強化安維辦法之資安標準規範
資通系統之資安防護

行政院資通安全處

110年2月3日

大綱

- 資通安全管理法相關規定
- 個人資料保護法-
  非公務機關個人資料檔案安全維護辦法(安維辦法)

資通安全管理法相關規定

資通安全管理法規範

- 108.1.1起施行，納管對象：**7,703個**(截至110年1月6日)
  - **機關**資安分級：
    應辦事項(管理面、技術面、認知與訓練面)
  - **資通系統**分級：
    系統分級(普中高)，**防護基準**(7大構面)

- 納管機關分級情形(A-C級具資通系統)

機關類型	A級	B級	C級	D級	E級	總數
中央機關	44	144	365	315	113	981
地方政府	0	106	532	4,979	678	6,295
特定非公務機關	46	121	156	84	20	427
全部類型	**90**	**371**	**1,053**	**5,378**	**811**	**7,703**

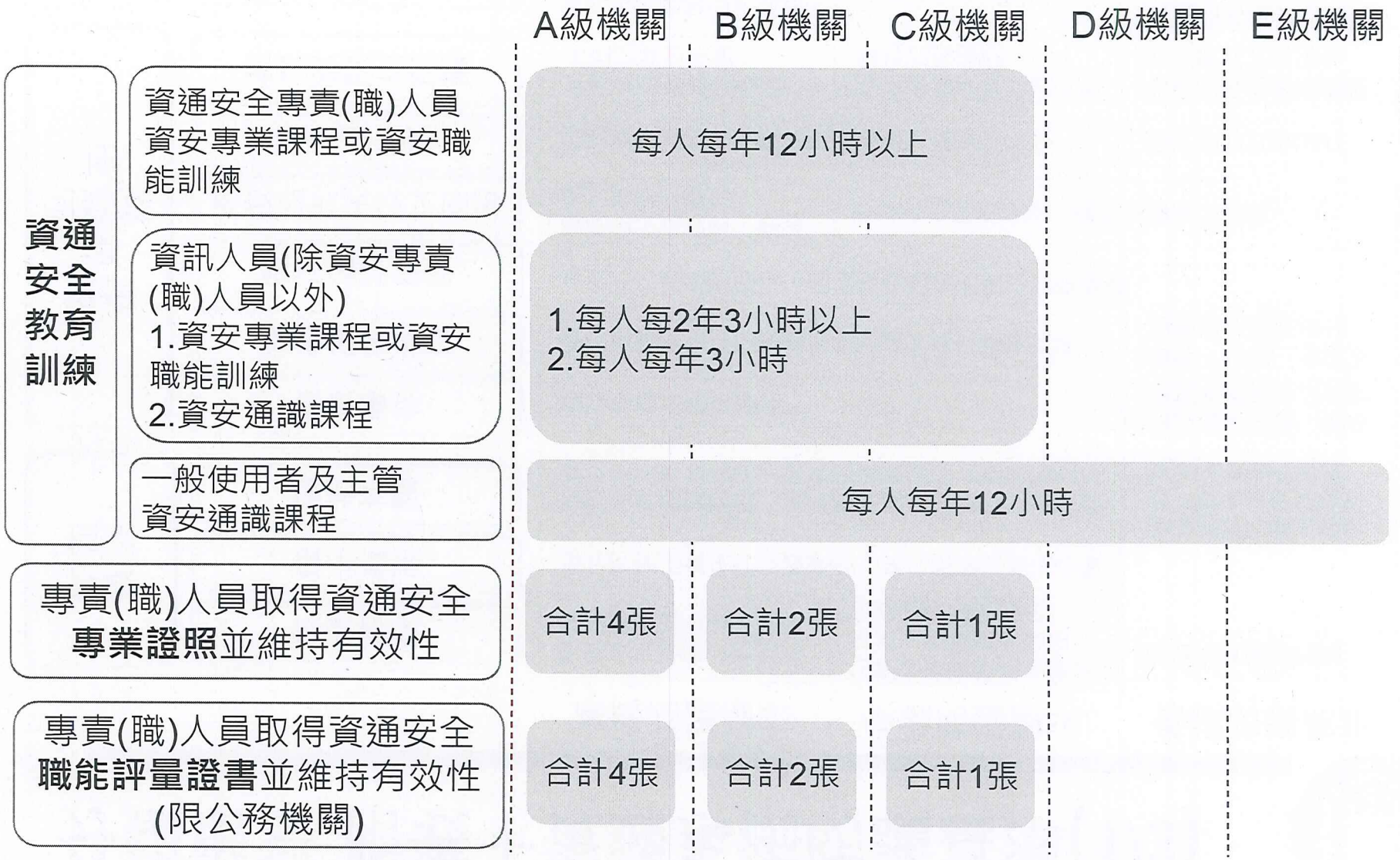
各等級機關應辦事項-管理面

	A級機關	B級機關	C級機關	D級機關	E級機關
資通系統分級及防護基準	1年內針對自行或委外開發之資通系統，依附表九原則完成分級，並每年檢視妥適性				
	1年內完成附表十之控制措施		2年內完成附表十之控制措施		
ISMS導入及通過第三方驗證	2年內全部核心資系統導入CNS27001同等以上之標準，並持續維持導入				
	3年內完成公正第三方驗證，並維持有效性				
資安專責(職)人員	4人	2人	1人		
資安內部稽核	每年2次	每年1次	2年1次		
核心資通系統業務持續運作演練	每年1次	2年1次			
資安治理成熟度評估(限公務機關)	每年1次				
限制使用危害國家資通安全產品	不得採購使用，已使用者應列冊管理且不得與公務網路環境介接				

各等級機關應辦事項-技術面

		A級機關	B級機關	C級機關	D級機關	E級機關
核心資通系統安全性檢測	網站安全**弱點檢測**	每年2次	每年1次	2年1次		
	系統**滲透測試**	每年1次	2年1次			
資通安全**健診**		每年1次	2年1次			
資通安全**威脅偵測**管理機制(SOC)		1年內完成並持續維運，公務機關應提交監控資料				
政府組態基準(限公務機關)		1年內導入並持續維運				
資通安全防護	防毒軟體	1年內完成各項防護措施啟用，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					
	電子郵件過濾機制					
	入侵偵測及防禦機制					
	應用程式防火牆					
	進階持續性威脅攻擊防禦措施					

各等級機關應辦事項-認知與訓練面



分級辦法-附表十資通系統防護基準(1/3)

		高級防護需求	中級防護需求	普級防護需求
存取控制	帳號管理	監控系統帳號、逾越閒置時間或使用期限處理	逾期之臨時帳號刪除或禁用、閒置帳號禁用、定期審核帳號管理	建立帳號管理機制
	最小權限	僅允許使用者依任務及業務，完成所需之授權存取		
	遠端存取	監控系統遠端連線、系統應採用加密機制、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		遠端存取均應取得授權，使用者權限檢查應於伺服器端完成
稽核與可歸責性	稽核事件	應定期審查稽核事件		保留稽核紀錄、稽核管理者帳號之各功能
	稽核紀錄內容	資通系統之稽核紀錄應依需求納入其他相關資訊		事件、時間、位置及相關之使用者身分
	稽核儲存容量	依稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量		
	稽核處理失效之回應	應於規定時效內，對特定人員提出警告	於稽核處理失效時，應採取適當之行為	
	時戳及校時	系統內部時鐘應定期與基準時間源同步		可對應UTC或GMT
	稽核資訊之保護	定期備份稽核紀錄至不同之實體系統	運用雜湊或其方式之完整性保護機制	稽核紀錄之管理僅限於有權限之使用者
營運持續計畫	系統備份	重要系統軟體與其他安全相關備份應與運作系統不同處存放	定期測試備份資訊	訂定可容忍資料損失之時間要求，執行系統源碼與資料備份
	系統備援	訂定系統中斷後至重新恢復服務之可容忍時間，服務中斷時，於可容忍時間內，由備援設備提供服務		

分級辦法-附表十資通系統防護基準(2/3)

		高級防護需求	中級防護需求	普級防護需求
識別與鑑別	內部使用者之識別與鑑別	對帳號之網路或本機存取採多重認證技術	應具備唯一識別及鑑別機關使用者之功能，禁止使用者共用帳號	
	身分驗證管理	應防範自動化程式登入或密碼更換嘗試、密碼重設機制對使用者確認身分，發送一次性及具有時效性符記		身分驗證不以明文傳輸、密碼複雜度及最短、最長之效期限制
	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	系統如以密碼進行鑑別，該密碼應加密或經雜湊處理後儲存		
	非內部使用者之識別與鑑別	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)進行檢核確認		
	系統發展生命週期設計階段	識別可能之威脅，進行風險分析及評估、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	執行源碼掃描安全檢測、具系統嚴重錯誤通知機制	針對安全實作必要控制措施、避免軟體常見漏洞及必要控制措施；錯誤時，頁面僅顯示簡短訊息及代碼	
	系統發展生命週期測試階段	執行滲透測試安全檢測	執行弱點掃描安全檢測	
	系統發展生命週期部屬與維運階段	注意版本控制與變更管理		進行更新與修補，關閉不必要服務、不用預設密碼
	獲得程序	開發、測試及正式作業環境應為區隔		
	系統文件	應儲存與管理系統發展生命週期之相關文件		

分級辦法-附表十資通系統防護基準(3/3)

		高級防護需求	中級防護需求	普級防護需求
系統與通訊保護	傳輸之機密性與完整性	採用加密機制，防止資訊揭露或偵測資訊變更；使用公開、國際機構驗證且未遭破解之演算法；支援演算法最大長度金鑰；加密金鑰或憑證定期更換；伺服器端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		
系統與資訊完整性	漏洞修復	定期確認資通系統相關漏洞修復之狀態		漏洞修復應測有效性及潛在影響，並定期更新
	資通系統監控	採用自動化工具監控進出之通信流量，發現不尋常或未授權之活動時，針對分析該事件	監控資通系統，偵測攻擊與未授權之連線，並識別資通系統之未授權使用	發現資通系統有被入侵跡象時，應通報機關特定人
	軟體及資訊完整性	應定期執行軟體與資訊完整性檢查	使用完整性驗證工具，偵測未授權變更特定軟體及資訊；使用者輸入資料合法性檢查應置於應用系統伺服器端；發現違反完整性時，應實施機關指定之安全保護措施。	

~~個人資料保護法~~-
非公務機關個人資料檔案安全維護辦法

提供電子商務服務系統之

非公務機關個人資料檔案安全維護辦法

- 依個資法第27條：
  - 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
  - 前項計畫及處理方法之標準等相關事項之辦法(以下簡稱安維辦法)，由中央目的事業主管機關定之。

- 目前已有14個中央目的事業主管機關訂定38個安維辦法

金管會非公務機關安維辦法-結構

指定適用之非公務機關

- 金融控股、銀行、證券、期貨、保險、電子票證、電子支付、公告之金融服務業及所管財團法人等9類

個資規劃保護

- 訂定檔案安全維護計畫
- 定期查核持有個資現況
- 因應個資事故，訂定應變、通報及預防機制
- 定期宣導所屬人員個資保護

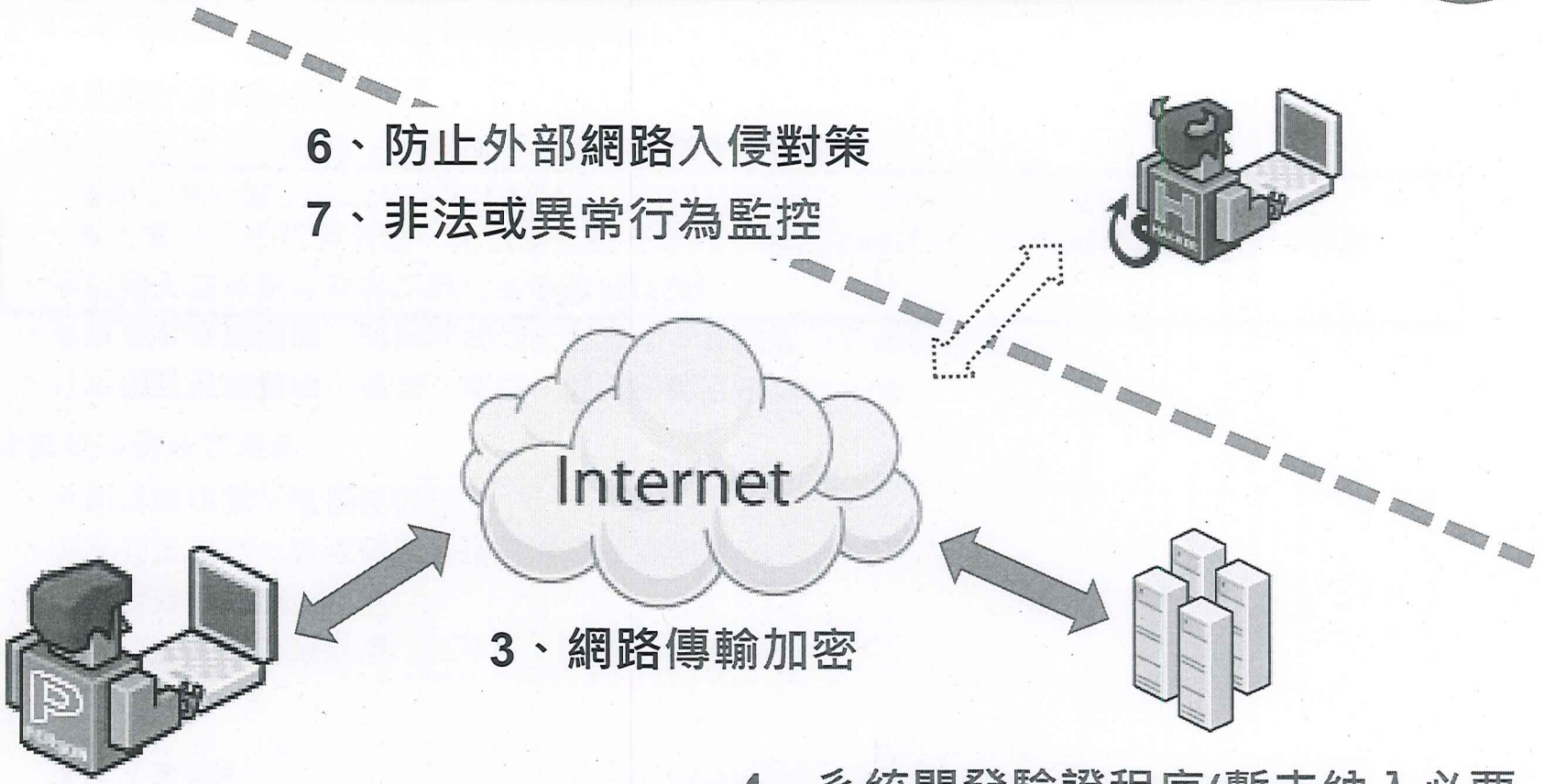
個資管理程序及措施

- 訂定**個資管理程序**：蒐集、處理、國際傳輸及刪除等10項
- **資料安全管理措施**：設備或儲存媒體使用、加密措施及備份保護
- **提供電子商務服務系統之資訊安全措施(7項)**
  - 使用者身分確認及保護、個資呈現隱碼機制、網路傳輸加密、系統開發驗證程序、個資檔案及資料庫存取控制與保護監控、防止外部網路入侵對策、非法或異常行為監控等
- 個資存放紙本、磁碟、電腦或其他**媒介**之**安全管理措施**
- 與所屬**人員**約定**保密**

個資之安全稽核、紀錄保存及持續改善機制

- 訂定個資安全稽核機制
- 記錄個資使用，留存軌跡或相關證據
- 定期提出自我評估

提供電子商務服務系統之資訊安全措施



6、防止外部網路入侵對策

7、非法或異常行為監控

3、網路傳輸加密

1、使用者身分確認及保護

2、個資呈現隱碼機制

4、系統開發驗證程序(暫未納入必要項目)

5、個資檔案及資料庫存取控制與保護監控

非公務機關安維辦法-資通系統安全措施(1/2)

- 國發會參考金管會所訂內容，並考量非公務機關差異，目前規劃明定6項必要項目，並提供相關說明：
  - 可參考資通安全責任等級分級辦法附表10相關規範

管制措施	說明
一、使用者身分確認及保護機制。	針對資通系統或個資檔案存取，提供使用者識別、鑑別及身分驗證管理機制。 如：帳密管制、多重認證技術、帳戶鎖定機制、密碼具一定複雜度等。
二、個人資料顯示之隱碼機制。	系統呈現介面上，如有個資資訊，應評估使用情境，予以適當且一致性之遮蔽，以為資訊保護。
三、網際網路傳輸之安全加密機制。	當個人資料進行網路傳輸時，應採用加密機制，包含使用加密傳輸管道、資料加密傳輸等。

非公務機關安維辦法-資通系統安全措施(2/2)

管制措施	說明
四、個人資料檔案及資料庫之存取控制與保護監控措施。	• 針對個人資料檔案及資料庫之儲存，應適當加密。 • 存取時，應提供使用者識別、鑑別及身分驗證管理機制。 • 留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。
五、防止外部網路入侵對策。	針對可能來自於網路的入侵，採取相關的偵測或防護作為。 如個人電腦安裝防毒軟體、使用電子郵件過濾機制、設定網路防火牆、架構應用程式防火牆、採用入侵偵測及防禦機制或進階持續性威脅攻擊防禦措施等。
六、非法或異常使用行為之監控與因應機制。	針對資通系統或個資檔案之存取，留存相關日誌紀錄並定期檢視，或設置存取監控之系統化預警機制。

非公務機關安維辦法之系統安全措施

非公務機關安維辦法，

涉個資處理之資通系統必要安全措施

(目前6項之規劃項目是否足夠？)

除系統必要安全措施外，應視非公務機關業別情形，參考資安法相關規定，予適當要求，以強化個資保護機制

(如於業別內再予分級，參考資安法應辦事項增補規範內容，以應實務需求)

強化產業資安防護，進而保護個人資料

資安是持續精進的風險管理