資通安全責任等級分級辦法部分條文修正條文對 照表

修正條文

- 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關鍵基礎設施事項。
 - 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 户數、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。

現行條文

- 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 户數、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。

說明

- 一、序文、第一款至第四 款與第六款及第七款 未修正。
- 二、考量未來關鍵基礎設 施之領域可能因應科 技發展、環境改變等 因素調整,爰修正第 五款以保留彈性及符 合實務需求。

- 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<u>、資助</u>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、業務涉及中央二級 機關及所屬各級機 關(構)共用性資通 系統之維運。
 - 五、屬公務機關,且業 務涉及區域性或地 區性之關鍵基礎設 施事項。
 - 六 屬 供 央 關 運 務 占 代 統 對 民 命 將鍵 稱 自 考 關 之 有 性 失 社 心 身 建 基 且 事 其 基 戶 區 認 或 公 氣 世 體 嚴 工 業 提 礎 數 域 真 影 利 民 產 數 越 溪 寰 影 利 民 產 影 越 經 管 或 施 市 可 通 響 益 眾 安 響 提 世 機 維 服 場 替 系 , 、 生 全 。
 - <u>七</u>、屬公立區域醫院或 地區醫院。

- 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,且業或務機關,且業或及區性之能源,也是就源土地資源、實施、資源、緊急,與 聚急 投票 項。
 - 五、屬提中管供礎戶率性失社心命全響關供央機或設數、,效會士、將。鍵者目關維施、區認或公氣射產基則的考運服市域其受共或體生基則的考運服市域其受共或體生人品替系,、眾產重設務業其鍵之占替系,、眾產重設務業其鍵之占核。
 - 六、屬公立區域醫院 或地區醫院。

- 一、序文、第二款及第三 款未修正。

- 五、現行第五款及第六款 款次配合遞移為第六 款及第七款,內容未 修正。

- 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。
- 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。
- 一、序文及第一款未修 正。
- 二、考量公務機關之全部 資通業務由其上級或 監督機關指定之公務

- 二、屬公務機關,且其 全部資通業務由 其上級機關、監督 機關或上開機關 指定之公務機關 兼辦或代管。
- 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、屬精業的中管機事管關業的中管機關業公目關於。主定共產,務業目,所中管機關業的中管機關,主定非人。其一,與關於,一、與關於,一、與關於,一、與關於,一、與關於,一、與關於,一、與關於,一、與關於,一、

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。

各之所分分資控機管系為行主規 關通資原,系措之關之定訂機關 自系通則並統施中就防之定訂機 實原,系措之關之定訂機 等於系完依防;央特護必護核 或應統成附護特目定基要基定 或應統成附護特目定基要基定 外附護通十準非事型認,,,

 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。

- 一、第一項、第四項及第 五項未修正。
- 二、考量除關鍵基礎設施 提供者外,其他特定 非公務機關之中央目 的事業主管機關亦有 可能須針對特定類型 資通系統之性質,例 如特定用途之工業控 制系統 (Industrial Control Systems, ICS),另定防護基準 之必要;為使其得衡 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, 爰將現 行第二項後段所定 「關鍵基礎設施提供 者」修正為「特定非公 務機關」。
- 三、考量主管機關辦理附 表一至至附表八所定 事項或執行附表十所

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; 其為主管機關者,經其 同意後,免予執行。

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。

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。

定控制措施時,亦可 能因技術限制、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,為利實務運作之 彈性,並能符合資通 安全維護之要求,爰 修正第三項。

第十二條 本辦法之施行 日期,由主管機關定之。 本辦法修正條文自 發布日施行。

第十二條 本辦法之施行 一、第一項未修正。

日期,由主管機關定之。 二、為明定本辦法修正條 文之施行日期,爰增 訂第二項規定。

附表一修正對照表

修正規定			現行規定			說明		
	1	A級之公務機關應		附表一 資道	通安全責任等級	A級之公務機關應	辦事項	一、於管理面之資
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辨理項目	辨理項目細項	辨理內容	訊安全管理系
	資通系統分級及防護基準 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,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 或 ISO 27001 等資訊安全管理系統標準、其他		對 資通系統分級及防護基準 九 控 通 初 部		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,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 安全管理系統國家標準、其他具有同等	統之導入及三導入及三導入及三次 過公證,配合 務需求明定 27001 等資訊標準 實明確。
			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	管理面	資訊安全管理系統之導入及通 過公正第三方之驗證		安全官理系統 <u>國家</u> 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	二、為強化各機關 之資通安全防 護,降低國家 資,爰於管理
	資通安全專責		置四人;須以專職人員配置之。		資通安全專責人員		置四人;須以專職人員配置之。	面中增訂限制 使用危害國家
管理面	內部資通安全		每年辦理二次。		內部資通安全		每年辦理二次。	資通安全產品
	業務持續運作		全部核心資通系統每年辦理一次。		業務持續運作	演練	全部核心資通系統每年辦理一次。	之規定。
	資安治理成熟	度評估	每年辦理一次。		資安治理成熟	度評估	每年辦理一次。	三、於認知與訓練
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定		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。	中,針對資通安全及資訊人
	限制使用危害國家資通安全產品		之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管機 關核可採購之危害國家資通安全產 品,應列冊管理,且不得與公務網路 環境介接。	技術面	資通安全健診	系統滲透測試 網檢	全部核心資通系統每年辦理一次。	員育為職年 二資訓他人資訓資人至小通練訊員少時安課訊二安,安每接以全程人年子,與無訊二人人人
技術面	安全性檢測資通安全健診	網站安全弱點 檢測 系統滲透測試 網路架構檢視 網路惡意活動 檢用者端電腦 惡意活動檢視	全部核心資通系統每年辦理二次。 全部核心資通系統每年辦理一次。 每年辦理一次。		資通安全威脅	線設定檢視	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 主管機關指定之方式提交監控管理資 料。	大接上專程 一三資訓 年一一三資訓 年 日 一三資訓 年 日 一三資訓 日 時 安 之 業 別 日 、 三 資 訓 日 、 日 、 日 、 日 、 日 、 日 、 日 、 日 、 日 、 日

	伺服器主機惡				
	ナンムルカ				
	意活動檢視				
	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,			
次区内入土石	为此训练和此儿	成威脅偵測機制建置,並持續維運及			
貝迪女主風質	育 俱測官	主管機關指定之方式提交監控管理			
		料。			
		初次受核定或等級變更後之一年內,			
政府組態基準	<u>ŧ</u>	主管機關公告之項目,完成政府組態			
		準導入作業,並持續維運。			
	防毒軟體				
資通安全		· 初次受核定或等級變更後之一年內, 成各項資通安全防護措施之啟用,並			
防護		續使用及適時進行軟、硬體之必要更			
		或升級。			
	攻擊防禦措施				
	資	<u>每人</u> 每年至少接受十二小時以上之			
		通安全專業課程訓練或資通安全職			
	<u> </u>	訓練。			
咨诵空入	咨诵它入重融人	<u>每人每二</u> 年至少接受 <u>三</u> 小時以上之			
1 ' '		通安全專業課程訓練或資通安全職			
我月 訓		訓練,且每年接受三小時以上之資通			
	<u>貝</u>	全通識教育訓練。			
	一般使用者及主	每人每年接受三小時以上之資通安			
	管	通識教育訓練。			
	カロム 3 ま 単 13 0	初次受核定或等級變更後之一年內,			
-h		通安全專職人員總計應持有四張以上			
	炽	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,			
能訓練證書	,, - , , , , , , , , , , , , , , , , ,	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。			
	政府 資務 資教 資業 建基基基	京			

	1					
	政府組態基準	隼	初次受核定或等級變更後之一年內,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。			
	資通安全 防護	防毒幣體 網有應機制 具有,過侵制 對資備 機制 人機有心,防階 時 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	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。			
	資通安全 教育訓練	資通安全及資訊 人員 一般使用者及主	每年至少 <u>四名人員各</u> 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 <u>一般</u> 資通			
認知與訓練	資通安全專 業證照及職 能訓練證書	管 資通安全專業證 照	安全教育訓練。 初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有四張以上, 並持續維持證照之有效性。			
		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四張以上, 並持續維持證書之有效性。			

供社・

- 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。

- 五、其餘內容未修 正。

- 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、資通安全專職人員,指應全職執行資通安全業務者。
- <u>五</u>、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。
- <u>六</u>、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。

附表二修正對照表

		修正規	定			現行規	足定		說明
		A級之特定非公孫		附表二 資達	通安全責任等級	A 級之特定非公務	务機關應辦事項	-,	於管理面之資
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	辦理項目	辨理項目細項	辦理內容		訊安全管理系
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 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。		統之導入及通過公正第三方之驗證,配合實務需求明定包	
			管理面	資訊安全管理過公正第三方	· !系統之導入及通 :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。	= '	含 ISO 27001 等 資訊安全管理 系統標準, 明確。 為資資。 養養 養養 養養 養養 養養 養養 養養 養養 養養	
	資通安全專責		初次受核定或等級變更後之一年內,配置四人。		資通安全專責	初次受核定式等級繼重後之一年內,两			資 通 安 全 压 險,爰於管理
	內部資通安全		每年辦理二次。		內部資通安全	·稽核	每年辦理二次。		面中增訂限制
	業務持續運作	海	全部核心資通系統每年辦理一次。		業務持續運作	演練	全部核心資通系統每年辦理一次。		使用危害國家
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定		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。		資通安全產品 之規定。
			之廠商生產、研發、製造或提供之			系統渗透測試	全部核心資通系統每年辦理一次。	三、	於認知與訓練
	度制使用危害國家資通安全產品。 一次須採購或使用危害國家資通安 全產品時,應具體敘明理由,經主 管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因 業務需求且無其他替代方案經主 管機關核可採購之危害國家資通 安全產品,應列冊管理,且不得與 業務網路環境介接。		技術面	資通安全健 診	伺服器主機惡 意活動檢視 目錄伺服器設	- 每年辦理一次。		中安員育為責年二資針及通練通員少時安對資安,安每接以全時安強人至小通	
技術面	安全性檢測	網站安全弱點 檢測 系統渗透測試	全部核心資通系統每年辦理二次。 全部核心資通系統每年辦理一次。		資通安全威脅	定及防火牆連線設定檢視 偵測管理機制	初次受核定或等級變更後之一年內,完		訓練課程;其他資訊人員每人每二年至少
	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	每年辦理一次。 -		資通安全 防護	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	成威脅偵測機制建置,並持續維運。 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。		接受三小時以 是資通練 是 業 訓 等 是 等 引 時 是 等 引 等 是 等 引 。 等 日 号 ら ら ら ら ら ら ら ら ら ら ら ら ら ら ら ら ら ら

		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,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、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	
		進階持續性威	
		脅攻擊防禦措	
		施	
認知	資通安全	容温力入亩丰	每人每年至少接受十二小時以上之資通
與訓練	教育訓練	資通安全專責	安全專業課程訓練或資通安全職能訓
		<u>人員</u>	練。
		資通安全專責	<u>每人</u> 每二年至少接受三小時以上之資通
		人員以外之資	安全專業課程訓練或資通安全職能訓
		訊人員	練,且每年接受三小時以上之資通安全
		四八只	通識教育訓練。
		一般使用者及	每人每年接受三小時以上之資通安全通
		主管	<u>識</u> 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四張以上,
			並持續維持證照之有效性。
	<u></u>		

- 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 四、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。

		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	每年至少四名人員各接受十二小時以上				
	資通安全	頁過安生及員 訊人員	之資通安全專業課程訓練或資通安全職				
	教育訓練	机人只	能訓練。				
認知	教育訓练	一般使用者及	每人每年接受三小時以上之一般資通安				
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。
- 一、「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。

- 識和是每三資教使,每時安訓練者正接上通,確明。
- 四、於備註之 養 就 配 等 是 義 配 第 是 義 配 第 黑 至 義 配 第 黑 主 之 。 移 一 死 无 。 移
- 五、其餘內容未修 正。

五、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。	
<u>六</u> 、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。	

附表三修正對照表

	修正規定			現行規定					說明
附表三 育 質 理 面	資通系統分級及防護基準 資訊安全管理系統之導入及通 過公正第三方之驗證 資通安全專責人員		辦理內容 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等級變更後之二年內,全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、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,配置二人;須以專職人員配置之。 每年辦理一次。 全部核心資通系統每二年辦理一次。	附表三 資通 管理面	辦理項目	里系統之導入及通 之驗證 一人員 一稽核 三演練	辦理內容 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所表之資,依於別別,就是一次,所以一次,所以一次,然為與一人,所以一次,然為與一人,就是一人,就是一人,就是一人,就是一人,就是一人,就是一人,就是一人,就是		於訊統過之務含等理資為之護資險面使資管安之公驗需 I 資系明強資,通,中用通理全導正證求 SO 訊統確化通降安差增危安面管入第配明 2700全
			一、除因業務需求且無其他替代方案外, 不得採購及使用主管機關核定之廠 商生產、研發、製造或提供之危害國 家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管機 關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管機 關核可採購之危害國家資通安全產 品,應列冊管理,且不得與公務網路 環境介接。	技術面	安全性檢測資通安全健診	網檢 系 網網檢 系 網網檢 所 不 不 不 不 不 不 不 不 不 不 不 不 不 不 不 不 不 不	全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。 - 每二年辦理一次。	三、	之於中安員育為職年二資訓他規認,全資訓資人至小通練資定知針及通練通員少時安課訊。與對資安,安每接以全程人。與對資訊全修全人受上專;員練通人教正專每十之業其每
技術面	安全性檢測 資通安全健 診	檢測 系統渗透測試 網路架構檢視 網路亞音活動	全部核心資通系統每年辦理一次。 全部核心資通系統每二年辦理一次。 每二年辦理一次。		資通安全威脅	線設定檢視	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 主管機關指定之方式提交監控管理資 料。		他人接上專程受之八年小通線年以通過與一個人人達之業,一個人工的一個人工的一個人工的一個人工的一個人工的一個人工的一個人工的一個人工的

		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,並持續維運及依主管機關指定之方式提交監控管理資料。
	政府組態基準		初次受核定或等級變更後之一年內,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。
	資通安全 防護	防毒軟門 網 異 器 郵 內 禦 揚 用 器 郵 件 債 傷 制 對 心 應 人 應 人 應 人 應 人 應 人 應 人 應 人 應 人 應 人 應	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。
		資通安全專職 人員	每人每年至少接受十二小時以上之資達安全專業課程訓練或資通安全職能記練。
認知	資通安全 教育訓練	資通安全專職 人員以外之資 訊人員	每人每二年至少接受三小時以上之資並安全專業課程訓練或資通安全職能記練,且每年接受三小時以上之資通安全通識教育訓練。
與訓練		一般使用者及 主管	每人每年接受三小時以上之資通安全 <u>i</u> 識教育訓練。
	資通安全專	資通安全專業 證照	初次受核定或等級變更後之一年內, 通安全專職人員總計應持有二張以上, 並持續維持證照之有效性。
	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, 通安全專職人員總計應持有二張以上, 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、「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。

	政府組態基準		初次受核定或等級變更後之一年內,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。
	資通安全 防護	防毒軟體 網有有 網有 網 門 門 門 門 門 門 門 門 門 門 門 門 門 門 門	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。
	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 <u>二名人員各</u> 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 <u>一般</u> 資通安 全教育訓練。
認知與訓練	資通安全專	資通安全專業 證照	初次受核定或等級變更後之一年內,資 通安全專職人員總計應持有二張以上, 並持續維持證照之有效性。
	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二張以上, 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、「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。

- 識和 一主每三資教 使期 解者 正接上 通,確則 解者 正接上 通,確則 解, 確則 與, 確則 與, 確則 與, 確, 。
- 五、其餘內容未修 正。

- 三、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
 四、資通安全專職人員,指應全職執行資通安全業務者。
 五、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。
- <u>六</u>、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。

附表四修正對照表

修正規定					現行規定				說明
附表四 資通	通安全責任等級	B級之特定非公務	機關應辦事項	附表四 資通	鱼安全责任等級	B級之特定非公務	機關應辦事項	- \	於管理面之資
制度面向	辨理項目	辦理項目細項	辨理內容	制度面向	辨理項目	辨理項目細項	辨理內容		訊安全管理系
資通系統分級及防護基		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 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。		資通系統分級	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,依附對自行或委外開發之資通系統,依附九完成資通系統分級,並完成附表十控制措施;其後應每年至少檢視一次通系統分級妥適性。 初次受核定或等級變更後之二年內,部核心資通系統導入 CNS 27001 資訊全管理系統。以上效果之系統或標準、其他具有同等以上效果之系統或標準,或其他公務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,並持維持其驗證有效性。			統之導入及通過公正第三才之驗證,配合實務需求明定包
	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 或 ISO 27001 等資訊安全管理系統標準、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。	管理面					含 ISO 27001等 資訊安全管 系統標準, 明確。 為資資。 為資資, 養養 養養 養養 養養 養養 養養 養養 養養
管理面	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。		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。		資通安全風 險,爰於管理
15.47.00	內部資通安全	稽核	每年辦理一次。		內部資通安全		每年辦理一次。		面中增訂限制
	業務持續運作	演練	全部核心資通系統每二年辦理一次。		業務持續運作演練		全部核心資通系統每二年辦理一次。		使用危害國家
			一、除因業務需求且無其他替代方案外,不得採購及使用主管機關核定		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。	= ,	資通安全產品 之規定。 、於認知與訓練
限制使用危害國家資通安全產品		國家資通安全產	之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安全 產品時,應具體敘明理由,經主管 機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因業 務需求且無其他替代方案經主管機 關核可採購之危害國家資通安全產 品,應列冊管理,且不得與業務網 路環境介接。	技術面	資通安全健診	系統溶透測試 網絡 網 網 網 網 網 網 機 用 活 器	全部核心資通系統每二年辦理一次。 每二年辦理一次。		中安員育為責年二資針及通練通員少時安對資安,安每接以全對資安,安每接以全資訊全
	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。	_	資通安全威脅	線設定檢視 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。		訓練課程;其 他資訊人員每 人每二年至少 接受三小時以
技術面 資通分	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	每二年辦理一次。		資通安全 防護	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	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。		上之資通安全專業,且每年接受三資通安全

		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,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	二. 4. 6. 14 P. 2. 2. 2. 2. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4. 4.
	~ · · · · · · · · · · · · · · · · · · ·	郵件過濾機制	初次受核定或等級變更後之一年內,完
	資通安全 防護	入侵偵測及防	成各項資通安全防護措施之啟用,並持
		禦機制	續使用及適時進行軟、硬體之必要更新
		具有對外服務	- 或升級。
		之核心資通系	
		統者,應備應用	
		程式防火牆	
		資通安全專責 人員	每人每年至少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	資通安全 教育訓練	資通安全專責 人員以外之資 訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練,且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及	每人每年接受三小時以上之資通安全通
		主管	識教育訓練。
			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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政 府運作或社會安定之資通系統或資通服務。
- 四、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。
- 五、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。
- <u>六</u>、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。

		入侵偵測及防 禦機制 具有對外服務 之核,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 <u>二名人員各</u> 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 <u>一般</u> 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。

- 五、其餘內容未修 正。

附表五修正對照表

		修正規	定			現行規	定		說明
付表五 資通	安全責任等級(公級之公務機關應	辨事項	I -	1	級之公務機關應到		- \	於管理面之
制度面向	辨理項目	辦理項目細項	辦理內容	制度面向	辨理項目	辦理項目細項	辨理內容		通系統分約
 	資通系統分級資訊安全管理	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 九完成資通系統分級;其後應每年至少 檢視一次資通系統分級妥適性;並應於 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 部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、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。	管理面	資通系統分級資訊安全管理		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妥適性; 一次資通系統分級妥適性; 一次資通系統分級妥適性; 一次資通系統分級妥適性; 一次資通系統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,資訊 一次資通系統國家標準、其他具有公子 一次公司, 一公公司, 一公公公司, 一公公公司, 一公公公司, 一公公公司, 一公公公司, 一公公公司, 一公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公		防除等者以級針外資完控護現級」明之對開通成制基行為之確公自發系附措準「『文規務行之統表施
資通安全專責人員 內部資通安全稽核 業務持續運作演練		稽核	初次受核定或等級變更後之一年內,配置一人;須以專職人員配置之。 每二年辦理一次。 全部核心資通系統每二年辦理一次。		準,並持續維持導入。 初次受核定或等級變更後之一年內, 置一人;須以專職人員配置之。 內部資通安全稽核 業務持續運作演練 全部核心資通系統每二年辦理一次。		ニ、	間。	
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之 危害國家資通安全產品。		安全性檢測	網站安全弱點檢測 系統渗透測試	全部核心資通系統每二年辦理一次。 全部核心資通系統每二年辦理一次。		合實務需 定包含 27001 等 安全管理
	限制使用危害	國家資通安全產	二、必須採購或使用危害國家資通安 全產品時,應具體敘明理由,經主 管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因 業務需求且無其他替代方案經主 管機關核可採購之危害國家資通 安全產品,應列冊管理,且不得與 公務網路環境介接。	技術面	資通安全健 診	網路架構檢視 網路惡意活動檢視 伊用活動檢視 電視 器 直 器 最 機 惡 意活動檢視 哥 章 最 最 最 最 最 最 最 最 最 最 最 最 最 最 最 最 最 最	- 每二年辦理一次。	三、	女標確為之護資險事, 化通降安於 人名安低全於
	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。			定及防火牆連 線設定檢視 防毒軟體			面中增訂 使用危害 資通安全
技術面	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	每二年辦理一次。		資通安全 防護	網路防火牆 具有郵件伺服器者,應備電子郵件過濾機制	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。	四、	之規認,全資資金。

		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	
		防毒軟體	初次受核定或等級變更後之一年內,完
	資通安全 防護	網路防火牆 具有郵件伺服 器者,應備電子 郵件過濾機制	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。
		資通安全專職 人員	每人每年至少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。
	資通安全 教育訓練	資通安全專職 人員以外之資 訊人員	每人每二年至少接受三小時以上之資 通安全專業課程訓練或資通安全職能 訓練,且每年接受三小時以上之資通安 全通識教育訓練。
與訓練		一般使用者及 主管	每人每年接受三小時以上之資通安全 <u>通識</u> 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 資通安全職能 評量證書	資通安全專職人員總計應持有一張以上,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 通安全專職人員總計應持有一張以上,
		資通安全職能 評量證書	

- 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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 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。
- <u>五</u>、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。

	資通安全 教育訓練	資通安全及資 訊人員	每年至少 <u>一名人員</u> 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	教月 訓練	一般使用者及 主管	每人每年接受三小時以上之 <u>一般</u> 資通 安全教育訓練。
與訓練		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	證照	上。
	業證照及職	 資通安全職能	初次受核定或等級變更後之一年內,資
	能訓練證書		通安全專職人員總計應持有一張以上,
		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、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。
- 育訓練,修正 為資通安全專 職人員每人每 年至少接受十 二小時以上之 資通安全專業 訓練課程;其 他資訊人員每 人每二年至少 接受三小時以 上之資通安全 專業訓練課 程,且每年接 受三小時以上 之資通安全通 識教育訓練; 一般使用者及 主管,修正為 每人每年接受 三小時以上之 資通安全通識 教育訓練,以 使規範明確。
- 五、於中安照續有定通員並附六致認,全,維效,安之與表之。知對專訂證性確專業表及與對專訂證性確專業表及與對專訂證性確專業表及與對專訂證與與對專試之保職性一附定無通證持之規資人,至表一
- 六、於備註增訂危 害國家資通安 全產品之定 義,以資明確,

	並配合將現行
	第二點至第四
	並配合將現行 第二點至第四 點 之 點 次 遞
	移。
	七、其餘內容未修
	正。

附表六修正對照表

		修正規	見定			現行為	見定	說明
付表六 資通	鱼安全责任等級	C級之特定非公務	機關應辦事項		1	C級之特定非公務		一、於管理面之
制度面向	辨理項目	辨理項目細項	辦理內容	制度面向	辨理項目	辦理項目細項	辦理內容	通系統分約
	資通系統分級		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 檢視一次資通系統分級妥適性; <u>並</u> 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。		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 九完成資通系統分級,其後應每年至少 檢視一次資通系統分級妥適性; <u>系統等</u> 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	防護基準 除現為 等級 之 東
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 或 ISO 27001 等資訊安全管理系統標準、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。初次受核定或等級變更後之一年內,配	管理面	資訊安全管理系統之導入		施。 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,並持續維持導入。	機關針對自 或委外開發 各級資 通 統,應完成表十之控制
管理面	資通安全專責人員 內部資通安全稽核		置一人。		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。		施之時間。二、於管理面之	
	業務持續運作		全部核心資通系統每二年辦理一次。		內部資通安全	稽核	每二年辦理一次。	訊安全管3
	来初初快 之下	八八八	一、除因業務需求且無其他替代方案		業務持續運作	演練	全部核心資通系統每二年辦理一次。	統之導入,
			外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之 危害國家資通安全產品。		安全性檢測	網站安全弱點 檢測 系統滲透測試	全部核心資通系統每二年辦理一次。	實務需求 包含 ISO 2
	限制使用危害國家資通安全產 品		一二、必須採購或使用危害國家資通安 全產品時,應具體敘明理由,經主 管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因 業務需求且無其他替代方案經主 管機關核可採購之危害國家資通 安全產品,應列冊管理,且不得與 業務網路環境介接。	技術面	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 同服器主機惡	每二年辦理一次。	等理系統確化通路等等。	
	安全性檢測	網站安全弱點 檢測 系統滲透測試	全部核心資通系統每二年辦理一次。			定及防火牆連 線設定檢視		面中增訂 使用危害 資通安全
技術面	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	每二年辦理一次。		資通安全 防護	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	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。	之規定四、於中安員 資訓練 對資 安,

		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	
		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 器者,應備電子	續使用及適時進行軟、硬體之必要更新 或升級。
		郵件過濾機制	
		資通安全專責人員	每人每年至少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	資通安全 教育訓練	資通安全專責 人員以外之資 訊人員	每人每二年至少接受三小時以上之資 通安全專業課程訓練或資通安全職能 訓練,且每年接受三小時以上之資通安 全通識教育訓練。
		一般使用者及 主管	每人每年接受三小時以上之資通安全 通識教育訓練。
	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、危害國家資通安全產品,指對國家資通安全具有直接或間接造成危害風險,影響政府運作或社會安定之資通系統或資通服務。
- 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。
- <u>五</u>、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。

認知	資通安全 教育訓練	資通安全及資 訊人員 一般使用者及	每年至少 <u>一名人員</u> 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 <u>一般</u> 資通
與訓練		主管	安全教育訓練。
			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一張以上,
			並持續維持證照之有效性。

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、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。

為資通安全專 責人員每人每 年至少接受十 二小時以上之 資通安全專業 訓練課程;其 他資訊人員每 人每二年至少 接受三小時以 上之資通安全 專業訓練課 程,且每年接 受三小時以上 之資通安全通 識教育訓練; 一般使用者及 主管,修正為 每人每年接受 三小時以上之 資通安全通識 教育訓練,以 使規範明確。

- 六、其餘內容未修 正。

附表七修正對照表

		修正規	定		現行規定				
附表七 資道	通安全責任等級	D級之各機關應辦	事項	附表七 資通	安全責任等級	D級之各機關應辦	事項	一、為強化	
制度面向	辨理項目	辨理項目細項	辨理內容	制度面向	之資通				
			一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定		防毒軟體	初次受核定或等級變更後之一年內,完	護,降資通,		
			之廠商生產、研發、製造或提供之		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	險,爰	
			危害國家資通安全產品。	技術面	防護	具有郵件伺服	續使用及適時進行軟、硬體之必要更新	面中增	
			二、必須採購或使用危害國家資通安			器者,應備電子	或升級。	使用危	
管理面	限制使用危害	2. 全產品時,應具體敘明理由,經主 郵件過濾機制	郵件過濾機制		資通安				
<u>виш</u>	<u> </u>		管機關核可後,以專案方式購置。					之規定	
				通 二、於認知與訓 中,針對一					
			業務需求且無其他替代方案經主	與訓練	教育訓練	主管	安全教育訓練。	世	
		管機關核可採購之危害國家資通 安全產品,應列冊管理,且不得與		備註:特定:					
			公務(業務)網路環境介接。	 範圍內,另	行訂定其所管集	寺定非公務機關之資	「通安全應辦事項。	管,修 人每年	
		4. + 1/ pl						小時以	
		防毒軟體	 初次受核定或等級變更後之一年內,完					通安全	
	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					育訓練	
技術面	防護	具有郵件伺服	續使用及適時進行軟、硬體之必要更新					規範明	
		器者,應備電子	或升級。					三、於備註	
		郵件過濾機制						害國家	
								全產品	
認知	資通安全	一般使用者及	每人每年接受三小時以上之資通安全					義,以資 四、其餘內	
與訓練	教育訓練	主管	通識教育訓練。					正。	
備註:	L	1						<u> </u>	
一、特定非	公務機關之中步	·目的事業主管機關	引得視實際需求,於符合本辦法規定之範圍						
			·通安全應辦事項。						
			全具有直接或間接造成危害風險,影響政						
		了通系統或資通服務							

附表八修正對照表

		修正規	定			現行規	定	說明
附表八 資達	通安全責任等級	E級之各機關應辦	事項	附表八 資通	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	辦理內容	制度面向	辨理項目	辨理項目細項	辦理內容	之資通安全防
管理面	限制使用危气品	害國家資通安全產	一、除因業務需求且無其他替代方案 外,不得採購及使用主管機關核定 之廠商生產、研發、製造或提供之 危害國家資通安全產品。 二、必須採購或使用危害國家資通安 全產品時,應具體敘明理由,經主 管機關核可後,以專案方式購置。 三、對本辦法修正施行前已使用或因 業務需求且無其他替代方案經主 管機關核可採購之危害國家資通 安全產品,應列冊管理,且不得與 公務(業務)網路環境介接。				每人每年接受三小時以上之 <u>一般</u> 資通 安全教育訓練。 機關得視實際需求,於符合本辦法規定之 機關之資通安全應辦事項。	護資險面使資之於中使管人、降安於訂害全。與對者正接、明,中用通規認,用,每個金管限國產 訓一及為受國金管限國產 訓一及為受家風理制家品 練般主每三次
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資通安全 通識教育訓練。					小時以上之資 通安全通識教 育訓練,以使
内,另 二、危害國	行訂定其所管料 家資通安全產品	毕定非公務機關之資	引得視實際需求,於符合本辦法規定之範圍 「通安全應辦事項。 「全具有直接或間接造成危害風險,影響政 多。					規範明確。

附表九修正對照表

	修正規定			現行規定 附表九 資通系統防護需求分級原則				
統防護需求分級原則			附表九 資通系					
高	中	普	防護需求 等級 構面	南	中	普		
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	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	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。	機密性	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	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	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。		
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	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	通系統受影響時,可能	完整性	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	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			
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	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	之存取或使用之中斷,	可用性	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	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	之存取或使用之中斷,		
設置或運作涉及之資通 支全相關法令,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	設置或運作涉及之資 資 選 其 報 法 令 等 響 所 等 等 通 系 統 受 影 響 , 或 影 影 響 , 或 影 。 表 。 表 。 表 。 表 。 、 、 、 、 、 、 、 、 、 、 、	作於法令有相關規範之	法律遵循性	設置或運作涉及之資 資 選 資 理 有 關 法 令 等 響 所 等 響 , 或 影 響 , 或 影 等 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。	設置或運作涉及之資 選 選 選 選 選 選 選 選 選 選 選 選 選 選 会 会 等 選 選 会 会 者 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。 。	作於法令有相關規範之		
	發通造露或常響 發通造等資生影 發通造之對信嚴 如設安資資他行性高 等統未對譽重 資統資事或常。 資統對取關等或 確或相系安合務並通受經關等或 通受訊,信嚴 通受資或之方災 實運關統全法之使事時之運關等或 通受訊,信嚴 通受資或之方災 實運關統全法之使事時之運將難 事時或副方災 事時資之、產之 資及,響,或性所外,資、產性 件,遭營將性 致可系斷產非響 系資能導影關正人致可說資生之 致可竄運將性 致可系斷產非響 系資能導影關正人資能揭產非影 資能改、產之 資能統,或常。 統通使致響執當員	統防護需求分級原則 中	病 中	病 中	病 中	於防護需求分級原則 新生質過安全事件效質 新生質過安全事件效質 接生質過安全事件效質 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 通系統受影響時,可能 通承旅授機構之質訊局 造成未經授權之質訊局 查或未經授權之資訊局 查或信學等方面將產生薪 家主責通安企事件效資 資金或學學中, 可能 過系統受影響時, 可能 過系統受影響時, 可能 過底或會等方面將產生原 查求等方面將產生原 查求等方面將產生原 查求等方面將產生原 查求等方面將產生原 查求等方面將產生原 查求等方面將產生原 查求等方面將產生原 查求等。 查求等等,可能 通系统受影響時, 可能 造成資訊網與或營運、 資產或信學等方面將產生 生有限之之影響。 完整性 資產或企業學時之 定至多學時效 資產統是影響時, 可能 造成對資訊、資通系統 查求等原 可能 造成對資訊、資通系統 查求等原 可能 造成對資訊、資通系統 查求等原 可能 造成對資訊、資通系統 查求等原 可能 查求等方面房產生有限 查求等方面房產生有限 查求等方面房產生有限 查求等方面房產生有限 查求等方面房產生有限 查求等方面房產生有限 查求等權 查求等方面房產生有限 查求等的事效 資產系統受影響而專致 資產系統受影響而專於 查求是實施表述 查求學學學學學學學學學學學學學學學學學學學學學學學學學學學學學學學學學學學		

附表十修正對照表

		修	正規定			現行規定					
附表十 賞	通系統防	護基準			附表十 資通系統防護基準						
系統 控制措施 構面	防護需求分級措施內	高	中	普	控制措施構面	防護需求 分級 措施內 容	高	中	華		
存取控制	帳號管理	期間 使應登應別通控如用。 內 內 經過期 動。 機條統通現時時度 規,使者級明明的。 機條統通現時的時度 人名 資發時 中, 一 於 過 於 過 報 的 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 報 一 一 於 過 一 一 一 於 過 一 一 一 於 過 一 一 一 於 過 一 一 一 於 過 一 一 於 過 一 一 一 於 過 一 一 一 於 過 一 一 一 一	緊禁通際期號 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內 內	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。	存取控	帳號管理	期間 医 医 医 医 医 医 医 医 医 医 医 医 医 医 医 医 医 医 医	或資號無無 為 別	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 者行為之程序)依機關 指派任務所需之授權存		無要求。		最小權限	採最小權限原則,僅允 者行為之程序)依機關 指派任務所需之授權存		無要求。		
	遠端存取	一、應監控資通系統遠 二、資通系統應採用加 三、資通系統遠端存取 定義及管理之存取 四、等級「普」之所有	密機制。 之來源應為機關已預先 控制點。	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 場 , 題 態 需 求 、 連 線 之 件 、 供 人 性 、 使 用 、 是 之 件 人 性 , 使 用 者 之 件 人 、 使 用 者 之 件 人 在 人 、 使 , 使 , 使 , 使 人 、 性 、 性 、 性 、 性 、 性 、 性 、 性 、 性 、 性 、		遠端存取	五、應監控資通系統遠 六、資通系統應採用加 七、資通系統遠端存取 定義及管理之存取 八、等級「普」之所有	密機制。 之來源應為機關已預先 控制點。	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、連規需 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 二、等級「普」之所有		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	稽核與 可歸責 性	稽核事件	三、應定期審查稽核事 四、等級「普」之所有	•	四、依規定時間週期 及紀錄留存政策, 保留稽核紀錄。 五、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
			三、應稽核資通系統
			一
			行之各項功能。
		一、資通系統產生之稽核紀錄,應依需求納入	資通系統產生之稽核
		其他相關資訊。	紀錄應包含事件類型、
		二、等級「普」之所有控制措施。	發生時間、發生位置及
	稽核紀	7 7 7 1 2 7 1 1 0	任何與事件相關之使
	錄內容		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	依據稽核紀錄儲存需求,配置稽核紀錄所需之儲	皆存容量。
	存容量		
		一、機關規定需要即 資通系統於稽核處理失	效時,應採取適當之行
		時通報之稽核失 動。	
		效事件發生時,資	
	稽核處	通系統應於機關	
	理失效	規定之時效內,對	
	之回應	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關規定之時間週期與	資通系統應使用系統
	- h mit	基準時間源進行同步。	內部時鐘產生稽核紀
	時戳及	二、等級「普」之所有控制措施。	録所需時戳,並可以對
	校時		應到世界協調時間
			(UTC)或格林威治標準
		户 Hn /性 /\) / · · · · · · · · · · · · · · · · · ·	時間(GMT)。
		一、定期備份稽核紀一、應運用雜湊或其	對稽核紀錄之存取管 四, 供四. 共和 大 拉 四 之 体
	稽核資	錄至與原稽核系 他適當方式之完	理,僅限於有權限之使 用者。
	訊之保	然不同之實體系 整性確保機制。 統。 二、等級「普」之所有	川 名 °
	護	二、等級「中」之所有 控制措施。	
		一、导級	
		一、應將備份還原,作一、應定期測試備份	一、訂定系統可容忍
		為營運持續計畫 資訊,以驗證備份	資料損失之時間
營運持	系統備	測試之一部分。 媒體之可靠性及	要求。
續計畫	份	二、應在與運作系統 資訊之完整性。	二、執行系統源碼與
		不同處之獨立設 二、等級「普」之所有	資料備份。
		施或防火櫃中,儲 控制措施。	
			

			功能,並決定應稽
			核之特定資通系
			統事件。
			六、應稽核資通系統
			管理者帳號所執
			行之各項功能。
		三、資通系統產生之稽核紀錄,應依需求納入	資通系統產生之稽核
		其他相關資訊。	紀錄應包含事件類型、
		四、等級「普」之所有控制措施。	發生時間、發生位置及
	稽核紀	- 4 (% H] - () // // // // // // // // // // // // //	任何與事件相關之使
	錄內容		用者身分識別等資訊,
	35/174		並採用單一日誌紀錄
			機制,確保輸出格式之
	4F. 12- 124	<u> </u>	一致性。
	稽核儲	依據稽核紀錄儲存需求,配置稽核紀錄所需之儲	f 仔 谷 里 °
	存容量		11 mh + 12 m - 1 11
		三、機關規定需要即 資通系統於稽核處理失	效時,應採取適當之行
		時通報之稽核失 動。	
		效事件發生時,資	
	稽核處	通系統應於機關	
	理失效	規定之時效內,對	
	之回應	特定人員提出警	
		告。	
		四、等級「中」及「普」	
		之所有控制措施。	
		三、系統內部時鐘應依機關規定之時間週期與	資通系統應使用系統
		基準時間源進行同步。	內部時鐘產生稽核紀
	時戳及	四、等級「普」之所有控制措施。	錄所需時戳,並可以對
	校時		應到世界協調時間
			(UTC)或格林威治標準
			時間(GMT)。
		三、定期備份稽核紀 三、應運用雜湊或其	對稽核紀錄之存取管
	优山次	錄至與原稽核系 他適當方式之完	理,僅限於有權限之使
	稽核資	統不同之實體系 整性確保機制。	用者。
	訊之保	統。 四、等級「普」之所有	
	護	四、等級「中」之所有 控制措施。	
		控制措施。	
		四、應將備份還原,作 三、應定期測試備份	三、訂定系統可容忍
		為營運持續計畫 資訊,以驗證備份	資料損失之時間
運持	系統備	測試之一部分。 媒體之可靠性及	要求。
計畫	份	五、應在與運作系統 資訊之完整性。	四、執行系統源碼與
·-1 ==	1/4	不同處之獨立設 四、等級「普」之所有	資料備份。
		施或防火櫃中,儲 控制措施。	另 们 两 四
		心风以八恨!'咱	

	I		
		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、訂定資通系統從中斷後至重新恢復服務之	無要求。
	系統備	可容忍時間要求。	
	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。	
		一、對帳號之網路或 資通系統應具備唯一識	別及鑑別機關使用者(或
	內部使	本機存取採取多 代表機關使用者行為之	程序)之功能,禁止使用
	用者之	重認證技術。 共用帳號。	
	識別與	二、等級「中」及「普」	
	鑑別	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	一、使用預設密碼登入
		密碼更換嘗試。	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,	後要求立即變更。
		發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
			ラスタ エクリ 五分 日 鐘内不允許該帳號
地口齿			
識別與			繼續嘗試登入或使
盤別	白八氏		用機關自建之失敗
	身分驗		驗證機制。
	證管理		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。
	鑑別資	資通系統應遮蔽鑑別過程中之資訊。	
	訊回饋		
	•		

			,
		存重要資通系統	
		軟體與其他安全	
		相關資訊之備份。	
		六、等級「中」之所有	
		控制措施。	
		三、訂定資通系統從中斷後至重新恢復服務之	無要求。
	系統備	可容忍時間要求。	
	援	四、原服務中斷時,於可容忍時間內,由備援設	
		備取代提供服務。	
		三、對帳號之網路或 資通系統應具備唯一識別	別及鑑別機關使用者(或
	內部使	本機存取採取多 代表機關使用者行為之利	程序)之功能,禁止使用
	用者之	重認證技術。 共用帳號。	
	識別與	四、等級「中」及「普」	
1	鑑別	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	一、使用預設密碼登入
1		密碼更換嘗試。	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,	後要求立即變更。
		發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
識別與			帳號繼續嘗試登
鑑別			入或使用機關自
	<i>(</i>)		建之失敗驗證機
	身分驗		制。
	證管理		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
			数期限制。
			五、使用者更換密碼
			時,至少不可以與
			前三次使用過之
			照 二
			一
			· ' '
			定措施,對非內部
			使用者,可依機關
			自行規範辦理。

	加密模	資通系統如以密碼進行鑑別時,該密碼應加密 無要求。
	組鑑別	或經雜湊處理後儲存。
	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
	展生命	確認。
	週期需	
	求階段	
	系統發	一、根據系統功能與要求,識別可能影響系統 無要求。
	展生命	之威脅,進行風險分析及評估。
	週期設	二、將風險評估結果回饋需求階段之檢核項
	計階段	目,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。
	系統發	安全檢測。 二、應注意避免軟體常見漏洞及實作必要控制
	展生命	二、具備系統嚴重錯 措施。
	週期開	誤之通知機制。 三、發生錯誤時,使用者頁面僅顯示簡短錯誤訊
	發階段	三、等級「中」及「普」 息及代碼,不包含詳細之錯誤訊息。
	XIIIX	之所有控制措
		施。
	系統發	一、執行「滲透測試」 執行「弱點掃描」安全檢測。
系統與	展生命	安全檢測。
服務獲	週期測	二、等級「中」及「普」
得	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,須注意一、於部署環境中應針
	系統發	版本控制與變更管理。 對相關資通安全
	展生命	二、等級「普」之所有控制措施。 威脅,進行更新與
	週期部	修補,並關閉不必
	署與維	要服務及埠口。
	運階段	二、資通系統相關軟
		體,不使用預設密
	1. 14 TV	碼。 次2.2.4.明7.1. 手列的四、麻肉久从7.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1
	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(A. M. S. S. M. D. M. D. A. M. D. M.
	展生命	需求(含機密性、可用性、完整性)納入委外契約。
	週期委	
	外階段	明水 "NJ-12-17-17-17-12-12-12-13-13-13-13-13-13-13-13-13-13-13-13-13-
	獲得程	開發、測試及正式作業環境應為區隔。 無要求。
	序	本丛大内然四久从水尺儿入四州上 5月111
	系統文	應儲存與管理系統發展生命週期之相關文件。
	件	

	鑑別資	資通系統應遮蔽鑑別過程中之資訊。	
	温 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	無要求。
	組鑑別	或經雜湊處理後儲存。	X 12
	非內部	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)。
	使用者	X CANONIC STATE OF THE PARTY OF	
	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	生),以檢核表方式進行
	展生命	確認。	
	週期需		
	求階段		
	系統發	三、根據系統功能與要求,識別可能影響系統	無要求。
	展生命	之威脅,進行風險分析及評估。	
	週期設	四、將風險評估結果回饋需求階段之檢核項	
	計階段	目,並提出安全需求修正。	
		四、執行「源碼掃描」四、應針對安全需求實行	作必要控制措施。
	色铁磁	安全檢測。 五、應注意避免軟體常	見漏洞及實作必要控制
	系統發 展生命	五、具備系統嚴重錯 措施。	
	展生部 週期開	誤之通知機制。 六、發生錯誤時,使用者	至 頁面僅顯示簡短錯誤訊
	過期 用 發階段	六、等級「中」及「普」 息及代碼,不包含言	羊細之錯誤訊息。
	贫 佰 权	之所有控制措	
		施。	
系統與	系統發	│三、執行「滲透測試」│執行「弱點掃描」安全세	<u></u>
水 % 类 服務獲		安全檢測。	
得	週期測	四、等級「中」及「普」	
13	試階段	之所有控制措	
	WIETZ	施。	
		三、於系統發展生命週期之維運階段,須注意	一、於部署環境中應針
	系統發	版本控制與變更管理。	對相關資通安全
	展生命	四、等級「普」之所有控制措施。	威脅,進行更新與
	週期部		修補,並關閉不必
	署與維		要服務及埠口。
	運階段		二、資通系統相關軟
			體,不使用預設密
	4 11 70		碼。
	系統發	資通系統開發如委外辦理,應將系統發展生命遇	•
	展生命	需求(含機密性、可用性、完整性)納入委外契	兴约 。
	週期委		
	外階段		l >
		1 阳水 "叫上17 工上从业理位应为后后	1 伝 邢 书 .
	養得程 序	開發、測試及正式作業環境應為區隔。	無要求。

				,
		一、資通系統應採用	無要求。	無要求。
		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。		
	傳輸之	二、使用公開、國際		
	機密性	機構驗證且未遭		
系統與	與完整	破解之演算法。		
通訊保	性	三、支援演算法最大		
護		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		
		之安全防護措		
		施。		
	資料儲	靜置資訊及相關具保	無要求。	無要求。
	存之安	護需求之機密資訊應		
	全	加密儲存。		
	漏洞修	一、定期確認資通系統	.相關漏洞修復之狀態。	系統之漏洞修復應測
	復	二、等級「普」之所有	控制措施。	試有效性及潛在影響,
			1	並定期更新。
		一、資通系統應採用	1	"
		自動化工具監控		侵跡象時,應通報機關
		進出之通信流量,		特定人員。
	資通系	並於發現不尋常		
系統與	統監控	或未授權之活動	_	
資訊完	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	時,針對該事件進	' ' ' '	
整性		行分析。	控制措施。	
		二、等級「中」之所有		
		控制措施。),	6 T. b
		一、應定期執行軟體		無要求。
		與資訊完整性檢		
	軟體及	查。	權變更特定軟體	
	資訊完	二、等級「中」之所有	及資訊。	
	整性	控制措施。	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。	1

	系統文 件	應儲存與管理系統發展	生命週期之相關文件。	
系通護網保	傳機與性之性整	六 大 證 鑰理有措	無要求。	無要求。
	資料儲 存之 全 漏洞修	施。 靜置資訊及相關具保護需求之機密資訊應加密儲存。 三、定期確認資通系統		無要求。
	復	四、等級「普」之所有 三、資通系統應採用		試有效性及潛在影響, 並定期更新。 發現資通系統有被入
系統 築 報 性	資通系 統監控	三、	偵測攻擊與未授 權之連線,並識別 資通系統之未授 權使用。	
	軟體及 資訊完 整性	三、應定期執行軟體 與資訊完整性檢 查。 四、等級「中」之所有 控制措施。	四、使用完整性驗證 工具,以偵測未授 權變更特定軟體 及資訊。 五、使用者輸入資料 合法性檢查應置	無要求。

	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。

	放於應用系統伺
	服器端。
	六、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。