資通安全責任等級分級辦法

- 第一條 本辦法依資通安全管理法(以下簡稱本法)第七條 第一項規定訂定之。
- 第二條 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。
- 第三條 主管機關應每二年核定自身資通安全責任等級。

行政院直屬機關應每二年提交自身、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, 報主管機關核定。

直轄市、縣(市)政府應每二年提交自身、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,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應每二年提交自身資通安全責任等級,由其所在區域之直轄市、縣(市)政府彙送主管機關核定。

總統府、國家安全會議、立法院、司法院、考試院 及監察院應每二年核定自身、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,送主管機 關備查。

各機關因組織或業務調整,致須變更原資通安全責任等級時,應即依前五項規定程序辦理等級變更;有新設機關時,亦同。

第一項至第五項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, 認有另列與該機關不同等級之必要者,得考量其業務性 質,依第四條至第十條規定認定之。

第四條 各機關有下列情形之一者,其資通安全責任等級為 A級:

一、業務涉及國家機密。

- 二、業務涉及外交、國防或國土安全事項。
- 三、業務涉及全國性民眾服務或跨公務機關共用性 資通系統之維運。
- 四、業務涉及全國性民眾或公務員個人資料檔案之 持有。
- 五、屬公務機關,且業務涉及全國性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。
- 六、屬關鍵基礎設施提供者,且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性,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。

七、屬公立醫學中心。

第五條 各機關有下列情形之一者,其資通安全責任等級為 B級:

- 一、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。
- 二、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。
- 三、業務涉及區域性或地區性民眾個人資料檔案之 持有。
- 四、屬公務機關,且業務涉及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。
- 五、屬關鍵基礎設施提供者,且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性,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影響。

六、屬公立區域醫院或地區醫院。

- 第六條 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。
- 第七條 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。
- 第八條 各機關有下列情形之一者,其資通安全責任等級為 E級:
 - 一、無資通系統且未提供資通服務。
 - 二、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。
 - 三、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。
- 第九條 各機關依第四條至前條規定,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。
- 第十條 各機關之資通安全責任等級依前六條規定認定之。 但第三條第一項至第五項之公務機關提交或核定資通安 全責任等級時,得考量下列事項對國家安全、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:
 - 一、業務涉及外交、國防、國土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者,其中斷或受妨礙。
 - 二、業務涉及個人資料、公務機密或其他依法規或 契約應秘密之資訊者,其資料、公務機密或其 他資訊之數量與性質,及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。
 - 三、各機關依層級之不同,其功能受影響、失效或中斷。
 - 四、其他與資通系統之提供、維運、規模或性質相

關之具體事項。

第十一條 各機關應依其資通安全責任等級,辦理附表一至 附表八之事項。

> 各機關自行或委外開發之資通系統應依附表九所 定資通系統防護需求分級原則完成資通系統分級,並 依附表十所定資通系統防護基準執行控制措施;關鍵 基礎設施提供者之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 擬訂防護基準,報請主管機關核定後,依其規定辦理。

> 各機關辦理附表一至附表八所定事項或執行附表 十所定控制措施,因技術限制、個別資通系統之設計、 結構或性質等因素,就特定事項或控制措施之辦理或 執行顯有困難者,得經第三條第二項至第四項所定其 等級提交機關或同條第五項所定其等級核定機關同意, 並報請主管機關備查後,免執行該事項或控制措施。

公務機關之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,提報第一項及第二項事項 之辦理情形。

中央目的事業主管機關得要求所管特定非公務機關,依其指定之方式提報第一項及第二項事項之辦理情形。

第十二條 本辦法之施行日期,由主管機關定之。

附表一 資通安全責任等級 A 級之公務機關應辦事項

 で で	制度面向	辨理項目	辦理項目細項	辦理內容
管理面 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,並完成附表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。 で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。 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;須以專職人員配置之。內部資通安全稽核每年辦理二次。業務持續運作演練會企業核心資通系統每年辦理一次。每年辦理一次。每年辦理一次。 資安治理成熟度評估 全部核心資通系統每年辦理一次。每年辦理一次。 安全性檢測 檢測	四尺四円	が下土穴口	/ / 生况口篇点	* * * * * * * * * * * * * * * * * * * *
管理面				
表十之控制措施;其後應每年至少檢視一次資通系統分級妥適性。 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。 初次受核定或等級變更後之一年內,配置四人;須以專職人員配置之。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 每年辦理一次。		咨诵系统分级	及防護其進	
 禮田 管理面 資訊安全管理系統之導入及通資通系統導入 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。 有通安全專責人員 內部資通安全稽核 實務持續運作演練 安全的核定或等級變更後之一年內,配置四人;須以專職人員配置之。 內部資通安全稽核 實務持續運作演練 全部核心資通系統每年辦理一次。 每年辦理一次。 每年辦理一次。 每年辦理一次。 每年辦理一次。 		负地尔沁刀 淡	及历或坐干	
管理面				
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 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。 初次受核定或等級變更後之一年內,配置四人;須以專職人員配置之。 內部資通安全稽核 每年辦理二次。				
管理面				
管理面				7
過公止第三万之驗證	答理面	資訊安全管理	! 系統之導入及通	
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。 初次受核定或等級變更後之一年內,配置四人;須以專職人員配置之。 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 每年辦理一次。 網站安全弱點 会部核心資通系統每年辦理二次。	各基画	過公正第三方	之驗證	
證,並持續維持其驗證有效性。 初次受核定或等級變更後之一年內, 配置四人;須以專職人員配置之。 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 每年辦理一次。 日本 日				
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;須以專職人員配置之。 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 每年辦理一次。 網站安全弱點 会部核心資通系統每年辦理二次。				
育通安全專責人員 配置四人;須以專職人員配置之。 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 每年辦理一次。 報站安全弱點 全部核心資通系統每年辦理二次。				
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 每年辦理一次。 網站安全弱點 全部核心資通系統每年辦理二次。		資通安全專責	人員	
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 每年辦理一次。 網站安全弱點 全部核心資通系統每年辦理二次。		內部咨诵安全		
資安治理成熟度評估 每年辦理一次。 網站安全弱點 安全性檢測 檢測 全部核心資通系統每年辦理二次。				
網站安全弱點 全部核心資通系統每年辦理二次。 檢測				
安全性檢測檢測全部核心貧通系統每年辦理二次。		负文化在 从然	1	41 m/4 - X
		安全性檢測		全部核心資通系統每年辦理二次。
系統渗透測試 全部核心資通系統每年辦理一次。				全部核心資通系統每年辦理一次。
網路架構檢視			網路架構檢視	
網路惡意活動			網路惡意活動	
檢視			檢視	
使用者端電腦			使用者端電腦	
資通安全健 惡意活動檢視 每年辦理一次。		資通安全健	惡意活動檢視	每年辦理一次。
診		診	伺服器主機惡	
意活動檢視			意活動檢視	
目錄伺服器設	14 カー エ		目錄伺服器設	
技術面 定及防火牆連	投術 由		定及防火牆連	
線設定檢視			線設定檢視	
初次受核定或等級變更後之一年內,				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,並持續維運		ウロムスドな	/ h m l 於 -四 l l l l l l l	完成威脅偵測機制建置,並持續維運
育通安全威脅偵測管理機制 及依主管機關指定之方式提交監控管		貧迪安全風智	偵測官埋機制	及依主管機關指定之方式提交監控管
理資料。				理資料。
初次受核定或等級變更後之一年內,				初次受核定或等級變更後之一年內,
		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。				態基準導入作業,並持續維運。
資通安全 防毒軟體 初次受核定或等級變更後之一年內,		資通安全	防毒軟體	初次受核定或等級變更後之一年內,
防護 網路防火牆 完成各項資通安全防護措施之啟用,		防護	網路防火牆	完成各項資通安全防護措施之啟用,

		具有郵件伺服器	並持續使用及適時進行軟、硬體之必
		者,應備電子郵	要更新或升級。
		件過濾機制	
		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	
		次召中入几次山	每年至少四名人員各接受十二小時以
	資通安全	資通安全及資訊 全 人員	上之資通安全專業課程訓練或資通安
			全職能訓練。
	教育訓練	一般使用者及主	每人每年接受三小時以上之一般資通
1n L		管	安全教育訓練。
認知		次记中入亩业地	初次受核定或等級變更後之一年內,
與訓練	資通安全	資通安全專業證	資通安全專職人員總計應持有四張以
	專業證照	照	上,並持續維持證照之有效性。
	及職能訓	次另中入毗外江	初次受核定或等級變更後之一年內,
	練證書	資通安全職能評	資通安全專職人員總計應持有四張以
		量證書	上,並持續維持證書之有效性。

- 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,指通過我國標準法主管機關委託機構認證之機構。
- 三、 資通安全專職人員,指應全職執行資通安全業務者。
- 四、 公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行 外,亦得採取經主管機關認可之其他具有同等或以上效用之措施。
- 五、 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。

附表二資通安全責任等級A級之特定非公務機關應辦事項

制度而台	1	※押佰日知佰	辦理內容
制度面向	辨理項目	辨理項目細項	7
	* 7 4 4 1 10 7 7 1 14 14 14		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
	資通系統分級	及防護基準	九完成資通系統分級,並完成附表十之
			控制措施;其後應每年至少檢視一次資
			通系統分級妥適性。
			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
管理面	資訊安全管理	系統之導入及通	全管理系統國家標準、其他具有同等或
百年四	過公正第三方	•	以上效果之系統或標準,或其他公務機
		~ 放 亞	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。
	次冯中入亩丰		初次受核定或等級變更後之一年內,配
	資通安全專責	八貝	置四人。
	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。
		網站安全弱點	入加上、次マタル与左前四一上
	安全性檢測	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	
技術面		線設定檢視	
	1		初次受核定或等級變更後之一年內,完
	資通安全威脅偵測管理機制		成威脅偵測機制建置,並持續維運。
		防毒軟體	
		網路防火牆	
		具有郵件伺服	
		器者,應備電	初次受核定或等級變更後之一年內,完
	資通安全	子郵件過濾機	成各項資通安全防護措施之啟用,並持
	防護	制	續使用及適時進行軟、硬體之必要更新
	" - 2	入侵偵測及防	或升級。
		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	
		次区户入几次	每年至少四名人員各接受十二小時以上
	資 通 安 全 教育訓練		之資通安全專業課程訓練或資通安全職
			能訓練。
認 知		教育訓練	一般使用者及
與訓練		主管	全教育訓練。
			初次受核定或等級變更後之一年內,資
資通安全專業		證照	通安全專責人員總計應持有四張以上,
			並持續維持證照之有效性。

- 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,指通過我國標準法主管機關委託機構認證之 機構。
- 三、特定非公務機關辦理本表「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。
- 四、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範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 五、 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。

附表三資通安全責任等級B級之公務機關應辦事項

制度而与	辦理百日	辦理項目細項	辦理內容
制度面向	辨理項目	洲廷坎日絀垻	* * * * * * * * * * * * * * * * * * * *
			初次受核定或等級變更後之一年內,針
		及叶雄甘淮	對自行或委外開發之資通系統,依附表
	資通系統分級	及防護基华	九完成資通系統分級,並完成附表十之
			控制措施;其後應每年至少檢視一次資
			通系統分級妥適性。
			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
然一里 丁	資訊安全管理	系統之導入及通	全管理系統國家標準、其他具有同等或
管理面	過公正第三方	之驗證	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。
	資通安全專責	人員	初次受核定或等級變更後之一年內,配
	7, 7, 7,		置二人;須以專職人員配置之。
	內部資通安全		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 网络中央 召叫		每年辦理一次。
	安全性檢測	網站安全弱點	全部核心資通系統每年辦理一次。
		檢測	入如抗心容温多处与一左蚰珊山
		系統渗透測試	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	
技術面		定及防火牆連	
		線設定檢視	初为巫拉宁式笙姐鳞面级为《左由》的
			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,並持續維運及依
	資通安全威脅	偵測管理機制	
			主管機關指定之方式提交監控管理資
			料。 动力应达它七签加磁面级力。在由,任
	龙		初次受核定或等級變更後之一年內,依
	政府組態基準		主管機關公告之項目,完成政府組態基準道》作業,並持續維護。
		ry 丰 勘 蛐	準導入作業,並持續維運。
		防毒軟體	初次受核定或等級變更後之一年內,完
	資通安全	網路防火牆	成各項資通安全防護措施之啟用,並持續供用及適時進行動、西豐之以西東新
	防護	具有郵件伺服	續使用及適時進行軟、硬體之必要更新
		器者,應備電	或升級。

		子郵件過濾機	
		制	
		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	
	資通安全	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。
	教育訓練	一般使用者及	每人每年接受三小時以上之一般資通安
認知		主管	全教育訓練。
與訓練		資通安全專業	初次受核定或等級變更後之一年內,資
兴训练	資通安全專 業證照及職 能訓練證書	· · · · · · · · · · · · · · · · · · ·	通安全專職人員總計應持有二張以上,
		显 黑	並持續維持證照之有效性。
			初次受核定或等級變更後之一年內,資
	ル訓 配音	資通安全職能	通安全專職人員總計應持有二張以上,
		評量證書	並持續維持證書之有效性。

- 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,指通過我國標準法主管機關委託機構認證之機構。
- 三、 資通安全專職人員,指應全職執行資通安全業務者。
- 四、公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行外,亦得採取經主管機關認可之其他具有同等或以上效用之措施。
- 五、 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。

附表四資通安全責任等級B級之特定非公務機關應辦事項

制度面向	辨理項目	辨理項目細項	辦理內容
11322111	71-71-	/ - X - X	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
	資通系統分級	及防護基準	附表九完成資通系統分級,並完成附
		,	表十之控制措施;其後應每年至少檢
			視一次資通系統分級妥適性。
			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
然四十	次加卢入然珊	1分从山道 2 几字	安全管理系統國家標準、其他具有同
管理面		系統之導入及通	等或以上效果之系統或標準,或其他
	過公正第三方	一 一	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。
	資通安全專責	人旨	初次受核定或等級變更後之一年內,
	只 型 又 王 寸 貝		配置二人。
	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。
		網站安全弱點	全部核心資通系統每年辦理一次。
	安全性檢測	檢測	
		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	
技術面		定及防火牆連	
		線設定檢視	二. L. D. L. P. D. L. M.
	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	佔洲签珊城出	初次受核定或等級變更後之一年內,
	貝迪女生風質	偵測管理機制	完成威脅偵測機制建置,並持續維 運。
		防毒軟體	(E)
		網路防火牆	
		具有郵件伺服	 初次受核定或等級變更後之一年內,
	資通安全		完成各項資通安全防護措施之啟用,
	防護	子郵件過濾機	· 並持續使用及適時進行軟、硬體之必
		制	要更新或升級。
		入侵偵測及防	
	八夜頂冽及! 禦機制		
	<u> </u>	214 P.N. T.4	

		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 一般使用者及 主管	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。 每人每年接受三小時以上之一般資通 安全教育訓練。
光 메冰	資通安全專業	,	初次受核定或等級變更後之一年內, 資通安全專責人員總計應持有二張以 上,並持續維持證照之有效性。

- 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,指通過我國標準法主管機關委託機構認證之機構。
- 三、特定非公務機關辦理本表「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。
- 四、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範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 五、 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。

附表五 資通安全責任等級 C 級之公務機關應辦事項

制度面向	辨理項目	辦理項目細項	辨理內容
11/又四四	バイエ・スロ	/"一"一下 日 ※四 "只	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
	資通系統分級	及防護基準	年至少檢視一次資通系統分級妥適
	A 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	次	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二年內,
管理面			全部核心資通系統導入 CNS 27001 資訊
		<i>k</i> . , >±	安全管理系統國家標準、其他具有同
	資訊安全管理	系統之導入	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。
	クローンキャ		初次受核定或等級變更後之一年內,
	資通安全專責	人貝	配置一人;須以專職人員配置之。
	內部資通安全		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。
	安全性檢測	網站安全弱點	入加上、农口人从后一斤加加
		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。
		網路架構檢視	
	資通安全健 診	網路惡意活動	
		檢視	
		使用者端電腦	
		惡意活動檢視	与一生 ^放 理 -
		伺服器主機惡	每二年辦理一次。
ルル エ		意活動檢視	
技術面		目錄伺服器設	
		定及防火牆連	
		線設定檢視	
		防毒軟體	
		網路防火牆	初次受核定或等級變更後之一年內,
	資通安全		完成各項資通安全防護措施之啟用,
	防護	具有郵件伺服 器者,應備電	並持續使用及適時進行軟、硬體之必
		高有,應備电 子郵件過濾機	要更新或升級。
		丁野什過應機 制	
		ा ।	每年至少一名人員接受十二小時以上
認 知	資通安全	資通安全及資	支資通安全專業課程訓練或資通安全
與訓練	教育訓練	訊人員	職能訓練。
	<u> </u>		THY ACI WIT WILL

		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。
 当	資通安全專	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。
	業證照及職 能訓練證書	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。

- 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、 資通安全專職人員,指應全職執行資通安全業務者。
- 三、公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行 外,亦得採取經主管機關認可之其他具有同等或以上效用之措施。
- 四、 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。

附表六 資通安全責任等級 C 級之特定非公務機關應辦事項

制度面向	辨理項目	辦理項目細項	辦理內容
171/X EI 17	/* *エ・ス ロ	/ˈ/ˈ	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
	資通系統分級	乃际维其淮	年至少檢視一次資通系統分級妥適
	貝地尔凯刀数	及闪设至十	十主ノ 做 代
			任, 京凯导級何 同」有 产 應 京 初 入 受 核 定 或 等 級 變 更 後 之 二 年 內 , 完 成
			附表十之控制措施。
然 珊 工			初次受核定或等級變更後之二年內, 入如持入次語系統道、CNC 27001 突却
管理面			全部核心資通系統導入 CNS 27001 資訊
	資訊安全管理	系統之導入	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,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。
	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。
	安全性檢測	網站安全弱點	全部核心資通系統每二年辦理一次。
		檢測	
		系統滲透測試	全部核心資通系統每二年辦理一次。
		網路架構檢視	
		網路惡意活動	
	資通安全健 診	檢視	
		使用者端電腦	
		惡意活動檢視	与一年顾珊
		伺服器主機惡	每二年辦理一次。
北 朱 工		意活動檢視	
技術面		目錄伺服器設	
		定及防火牆連	
		線設定檢視	
		防毒軟體	
		17 安秋胆	
		網路防火牆	初次受核定或等級變更後之一年內,
	資通安全	具有郵件伺服	完成各項資通安全防護措施之啟用,
	防護	一 器者,應備電	並持續使用及適時進行軟、硬體之必
		子郵件過濾機	要更新或升級。
		制	
			每年至少一名人員接受十二小時以上
認 知	資通安全	資通安全及資	之資通安全專業課程訓練或資通安全
與訓練	教育訓練 訊人員		~ 頁 .
	<u> </u>		기자 사다 마기 씨는

			每人每年接受三小時以上之一般資通
			安全教育訓練。
			初次受核定或等級變更後之一年內,
	資通安全專業證照		資通安全專責人員總計應持有一張以
			上,並持續維持證照之有效性。

- 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、特定非公務機關辦理本表「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。
- 三、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範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 四、 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。

附表七資通安全責任等級D級之各機關應辦事項

制度面向		辨理項目	辨理項目細項	辦理內容
			防毒軟體	
		資通安全	網路防火牆	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,
技術面		防護	具有郵件伺服 器者,應備電 子郵件過濾機 制	並持續使用及適時進行軟、硬體之必要更新或升級。
認與訓練	知	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: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 之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

附表八資通安全責任等級E級之各機關應辦事項

制度面向	辨理項目	辨理項目細項	辨理內容
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。

備註: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 之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。

附表九 資通系統防護需求分級原則

小块五子			•
防護需求			
等級	高	中	普
構面			
	發生資通安全事件致資	發生資通安全事件致資	發生資通安全事件致資
	通系統受影響時,可能	通系統受影響時,可能	通系統受影響時,可能
	造成未經授權之資訊揭	造成未經授權之資訊揭	造成未經授權之資訊揭
機密性	露,對機關之營運、資	露,對機關之營運、資	露,對機關之營運、資
	產或信譽等方面將產生	產或信譽等方面將產生	產或信譽等方面將產生
	非常嚴重或災難性之影	嚴重之影響。	有限之影響。
	響。		
	發生資通安全事件致資	發生資通安全事件致資	發生資通安全事件致資
	通系統受影響時,可能	通系統受影響時,可能	通系統受影響時,可能
	造成資訊錯誤或遭竄改	造成資訊錯誤或遭竄改	造成資訊錯誤或遭竄改
完整性	等情事,對機關之營	等情事,對機關之營	等情事,對機關之營
	運、資產或信譽等方面	運、資產或信譽等方面	運、資產或信譽等方面
	將產生非常嚴重或災難	將產生嚴重之影響。	將產生有限之影響。
	性之影響。		
	發生資通安全事件致資	發生資通安全事件致資	發生資通安全事件致資
	通系統受影響時,可能	通系統受影響時,可能	通系統受影響時,可能
	造成對資訊、資通系統	造成對資訊、資通系統	造成對資訊、資通系統
可用性	之存取或使用之中斷,	之存取或使用之中斷,	之存取或使用之中斷,
	對機關之營運、資產或	對機關之營運、資產或	對機關之營運、資產或
	信譽等方面將產生非常	信譽等方面將產生嚴重	信譽等方面將產生有限
	嚴重或災難性之影響。	之影響。	之影響。
	如未確實遵循資通系統	如未確實遵循資通系統	其他資通系統設置或運
	設置或運作涉及之資通	設置或運作涉及之資通	作於法令有相關規範之
	安全相關法令,可能使	安全相關法令,可能使	情形。
	資通系統受影響而導致	資通系統受影響而導致	
计伊浦纸料	資通安全事件,或影響	資通安全事件,或影響	
法律遵循性	他人合法權益或機關執	他人合法權益或機關執	
	行業務之公正性及正當	行業務之公正性及正當	
	性,並使機關所屬人員	性,並使機關或其所屬	
	負刑事責任。	人員受行政罰、懲戒或	
		懲處。	

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。

附表十 資通系統防護基準

			迪尔 奶防设 <u>基</u> 干	
系統防護需求				
分級		高	中	普
控制措施		10)		E E
構面	措施內容			
		一、逾越機關所定預期	一、已逾期之臨時或緊	建立帳號管理機制,包
		閒置時間或可使用	急帳號應刪除或禁	含帳號之申請、開通、
		期限時,系統應自	用。	停用及删除之程序。
		動將使用者登出。	二、資通系統閒置帳號	
		二、應依機關規定之情	應禁用。	
	 帳號管	況及條件,使用資	三、定期審核資通系統	
	理	通系統。	帳號之建立、修	
	连	三、監控資通系統帳	改、啟用、禁用及	
		號,如發現帳號違	刪除。	
		常使用時回報管理	四、等級「普」之所有	
大 the line		者。	控制措施。	
存取控制		四、等級「中」之所有		
制		控制措施。		
	国 1 以	採最小權限原則,僅允許	F使用者(或代表使用者	無要求。
	最小權	行為之程序)依機關任務	及業務功能,完成指派	
	限	任務所需之授權存取。		
		一、應監控資通系統遠端	遠線 。	對於每一種允許之遠端
		二、資通系統應採用加密	容機制 。	存取類型,均應先取得
	告业方	三、資通系統遠端存取之	之來源應為機關已預先定	授權,建立使用限制、
	遠端存	義及管理之存取控制	點。	組態需求、連線需求及
	取	四、等級「普」之所有招	空制措施。	文件化,使用者之權限
				檢查作業應於伺服器端
				完成。
	龙 上 古	一、應定期審查稽核事件	- 0	一、依規定時間週期及
		二、等級「普」之所有招	空制措施。	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
	稽核事			能,並決定應稽核
稽核與	件			之特定資通系統事
可歸責				件。
性				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、資通系統產生之稽村	亥紀錄,應依需求納入其	資通系統產生之稽核紀
		他相關資訊。		錄應包含事件類型、發
		二、等級「普」之所有招	空制措施。	生時間、發生位置及任
				何與事件相關之使用者
L	I	<u> </u>		

		<u> </u>		白.八.沙口. 悠.次	
				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	
	稽核儲	 	和里犹拉勿绝的乘力做力	性。	
	指核陷 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。			
	17石王	一、機關規定需要即時	音诵系統於稽核處理失	· · · · · · · · · · · · · · · · · · ·	
		通報之稽核失效事	動。		
		件發生時,資通系			
	稽核處	統應於機關規定之			
	理失效	時效內,對特定人			
	之回應	員提出警告。			
		二、等級「中」及			
		「普」之所有控制			
		措施。			
		一、系統內部時鐘應依機	&關規定之時間週期與基	資通系統應使用系統內	
	時戳及	準時間源進行同步。		部時鐘產生稽核紀錄所	
	校時	二、等級「普」之所有哲	E制措施。	需時戳,並可以對應到	
	权啊			世界協調時間(UTC)或格	
				林威治標準時間(GMT)。	
		一、定期備份稽核紀錄	一、應運用雜湊或其他	對稽核紀錄之存取管	
	稽核資	至與原稽核系統不		理,僅限於有權限之使	
	訊之保	同之實體系統。	確保機制。	用者。	
	護	二、等級「中」之所有	-		
		控制措施。	控制措施。		
				一、訂定系統可容忍資	
		為營運持續計畫測		料損失之時間要	
	系統備	試之一部分。	體之可靠性及資訊		
		二、應在與運作系統不	之完整性。	二、執行系統源碼與資	
			二、等級「普」之所	料備份。	
	份	防火櫃中,儲存重	有控制措施。		
營運持		要資通系統軟體與 其他安全相關資訊			
續計畫		文備份。 之備份。			
		一 寸級 「」之////// 控制措施。			
		一、訂定資通系統從中幽			
	系統備	容忍時間要求。		W > 4-	
	援	二、原服務中斷時,於可	「容忍時間內,由備接設」		
	12	備取代提供服務。	TO THE WAY		
- 計 口.1 水o	南部件	一、對帳號之網路或本	資通系統應具備唯一識	別及鑑別機關使用者(或代	
識別與	內部使	機存取採取多重認	表機關使用者行為之程	序)之功能,禁止使用共用	
鑑別	用者之	證技術。	帳號。		
	t	1			

	고사 p.1 /b	一	
	識別與	二、等級「中」及	
	鑑別	「普」之所有控制	
		措施。	
		一、身分驗證機制應防範自動化程式之登入或密	一、使用預設密碼登入
		碼更換嘗試。	系統時,應於登入
		二、密碼重設機制對使用者重新身分確認後,發	後要求立即變更。
		送一次性及具有時效性符記。	二、身分驗證相關資訊
		三、等級「普」之所有控制措施。	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
	身分驗		般證機制。
	ラカー版 證管理		四、基於密碼之鑑別資
	西日生		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。 工、佐田 女再 按 突 涯
			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
	lπι → 1 -h		自行規範辦理。
	鑑別資	資通系統應遮蔽鑑別過程中之資訊。	
	訊回饋		1- m h
	加密模	資通系統如以密碼進行鑑別時,該密碼應加密或	無要求。
	組鑑別	經雜湊處理後儲存。	
	非內部	資通系統應識別及鑑別非機關使用者(或代表機關係	使用者行為之程序)。
	使用者		
	之識別		
	與鑑別		
	系統發	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
系統與	展生命	認。	
服務獲	週期需		
旅游投 得	求階段		
14	系統發	一、根據系統功能與要求,識別可能影響系統之	無要求。
	展生命	威脅,進行風險分析及評估。	
·	-		<u> </u>

	T			
	週期設	一、將風險評估結果回饋需		
	計階段	並提出安全需求修正。		
		│一、執行「源碼掃描」	一、應針對安全需求實作	必要控制措施。
	多纮淼	安全檢測。	 應注意避免軟體常見 	見漏洞及實作必要控制措
	系統發展生命	二、具備系統嚴重錯誤	施。	
		之通知機制。	E、發生錯誤時,使用之	者頁面僅顯示簡短錯誤訊
	週期開	三、等級「中」及	息及代碼,不包含詳	細之錯誤訊息。
	發階段	「普」之所有控制		_
		措施。		
	A			
	系統發	安全檢測。		
	展生命	二、等級「中」及		
	週期測	「普」之所有控制		
	試階段	措施。		
		□、於系統發展生命週期之	· 維運聯船, 須注音版	一、於部署環境中應針
		本控制與變更管理。	- 阵 社 旧 权 一 次 在 心 欣	對相關資通安全威
	系統發	本程前與愛文官母。 二、等級「普」之所有控制	11性故。	對相關 貞 過 安 主 威 曾 , 進 行 更 新 與 修
	展生命	二、寻《 百」之所有控制	11百00。	
	週期部			補,並關閉不必要
	署與維			服務及埠口。
	運階段			二、資通系統相關軟
				體,不使用預設密
	A 11 70	** ** ** * * * * * * * * * * * * * * *	产的人从水口 J 人 m lin	碼。
	系統發	資通系統開發如委外辦理,	•	各階段依等級將安全需求
	展生命	(含機密性、可用性、完整	性)納入委外契約。	
	週期委			
	外階段			
	獲得程	開發、測試及正式作業環境	5應為區隔。	無要求。
	序			
	系統文	應儲存與管理系統發展生命)週期之相關文件。	
	件			
		一、資通系統應採用加 無	無要求。	無要求。
		密機制,以防止未		
		授權之資訊揭露或		
		偵測資訊之變更。		
2 44 da	傳輸之	但傳輸過程中有替		
系統與	機密性	代之實體保護措施		
通訊保	與完整	者,不在此限。		
護	性	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。		
		/A = -m		

	ı			
		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	静置資訊及相關具保護	無要求。	無要求。
	存之安	需求之機密資訊應加密	, 24 · V	21
	全	儲存。		
		一、定期確認資通系統相	1 關漏洞修復之狀態。	系統之漏洞修復應測試
	漏洞修	、等級「普」之所有控		有效性及潛在影響,並
	復		- 1444E 50	定期更新。
		次沼久从麻护田台		
	資通系 統監控		一、監控資通系統,以	
		動化工具監控進出	負測攻擊與未授權	跡象時,應通報機關特
		之通信流量,並於	之連線,並識別資	定人員。
		發現不尋常或未授	通系統之未授權使	
		權之活動時,針對	用。	
		該事件進行分析。	二、等級「普」之所有	
系統與		二、等級「中」之所有	控制措施。	
資訊完		控制措施。		
整性	軟體及 資訊完 整性	一、應定期執行軟體與	一、使用完整性驗證工	無要求。
		資訊完整性檢查。	具,以偵測未授權	
		二、等級「中」之所有	變更特定軟體及資	
		控制措施。	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	
			恋 / \	
			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。	

借註:

- 一、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。
- 二、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範圍內,另 行訂定其所管特定非公務機關之系統防護基準。