## 資通安全責任等級分級辦法總說明

「資通安全管理法」(以下簡稱本法)業於一百零七年六月六日制定公布,其施行日期由主管機關定之。依本法第七條第一項規定,主管機關應衡的公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件,訂定資通安全責任等級之分級。為明確規範資通安全責任等級之分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項,以利各受規範對象得妥適辦理資通安全維護事務,強化資通安全管理能量,爰訂定「資通安全責任等級分級辦法」(以下簡稱本辦法),其要點如下:

- 一、本辦法訂定之依據。(第一條)
- 二、資通安全責任等級之級別。(第二條)
- 三、資通安全責任等級之提交、核定及變更程序。(第三條)
- 四、資通安全責任等級分級原則及例外考量因素。(第四條至第十條)
- 五、各機關應依附表規定辦理其資通安全責任等級應辦事項。(第十一條)
- 六、本辦法之施行日期。(第十二條)

## 資通安全責任等級分級辦法

條文 第一條 本辦法依資通安全管理法(以 明 下簡稱本法)第七條第一項規定訂定

明定本辦法訂定之依據。

- 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。
- 一、明定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 級至 E 級。
- 二、有關資通安全責任等級之核定方式、 區分原則及認定等級之其他考量因 素,依第三條至第十條規定為之。
- 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。

- 一、第一項明定主管機關應每二年核定 自身之資通安全責任等級。
- 三、各機關之資通安全責任等級如因應 組織或業務調整,致須配合變更者, 應即依第一項至第五項規定辦理其 等級變更事宜;有新設機關時,亦應 立即辦理該機關資通安全責任等級 之認定,爰為第六項規定。
- 四、考量各機關可能有特定內部單位業 務性質特殊,其辦理資通安全維護 業務相較同機關之其他單位,須為 更嚴格要求之情形,此時宜單獨將 該單位之資通安全責任等級分級為 不同之處理,爰為第七項規定。

- 第四條 各機關有下列情形之一者,其 一、明定各機關資通安全責任等級應列 資通安全責任等級為A級: 為A級之情形。於該等情形,因其
  - 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。

  - 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 用戶數、市場占有率、區域 時代性,認其資通系統失效或 對社會公共利益、民 完 影響,對社會公共利益、財產安 系或民眾生命、身體、財產安全 將產生嚴重影響。

- 一、明定各機關資通安全責任等級應列 為 A 級之情形。於該等情形,因其 機關業務所涉重要性或機敏性較 高,具有較高之資通安全風險,爰應 予以較高程度之資通安全維護責 任。
- 二、第三款所稱全國性,指含括全國之地域範圍;所稱跨公務機關共用性資通系統,指單一公務機關主責設置、維護或開發伺服器、網路通訊服務之機房設施或其他資通系統,其餘公務機關僅為該資通系統之使用者之情形。
- 三、第四款所稱全國性民眾或公務員個 人資料檔案,指含括全國地域範圍 內之絕大部分民眾或公務員之個人 資料檔案。
- 一、明定各機關資通安全責任等級應列 為 B 級之情形。於該等情形,其機 關業務所涉重要性或機敏性雖較第 四條所定情形為低,惟亦具有相當 之資通安全風險,爰應予以相當之 資通安全維護責任。
- 二、第二款所稱區域性,指跨直轄市、縣 (市)之地域範圍;所稱地區性,指 單一直轄市或縣(市)之地域範圍; 所稱跨公務機關共用性資通系統, 如第四條說明二。
- 三、第三款所稱區域性或地區性民眾個 人資料檔案,指含括跨直轄市、縣 (市)或單一直轄市、縣(市)地域 範圍內之絕大部分民眾之個人資料 檔案。

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。 各機關倘無第四條或第五條規定之情 形,而有維運自行或委外開發之資通系 統者,資通安全風險較有前二條所列情 形之機關為低,其資通安全責任等級應 列為 C級,爰為本條規定。

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。 考量各機關如屬自行辦理資通業務,未 維運自行或委外開發之資通系統,其資 通安全風險較低,其資通安全責任等級 應列為 D級,爰為本條規定。本條及第 八條所定資通業務,包含資通系統之維 運及資通服務之提供等業務。

- 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。

考量各機關如無資通系統且未提供資通 服務,或全部資通業務由其上級或監督 機關、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,其資通安全風險較第四條至第 七條所定情形更低,資通安全責任等級 應列為E級,爰為本條規定。

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。 為避免各機關依第四條至第八條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,於辦理其等級之提交或核定將發生疑義,爰明定有上開情形者,應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

有關各機關資通安全責任等級之認定, 除第四條至第八條規定外,因業務機 性、個人資料檔案之數量等不同因素,仍 可能有其他應考量事項,而有調整分級 之必務機關於提交或核定資通安全責任等 級時,得有調整之彈性,爰為本條規定 級時,得有調整之彈性,爰為本條規定等 終關資通安全責任等級之認定,例外則 應依第四條至第九條規定辦理,例外則 整其等級。 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 三條第二項至第四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。

- 一、考量不同資通安全責任等級之機 關,其業務所涉範圍與機敏性等有 所不同, 資通安全風險程度亦有所 差異,爰於第一項規定各機關應依 其資通安全責任等級辦理附表一 至附表八之事項,並於第二項明定 各機關自行或委外開發之資通系 統應依附表九及附表十辦理資通 系統分級及控制措施。另關鍵基礎 設施提供者之中央目的事業主管 機關考量特定類型資通系統之性 質,例如特定用途之工業控制系統 (Industrial Control Systems, ICS), 認有對之另定防護基準之必要者, 宜使其得衡酌實務需求,於充分考 量附表十所定各項控制措施於此 類系統之適用性後,自行擬訂防護 基準,並報請主管機關核定後,依 其規定辦理,爰於第二項後段明定 之。
- 三、 資通安全責任等級為 A 級或 B 級 之公務機關,宜強化對該等機關資 通安全維護情形之管考,爰於第四

	項明定其應依主管機關指定之方 式,提報第一項及第二項所定事項 之辦理情形。 四、考量特定非公務機關資通安全維 護情形之管考,宜由其中央目的事 業主管機關執行,爰為第五項規 定。
第十二條 本辦法之施行日期,由主管	明定本辦法之施行日期,由主管機關定
機關定之。	之。

## 附表一 資通安全責任等級 A 級之公務機關應辦事項

制度面向	辨理項目	辨理項目細項	辨理內容
中华人工	7-7-7-7 G	1 777- 7 B VO R	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
	京亚小州 <b>以</b> 次/// <b>设</b>		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
	-tr ) - do 2 tt -n	9.4 4 5 苯 - 9 22	安全管理系統國家標準、其他具有同等
管理面		星系統之導入及通	或以上效果之系統或標準,或其他公務
	過公正第三方	之驗證	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。
	次记户入市主		初次受核定或等級變更後之一年內,配
	資通安全專責	人貝	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	全部核心資通系統每年辦理二次。
	安全性檢測	檢測	
		系統滲透測試	全部核心資通系統每年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
		使用者端電腦	
	資通安全健	惡意活動檢視	每年辦理一次。
	診	伺服器主機惡	
		意活動檢視	
技術面		目錄伺服器設	
1文7的四		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
	   咨诵	'偵測管理機制	成威脅偵測機制建置,並持續維運及依
	貝四女王成月	识内占土域制	主管機關指定之方式提交監控管理資
			料。
			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,完
	防護	網路防火牆	成各項資通安全防護措施之啟用,並持

者,應備電子郵 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 進階持續性威脅 攻擊防禦措施 每項全及資訊		I	T	
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			具有郵件伺服器	續使用及適時進行軟、硬體之必要更新
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 資通安全及資訊 每年至少四名人員各接受十二小時以			者,應備電子郵	或升級。
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  每年至少四名人員各接受十二小時以			件過濾機制	
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 每項安全及資訊 每年至少四名人員各接受十二小時以			入侵偵測及防禦	
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 每年至少四名人員各接受十二小時以			機制	
者,應備應用程式防火牆 進階持續性威脅 攻擊防禦措施 資通安全及資訊 每年至少四名人員各接受十二小時以			具有對外服務之	
式防火牆 進階持續性威脅 攻擊防禦措施 資通安全及資訊 每年至少四名人員各接受十二小時以			核心資通系統	
進階持續性威脅 攻擊防禦措施 資通安全及資訊 每年至少四名人員各接受十二小時以			者,應備應用程	
攻擊防禦措施 每年至少四名人員各接受十二小時以 資通安全及資訊 每年至少四名人員各接受十二小時以			式防火牆	
音诵安全及音訊 每年至少四名人員各接受十二小時以			進階持續性威脅	
首補安全及資訊			攻擊防禦措施	
			<b>容温它入耳容</b> 却	每年至少四名人員各接受十二小時以
次字中入   1号   工人员也女王哥未诉任训练以员进女		~ ~ ~ ~ ~ ~		上之資通安全專業課程訓練或資通安
資通安全 人員 全職能訓練。			八月	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		教月訓練	一般使用者及主	每人每年接受三小時以上之一般資通
安全教育訓練。 安全教育訓練。	171 k -		管	安全教育訓練。
認知			次环户入亩业地	初次受核定或等級變更後之一年內,資
與訓練 資通安全專業證 通安全專職人員總計應持有四張以上,	兴训練	次记户入市		通安全專職人員總計應持有四張以上,
亚持續維持證照之有效性。		資通安全專	, KR	並持續維持證照之有效性。
業證照及職 初次受核定或等級變更後之一年內,資			次记的入助公共	初次受核定或等級變更後之一年內,資
通知   通知   通知   通知   通知   通知   通知   通知		能訓練證書	資通安全職能評	通安全專職人員總計應持有四張以上,
量證書 並持續維持證書之有效性。			重證書	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。

## 附表二 資通安全責任等級 A 級之特定非公務機關應辦事項

	1	I	277 スケース 4万 4人 7月 1人 7月 1日 7日 7日 7日 7日 7日 7月 7日
制度面向	辨理項目	辨理項目細項	辨理內容
			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	· 資訊安全答理	系統之導入及通	全管理系統國家標準、其他具有同等或
百姓國	過公正第三方	•	以上效果之系統或標準,或其他公務機
		一	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,配
	貝地女王寺貝	八只 	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	全部核心資通系統每年辦理二次。
	安全性檢測	檢測	至 市 核心 貝 通 系 統 母 十 辦 珪 一 火 。
		系統滲透測試	全部核心資通系統每年辦理一次。
		網路架構檢視	
		網路惡意活動	
		檢視	
		使用者端電腦	
	資通安全健	惡意活動檢視	每年辦理一次。
	診	伺服器主機惡	
		意活動檢視	
		目錄伺服器設	
ルルー		定及防火牆連	
技術面		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,並持續維運。
		防毒軟體	
		網路防火牆	
		具有郵件伺服	
		器者,應備電子	初次受核定或等級變更後之一年內,完
	資通安全	郵件過濾機制	成各項資通安全防護措施之啟用,並持
	防護	入侵偵測及防	續使用及適時進行軟、硬體之必要更新
		架機制	或升級。
	_	具有對外服務	
		之核心資通系	
		一似 5 只 也 示	

		統者,應備應用 程式防火牆 進階持續性威	
		脅攻擊防禦措 施	
	資通安全	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。
認知 與訓練	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。
資通安全專業證		證照	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

制度面向 辦理項目 辦理項目細項 辦理內容 初次受核定或等級變更後之一年內 對自行或委外開發之資通系統,依	附表 十之
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 九完成資通系統分級,並完成附表 控制措施;其後應每年至少檢視一 通系統分級妥適性。 初次受核定或等級變更後之二年內	附表 十之
資通系統分級及防護基準 九完成資通系統分級,並完成附表控制措施;其後應每年至少檢視一通系統分級妥適性。 初次受核定或等級變更後之二年內	十之
控制措施;其後應每年至少檢視一 通系統分級妥適性。 初次受核定或等級變更後之二年內	
通系統分級妥適性。 初次受核定或等級變更後之二年內	~~
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	
全管理系統國家標準、其他且有同	
管理面     貧訊安全管理系統之導入及連   以上於果之系統或標準,或其他公	
過公正第三方之驗證 關自行發展並經主管機關認可之標	
於三年內完成公正第三方驗證,並	
維持其驗證有效性。	
初次受核定或等級變更後之一年內	,配
資通安全專責人員 置二人;須以專職人員配置之。	
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	0
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一次。	
系統渗透測試 全部核心資通系統每二年辦理一次	0
網路架構檢視	
網路惡意活動	
檢視	
使用者端電腦	
資通安全健 惡意活動檢視 与一年 蜿珊 中	
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	
初次受核定或等級變更後之一年內	,完
次 3 c 2 c 2 c 4 c 2 c 2 c 2 c 2 c 2 c 2 c 2	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。	
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	,完
防護 網路防火牆 成各項資通安全防護措施之啟用,	並持

具有郵件伺服 續使用及適時進行軟、在 器者,應備電子 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	
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	<b>D體之必要更新</b>
入侵偵測及防 禦機制 具有對外服務 之核心資通系	
禦機制 具有對外服務 之核心資通系	
具有對外服務之核心資通系	
之核心資通系	
<b>公</b> 4 , 應 供 應 用	
程式防火牆	
資通安全及資 每年至少二名人員各接受	を十二小時以上
	東或資通安全職
資通安全 訊人員 能訓練。	
教育訓練 一般使用者及 每人每年接受三小時以_	
主管全教育訓練。	
認知	<b>支之一年內,資</b>
與訓練	<b>持有二張以上</b> ,
資通安全專 證照 並持續維持證照之有效性	•
業證照及職 初次受核定或等級變更行	<b>送之一年內,資</b>
	<b>持有二張以上</b> ,
評重證書   並持續維持證書之有效性	<u> </u>
能訓練證書 貧 選 安全 職能 通安全 專職人員總計應打	<b>持有二張以上</b> ,

- 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	辨理內容
<b></b>	洲坯坝口	州廷坎日絀垻	
			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
管理面	· 資訊安全答理	系統之導入及通	安全管理系統國家標準、其他具有同等
百姓曲	過公正第三方	•	或以上效果之系統或標準,或其他公務
	超公正另一刀	之	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。
	次诏户入亩丰	, ,	初次受核定或等級變更後之一年內,配
	資通安全專責	人貝	置二人。
	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。
	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。
		網路架構檢視	
		網路惡意活動	每二年辦理一次。
	資通安全健診	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		初为公林宁北学加磁西级上。上中、中
	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
		고도 본 4시 RHb	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	初次受核定或等級變更後之一年內,完
	資通安全	器者,應備電子	成各項資通安全防護措施之啟用,並持
	防護	郵件過濾機制	續使用及適時進行軟、硬體之必要更新
	沙哉	入侵偵測及防	或升級。
		禦機制	· 以开級。 
		具有對外服務	
		之核心資通系	
		人 做 心 貝 琎 杀	

		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。
	資通安全專業證照		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	辨理項目細項	辨理內容
中小人田門	バーエ・バロ	/"一一一八日 /四一八	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,其後應每年至少
	資通系統分級	及防護基準	檢視一次資通系統分級妥適性;系統等
	· 英型水杨为杨	<b>人</b> 历 贬至 1	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,全
管理面			部核心資通系統導入 CNS 27001 資訊
B-Z-W			安全管理系統國家標準、其他具有同等
	資訊安全管理	系統之導入	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。
		_	初次受核定或等級變更後之一年內,配
資	資通安全專責人員		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。
	2K 4/2 (1 / X C )	網站安全弱點	
	安全性檢測	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	2 T M X C4.06 V 171 = 30
		網路惡意活動	
		檢視	每二年辦理一次。
		使用者端電腦	
	資通安全健	惡意活動檢視	
	診	伺服器主機惡	
技術面		意活動檢視	
		目錄伺服器設	
		定及防火牆連	
		線設定檢視	
		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
	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,應備電子	或升級。
		郵件過濾機制	
			<b>每年至少一名人員接受十二小時以上</b>
		資通安全及資	之資通安全專業課程訓練或資通安全
認知	資通安全	訊人員	職能訓練。
與訓練	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
		主管	安全教育訓練。
	1	и	7 - 3/4 N = 1 m =

次温中入亩	資通安全專業	資通安全專職人員總計應持有一張以
資通安全專 業證照及職 能訓練證書	證照 資通安全職能 評量證書	上。 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	辨理項目細項	○
11/文田円	7″1~エ・穴 口	////	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
			力完成資通系統分級,其後應每年至少
	   資通系統分級	及防護其進	一般視一次資通系統分級妥適性;系統等
		<b>人// 岐</b>	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,全
管理面			部核心資通系統導入 CNS 27001 資訊
18 坯 Щ			安全管理系統國家標準、其他具有同等
	資訊安全管理	系統之導入	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
			推
			初次受核定或等級變更後之一年內,配
	資通安全專責	人員	
	南郊容泽中入	<b>班</b> 拉	置一人。 每二年辦理一次。
	內部資通安全		* ' ' '
	業務持續運作	1	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	2 20 12 - 20 20 11 - 20 20 20 20 20 20 20 20 20 20 20 20 20
		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	
		檢視	
		使用者端電腦	
	資通安全健	惡意活動檢視	   每二年辦理一次。
	診	伺服器主機惡	
技術面		意活動檢視	
		目錄伺服器設	
		定及防火牆連	
		線設定檢視	
		防毒軟體	
		NA WENT	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
	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,應備電子	或升級。
		郵件過濾機制	
			每年至少一名人員接受十二小時以上
	資通安全 教育訓練	資通安全及資	之資通安全專業課程訓練或資通安全
認知		訊人員	職能訓練。
與訓練		一般使用者及	每人每年接受三小時以上之一般資通
	主管		安全教育訓練。
	I	· · P	St = 45/4 S D D

資通安全專業證照	資通	安全	車業	證照
----------	----	----	----	----

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	动力 巫坛 宁 士 笠 加 綫 西 悠 为 。 左 南 , 宁
技術面	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,並持續使用及適時進行軟、硬體之必要更新或升級。
	防護	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: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

		7, 1001/4 of 110 de 1/4 (100/1/1)	<u>'</u>
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、資產	露,對機關之營運、資產	露,對機關之營運、資產
	或信譽等方面將產生非	或信譽等方面將產生嚴	或信譽等方面將產生有
	常嚴重或災難性之影	重之影響。	限之影響。
	鄉。		
	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,對機關之營運、	等情事,對機關之營運、	等情事,對機關之營運、
	資產或信譽等方面將產	資產或信譽等方面將產	資產或信譽等方面將產
	生非常嚴重或災難性之	生嚴重之影響。	生有限之影響。
	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	
	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。	
	4、11、按西上於加 、 2、1924	上久 44 1.2 1.3 1.4 1.4 1.4 1.4 1.4 1.4 1.4 1.4 1.4 1.4	11 一丁四月刀斗母弟佐

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

		111 代 1 月 2	<b>世系統防護基準</b>	
系	統防護需求			
分級		高	中	<u> </u>
控制措施		lαj	'	Ħ
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,包含
		閒置時間或可使用	急帳號應刪除或禁	帳號之申請、開通、停用
		期限時,系統應自	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、修改、	
		三、監控資通系統帳	啟用、禁用及刪除。	
		號,如發現帳號違	四、等級「普」之所有控	
+ 11- lin		常使用時回報管理	制措施。	
存取控制		者。		
制		四、等級「中」之所有控		
		制措施。	· / · · · · · / · · · · · · · · · · · ·	<b>左</b> 五 よ
	最小權	採最小權限原則,僅允許		無要求。
	限	行為之程序)依機關任務	6及耒務切肥, 元成相派	
		任務所需之授權存取。 一、應監控資通系統遠端	油柏。	對於每一種允許之遠端
	遠端存取	一、應監控員通系統逐 <sup>編</sup> 二、資通系統應採用加密		對於每一種允許之逐端
		,	之來源應為機關已預先定	權,建立使用限制、組態
		一 · 黄远水 · 成 · 远 · · · · · · · · · · · · · · · ·		需求、連線需求及文件
		四、等級「普」之所有招		化,使用者之權限檢查作
			- 141 14 4 <b>0</b>	業應於伺服器端完成。
		一、應定期審查稽核事件	- 0	一、依規定時間週期及
		二、等級「普」之所有哲		紀錄留存政策,保留
		, , , , , ,	- 1,1,1,1	稽核紀錄。
				二、確保資通系統有稽
	稽核事			核特定事件之功能,
	件			並決定應稽核之特
稽核與				定資通系統事件。
可歸責				三、應稽核資通系統管
性				理者帳號所執行之
				各項功能。
		一、資通系統產生之稽核	<b>该紀錄,應依需求納入其</b>	資通系統產生之稽核紀
	稽核紀	他相關資訊。		錄應包含事件類型、發生
	精核紀 錄內容	二、等級「普」之所有招	E制措施。	時間、發生位置及任何與
	-41.1 4 /D-			事件相關之使用者身分
				識別等資訊,並採用單一

				口计如约姚州,加州口机
				日誌紀錄機制,確保輸出
	14. 12 44	<b>公园</b>	西里龙山石石石石石工业士	格式之一致性。
	稽核儲	依據稽核紀錄儲仔需求,	配置稽核紀錄所需之儲存	·谷里。 
	存容量	14 8 日 中 西 五 田 叶	次亿名从从优比占四小上	1.吐 应应压证出上户的
		一、機關規定需要即時	貝迪系統於稽核處理失效	女時,應採取適當之行動。
		通報之稽核失效事		
	稽核處	件發生時,資通系		
	理失效	統應於機關規定之		
	之回應	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。 一、系統內部時鐘應依機	《朗祖令》时明细知的甘	
		本 · 京 · 於 內 部 · 时 雖 應 依 · 依 · 本 時 間 源 進 行 同 步 。	《關稅及之时间週期與益	部時鐘產生稽核紀錄所
	時戳及	二、等級「普」之所有控	241世	部 时
	校時	一、寻談「百」之川有拉 	的有他。	界協調時間(UTC)或格林
				成治標準時間(GMT)。
		一、定期備份稽核紀錄	<ul><li>一、應運用雜湊或其他</li></ul>	對稽核紀錄之存取管理,
	稽核資	至與原稽核系統不	適當方式之完整性	重相核紅蘇之行取官亞, 僅限於有權限之使用者。
	祖依貝訊之保	三 三 三 三 三 三 三 三 三 三 三 三 三 三 三 三 三 三 三	確保機制。	<b>建</b>
	護	二、等級「中 <sub> </sub> 之所有控	二、等級「普」之所有	
	吺	制措施。	控制措施。	
		一、應將備份還原,作	一、應定期測試備份資	一、訂定系統可容忍資
		為營運持續計畫測	訊,以驗證備份媒	
		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。	料備份。
		同處之獨立設施或	二、等級「普」之所有	11 100 100
	系統備	防火櫃中,儲存重	控制措施。	
.,	份	要資通系統軟體與	12 11111	
營運持		其他安全相關資訊		
續計畫		之備份。		
		三、等級「中」之所有控		
		制措施。		
		一、訂定資通系統從中斷	f後至重新恢復服務之可 「	無要求。
	系統備	容忍時間要求。		
	援	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。		
	南加州	一、對帳號之網路或本	資通系統應具備唯一識別	引及鑑別機關使用者(或代
北 口 小	內部使	機存取採取多重認	表機關使用者行為之程序	下)之功能,禁止使用共用帳
識別與	用者之	證技術。	號。	
鑑別	識別與	二、等級「中」及「普」		
	鑑別	之所有控制措施。		

		<ul><li>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。</li><li>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。</li></ul>	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
	身證管理	三、等級「普」之所有控制措施。	三 四 五 六、 八、 一、
	鑑別資	資通系統應遮蔽鑑別過程中之資訊。	範辨理。
	訊回饋		
	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	b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認。
	展生命		
	週期需		
会休曲	求階段		
系統與 服務獲	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。
服務獲 得	展生命	威脅,進行風險分析及評估。	
付	週期設	二、將風險評估結果回饋需求階段之檢核項目,	
	計階段	並提出安全需求修正。	
	系統發	一、執行「源碼掃描」安 一、應針對安全需求實价	F必要控制措施。
	展生命	全檢測。	
		24	

	週期開	二、具備系統嚴重錯誤二	、應注意避免軟體常!	<b>見漏洞及實作必要控制措</b>
	發階段	之通知機制。	施。	
		三、等級「中」及「普」 三	、 發生錯誤時,使用者	頁面僅顯示簡短錯誤訊息
		之所有控制措施。	及代碼,不包含詳細	之錯誤訊息。
	系統發	一、執行「滲透測試」安 │ 執	.行「弱點掃描」安全檢	[測]。
	展生命	全檢測。		
	週期測	二、等級「中」及「普」		
	試階段	之所有控制措施。		
		一、於系統發展生命週期之	.維運階段,須注意版	一、於部署環境中應針對
	系統發	本控制與變更管理。		相關資通安全威脅,
	展生命	二、等級「普」之所有控制:	措施。	進行更新與修補,並
	週期部			關閉不必要服務及
	署與維			埠口。
	運階段			二、資通系統相關軟體,
				不使用預設密碼。
	系統發	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
	展生命	(含機密性、可用性、完整		
	週期委			
	外階段			
	獲得程	開發、測試及正式作業環境應為區隔。		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	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。		
		但傳輸過程中有替		
		代之實體保護措施		
		者,不在此限。		
	傳輸之	二、使用公開、國際機		
系統與	機密性	構驗證且未遭破解		
通訊保	與完整	之演算法。		
護	性	三、支援演算法最大長		
	1-	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		
		<u>エー内版品端</u> 之玉編		
		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		50
	全	儲存。		
	中田坊	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	二、等級「普」之所有哲	E制措施。	有效性及潛在影響,並定
	復			期更新。
		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
		動化工具監控進出	偵測攻擊與未授權	跡象時,應通報機關特定
		之通信流量,並於	之連線,並識別資	人員。
	資通系	發現不尋常或未授	通系統之未授權使	
	統監控	權之活動時,針對	用。	
		該事件進行分析。	二、等級「普」之所有控	
系統與		二、等級「中」之所有控	制措施。	
資訊完		制措施。		
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」之所有控	變更特定軟體及資	
		制措施。	訊。	
	軟體及		二、使用者輸入資料合	
	<b>新祖</b> 次 資訊完		法性檢查應置放於	
	整性		應用系統伺服器	
	正江		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、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。