驗證，並持續維持其驗證有效性。

新

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 或 ISO 27001 等資訊安全管理系統標準、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，於三年內完成公正第三方驗證，並持續維持其驗證有效性。

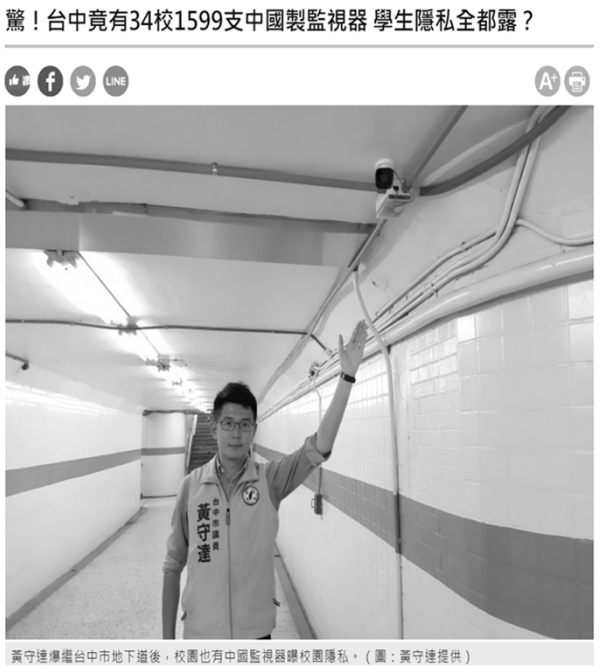
備註：

「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。

持續滾動式調整的資安法(cont.)

- 限制使用危害國家資通安全產品

限制使用危害國家資通安全產品	一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務網路環境介接。



資料來源：自由時報

資通安全責任等級D級單位應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	限制使用危害國家資通安全產品		一、除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 二、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。 三、對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務（業務）網路環境介接。
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資通安全通識教育訓練。

持續滾動式調整的資安法(cont.)

- 認知與訓練(以C級公務機關為例)

舊

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	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。

新

資通安全專職人員	每人每年至少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。
資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
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，並持續維持證照之有效性。
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。

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

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	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。	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。 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	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(cont.)

稽核與可歸責性	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	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

資通系統防護基準(cont.)

				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。		
	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(cont.)

營運持續計畫	系統備份	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。	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。	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	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。
識別與鑑別	內部使用者之	一、對帳號之網路或本機存取採取多重認證技術。	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。	

資通系統防護基準(cont.)

	識別與鑑別	二、等級「中」及「普」之所有控制措施。	
	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、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。	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制。 五、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。 六、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(cont.)

	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)。	
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	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。	無要求。

資通系統防護基準(cont.)

	週期設計階段	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。	
	系統發展生命週期開發階段	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。	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與維運階段	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。	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(cont.)

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。	無要求。	無要求。
		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。		
	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(cont.)

系統與資訊完整性	漏洞修復	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	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。	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	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。	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。

校園資通安全維護計畫說明

核心與非核心業務

- 核心業務
  - 核心業務名稱
  - 支持核心業務之資通系統
  - 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。
  - 最大可容忍中斷時間單位以小時計

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間

核心與非核心業務(cont.)

- 僅為範例，非屬標準答案

核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
教務業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1個工作天
總務業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1個工作天
學輔業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1個工作天

核心與非核心業務(cont.)

- 僅為範例，非屬標準答案

非核心業務及說明如下表:

會計業務	地方教育發展基金 會計資訊系統	會計部分業務無法運作	1個工作天
資訊業務	校園網站	對外公告資訊無法運作	1個工作天
出納業務	薪資管理系統	出納部分業務無法運作	1個工作天
出納業務	台灣銀行e企合成網	出納部分業務無法運作	1個工作天
午餐業務	[redacted]國中小 免費學生午餐	午餐部分業務無法運作	1個工作天
環教業務	花蓮縣環境教育網	環教部分業務無法運作	1個工作天
文書業務	公文收發系統	文書部分業務無法運作	1個工作天
校護業務	學生健康資訊網	校護部分業務無法運作	1個工作天

資通安全政策及目標(範例)

- 為使本機關業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）及法律遵循性，特制訂本政策如下，以供全體同仁共同遵循：
  - 定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
  - 針對各資料的機密性與完整性應妥善保護，避免資料遭竄改。
  - 建立資通安全防護(如:防火牆、防毒軟體)。
  - 辦理資通安全教育訓練(一般使用者與主管，每人每年三小時以上之一般資通安全教育訓練)，提升同仁資通安全意識。
  - 針對辦理資通安全業務有功相關人員應依資通安全管理法子法之「公務機關所屬人員資通安全事項獎懲辦法」進行獎勵。
  - 禁止多人共用同一帳號。
  - 落實資通安全通報機制。

資通安全目標

❑ 量化型目標(範例)

1. 核心資通系統可用性達 99%以上。（中斷時數/總運作時數≤1%）
2. 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
3. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。
4. 全球資訊網內容遭置換次數≤0 次。
5. 資安事件等級 3 或 4 級發生的次數≤0 次。
6. 資安事件等級 1 或 2 級發生的次數≤2 次。

❑ 質化型目標(範例)

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免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。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。
3. 提升人員資安防護意識、防止發生中毒或入侵事件。

資通安全政策核定、宣導、定期檢討

- 資通安全政策及目標之核定程序
  - 資通安全政策由本機關○○單位簽陳資通安全長核定。

第 11 條　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

- 資通安全政策及目標之宣導
  - 每年透過教育訓練、內部會議、張貼公告等方式，向機關內所有人員進行宣導，並檢視執行成效。
  - 每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。
- 資通安全政策及目標定期檢討程序
  - 定期於資通安全管理審查會議中檢討其適切性。

資通安全推動組織

- 資通安全長
- 資通安全推動小組(範例)

(一) 組織

本校設置「資通安全推動小組」負責督導校內資訊安全相關事項，為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理，由資通安全管理代表召集各業務人員代表成立資通安全推動小組，其任務包括：

1. 跨處室資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

資通安全推動組織(cont.)

❑ 資通安全推動小組(範例)

本校之資通安全推動小組依下列分工進行責任分組，並依資通安全管理代表指示負責下列事項，本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

1. 資通安全推動小組：

(1) 資通安全政策及目標之研議。

(2) 訂定本校資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。

(3) 依據資通安全目標擬定年度工作計畫。

(4) 傳達資通安全政策與目標。

(5) 其他資通安全事項之規劃。

(6) 資訊及資通系統之盤點及風險評估。

(7) 資通安全相關規章與程序、制度之執行。

(8) 資料及資通系統之安全防護事項之執行。

(9) 資通安全事件之通報及應變機制之執行。

(10)每年得須參加縣市辦理之相關資訊安全研習。

專職(責)人力及經費配置

- 加強資通安全人員之培訓，並提升學校內資通安全專業人員之資通安全管理能力。得洽請相關學者專家或專業學校（構）提供顧問諮詢服務。
- 負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。
- 首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。
- 專業人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

專職(責)人力及經費配置(cont.)

- 經費之配置
  - 提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。
  - 於整體預算中合理分配資通安全預算所佔之比例。
  - 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

資訊及資通系統之盤點

- 依資產屬性進行分類，可分類為人員類、資訊類、硬體類、軟體類、環境保護類(範例)

資訊資產清單

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	擁有者	機密性	完整性	可用性	資產價值
HSPS-PE-001	PE	管理階層人員	校長、教務主任、資訊組長	人事室	人事室	人事室	1	1	1	1
HSPS-PE-002	PE	網路、系統維護人員	代理資訊教師	人事室	人事室	人事室	1	1	1	1
HSPS-PE-003	PE	一般使用人員	教職員	人事室	人事室	人事室	1	1	1	1
HSPS-IF-001	IF	作業文件	資料庫與資料檔案、備份資料	教務處	資訊組	資訊組長	1	1	1	1
HSPS-IF-002	IF	系統文件	網路架構圖	教務處	資訊組	資訊組長	1	1	1	1
HSPS-IF-003	IF	資訊紀錄（電子/紙本）	啟用與報廢紀錄單、資訊工作日誌、系統特權帳號清單、設備進出紀錄表	教務處	資訊組	資訊組長	1	1	1	1
HSPS-IF-004	IF	系統紀錄（Log）	防火牆Log紀錄(一個月一次)	教務處	資訊組	資訊組長	1	1	1	1
HSPS-HW-001	HW	伺服器	學校Web主機	教務處	資訊組	資訊組長	1	1	1	1
HSPS-HW-002	HW	其他硬體	印表機、影印機	總務處	總務處	總務處	1	1	1	1
HSPS-HW-003	HW	個人電腦	桌上型電腦	教務處	資訊組	資訊組長	1	1	1	1
HSPS-HW-004	HW	可攜式電腦	筆記型電腦	教導處	教導處	教導主任	1	1	1	1
HSPS-HW-005	HW	資安設備	Zyxel防火牆	教務處	資訊組	資訊組長	1	1	1	1
HSPS-HW-006	HW	網路設備	Zyxel交換器、L3交換器	教務處	資訊組	資訊組長	1	1	1	1
HSPS-HW-007	HW	可攜式儲存媒體	USB、記憶卡、CD、DVD、投影機。	教務處	資訊組	資訊組長	1	1	1	1
HSPS-SW-001	SW	作業系統	KMS	教務處	資訊組	資訊組長	1	1	1	1
HSPS-SW-002	SW	資訊安全系統	防火牆軟體(Zyxel)	教務處	資訊組	資訊組長	1	1	1	1
HSPS-EV-001	EV	一般辦公區域	辦公室、會議室。	學校	學校	學校	1	1	1	1
HSPS-EV-002	EV	資訊機房	電腦機房	教務處	資訊組	資訊組長	1	1	1	1
HSPS-EV-003	EV	建築保護設施	不斷電系統、穩壓器、機櫃、滅火器、發電機	總務處	總務處	總務處	1	1	1	1

參考「資訊系統風險評鑑參考指引」

資通安全風險評估(cont.)

- 範例

威脅弱點評估表

資產編號	資產類別	資產名稱	資產價值	威脅	弱點（被利用而造成威脅）	威脅等級（發生之可能性）			弱點等級（受到威脅利用之容易）			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
				操作失誤	操作文件不足	1			1			2
-002	IF	系統文件	2	使用者失誤	教育訓練不足	1			1			2
				操作失誤	操作文件不足	1			1			2
-003	IF	資訊紀錄（電子/紙本）	2	操作失誤	機密資料的外洩(E-mail or 儲存媒體)	1			1			2
				資料外洩	缺乏人員安全審查程序	1			1			2
				備份資料失敗	電腦異常導致備份失敗	1			1			2
-004	IF	系統紀錄（Log）	2	操作失誤	機密資料的外洩(E-mail or 儲存媒體)	1			1			2
				資料外洩	缺乏人員安全審查程序	1			1			2
				備份資料失敗	電腦異常導致備份失敗	1			1			2
				硬體失效	維護服務回應時間過長	1			1			2
				硬體失效	缺乏硬體耗損控管	1			1			2
				硬體失效	缺乏有效變更控制	1			1			2
				電源供應中斷	不穩定的電壓	1			1			2
W-	HW	伺服器	2	未經授權存取或使用	未確實陪同外部人員或清潔人員執行相關作	1			1			2
				未經授權存取或使用	存取權限授與不當或未定期審查	1			1			2
				未經授權存取或使用	通行碼管理不足	1			1			2
				未經授權存取或使用	離開工作站未進行「登出」作業	1			1			2
				未經授權存取或使用	缺乏監督與稽核機制	1			1			2
				操作失誤	複雜的操作介面	1			1			2
				操作失誤	操作文件不足	1			1			2
				操作失誤	專業訓練不足	1			1			2
				硬體失效	維護服務回應時間過長	1			1			1
				硬體失效	缺乏硬體耗損控管	1			1			1
				硬體失效	缺乏有效變更控制	1			1			1
				電源供應中斷	不穩定的電壓	1			1			1
W-	HW	其他硬體	1	未經授權存取或使用	未確實陪同外部人員或清潔人員執行相關作	1			1			1
002				未經授權存取或使用	存取權限授與不當或未定期審查	1			1			1
				未經授權存取或使用	通行碼管理不足	1			1			1

資通安全風險評估(cont.)

- 風險評估注意事項
  - 相關資訊資產是否皆納入風險評估範圍？
  - 風險評估之影響程度、發生可能性之判斷原則。
  - 可能面對的潛在風險因子(威脅、弱點)
  - 是否識別出可接受風險值？
  - 針對高於可接受風險值之項目採取改善措施！

資通安全防護及控制措施

- 資訊及資通系統之管理
  - 保管
    - 盤點、造冊與持續更新
    - 妥善保存或備份
    - 適當存取控制政策
  - 使用
    - 授權與資通安全要求事項(可被接受之使用規則)
  - 刪除或汰除
    - 資料的妥善移轉或備份
    - 移除或安全覆寫
    - 實體銷毀或毀損，使原始資料無法被讀取

資通安全防護及控制措施(cont.)

- 存取控制與加密機制管理
  - 網路安全控管
    - 網路區域劃分
    - 防火牆存取控制
    - 防火牆規則檢視與系統更新
    - 存取紀錄的留存及欄位資訊確保
    - 操作紀錄和日誌的留存
    - 禁止私人設備與通訊服務
    - DNS防護
    - 無線網路防護

資通安全防護及控制措施(cont.)

- 資通系統權限管理
  - 通行碼(password)管理：長度、複雜度、更換頻率、個人保存責任
  - 權限授權及避免帳號共用
  - 定期權限清查與帳號停用、移除
- 特權帳號之存取管理
  - 申請、授權與紀錄留存
  - 避免帳號共用
  - 與日常帳號的區隔
  - 特權帳號使用軌跡留存
  - 定期清查與逾期處理
- 加密管理
  - 儲存或傳輸時的加密
  - 避免留存解密資訊
  - 疑似遭破解之立即更改

(1) 通行碼長度 8 碼以上。

(2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3) 使用者每 90 天應更換一次通行碼。

資通安全防護及控制措施(cont.)

- 作業與通訊安全管理
  - 防範惡意軟體之控制措施
    - 安裝防毒軟體及軟、硬體更新或升級
    - 應用軟體清查
    - 避免使用已知或疑似惡意網站
    - 作業系統與軟體更新
  - 遠距工作之安全措施
    - 以現場操作為原則
    - 應定期審查已授權之遠距工作
    - 採適當之防護措施

資通安全防護及控制措施(cont.)

- 作業與通訊安全管理
  - 電子郵件安全管理
    - 電子郵件帳號的申請與刪除
    - 定期郵件帳號清查
    - 防毒及過濾機制
    - 個人電子郵件使用之防護與社交工程演練
  - 實體與環境安全管理
    - 機房實體隔離與進出入管控
    - 機房空調、電力及溫濕度管控
    - 辦公室區域之實體與環境安全(桌面淨空、機密/敏感資訊保護、資訊設備管理)

教育體系電子郵件服務與安全管理指引(教育部109年3月2日臺教資(四)字第1090008789號函)

- 一、教育部（以下簡稱本部）為確保各級學校、臺灣學術網路區域網路中心、各直轄市、縣（市）教育網路中心電子郵件服務安全使用，減少不當使用及降低資通安全威脅，特訂定教育體系電子郵件服務與安全管理指引（以下簡稱本指引）。
- 二、本指引適用對象為各級學校、臺灣學術網路區域網路中心、各直轄市、縣（市）教育網路中心（以下簡稱各單位）。
- 三、各單位辦理公務業務或核心業務時，應使用單位配發之電子信箱收發公務所需資訊，不得使用非公務信箱進行公務郵件收發等事宜。

教育體系電子郵件服務與安全管理指引(cont.)

- 四、各單位建立電子郵件服務時，應明確規範電子郵件服務對象（教職員、學生、校友、校外人士、電子郵件服務人員及廠商、資安人員）、申請方式、使用用途範圍及使用期限，且不得提供服務對象以外者使用電子郵件服務。
- 各單位建立前項電子郵件服務，應訂定電子郵件服務使用相關規範，明確規範使用者之權利、責任及相關安全原則如下：
- （一）初次申請者應驗證使用者身份。
- （二）應強制使用者最低密碼複雜度；強制密碼最短及最長之效期。
- （三）使用者使用電子郵件服務時，不得散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息，導致他人權益受損。

教育體系電子郵件服務與安全管理指引(cont.)

- （四）使用者使用電子郵件服務時應尊重智慧財產權，不得有違法傳送或侵害他人智慧財產權之行為。
- （五）使用者使用電子郵件服務時不可作為商業用途。
- （六）使用者使用電子郵件服務時，應尊重網路隱私權，不得任意窺視其他使用者之個人資料或有其他侵犯隱私權之行為。不得盜用他人或系統資源，或以任何方式影響系統正常運作。
- （七）使用者辦理公務、及重要（或敏感）專案使用之電子郵件信箱（可規劃專用電子郵件信箱），不得轉至外部私人信箱收發公務資訊。

教育體系電子郵件服務與安全管理指引(cont.)

- （八）教職員如轉任或借調至公務機關服務者，不得使用學校電子郵件信箱收發公務機關相關電子郵件。
- （九）使用者如因故無法使用公務信箱讀取訊息，以致影響公務執行，得由直屬單位主管指定代理人提出申請，並經郵件維護負責單位審核必要性後，授權代理人讀取公務信箱相關內容。
- 各單位訂定之前項規範，應辦理教育訓練，以利使用者了解並落實遵守相關規範。

教育體系電子郵件服務與安全管理指引(cont.)

- 六、各級學校應將應用於學校校務行政及教學等重要業務之電子郵件服務納入核心資通系統，辦理業務持續運作演練及網站安全弱點檢測，並導入資訊安全管理系統，大專校院應通過第三方驗證。
- 各單位視資源能力設置適當之安全防護系統及設備，並應注意資通安全管理法相關規定。
- 各單位應備電子郵件過濾機制，視資源能力對電子郵件特徵（來源網域名稱、IP、電子郵件地址，發信量、發信次數等）實施必要檢查，以強化電子郵件服務安全。

教育體系電子郵件服務與安全管理指引(cont.)

- 九、各單位應定期辦理使用電子郵件服務教育訓練，提醒使用者勿開啟來路不明之電子郵件，並加強如電子郵件相關政策、管理、使用注意事項及新型態威脅等資安宣導。
- 各單位應配合本部每年定期辦理防範惡意電子郵件社交工程之演練作業，進行單位人員教育訓練，並勿過濾測試郵件，以加強使用者之安全警覺意識。
- 各單位應針對前項演練不合格人員加強資安訓練及宣導。

資通安全防護及控制措施(cont.)

- 作業與通訊安全管理
  - 資料備份
    - 備份的標的、週期與異地存放的考量
    - 備份的有效性確認
    - 備份資料加密需求
  - 媒體防護措施
    - 機密/敏感資料的保護
    - 實體傳送之確保
  - 電腦使用之安全
    - 螢幕保護程式啟用或自動登出設定
    - 作業系統更新、應用程式漏洞修補及防毒

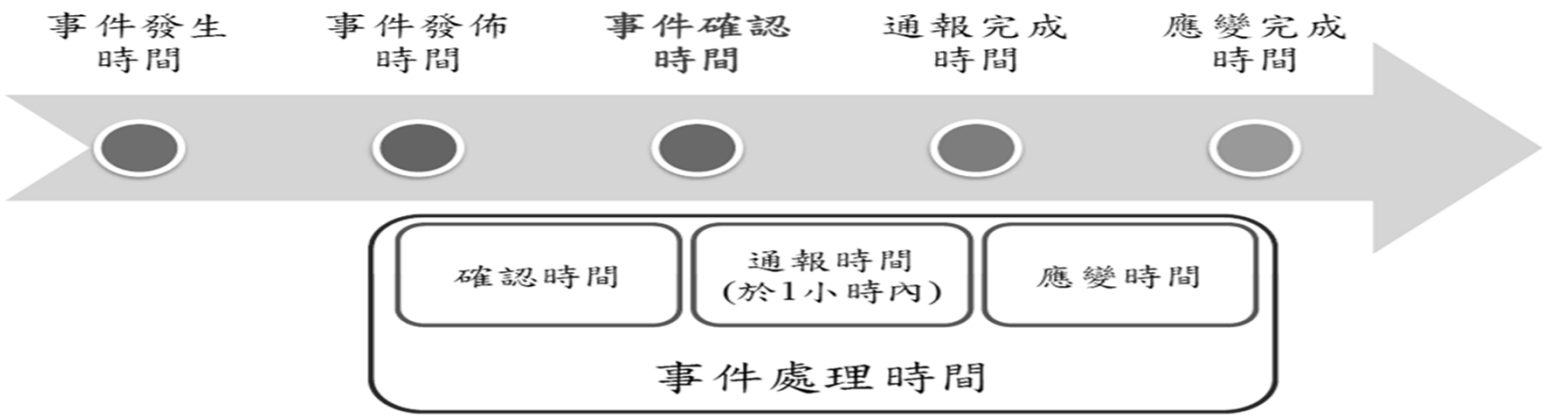
資通安全防護及控制措施(cont.)

- 作業與通訊安全管理
  - 行動設備之安全管理
    - 機密資料之存取、處理或傳送管控
  - 即時通訊軟體之安全管理
- 系統獲取、開發及維護
- 資通安全防護設備
  - 置防毒軟體、網路防火牆、電子郵件過濾裝置
  - 資安設備應定期備份日誌紀錄

資通安全事件通報、應變及演練相關機制

臺灣學術網路各級學校資通安全通報應變作業程序

- 依據臺灣學術網路各級學校資通安全通報應變作業程序第三章第一節第二條規定：
  - 各連線單位發現資安事件後可先進行事件確認，經確認為資安事件後，須於一小時內，至通報應變網站通報登錄資安事件細節、影響等級及是否申請支援等資訊，並評估該事件是否影響其他連線單位運作。



個資事故=資安事故

銓敘部個資外洩通知

本部於108年6月22日接獲外部情資知悉國外網站揭露疑似本部所掌理之個人資料餘59萬筆，本部依個人資料保護法第12條及施行細則第22條規定通知當事人相關事項如下：

一、影響範圍：94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，實際影響人數為243,376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。

二、已採取因應措施：

(一) 依資通安全管理法向行政院國家資通安全會報技術服務中心進行資安事件通報。

(二) 疑似外洩資料之資訊系統早已於104年3月下線，為求審慎，本部即刻對本案現行運作相關資通系統進行弱點檢測及重新檢視防護措施。

針對本事件，本部已協請行政院資通安全處協助進行根因調查及全機關全面性資通安全檢測，本部將確實檢討改進，並依資通安全管理法及個人資料保護法持續精進各項資通安全及個資保護相關作為。

銓敘部外洩59萬筆公務人員個資，影響超過24萬名公務人員的資安事件，因為包含許多國家情治人員的資料也在外洩清單中，行政院資安處亦將此資安事件定義為「第三級資安事件」，後續影響餘波盪漾。

資料來源：iThome

個資事故?資安事故?

【 國立中正大學 通知 】

您好，國立中正大學通知，您的部分學籍資料因服務學習承辦人員作業疏失，不慎於 109 年 10 月 12 日在服務學習講座通知之電子郵件中以附件檔案誤傳給校內約 220 位學生，該檔案學籍資料欄位包含：學號、中文姓名、身份證字號、目前系所代號、目前系所名稱、目前班級、目前年級、性別、出生年月日、聯絡人姓名、在校狀態、電子郵件、行動電話。本校特此致上最大歉意，並依個人資料保護法第 12 條規定通知當事人。本校已掌握學生名單，並已通知他們立刻刪除檔案不得轉傳，以免觸法。本校將持續追蹤後續狀況，目前並無證據顯示資料有流至校外。本校將深切檢討作業流程，並立即改善個人資料之管理。若您有任何疑問，請隨時與通識教育中心聯絡。

承辦人：黃阡淇
電話：(05)272-0411 #17305
E-mail：huangsl@ccu.edu.tw

國立中正大學通識教育中心 敬上
109 年 10 月 14 日

可怕的「敏感資訊」

- 資通安全事件等級-3級事件
  - 未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、**敏感資訊**或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
  - 未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。
  - 未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

什麼？！原來國中小學校也有機會發生三級資安事件

- 資通安全事件通報及應變辦法總說明
  - 所定核心業務，依資通安全管理法施行細則第七條第一項之規定認定；所定核心資通系統，依該細則第七條第二項之規定認定，併予敘明。
  - 所稱一般公務機密，參考行政院訂定之文書處理手冊第五十一點規定，係指公務機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。
  - 所稱敏感資訊，指包含**個人資料**等**非一般公務機密或國家機密**之資訊，**如遭洩漏可能造成機關本身或他人之損害或困擾**，而具保護價值之資訊。
  - 所稱國家機密，依國家機密保護法第二條規定，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依該法核定機密等級者。

資通安全管理法常見問題

- 外力、大範圍影響並非資安事件判斷的唯一準則

議題	回應
7.1. 資安事件通報及應變辦法第二條第二項中，如影響系統可用性是非外力（非機關外的駭客）造成的，是不是要通報？（例如 UPS 造成的中斷）	不論是否屬機關內外因素導致，均須通報。
7.2. 1 台 PC 故障，或是 1 個感探器故障，是否要進行通報？	需視其是否影響核心或非核心業務運作，或造成機關日常作業影響而定，如已造成前述事項之影響，則須通報。

資通安全情資之評估及因應

- 資通安全情資之分類評估
- 資通安全情資之因應措施

資通系統或服務委外辦理之管理

- 若另有需求時得應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

資通安全教育訓練

- 一般使用者與主管，每人每年接受3 小時以上之一般資通安全教育訓練。
- 應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及「教育訓練計畫（表）」，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練上課紀錄（表）。

資通安全教育訓練(cont.)

- 資通安全認知宣導及教育訓練之內容得包含：
  - 資通安全政策
  - 通安全法令規定
  - 資通安全作業內容
  - 資通安全技術訓練
- 員工報到時，應使其充分瞭解本機關資通安全相關作業規範及 其重要性。
- 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部 的使用者，亦應一體適用。

公務機關所屬人員辦理業務涉及資通安全事項之考核機制

- 所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法，及本校各相關規定辦理之。

（十二）辦理各項資安業務，有公務機關所屬人員資通安全事項獎懲辦法第三條規定之情形，並圓滿達成任務，具有成效或領導有方，有具體優異事蹟者。

公務機關所屬人員辦理業務涉及資通安全事項之考核機制(cont.)

第 3 條　有下列情形之一者，予以獎勵：

一、依本法、本法授權訂定之法規或機關內部規範，訂定、修正及實施資通安全維護計畫，績效優良。

二、稽核所屬或監督機關之資通安全維護計畫實施情形，或辦理資通安全演練作業，績效優良。

三、配合主管機關、上級或監督機關辦理資通安全維護計畫實施情形之稽核或資通安全演練作業，經評定績效優良。

四、辦理資通安全業務切合機宜，防止資通安全事件之發生，避免本機關、其他機關或人民遭受損害。

五、主動發現新型態之資通安全弱點或入侵威脅，並進行資通安全情資分享，防止資通安全事件之發生或降低其損害。

六、積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。

七、對資通安全業務提出具體建議或革新方案，並經採行。

八、辦理資通安全人才培育事務，有具體貢獻。

九、辦理資通安全科技之研發、整合、應用、產學合作或產業發展事務，有具體貢獻。

十、辦理資通安全軟硬體技術規範、相關服務及審驗機制發展等事務，有具體貢獻。

十一、辦理資通安全政策、法制研析或國際合作事務，有具體貢獻。

資通安全維護計畫及實施情形之持續精進及績效管理機制

- 資通安全維護計畫之實施
  - 為落實本安全維護計畫，使之資通安全管理有效運作，於訂定各階文件、流程、程序或控制措施時，應與資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

資通安全維護計畫及實施情形之持續精進及績效管理機制(cont.)

- 資通安全維護計畫之持續精進及績效管理
  - 召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
  - 管理審查議題應包含下列討論事項：
    - 過往管理審查議案之處理狀態
    - 與資通安全管理系統有關之內部及外部議題的變更
    - 資通安全維護計畫內容之適切性
    - 資通安全績效之回饋
    - 風險評鑑結果及風險處理計畫執行進度
    - 重大資通安全事件之處理及改善情形
    - 利害關係人之回饋
    - 持續改善之機會
  - 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存

結論

滾動修正ing

> 首頁 > 最新公告列表

最新公告

行政院資通安全處訂於109年11月9日至11月30日，於北、中、南、東部，共辦理5場次「資通安全管理法修法說明會」，敬請各納管機關踴躍報名

1.資安法自108年1月1日起施行，為利各機關更妥適執行相關法遵事項，遂於109年啟動資安法檢討作業，綜整近期威脅趨勢及各納管機關執行情形，研擬法規調修內容，並辦理旨揭說明會，就資安法目前施行情形及整體修法重點作說明，與各界進一步交流及凝聚共識，以持續協助各納管機關強化相關資安防護作業，提升資訊服務之安全性。

2.報名網址：https://www.cisanet.org.tw/News/news_more?id=4354

3.備註：各機關參加人數不限，惟各場次因場地因素有人數限額，如遇名額已滿即停止報名，報名期限於每場座談會前1個工作天截止。

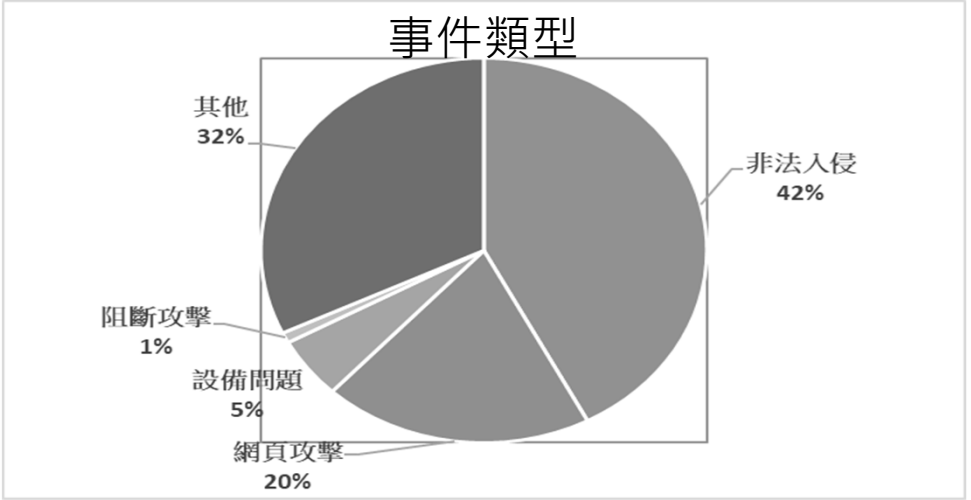
說明會簡章下載：資安法修法說明會簡章

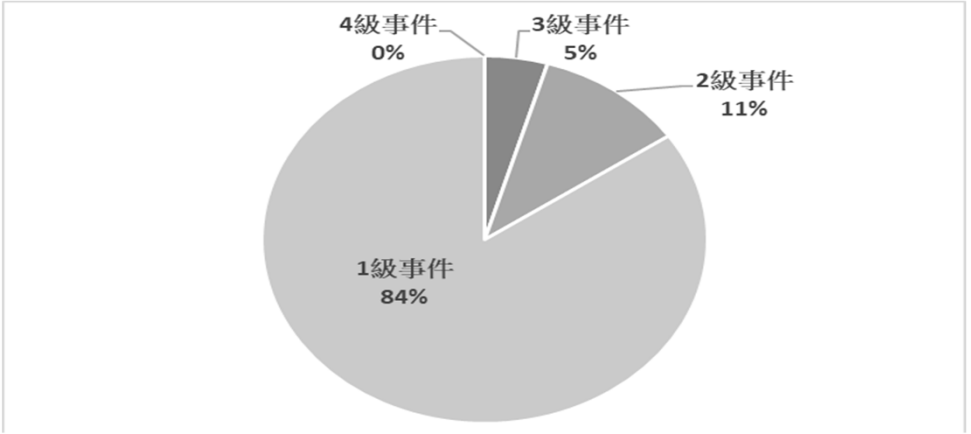
2020/10/30 15:23:08

政府機關資安事件統計(107年～109年7月)

近年政府機關資安事件統計

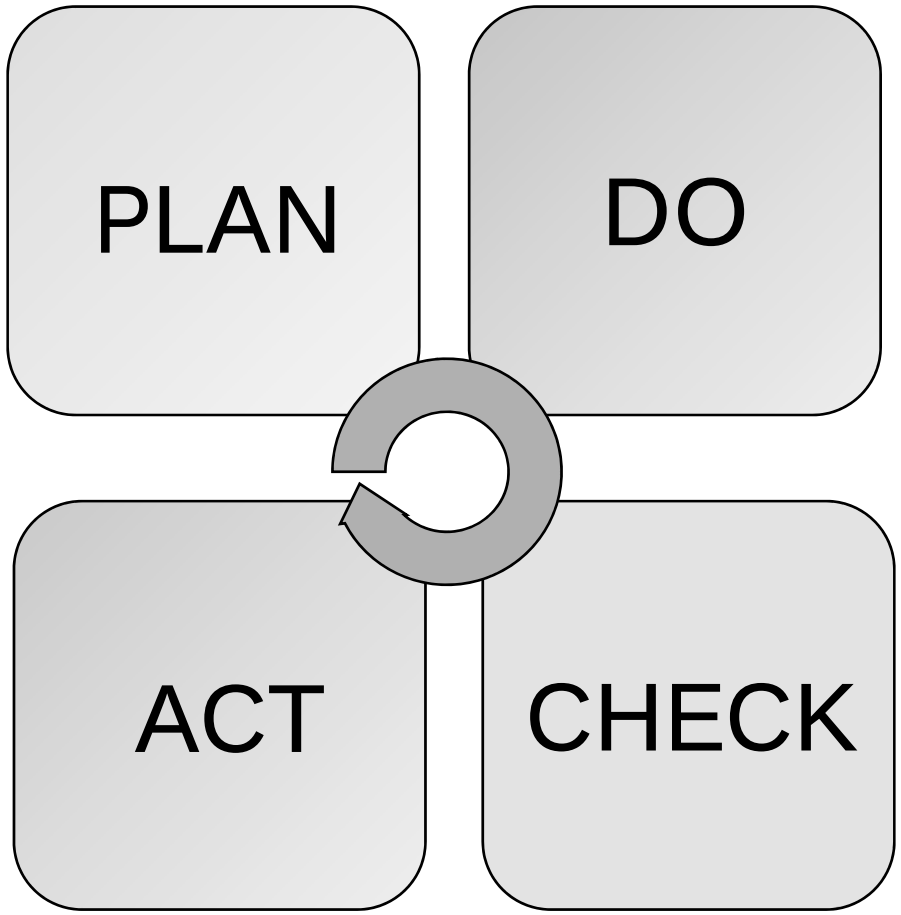
資料來源：自由時報



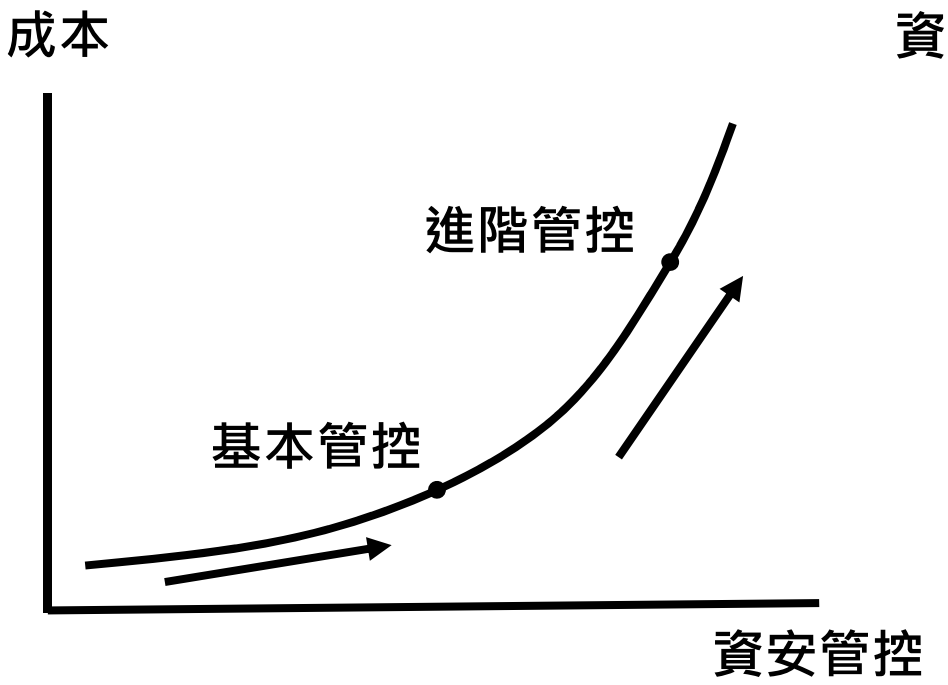


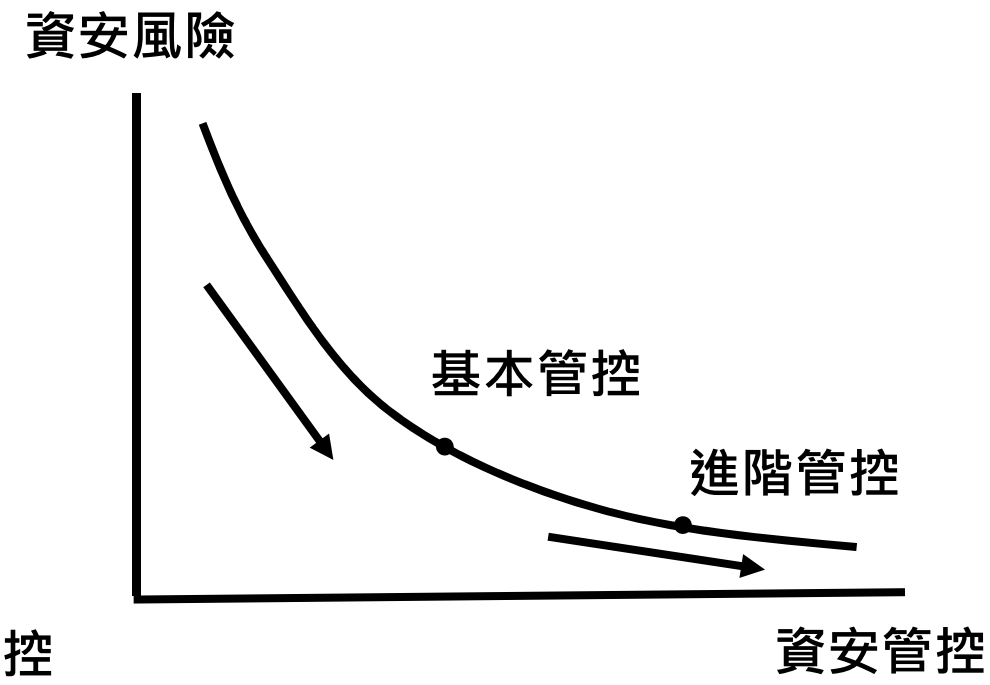
結論

- 知錯能改
- 持續精進



資安管控與成本考量






QUESTIONS
ANSWERS