資通安全責任等級分級及應辦事項說明

行政院資通安全處

107年11月

大綱

- 適用對象
- 分級辦法
- 應辦事項
- 資通系統防護需求分級原則
- 資通系統防護基準

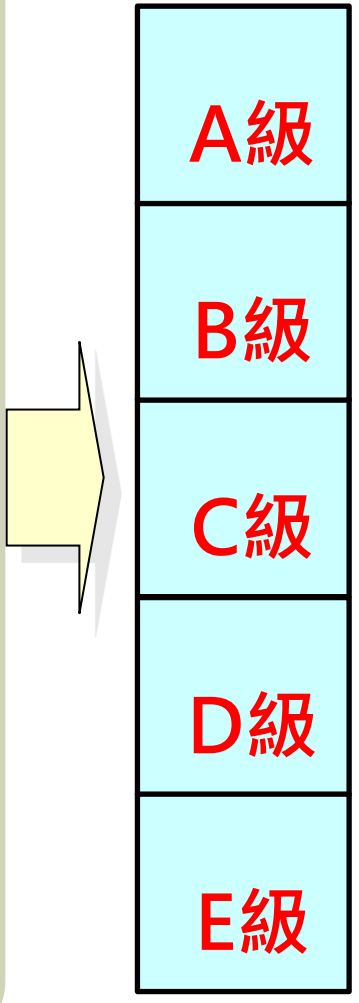
適用對象

依據資通安全管理法第三條第五、六款

- 公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。
- 特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

分級辦法_資安責任等級分級原則

涉及外交、國防、國土安全事項
公務機關涉及能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項
關鍵基礎設施服務，對社會公共利益、民心士氣，或民眾生命、身體、財產之影響
持有民眾或公務員個人資料檔案、國家機密、公務機關捐助或研發之敏感科學技術資訊
資通系統服務民眾之範圍
跨公務機關共用性資通系統之服務範圍
醫院分級



資安責任等級

符合二個以上之資通安全責任等級者，列為其符合之最高等級

資安責任等級(1/4)

分級原則	範圍	等級
業務涉及外交、國防或國土安全事項公務機關		A
業務涉及能源、水資源、通訊傳播、交通銀行與金融、緊急救援事項	全國	A
	區域性、地區性	
關鍵基礎設施提供者，其資通系統失效或受影響	將產生災難性或非常嚴重之影響	A
	將產生嚴重之影響	B
業務涉及國家機密		A
公務機關捐助或研發之敏感科學技術資訊		B
業務涉及民眾或公務員個人資料檔案之持有	全國	A
	區域性、地區性	B

資安責任等級(2/4)

分級原則	範圍	等級
民眾服務之資通系統之維運	全國	A
	區域性、地區性	B
跨公務機關共用性資通系統之維運	全國	A
	區域性、地區性	B
醫院分級	公立醫學中心	A
	公立區域醫院或地區醫院	B

資安責任等級(3/4)

C級機關	D級機關
維運自行或委外開發之資通系統	自行辦理資通業務，未維運自行或委外開發之資通系統

- 機關雖僅辦理PC採購與維護，因有自行辦理資通業務故應列為D級 (資通業務包含資通系統之維運及資通服務之提供等業務)

資安責任等級(4/4)

E級機關	
公務機關	特定非公務機關
無資通系統且未提供資通服務	
全部資通業務由其上級或監督機關兼辦或代管	全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關兼辦或代管

等級調整

- 公務機關提交或核定資通安全責任等級時，得考量對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級

等級核定(1/3)

- 提報機關
  - 行政院直屬機關、提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，備文報主管機關核定
  - 特定非公務機關由中央目的事業主管機關提報
  - 直轄市、縣（市）政府提交自身、所屬或監督之公務機關，與所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級，備文報主管機關核定
  - 直轄市及縣（市）議會、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會提交自身資通安全責任等級，由其所在區域之直轄市、縣（市）政府備文彙送主管機關核定

等級核定(2/3)

- 總統府、國家安全會議、立法院、司法院、考試院及監察院，核定自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，備文送主管機關備查
- 各機關內部單位，認有另列與該機關不同責任等級之必要者，得考量其業務性質另行認定。

等級核定(3/3)

- 提報時機
  - 本法通過當年提報完整資料後，應每二年再行提報完整資料
  - 組織或業務調整，致須變更原資通安全責任等級時
  - 有新設機關時

資通安全責任等級表_機關屬性

主屬性	公務機關	特定非公務機關
機關屬性	中央機關	關鍵基礎設施提供者
	地方機關	公營事業
	中央機關所屬機構	財團法人
	地方機關所屬機構	
	行政法人	

資通安全責任等級表_公務機關 (1/3)

分級判斷之類別	業務重要性與機敏性	資訊種類、數量及性質
次類別	業務涉及外交、國防或國土安全事項	業務涉及國家機密
	全國性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項	業務涉及公務機關所捐助或研發之敏感科學技術資訊之安全維護及管理
	區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項	全國性民眾或公務員個人資料檔案之持有
	關鍵基礎設施提供者，業務經中央目的事業主管機關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	區域性或地區性民眾個人資料檔案之持有
	關鍵基礎設施提供者，業務經中央目的事業主管機關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之影響	

資通安全責任等級表_公務機關 (2/3)

分級判斷之類別	資通系統規模及性質	機關層級	其他
次類別	全國性跨公務機關共用性資通系統之維運	公立醫學中心	無資通系統且未提供資通服務。
	區域性或地區性跨公務機關共用性資通系統之維運	公立區域醫院	屬公務機關，且其全部資通業務由其上級或監督機關兼辦或代管。
	全國性民眾服務之資通系統之維運	公立地區醫院	
	區域性或地區性民眾服務之資通系統之維運		
	維運自行或委外開發之資通系統		
	未維運自行或委外開發之資通系統，惟仍自辦資訊業務者		

資通安全責任等級表_公務機關 (3/3)

項次	OID	機關名稱	上級機關或監督機關	機關屬性	依資安責任等級分級辦法第4-8條調整等級			依資安責任等級分級辦法第9條符合之最高等級	依資安責任等級分級辦法第10條調整等級 (未調整者免填)		備考
					分級判斷之類別	納管理由	等級	等級	調整理由	調整後等級	
範例1	XXXXX.XXXXX.XXXX.XXXX	○○○○	○○○○	中央機關所屬機構	機關層級	公立醫學中心	A				
範例2	XXXXX.XXXXX.XXXX.XXXX	○○○○	○○○○	中央機關	業務重要性與機敏性	關鍵基礎設施提供者，業務經中央目的事業主管機關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之影響	B	A			同時符合二個以上之資通安全責任等級者
				中央機關	資通系統規模及性質	全國性跨公務機關共用性資通系統之維運	A				

資通安全責任等級表_特定非公務機關 (1/3)

分級判斷之類別	業務重要性與機敏性	資訊種類、數量及性質
次類別	業務涉及外交、國防或國土安全事項	業務涉及國家機密
	關鍵基礎設施提供者，業務經中央目的事業主管機關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	業務涉及公務機關所捐助或研發之敏感科學技術資訊之安全維護及管理
	關鍵基礎設施提供者，業務經中央目的事業主管機關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之影響	全國性民眾個人資料檔案之持有
		區域性或地區性民眾個人資料檔案之持有

資通安全責任等級表_特定非公務機關 (2/3)

分級判斷之類別	資通系統規模及性質	其他
次類別	全國性民眾服務之資通系統之維運	無資通系統且未提供資通服務。
	區域性或地區性民眾服務之資通系統之維運	屬特定非公務機關，且其全部資通業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關兼辦或代管。
	維運自行或委外開發之資通系統	
	未維運自行或委外開發之資通系統，惟仍自辦資訊業務者	

資通安全責任等級表_特定非公務機關 (3/3)

項次	OID	機關名稱	上級機關或監督機關	機關屬性	依資安責任等級分級辦法第4-8條調整等級			依資安責任等級分級辦法第9條符合之最高等級	依資安責任等級分級辦法第10條調整等級 (未調整者免填)		備考
					分級判斷之類別	納管理由	等級	等級	調整理由	調整後等級	
範例1	XXXXX.XXXXX.XX.XXXX	○○○○	○○○○	關鍵基礎設施提供者	業務重要性與機敏性	關鍵基礎設施提供者，業務經中央目的事業主管機關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	A				
範例2	XXXXX.XXXXX.XX.XXXX	○○○○	○○○○	公營事業	業務重要性與機敏性	關鍵基礎設施提供者，業務經中央目的事業主管機關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之影響	B	A			同時符合二個以上之資通安全責任等級者
				公營事業	資訊種類、數量及性質	全國性民眾個人資料檔案之持有	A				

應辦事項、資通系統防護分級

- 應辦事項：詳附表一至附表八
- 資通系統防護分級及防護基準：詳附件九及附表十
- 提報執行情形
  - 公務機關
    - 資通安全責任等級為A級或B級者，應依主管機關指定之方式，提報應辦事項之辦理情形
  - 特定非公務機關
    - 中央目的事業主管機關得要求所管，依指定之方式提報應辦事項之辦理情形

應辦事項_管理面

辦理項目	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內	1年內	2年內
資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入資訊安全管理系統，並於三年內完成第三方驗證；並持續維持其驗證有效性	2年內	2年內	2年內
業務持續運作演練	全部核心資通系統	每年1次	每2年1次	每2年1次
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專責人員(一年內)		專職(責)4人	專職(責)2人	專職(責)1人
資安治理成熟度評估(公務機關)		每年1次	每年1次	

應辦事項_技術面(1/2)

辦理項目	辦理內容	A	B	C
安全性檢測	全部核心資通系統網站安全弱點檢測	每年2次	每年1次	每2年1次
	全部核心資通系統系統滲透測試	每年1次	每2年1次	每2年1次
資通安全健診	網路架構檢視、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	每年1次	每2年1次	每2年1次
資通安全威脅偵測管理機制	完成威脅偵測機制建置，並持續維運	1年內	1年內	
	依主管機關指定之方式提交監控管理資料(公務機關)	V	V	

應辦事項_技術面(2/2)

辦理項目	辦理內容	A	B	C
資通安全防護(啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內	1年內	1年內
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆(WAF)	1年內	1年內	
	APT攻擊防禦	1年內		
政府組態基準	依主管機關公告之項目，完成政府組態基準導入作業，並持續維運(公務機關)	1年內	1年內	

應辦事項_認知與訓練

辦理項目	辦理內容	A	B	C
資通安全教育訓練	資通安全及資訊人員，每年接受之資通安全專業課程訓練或資通安全職能訓練	4名各12小時	2名各12小時	1名12小時
	一般使用者及主管，每人每年至少接受之一般資通安全教育訓練	3小時	3小時	3小時
資通安全專業證照及職能訓練證書	初次受核定或等級變更後之一年內，資通安全專職(責)人員總計應持有之資通安全專業證照，並持續維持證照之有效性	4張	2張	1張
	資通安全專職人員總計應持有之資通安全職能評量證書，並持續維持證照之有效性(公務機關)	4張	2張	1張

應辦事項_D級、E級

面向 作業 名稱 等級	技術面	認知與訓練
	資通安全防護	資通安全教育訓練
D級	初次受核定或等級變更後之一年內，完成下列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 一、防毒軟體 二、網路防火牆 三、具有郵件伺服器者，應備電子郵件過濾機制	一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練
E級		一般使用者及主管，每人每年至少接受三小時以上之一般資通安全教育訓練

附加說明(1/3)

- 共用性系統者
  - ✓由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統
- 「公正第三方驗證」
  - ✓第三方係指通過我國標準法主管機關委託機構認證之機構
- 資通安全專職人員
  - ✓指應全職執行資通安全業務者

附加說明(2/3)

- 資通安全健診
  - ✓公務機關得採取經主管機關認可之其他具有同等或以上效用之措施
  - ✓特定非公務機關得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施
- 資通安全專業證照
  - ✓指由主管機關認可之國內外發證機關（構）所核發之資通安全證照
- 關鍵基礎設施提供者之防護基準
  - ✓中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂該基準，並報請主管機關核定後，依其規定辦理

附加說明(3/3)

- 核心資通系統
  - ✓公務機關依其組織法規，足認該業務為機關核心權責所在
  - ✓公營事業及政府捐助之財團法人之主要服務或功能
  - ✓各機關維運、提供關鍵基礎設施所必要之業務
  - ✓各機關依資通安全責任等級分級辦法第四條(A級分級原則)第一款至第五款及第五條(B級分級原則)第一款至第四款涉及之業務
    - ➢國家機密
    - ➢外交、國防或國土安全事項
    - ➢全國、區域性、地區性之民眾服務或跨公務機關共用性資通系統
    - ➢全國、區域性、地區性之民眾或公務員個人資料檔案之持有
    - ➢全國、區域性、地區性之CII
    - ➢公務機關捐助或研發之敏感科學技術資訊之安全維護及管理

資通系統防護需求分級原則(1/4)

等級 / 構面	普	中	高
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有限之影響。	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非常嚴重或災難性之影響。

資通系統防護需求分級原則(2/4)

構面＼等級	普	中	高
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有限之影響。	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非常嚴重或災難性之影響

資通系統防護需求分級原則(3/4)

構面 \ 等級	普	中	高
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有限之影響	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非常嚴重或災難性之影響

資通系統防護需求分級原則(4/4)

構面＼等級	普	中	高
法律遵循性	其他資通系統設置或運作於法令有相關規範之情形。	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。	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。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

資通系統防護基準(1/4)

構面	措施內容	控制措施
7	29	75

高	中	普
75	57	31

資通系統防護基準(2/4)

構面	措施內容	控制措施
存取控制(3)	帳號管理	7
	最小權限	1
	遠端存取	4
稽核與可歸責性(6)	稽核事件	4
	稽核紀錄內容	2
	稽核儲存容量	1
	稽核處理失效之回應	2
	時戳及校時	2
	稽核資訊之保護	3
營運持續計畫(2)	系統備份	5
	系統備援	2

資通系統防護基準(3/4)

構面	措施內容	控制措施
識別與鑑別(5)	內部使用者之識別與鑑別	2
	身分驗證管理	7
	鑑別資訊回饋	1
	加密模組鑑別	1
	非內部使用者之識別與鑑別	1
系統與服務獲得 (8)	系統發展生命週期需求階段	1
	系統發展生命週期設計階段	2
	系統發展生命週期開發階段	5
	系統發展生命週期測試階段	2
	系統發展生命週期部署與維運階段	3
	系統發展生命週期委外階段	1
	獲得程序	1
	系統文件	1

資通系統防護基準(4/4)

構面	措施內容	控制措施
系統與通訊保護(2)	傳輸之機密性與完整性	4
	資料儲存之安全	1
系統與資訊完整性(3)	漏洞修復	2
	資通系統監控	3
	軟體及資訊完整性	4

Q&A

1. 國(公)營事業全公司是否視為一體
   - 國(公)營事業全公司視為一體
   - 公務機關辦理資通安全責任等級之提交或核定，就公務機關或特定非公務機關內之單位，有另列與該機關不同等級之必要者，得考量其業務性質，依第四條至十條認定之
2. 醫院資安責任等級應提報主管機關或中央目的主管機關？
   - 公立醫療機構(或同時為CI)-上級或監督機關。
   - 特定非公務機關(CI)-衛福部。

Q&A

3. 教育體系ISMS是否屬於其他公務機關自行發展並經主管機關認可之標準？
   - 是，其第三方驗證亦同。
4. 機關僅辦理PC採購與維護，其資安責任等級為何？
   - 因有自行辦理資通業務故應列為D級

謝謝聆聽
敬請指教

附件

資通系統防護基準(1/12)

控制措施	系統防護需求分級		
	普	中	高
存取控制(Access Control)(3)			
帳號管理	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. 已逾期之臨時或緊急帳號應刪除或禁用 3.資通系統閒置帳號應禁用 4.定期審核資通系統帳號之建立、修改、啟用、禁用及刪除	1.執行等級「中」之所有控制措施 2.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 3.應依機關規定之情況及條件，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

資通系統防護基準(2/12)

控制措施	系統防護需求分級		
	普	中	高
最小權限		採用最小權限原則，僅允許使用者(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	
遠端存取	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	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 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	

資通系統防護基準(3/12)

控制措施	系統防護需求分級		
	普	中	高
稽核與可歸責性(6)			
稽核事件	1.依規定時間週期及紀錄留存政策，保留稽核紀錄 2.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 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.應定期審查稽核事件	
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，應依需求納入額外的資訊	

資通系統防護基準(4/12)

控制措施	系統防護需求分級		
	普	中	高
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	資通系統應在稽核處理失效時，應採取適當之行動		1.執行等級「中」及「普」之所有控制措施 2.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
時戳及校時	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)	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	
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

資通系統防護基準(5/12)

控制措施	系統防護需求分級		
	普	中	高
營運持續計畫(Contingency Planning)(2)			
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，以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
系統備援		1.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 2.原服務中斷時，於可容忍時間內，由備援設備取代提供服務	

資通系統防護基準(6/12)

控制措施	系統防護需求分級		
	普	中	高
識別與鑑別(5)			
內部使用者之識別與鑑別	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		1.執行等級等級「中」及「普」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
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3次後，至少15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	

資通系統防護基準(7/12)

控制措施	系統防護需求分級		
	普	中	高
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	
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的程序)		

資通系統防護基準(8/12)

控制措施	系統防護需求分級		
	普	中	高
系統與服務獲得 (8)			
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		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	
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		1.執行等級「中」及「普」之所有控制措施 2.執行「源碼掃描」安全檢測 3.具備系統嚴重錯誤之通知機制
系統發展生命週期測試階段	執行「弱點掃描」安全檢測		1.執行等級「中」及「普」之所有控制措施 2.執行「滲透測試」安全檢測

資通系統防護基準(9/12)

控制措施	系統防護需求分級		
	普	中	高
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.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	
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、測試以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		

資通系統防護基準(10/12)

控制措施	系統防護需求分級		
	普	中	高
系統與通訊保護(2)			
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的演算法 3.支援演算法的最大長度金鑰 4.加密金鑰或憑證週期性更換 5.伺服器端之金鑰保管應製定管理規則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

資通系統防護基準(11/12)

控制措施	系統防護需求分級		
	普	中	高
系統與資訊完整性(3)			
漏洞修復	系統的漏洞修復應測試有效性及潛在影響，並定期更新	1.執行等級「普」之所有控制措施。 2.定期確認資通系統相關漏洞修復之狀態	
資通系統監控	發現資通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.監控資通系統，以偵測攻擊和未授權之連線，並識別資通系統之未授權使用	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
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.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	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

資通系統防護基準(12/12)

- 靜置資訊，指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊
- 特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之前提下，訂定其所管特定非公務機關之系統防護基準