

教育體系資通安全責任等級分級作業規定(草案)

條文	說明
一、教育部(以下簡稱本部)為因應資通安全管理法施行，明確規範教育體系各級公私立學校、教育及研究機構(以下簡稱各學校)資通安全責任等級分級作業流程，透過資通安全管理，以防範教育體系潛在資安威脅，特訂定教育體系資通安全責任等級分級作業規定(以下簡稱本規定)。	明定本規定訂定之目的。
二、本規定適用對象如下： (一)全國各級學校及其附設機構。 (二)臺灣學術網路各區域網路中心、各直轄市及縣(市)教育網路中心。 (三)接受公務機關及學校委託辦理各類招生入學、分發、考試、評鑑等相關工作之團體、機構或財團法人。	明定本規定適用對象。
三、前點第一款全國各級學校其附設醫院及其分院，其資通安全相關作業事宜，依資通安全管理法及衛生福利部相關規定辦理，不適用本規定。	明定大學附設醫院及其分院不適用本規定。
四、各學校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。	一、明定各學校之資通安全責任等級，由高至低，分為A級至E級。 二、有關資通安全責任等級之區分原則，依第五點至九點規定為之。
五、各學校有下列之情形者，其資通安全責任等級為A級： (一)接受委託辦理全國性考試、測驗，且持有全國性考生個人資料檔案之團體或財團法人。 (二)涉及公務機關委託研究國家安全、機密之學校，其領域如下： 1. 涉及國家安全資訊、國家機密資訊之領域： (1)國土調查資訊。 (2)水域調查資訊。 (3)災害防救資訊。 (4)大陸及外交情資。	一、明定各機關資通安全責任等級應列為A級之情形。 二、第一款所稱全國性考試、測驗指大學入學考試、技專校院入學測驗及國中教育會考等。 三、第二款之領域指本部100年1月7日臺高(一)字第1000001237號公告之專業領域。

(5)軍事計畫、軍事行動資訊。 2. 涉及國家安全技術、國家機密技術領域： (1)國防科技、軍事武器及元件製造技術。 (2)航太關鍵技術。 (3)衛星遙測關鍵技術。 (4)核子工程技術。 (5)資通安全、光電、IC、資通訊及精密機械等自主研發或關鍵技術。 (6)關鍵材料之製造技術。 (7)能源科技之關鍵技術。 (8)農業品種改良、栽培及繁殖之關鍵技術。 (9)醫學、藥學及生物科技之關鍵技術。 3. 各學校符合資通安全責任等級分級辦法（以下簡稱分級辦法）第四條規定者。	
六、各學校有下列之情形者，其資通安全責任等級為B級： (一) 各公私立大學。 (二) 各學校辦理聯合招生組成之聯合會及其附設機構，辦理入學分發、甄選等相關招生作業，且持有區域性、地區性學生個人資料檔案者。 (三) 各學校涉及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者。 (四) 臺灣學術網路各區域網路中心、各直轄市及縣（市）教育網路中心。 (五) 各學校符合分級辦法第五條規定者。	一、考量各大學業務涉及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，爰其資通安全責任等級為B級。 二、考量招生為各大學核心業務，各大學為辦理招生或聯合招生，組成大學招生委員會或聯合會及其附設機構，辦理入學分發、甄選等相關招生業務，且持有區域性、地區性學生個資之單位，其等級與各大學一致為B級。 三、考量臺灣學術網路各區域網路中心、各直轄市及縣（市）教育網路中心業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運，爰其資通安全責任等級為B級。
七、各學校有下列之情形者，其資通安全責任等級為C級： (一) 各公私立學院及專科學校。 (二) 各公立高級中等以下學校維運自行或委外開發之資通系統，且由分級辦法第三條第	明定各學校資通安全責任等級應列為C級之情形。

一項至第二項之公務機關（本部、直轄市、縣（市）政府，以下簡稱提交機關）依分級辦法第六條提交其資通安全責任等級為 C 級，經行政院核定者。 （三）各學校附設機構維運自行或委外開發之資通系統者。	
八、各學校有下列之情形者，其資通安全責任等級為 D 級： （一）第一類： 1. 各公立高級中等以下學校維運自行或委外開發之資通系統，惟其全部核心資通系統已向上集中由其上級或監督機關維運，由其提交機關依分級辦法第十條第四款調整其責任等級為 D 級，經行政院核定者。 2. 各私立高級中等以下學校維運自行或委外開發之資通系統者。 （三）第二類：各學校自行辦理資通業務，未維運資通系統者。	考量高級中等以下學校經費資源較少，為鼓勵學校資通系統向上集中，公立學校其全部核心資通系統已向上集中，由其上級機關維運者，其資通安全風險較低，公立學校得由其依提交機關依分級辦法第十條第四款調整為 D 級，因其尚須維運非核心資通系統，仍須辦理相關資安防護，爰增加第一款規定，私立高級中等以下學校如維運資通系統者，依第一款規定辦理。
九、各學校有下列之情形者，其資通安全責任等級為 E 級： （一）各學校無維運資通系統且未提供資通服務。 （二）各學校之全部資通業務由其上級或監督機關兼辦或代管者。 （三）各級學校之分校、分部全部資通業務由其學校本校兼辦或代管者。 （四）大學附屬（設）各級學校之全部資通業務由其隸屬大學兼辦或代管者。	各學校其資通系統、資通業務均由其上級機關、學校兼辦或代管者，其責任等級為 E 級。
十、各學校依本分級原則之規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。	為避免各學校依第五點至第九點規定認定資通安全責任等級時，可能有符合二個以上之資通安全責任等級之情形，爰明定有前開情形者，應列為其符合之最高等級。
十一、第八點第一款所稱核心資通系統，指資通安全管理法施行細則第	明定第八點各學校之核心資通系統。

七條第二項之核心資通系統（如應用於全校校務行政及教學等重要業務之電子郵件服務系統、學籍系統及其他涉及持有學生或教職員個人資料檔案資通系統等）。	
十二、各學校應依其資通安全責任等級，辦理附表一至附表六之事項。各學校自行或委外開發之資通系統應依附表七所定資通系統防護需求分級原則完成資通系統分級，並依附表八所定資通系統防護基準執行控制措施。	明定各學校其資通安全責任等級應辦事項。

附表一 資通安全責任等級 A 級之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	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，依附表七完成資通系統分級，並完成附表八之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	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，或教育體系資通安全暨個人資料管理規範，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人；公立學校應以專職人員配置之。
	內部資通安全稽核		每年辦理二次。
	業務持續運作演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		公立學校須每年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理二次。
		系統滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		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	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，臺灣學術網路連線單位得結合臺灣學術網路資安監控系統。
	政府組態基準		公立學校初次受核定或等級變更後之一年內，依本部公告之項目，完成政府組態基準導入作業，並持續維運。
	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
		網路防火牆	
		具有郵件伺服器	

		者，應備電子郵件過濾機制	要更新或升級。
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
		進階持續性威脅攻擊防禦措施	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少四名人員各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，資通安全專職人員總計應持有四張以上「資通安全專業證照」及四張以上「資通安全職能評量證書」；私立學校應持有四張以上「資通安全專業證照」或「資通安全職能評量證書」，並持續維持證照、證書之有效性。	

備註：

- 一、資通系統之性質為共用性系統者，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。
- 二、「公正第三方驗證」所稱第三方，指教育機構資安驗證中心或通過我國標準法主管機關委託機構認證之機構。
- 三、各學校辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經本部認可之其他具有同等或以上效用之措施。
- 四、臺灣學術網路資安監控系統，指北區教育學術資訊安全監控中心（N-ASOC）、南區教育學術資訊安全監控中心（S-ASOC）、縣市教育網路中心迷你資訊安全維運中心（MINI-SOC）、臺灣學術網路危機處理中心（TACERT）。
- 五、資通安全專業證照，指由本部認可之國內外發證機關（構）所核發之資通安全證照。

附表二 資通安全責任等級 B 級之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	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，依附表七完成資通系統分級，並完成附表八之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	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，或教育體系資通安全暨個人資料管理規範，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；公立學校應以專職人員配置之。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	資安治理成熟度評估		公立學校須每年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		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	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，臺灣學術網路連線單位得結合臺灣學術網路資安監控系統。
	政府組態基準		公立學校初次受核定或等級變更後之一年內，依本部公告之項目，完成政府組態基準導入作業，並持續維運。
	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
		網路防火牆	
		具有郵件伺服器	

		者，應備電子郵件過濾機制	要更新或升級。
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少二名人員各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，資通安全專職人員總計應持有二張以上「資通安全專業證照」及二張以上「資通安全職能評量證書」；私立學校應持有二張以上「資通安全專業證照」或「資通安全職能評量證書」，並持續維持證照、證書之有效性。	

備註：

- 一、資通系統之性質為共用性系統者，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。
- 二、「公正第三方驗證」所稱第三方，指通過教育機構資安驗證中心或我國標準法主管機關委託機構認證之機構。
- 三、各學校辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經本部認可之其他具有同等或以上效用之措施。
- 四、臺灣學術網路資安監控系統，指北區教育學術資訊安全監控中心（N-ASOC）、南區教育學術資訊安全監控中心（S-ASOC）、縣市教育網路中心迷你資訊安全維運中心（MINI-SOC）、臺灣學術網路危機處理中心（TACERT）。
- 五、資通安全專業證照，指由本部認可之國內外發證機關（構）所核發之資通安全證照。

附表三 資通安全責任等級 C 級之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	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，依附表七完成資通系統分級，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，完成附表八之控制措施。
	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 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，或教育體系資通安全暨個人資料管理規範，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；公立學校應以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		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	
	資通安全防護	目錄伺服器設定及防火牆連線設定檢視	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。
		防毒軟體	
		網路防火牆	
認知與訓練	資通安全教育訓練	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	每人每年接受三小時以上之一般資通

		管	安全教育訓練。
	資通安全專業證照及職能訓練證書	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「資通安全專業證照」及一張以上「資通安全職能評量證書」；私立學校應持有一張以上「資通安全專業證照」或「資通安全職能評量證書」，並持續維持證照、證書之有效性。

備註：

- 一、資通系統之性質為共用性系統者，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。
- 二、各學校辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經本部認可之其他具有同等或以上效用之措施。
- 三、資通安全專業證照，指由本部認可之國內外發證機關（構）所核發之資通安全證照。

附表四 資通安全責任等級 D 級第一類之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	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，依附表七完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性。
	內部資通安全稽核		結合學校內部管理機制，每年辦理一次資通安全自我檢查作業。
	資通安全專責人員		各學校得配置一人。
技術面	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		具有伺服器主機者，應檢視伺服器主機惡意活動	
		具有目錄伺服器者，應檢視目錄伺服器設定	
		具有防火牆者，應檢視防火牆連線設定	
	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一般資通安全教育訓練。

備註：

- 一、各學校辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經本部認可之其他具有同等或以上效用之措施。

附表五 資通安全責任等級 D 級第二類之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
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一般資通安全教育訓練。

附表六 資通安全責任等級 E 級之各學校應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
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一般資通 安全教育訓練。

附表七 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。

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、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。

附表八 附表十 資通系統防護基準

系統防護需求 分級		高	中	普
控制措施	措施內容			
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。
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。
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	內部使用者之識別與鑑別	一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	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。	
	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。	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	

		三、等級「普」之所有控制措施。		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。
	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。		
	系統發展生命週期設計階段	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。		無要求。
	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。	四、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。		
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。 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护措施。	無要求。	無要求。
	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。
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	一、資通系統應採用自	一、監控資通系統，以	發現資通系統有被入侵

	統監控	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。	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。	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。

備註：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。