附表一 資通安全責任等級 A 級之公務機關應辦事項修正規定

初次受核定或等級變更後之一年內對自行或奏外開發之資通系統,名附表九完成資通系統分級人防護基準 初次受核定或等級變更後之二年內一 全部核心資通系統等入 CNS 27001 写 180 27001 等 資訊安全管理系統之事人及通		1		6機關應辦事項修正放及	
等通系統分級及防護基準 針對自行或委外開發之資通系統,係 所表九完成資通系統分級及防護基準 初大党核定通通系統分級交通性。 初次受核定或等級變更後之二年內 空部核心資通系統等入 CNS 27001 可 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者 準 执 其他公務機關自行资發展並經經 上	制度面向	辨理項目	辨理項目細項	辨理內容	
 遭通系統分級及防護基準	管理面				
表十之控制措施;其後應每年至少物。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。全部核心資通系統等入 CNS 27001 目 ISO 27001 等資訊安全管理系統之等入及通期 其他具有同等或以上效果之系統或者 集中,或其他公務機關自行發展並經濟管機關認可之標準,於三年內完成 2 正第三方驗證,並持續維持其驗證的 放大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。 每年辦理二次。 第點掃描 全部核心資通系統每年辦理一次。 對點掃描 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。 每年辦理一次。 每年辦理一次。 每年辦理一次。 對點掃描 全部核心資通系統每年辦理一次。 例				針對自行或委外開發之資通系統,依	
 觀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。全部核心資通系統學入CNS 27001 等資訊安全管理系統標準其他具有同等或以上效果之營理系統標準其他具有同等或以上效果之為或者變更後之一年內。		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	
被求受核定或等級變更後之二年內。全部核心資通系統等入 CNS 27001 頁 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核學,或上學性內方於發展主經經過公正第三方之驗證 對他具有同等或以上致果之系統或核學,或其持續維持其驗證材效性。 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。 每年辦理二次。 全年核心資通系統每年辦理一次。 資本方理成熟度評估 每年辦理一次。 資本核心資通系統每年辦理一次。 海路掃描 全部核心資通系統每年辦理一次。 海路掃描 全部核心資通系統每年辦理一次。 海路掃描 全部核心資通系統每年辦理一次。 海路掃檢視 網路惡意活動檢視 阿路器其機惡意活動檢視 日錄伺服器設定及防火牆連線設定檢視 和次受核定或等級變更後之一年內。完成成會偵測機制建置,並持續維護發度檢測,與所發或應人主管機關指定之方式提交監控資度 以與實料。其監控範圍的發展,對於政策與機制,與所發系統實質,其一數,與所發系統實質,與關稅或應用程式紀錄。 初次受核定或等級變更後之一年內。 公職服務或應用程式紀錄。 初次受核定或等級變更後之一年內,這場服務或應用程式紀錄。 初次受核定或等級變更後之一年內,				表十之控制措施;其後應每年至少檢	
全部核心資通系統導入 CNS 27001 m 1SO 27001 m 1SO 27001 m 1SO 27001 m 1 m 27001 m 1SO 27001 m 2 m 2 m 2 m 2 m 2 m 2 m 2 m 2 m 2 m				視一次資通系統分級妥適性。	
管理面				初次受核定或等級變更後之二年內,	
 資訊安全管理系統之導入及通過公正第三方之驗證 其他具有同等或以上效果之系統或核常與認可之標準,於三年內完成或性機關自行發展並經經濟機關認可之標準,於三年內完成或性。 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。 每年辦理一次。 查部核心資通系統每年辦理一次。 會本的核心資通系統每年辦理一次。 有數學聚構檢視網路惡意活動檢視。 有所與需要之健康 意活動檢視。 自錄用器設定及防火牆連線設定檢視 方活動檢視。 百餘用器設定及防火牆連線設定檢視 有數學更後之一年內完成或會負測機制建置,並持續維持其監控整價,與內容監控管理資料。 資訊股務或應用程式紀錄。 內次受核定或等級變更後之一年內完於護」之辦理內容、目錄服務系統與機關核心資通系統之資通政備紀針及資訊服務或應用程式紀錄。 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。 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。 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。 初次受核定或等級變更後之一年內。 可以限務或應用程式紀錄。 初次受核定或等級變更後之一年內。 可以限務或應用程式紀錄。 初次受核定或等級變更後之一年內。 可以股份可以股份可以股份可以股份可以股份可以股份可以股份可以股份可以股份可以股份				全部核心資通系統導入 CNS 27001 或	
選公正第三方之驗證				ISO 27001 等資訊安全管理系統標準、	
理公止第三方 之驗證 中,與其他公務機關目行等在內完成名 正第三方驗證,並持續維持其驗證核 效性。 前通安全稽核 業務持續運作演練 責安治理成熟度評估 安全性檢測 所點掃描 安全性檢測 一方方面。 一方方面。 一方方面。 一方方面。 一方方面。 一方面。 一面。 一					
管機關認可之標準,於三年內完成在正第三方驗證,並持續維持其驗證析效性。					
正第三方驗證,並持續維持其驗證有效性。					
数性。					
資通安全專責人員 初次受核定或等級變更後之一年內。 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。 安全性檢測 奶點掃描 安全性檢測 全部核心資通系統每年辦理二次。 渗透測試 全部核心資通系統每年辦理一次。 網路架構檢視 網路票書機惡意活動檢視 (使用者端電腦惡意活動檢視 日銀器書機惡意活動檢視 目錄何服器主機惡意活動檢視 日錄同服器設定及防火牆連線設定檢視 被設定檢視 初次受核定或等級變更後之一年內等 方成成會負測機制建置,並持續維近及依主管機關指定之方式提交監控行場談。 工場監控範圍應包括本表所與機關核心資通系統之資通設備紀銀及資訊服務或應用程式紀錄。 有關服務或應用程式紀錄。 初次受核定或等級變更後之一年內					
大海面 中国					
內部資通安全稽核 業務持續運作演練 資安治理成熟度評估 安全性檢測 好點掃描 多透測試 全部核心資通系統每年辦理二次。 会部核心資通系統每年辦理二次。 經路架構檢視 網路惡意活動 檢視 使用者端電腦 意活動檢視 同服器主機惡 意活動檢視 目錄伺服器設定及防火牆連 線設定檢視 技術面 技術面		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。 每年辦理一次。 安全性檢測		內部資通安全			
資安治理成熟度評估 每年辦理一次。 安全性檢測 預點掃描 全部核心資通系統每年辦理二次。 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 惡意活動檢視 信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 每年辦理一次。 技術面 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,並持續維護 及依主管機關指定之方式提交監控管 以上對於關係之資資料。其監控範圍應包括本表所沒完成整價,與是監控範圍。包括本表所沒定 對理內容、目錄服務系統與機關核心資通系統之資通設備紀銀及資訊服務或應用程式紀錄。 技術面 初次受核定或等級變更後之一年內完成或會通設備紀載及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內完成或等級變更後之一年內完成或等級變更後之一年內完成。					
安全性檢測					
安全性檢測		安全性檢測			
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 同服器主機惡意活動檢視 目錄伺服器設定及防火牆連 線設定檢視					
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 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 完成威脅偵測機制建置,並持續維 及依主管機關指定之方式提交監控管 理資料。其監控範圍應包括本表所 写演出。其監控範圍應包括本表所 写演出。其監控範圍應包括本表所 可端點偵測及應變機制」與「資通等 全防護」之之辨理內容、自錄服務系統 與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內				生部核心貝迪尔統母中辦理一人。	
檢視 使用者端電腦 惡意活動檢視 同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 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,並持續維護 及依主管機關指定之方式提交監控管 理資料。其監控範圍應包括本表所定 單資料。其監控範圍應包括本表所定 "端點偵測及應變機制」與「資點。其監控範圍。包括本表所與 "以辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內			· · · · · · · · · · · · · · · · · · ·	恶意活動	
使用者端電腦 惡意活動檢視 同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 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,並持續維定及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所足以端點偵測及應變機制」與「資過等全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內					
資通安全健 惡意活動檢視					
移術面 持術面 持術面 持術面 持術面 持術面 持術面 持術面 持術面 表示 表示 表示 表示 表示 表示 表示 表					
意活動檢視 日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威脅偵測機制建置,並持續維護及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所欠「端點偵測及應變機制」與「資通安全成費的護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內					
接術面					
技術面			意活動檢視		
接術面 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,並持續維護及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所以 "			目錄伺服器設		
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,並持續維護及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定可以 以 與 與 與 人 與 人 與 人 與 機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。			定及防火牆連		
完成威脅偵測機制建置,並持續維護及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定可端點偵測及應變機制」與「資通等全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內	技術面		線設定檢視		
及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所知 可以以及應變機制」與「資通等 全防護」之辦理內容、目錄服務系統 與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內		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,	
資通安全威脅偵測管理機制 理資料。其監控範圍應包括本表所定 「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統 與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 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	
算通安全威賀偵測管理機制 「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統 與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內:				及依主管機關指定之方式提交監控管	
一端點負測及應變機制」與一頁通名 全防護」之辦理內容、目錄服務系統 與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內:				理資料。其監控範圍應包括本表所定	
與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內				「端點偵測及應變機制」與「資通安	
與機關核心資通系統之資通設備紀錄 及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內				全防護」之辦理內容、目錄服務系統	
及資訊服務或應用程式紀錄。 初次受核定或等級變更後之一年內:				與機關核心資通系統之資通設備紀錄	
初次受核定或等級變更後之一年內					
		政府組態基準			
以灯組然本午 化土宝碳 圖公古之 埧 目 , 元				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。	
		北京仙作甘油		初次受核定或等級變更後之一年內,	

	1			
	資通安全弱點通報機制		· - -	初次受核 東 東 東 大 一 一 一 一 一 一 一 一 一 一 一 一 一
	端點偵測及應變機制		· · ·	初次受核定或等級變更後之二年內,完成端點偵測及應變機制導人作業,並持續維運及依主管機關指定之方式提交偵測資料。本辦法中華民國一百十年八月十二十三修正施行後二年內,完者以此一次修正施行後二年內,完成此點偵測及應變機制導入作業之方式提交偵測資料。
	資 通 安 全	防毒軟門 網有,過信 時期 時期 時期 時期 時期 時期 時期 時期 時期 時期 時期 時期 時期	完成.	受核定或等級變更後之一年內, 各項資通安全防護措施之啟用, 續使用及適時進行軟、硬體之必 新或升級。
認知與訓練	資 通 安 全 教育訓練	資 資 資 選 安全專職 過 安全專 選 以 外 之 員 一般使用者及主 管	通訓每通訓安每安練人安練全人	每年至少接受十二小時以上之資 全專業課程訓練或資通安全職能 每二年至少接受三小時以上之資 全專業課程訓練或資通安全職能 ,且每年接受三小時以上之資通 通識教育訓練。 每年接受三小時以上之資通安全 教育訓練。

資通安全專業證照及職能訓練 證書

- 一、初次受核定或等級變更後之一年內,至少四名資通安全專職人員,分別各自持有證照及證書各一張以上,並持續維持證照及證書之有效性。
- 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者, 應於修正施行後一年內符合規定。

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,指通過我國標準法主管機關委託機構認證 之機構;第三方核發之驗證證書應有前開委託機構之認證標誌。
- 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、資通安全弱點通報機制,指結合資訊資產管理與弱點管理,掌握整體風險情勢,並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。
- 六、端點偵測及應變機制,指具備對端點進行主動式掃描偵測、漏洞防護、可疑 程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。
- 七、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。