防護基準作業説明

緣起I

* 政府機關（構）資通安全責任等級分級作業規定

學術機構部分

各級學校	A級：凡涉及各相關機關委託研究具國家安全機密性或敏感性之學校 B級：各大學 C級：各學院、專科學校及各高中職（含）以下學校
學術研究機構與網路中心	B級：臺灣學術網路各區域網路中心暨各直轄市、縣（市）教育網路中心 C級：教育部所屬研究機構

緣起II

增修項目：以紅色字體顯示

面向 / 作業名稱 / 等級	政策面	管理面			
	資訊系統分級	ISMS推動作業	資安專責人力	稽核方式	業務持續運作演練
A	一、完成資訊系統分級(104年底前) 二、完成資訊系統資安防護基準要求(105年底前)	一、全部核心資訊系統完成ISMS導入(105年底前) 二、全部核心資訊系統通過第三方驗證(106年底前)	指派資安專責人力2人	每年至少2次內稽	每年至少辦理1次核心資訊系統持續運作演練
B	一、完成資訊系統分級(104年底前) 二、完成資訊系統資安防護基準要求(105年底前)	一、至少2項核心資訊系統完成ISMS導入(106年底前) 二、至少2項核心資訊系統通過第三方驗證(107年底前)	指派資安專責人力1人	每年至少1次內稽	每2年至少辦理1次核心資訊系統持續運作演練
C	依各主管機關規定	自行成立推動小組規劃作業	依各主管機關規定	依各主管機關規定	依各主管機關規定

教育部　函

機關地址：10051臺北市中山南路5號
承 辦 人：林文信
聯絡電話：02-7712-9092
電子郵件：：ansel@mail.moe.gov.tw

受 文 者：

發文日期：中華民國108年03月06日
發文字號：臺教資(四)字第1080032874號
速　　別：普通件
密等及解密條件或保密期限：
附　　件：(1件) 行政院原函(1080032874_Attach1.pdf，共一個電子檔案) 1081291600_1_1080032874_Attach1.pdf （附件一）

主旨：轉知行政院函，有關「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」自即日停止適用，請查照。

說明：依據行政院108年3月5日院臺護字第1080166960號函辦理。

緣起III
資通安全管理法-子法

- 機關資安責任等級分級提報

資通安全責任等級分級辦法

- 訂定

資通
細則

- 提出資安維護計劃實施情形
- 進行稽核

特定非公務機關資通安全維護計畫

第 2 條　公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。

- 附表九 資通系統防護需求分級原則.PDF
- 附表十 資通系統防護基準.PDF

- 提出
- 情資

資通安全情資分享辦法

- 人員獎懲

公務機關所屬人員資通安全事項獎懲辦法

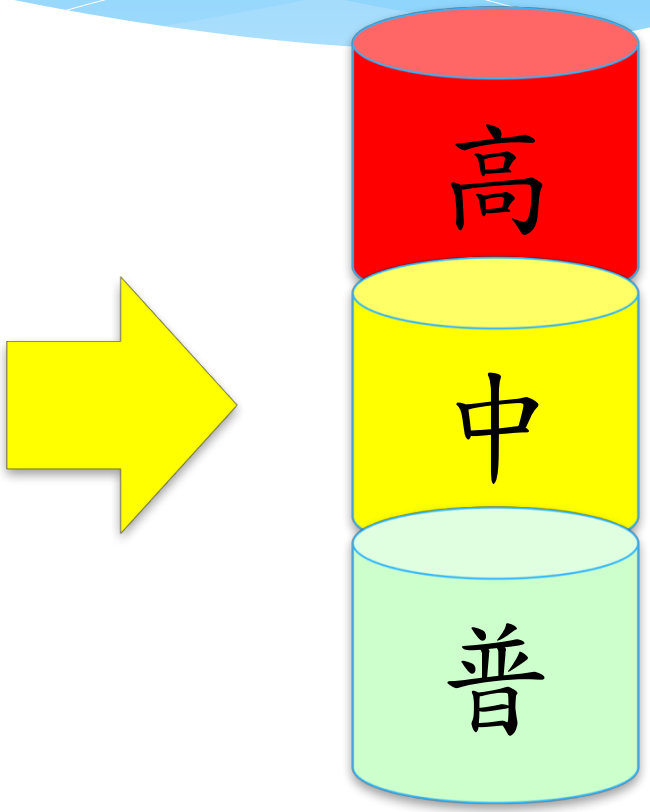
- 通報資安事件
- 提出事件調查改善報告

資通安全事件通報及應變辦法

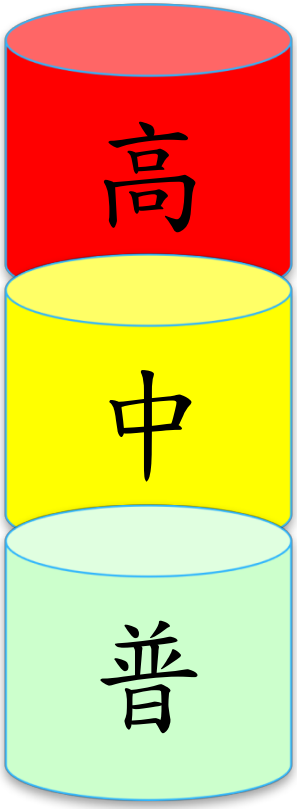
資通系統防護需求分級原則

附表九 資通系統防護需求分級原則

構面 \ 防護需求等級	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。



資通系統防護需求分級原則



存取控制-3（A.9）
稽核與可歸責性-6（A.12）
營運持續計畫-2（A.17）
識別與鑑別-5（A.13）
系統與服務獲得-8（A.14）
系統與通訊保護-2（A.13）
系統與資訊完整性-3（A.12）

共7個控制面向；29項控制措施

資通系統防護基準項目說明

資通系統防護基準項目說明
存取控制（3）

控制措施	系統防護需求分級		
	普級	中級	高級
存取控制(3)			
帳號管理	建立帳號管理機制，包括帳號之申請、開通、停用及刪除之程序。	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、定期審查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。	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。Session time out 二、應依據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。

資通系統防護基準項目說明
存取控制（3）

控制措施	系統防護需求分級		
	普級	中級	高級
存取控制(3)			
最小權限	無要求。	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。	

資通系統防護基準項目說明
存取控制（3）

控制措施	系統防護需求分級		
	普級	中級	高級
存取控制(3)			
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。	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。	

資通系統防護基準項目說明
稽核與可歸責性（6）

控制措施	系統防護需求分級		
	普級	中級	高級
稽核與可歸責性(6)			
稽核事件	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。	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。	

資通系統防護基準項目說明
稽核與可歸責性（6）

控制措施	系統防護需求分級		
	普級	中級	高級
稽核與可歸責性(6)			
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。	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。	

資通系統防護基準項目說明
稽核與可歸責性（6）

控制措施	系統防護需求分級		
	普級	中級	高級
稽核與可歸責性(6)			
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。		

資通系統防護基準項目說明
稽核與可歸責性（6）

控制措施	系統防護需求分級		
	普級	中級	高級
稽核與可歸責性(6)			
稽核處理失效之回應	資通系統於稽核處理失效時，應採取適當之行動。		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。

資通系統防護基準項目說明
稽核與可歸責性（6）

控制措施	系統防護需求分級		
	普級	中級	高級
稽核與可歸責性(6)			
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）。	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。	

資通系統防護基準項目說明
稽核與可歸責性（6）

控制措施	系統防護需求分級		
	普級	中級	高級
稽核與可歸責性(6)			
稽核資訊之保護	對稽核紀錄之存取管理，僅限有權限之使用者。	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。	一、定期備份稽核紀錄至原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。

資通系統防護基準項目說明
營運持續計畫（2）

控制措施	系統防護需求分級		
	普級	中級	高級
營運持續計畫(2)			
系統備份	一、訂定系統可容忍資料損失之時間要求。RPO 二、執行系統源碼與資料備份。	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、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。異地備份 三、等級「中」之所有控制措施。

資通系統防護基準項目說明
營運持續計畫（2）

控制措施	系統防護需求分級		
	普級	中級	高級
營運持續計畫(2)			
系統備援	無要求。	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。RTO 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。	

資通系統防護基準項目說明
識別與鑑別（5）

控制措施	系統防護需求分級		
	普級	中級	高級
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，禁止使用共同帳號。		一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」、「普」之所有控制措施。

資通系統防護基準項目說明
識別與鑑別（5）

控制措施	系統防護需求分級		
	普級	中級	高級
識別與鑑別(5)			
身分驗證管理	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、具備帳戶銷定機制，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。	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。	

資通系統防護基準項目說明
識別與鑑別（5）

控制措施	系統防護需求分級		
	普級	中級	高級
識別與鑑別(5)			
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		

資通系統防護基準項目說明
識別與鑑別（5）

控制措施	系統防護需求分級		
	普級	中級	高級
識別與鑑別(5)			
加密模組鑑別	無要求。	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。	

資通系統防護基準項目說明
識別與鑑別（5）

控制措施	系統防護需求分級		
	普級	中級	高級
識別與鑑別(5)			
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）。		

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
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（機密性、完整性、可用性），以檢核表方式進行確認。		

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
系統發展生命週期設計階段	無要求。	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。	

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
系統發展生命週期開發階段	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。		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」、「普」之所有控制措施。

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
系統發展生命週期測試階段	執行「弱點掃描」安全檢測。		一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
系統發展生命週期部署與維運階段	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。	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。	

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
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。		

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
獲得程序	無要求。	開發、測試及正式作業環境應為區隔。	

資通系統防護基準項目說明
系統與服務獲得（8）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與服務獲得(8)			
系統文件	應儲存與管理系統發展生命週期之相關文件。		

資通系統防護基準項目說明
系統與通訊保護（2）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與通訊保護(2)			
傳輸之機密性與完整性	無需求。		一、資通系統應採取加密機制，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管理規範及實施應有之安全防護措施。

資通系統防護基準項目說明
系統與通訊保護（2）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與通訊保護(2)			
資料儲存之安全	無需求。		靜置資訊及相關具保護需求之機密資訊應加密儲存。

註：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。

資通系統防護基準項目說明
系統與資訊完整性（3）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與資訊完整性(3)			
漏洞修復	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	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。	

資通系統防護基準項目說明
系統與資訊完整性（3）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與資訊完整性(3)			
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。	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。	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。

資通系統防護基準項目說明
系統與資訊完整性（3）

控制措施	系統防護需求分級		
	普級	中級	高級
系統與資訊完整性(3)			
軟體及資訊完整性	無要求。	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。	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。