

教育部 函

機關地址：10051臺北市中山南路5號

聯絡人：林文信

電話：02-7712-9092

Email：ansel@mail.moe.gov.tw

受文者：國立暨南國際大學

發文日期：中華民國107年11月28日

發文字號：臺教資(四)字第1070206590號

速別：普通件

密等及解密條件或保密期限：

附件：原函、資通安全管理法施行細則、資通安全責任等級分級辦法、資通安全事件通報及應變辦法、特定非公務機關資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法、公務機關所屬人員資通安全事項獎懲辦法

主旨：函轉行政院函送資通安全管理法相關子辦法業經行政院於中華民國107年11月21日以院臺護字第1070213547號令訂定發布，請查照並轉知所屬機關(構)、監督之行政法人及所管公營事業與政府捐助之財團法人。

說明：

- 一、依據行政院107年11月21日院臺護字第1070213547B號函辦理。
- 二、檢送「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法」、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」、「公務機關所屬人員資通安全事項獎懲辦法」法規條文各1份。

正本：部屬機關(構)及國家運動訓練中心、各公立大學校院、各國立專科學校、臺灣學術網路區域網路中心、各直轄市及縣市教育網路中心、財團法人教育部接受捐助獎學基金會、財團法人大學入學考試中心基金會、財團法人私立學校興學基金會、財團法人高等教育評鑑中心基金會、財團法人中華幼兒教育發展基金會、財團法人台灣省中小學校教職員福利文教基金會、財團法人國民教育測驗與評量中心教育基金會、財團法人高等教育國際合作基金會、財團法人蔣經國國際學術交流基金會、財團法人社教文化基金會、財團法人臺灣省童軍文教基金會、財團法人吳健雄學術基金會

副本：

107/11/29
電子印章
09:44:13



行政院 函

地址：10058臺北市忠孝東路1段1號
傳真：02-23973457
聯絡人：王詠萱02-33566500#8207
電子信箱：yswang@ey.gov.tw

受文者：教育部

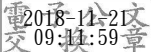
發文日期：中華民國107年11月21日
發文字號：院臺護字第1070213547B號
速別：普通件
密等及解密條件或保密期限：
附件：如文(1070213547B-0-0.docx、1070213547B-0-1.docx、1070213547B-0-2.docx、1070213547B-0-3.docx、1070213547B-0-4.docx、1070213547B-0-5.docx)

主旨：「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報及應變辦法」、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」、「公務機關所屬人員資通安全事項獎懲辦法」，業經本院於中華民國107年11月21日以院臺護字第1070213547號令訂定發布，請查照並轉知所屬機關(構)、監督之行政法人及所管公營事業與政府捐助之財團法人。

說明：

- 一、依據資通安全管理法第7條第1項、第7條第2項、第8條第2項、第14條第4項及第18條第4項、第15條第2項及第19條第2項、第22條規定辦理。
- 二、檢送旨揭法規條文各1份。

正本：總統府、國家安全會議、立法院、司法院、考試院、監察院、各部會行總處署、省政府、各直轄市政府、各縣市政府

副本： 



資通安全管理法施行細則

第一條 本細則依資通安全管理法(以下簡稱本法)第二十二條規定訂定之。

第二條 本法第三條第五款所稱軍事機關，指國防部及其所屬機關(構)、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款及第二項規定之機關。

第三條 公務機關或特定非公務機關(以下簡稱各機關)依本法第七條第三項、第十三條第二項、第十六條第五項或第十七條第三項提出改善報告，應針對資通安全維護計畫實施情形之稽核結果提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形：

- 一、缺失或待改善之項目及內容。
- 二、發生原因。
- 三、為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施。
- 四、前款措施之預定完成時程及執行進度之追蹤方式。

第四條 各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供(以下簡稱受託業務)，選任及監督受託者時，應注意下列事項：

- 一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
- 二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
- 三、受託者辦理受託業務得否複委託、得複委託之

範圍與對象，及複委託之受託者應具備之資通安全維護措施。

- 四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。
- 五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
- 六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
- 七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。
- 八、受託者應採取之其他資通安全相關維護措施。
- 九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項：

- 一、曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。
- 二、曾任公務員，因違反相關安全保密規定受懲戒

或記過以上行政懲處。

三、曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

四、其他與國家機密保護相關之具體項目。

第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。

第五條 前條第三項及本法第十六條第一項之書面，依電子簽章法之規定，得以電子文件為之。

第六條 本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

- 一、核心業務及其重要性。
- 二、資通安全政策及目標。
- 三、資通安全推動組織。
- 四、專責人力及經費之配置。
- 五、公務機關資通安全長之配置。
- 六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。
- 七、資通安全風險評估。
- 八、資通安全防護及控制措施。
- 九、資通安全事件通報、應變及演練相關機制。
- 十、資通安全情資之評估及因應機制。
- 十一、資通系統或服務委外辦理之管理措施。
- 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。
- 十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括

前項各款之執行成果及相關說明。

第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關得由其上級或監督機關辦理；特定非公務機關得由其中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辦理，或經中央目的事業主管機關同意，由其所管特定非公務機關辦理。

第七條 前條第一項第一款所定核心業務，其範圍如下：

- 一、公務機關依其組織法規，足認該業務為機關核心權責所在。
- 二、公營事業及政府捐助之財團法人之主要服務或功能。
- 三、各機關維運、提供關鍵基礎設施所必要之業務。
- 四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第四款涉及之業務。

前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。

第八條 本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告，應包括下列事項：

- 一、事件發生或知悉其發生、完成損害控制或復原作業之時間。
- 二、事件影響之範圍及損害評估。
- 三、損害控制及復原作業之歷程。
- 四、事件調查及處理作業之歷程。
- 五、事件根因分析。
- 六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

七、前款措施之預定完成時程及成效追蹤機制。

第九條 中央目的事業主管機關依本法第十六條第一項規定指定關鍵基礎設施提供者前，應給予其陳述意見之機會。

第十條 本法第十八條第三項及第五項所稱重大資通安全事件，指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。

第十一條 主管機關或中央目的事業主管機關知悉重大資通安全事件，依本法第十八條第五項規定公告與事件相關之必要內容及因應措施時，應載明事件之發生或知悉其發生之時間、原因、影響程度、控制情形及後續改善措施。

前項與事件相關之必要內容及因應措施，有下列情形之一者，不予公告：

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或公開有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。

二、其他依法規規定應秘密、限制或禁止公開之情形。

第一項與事件相關之必要內容及因應措施含有前項不予公告之情形者，得僅就其他部分公告之。

第十二條 特定非公務機關之業務涉及數中央目的事業主管機關之權責者，主管機關得協調指定一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。

第十三條 本細則之施行日期，由主管機關定之。

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

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		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。
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，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
		網路防火牆	
		具有郵件伺服器	

		者，應備電子郵件過濾機制	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	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。

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。
- 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。
	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。
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，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	
		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		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。

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。
- 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
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。
	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。
	資安治理成熟度評估		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，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	

認知 與訓練		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	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。
		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。

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。
- 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	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。
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，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	
		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		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。

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。
- 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	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；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。
	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；須以專職人員配置之。
	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	具有郵件伺服器者，應備電子郵件過濾機制	
		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	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。

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、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	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；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。
	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。
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	具有郵件伺服器者，應備電子郵件過濾機制	
		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	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。
--	----------	--

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。

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	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。

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	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。

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

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。	一、使用預設密碼登入系統時，應於登入後要	

		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。 三、等級「普」之所有控制措施。		求立即變更。 二、身分驗證相關資訊不以明文傳輸。 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。	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	

		三、等級「中」及「普」之所有控制措施。	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。	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	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試

資訊完整性	復	二、等級「普」之所有控制措施。		有效性及潛在影響，並定期更新。
	資通系統監控	一、資通系統應採用自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。	一、監控資通系統，以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。	發現資通系統有被入侵跡象時，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：

- 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、開道器、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。

資通安全事件通報及應變辦法

第一章 總則

第一條 本辦法依資通安全管理法（以下簡稱本法）第十四條第四項及第十八條第四項規定訂定之。

第二條 資通安全事件分為四級。

公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件：

- 一、非核心業務資訊遭輕微洩漏。
- 二、非核心業務資訊或非核心資通系統遭輕微竄改。
- 三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。

各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件：

- 一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。
- 二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。
- 三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：

- 一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴

重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。

二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。

三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。

各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件：

一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。

二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。

三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

第三條 資通安全事件之通報內容，應包括下列項目：

一、發生機關。

二、發生或知悉時間。

三、狀況之描述。

四、等級之評估。

五、因應事件所採取之措施。

六、外部支援需求評估。

七、其他相關事項。

第二章 公務機關資通安全事件之通報及應變

第四條 公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。

前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。

公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

第五條 主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。

二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。

總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。

前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審核結果通知主管機關，並提供審核依據之相關資訊。

總統府、國家安全會議、立法院、司法院、考試院、

監察院及直轄市、縣（市）議會，應於其自身完成資通安全事件之通報後，依第一項規定時間完成該資通安全事件等級之審核，並依前項規定通知主管機關及提供相關資訊。

主管機關接獲前二項之通知後，應依相關資訊，就資通安全事件之等級進行覆核，並得依覆核結果變更其等級。但主管機關認有必要，或第二項及前項之機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。

第六條 公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜：

一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。

前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。

上級、監督機關或主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。

第七條 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，就所屬、監督、所轄或業務相關之公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。

主管機關就公務機關執行資通安全事件之應變作

業，得視情形提供必要支援或協助。

公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。

第八條 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。

前項演練作業之內容，應至少包括下列項目：

一、每半年辦理一次社交工程演練。

二、每年辦理一次資通安全事件通報及應變演練。

總統府與中央一級機關及直轄市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。

第九條 公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

一、判定事件等級之流程及權責。

二、事件之影響範圍、損害程度及機關因應能力之評估。

三、資通安全事件之內部通報流程。

四、通知受資通安全事件影響之其他機關之方式。

五、前四款事項之演練。

六、資通安全事件通報窗口及聯繫方式。

七、其他資通安全事件通報相關事項。

第十條 公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

一、應變小組之組織。

二、事件發生前之演練作業。

三、事件發生時之損害控制機制。

四、事件發生後之復原、鑑識、調查及改善機制。

五、事件相關紀錄之保全。

六、其他資通安全事件應變相關事項。

第三章 特定非公務機關資通安全事件之通報及應變

第十一條 特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。

前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。

特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。

特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。

第十二條 中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級：

一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。

二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。

中央目的事業主管機關依前項規定完成資通安全事件之審核後，應依下列規定辦理：

一、審核結果為第一級或第二級資通安全事件者，應定期彙整審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。

二、審核結果為第三級或第四級資通安全事件者，應於審核完成後一小時內，將審核結果、

依據及其他必要資訊，依主管機關指定之方式送交主管機關。

主管機關接獲前項資料後，得就資通安全事件之等級進行覆核，並得為等級之變更。

第十三條 特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：

一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。

前項調查、處理及改善報告送交之時限，得經中央目的事業主管機關同意後延長之。

中央目的事業主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。

特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應於審查後送交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。

第十四條 中央目的事業主管機關就所管特定非公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。

主管機關就特定非公務機關執行資通安全事件應變作業，得視情形提供必要支援或協助。

特定非公務機關知悉第三級或第四級資通安全事件後，應召開會議研商相關事宜。

第十五條 特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項：

- 一、判定事件等級之流程及權責。
- 二、事件之影響範圍、損害程度及機關因應能力之評估。
- 三、資通安全事件之內部通報流程。
- 四、通知受資通安全事件影響之其他機關之時機及方式。
- 五、前四款事項之演練。
- 六、資通安全事件通報窗口及聯繫方式。
- 七、其他資通安全事件通報相關事項。

第十六條 特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：

- 一、應變小組之組織。
- 二、事件發生前之演練作業。
- 三、事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。
- 四、事件發生後之復原、鑑識、調查及改善機制。
- 五、事件相關紀錄之保全。
- 六、其他資通安全事件應變相關事項。

第四章 附則

第十七條 主管機關就各機關之第三級或第四級資通安全事件，得召開會議，邀請相關機關研商該事件之損害控制、復原及其他相關事宜。

第十八條 公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：

- 一、社交工程演練。
- 二、資通安全事件通報及應變演練。
- 三、網路攻防演練。
- 四、情境演練。
- 五、其他必要之演練。

第十九條 特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目：

- 一、網路攻防演練。
- 二、情境演練。
- 三、其他必要之演練。

主管機關規劃、辦理之資通安全演練作業，有侵害特定非公務機關之權利或正當利益之虞者，應先經其書面同意，始得為之。

前項書面同意之方式，依電子簽章法之規定，得以電子文件為之。

第二十條 公務機關於本辦法施行前，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安全事件之通報及應變。

前項通報及應變機制如有變更，應送主管機關重為核定。

第二十一條 本辦法之施行日期，由主管機關定之。

特定非公務機關資通安全維護計畫實施情形稽核辦法

第一條 本辦法依資通安全管理法（以下簡稱本法）第七條第二項規定訂定之。

第二條 本辦法所定書面，依電子簽章法之規定，得以電子文件為之。

第三條 主管機關應每年擇定當年度各季受稽核之特定非公務機關（以下簡稱受稽核機關），並以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。

主管機關擇定前項受稽核機關時，應綜合考量其業務之重要性與機敏性、資通系統之規模與性質、資通安全事件發生之頻率與程度、資通安全演練之成果、歷年受主管機關或中央目的事業主管機關稽核之頻率與結果或其他與資通安全相關之因素。

主管機關為辦理第一項稽核，應訂定稽核計畫，其內容包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及中央目的事業主管機關協助事項。

主管機關決定前項稽核之重點領域與基準及項目時，應綜合考量我國資通安全政策、國內外資通安全趨勢、過往稽核計畫之內容與稽核結果，及其他與稽核資源之適當分配或稽核成效相關之因素。

第四條 主管機關辦理前條第一項之稽核，應將稽核計畫於一個月前以書面通知受稽核機關。

受稽核機關如因業務因素或有其他正當理由，得於收受前項通知後五日內，以書面敘明理由向主管機關申請調整稽核日期。

前項申請，除有不可抗力之事由外，以一次為限。

第五條 主管機關辦理第三條第一項之稽核，得要求受稽核機關為資通安全維護計畫實施情形之說明、協力或提出相關之文件、證明資料供現場查閱，並執行下列事項，受稽核機關及其所屬人員應予配合：

- 一、稽核前訪談。
- 二、現場實地稽核。

受稽核機關依法律有正當理由，未能為前項說明、協力或提出資料供現場查閱者，應以書面敘明理由，向主管機關提出。

主管機關收受前項書面後，應進行審核，依下列規定辦理，並得停止稽核作業之全部或一部：

- 一、認有理由者，應將審核之依據及相關資訊記載於稽核結果報告。
- 二、認無理由者，應要求受稽核機關依第一項規定辦理；已停止稽核作業者，得擇期續行辦理，並於十日前以書面通知受稽核機關。

第六條 主管機關辦理第三條第一項之稽核，應依同條第二項所定考量因素，就各受稽核機關分別組成三人至七人之稽核小組。

主管機關組成前項稽核小組時，應考量稽核之需求，邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者擔任小組成員，其中公務機關代表不得少於全體成員人數之三分之一。

主管機關應以書面與稽核小組成員約定利益衝突之迴避及保密義務。

第二項之公務機關代表或專家學者，有下列情形之一者，應主動迴避擔任該次稽核之稽核小組成員：

- 一、本人、其配偶、三親等內親屬、家屬或上開人

員財產信託之受託人，與受稽核機關或其負責人間有財產上或非財產上之利害關係。

二、本人、其配偶、三親等內親屬或家屬，與受稽核機關或其負責人間，目前或過去二年內有僱傭、承攬、委任、代理或其他類似之關係。

三、本人目前或過去二年內任職之機關（構）或單位，曾為受稽核機關之顧問，其輔導項目與受稽核項目相關。

四、其他情形足認擔任稽核小組成員，將對稽核結果之公正性造成影響。

第七條 主管機關應於每季所定受稽核機關之稽核作業完成後一個月內，將稽核結果報告交付該季受稽核機關。

前項稽核結果報告之內容，應包括稽核之範圍、缺失或待改善事項、第五條第二項所定受稽核機關未能為說明、協力或提出資料供現場查閱之情形、理由與同條第三項所定主管機關審核結果，及其他與稽核相關之必要內容。

第八條 受稽核機關經發現其資通安全維護計畫實施情形有缺失或待改善者，應於主管機關交付稽核結果報告後一個月內，依主管機關指定之方式提出改善報告，並送交中央目的事業主管機關；主管機關及中央目的事業主管機關認有必要時，得要求該受稽核機關進行說明或調整。

前項受稽核機關提出改善報告後，應依主管機關指定之方式及時間，提出改善報告之執行情形，並送交中央目的事業主管機關；主管機關認有必要時，得要求該受稽核機關進行說明或調整。

第九條 主管機關辦理第三條第一項之稽核，得要求受稽核機關之中央目的事業主管機關派員為必要協助。

第十條 本辦法之施行日期，由主管機關定之。

資通安全情資分享辦法

第一條 本辦法依資通安全管理法（以下簡稱本法）第八條第二項規定訂定之。

第二條 本辦法所稱資通安全情資（以下簡稱情資），指包括下列任一款內容之資訊：

- 一、資通系統之惡意偵察或情蒐活動。
- 二、資通系統之安全漏洞。
- 三、使資通系統安全控制措施無效或利用安全漏洞之方法。
- 四、與惡意程式相關之資訊。
- 五、資通安全事件造成之實際損害或可能產生之負面影響。
- 六、用以偵測、預防或因應前五款情形，或降低其損害之相關措施。
- 七、其他與資通安全事件相關之技術性資訊。

第三條 主管機關應就情資分享事宜進行國際合作。

主管機關應適時與公務機關進行情資分享。

公務機關應適時與主管機關進行情資分享。但情資已依前項規定分享或已經公開者，不在此限。

中央目的事業主管機關應適時與其所管之特定非公務機關進行情資分享。

特定非公務機關得與中央目的事業主管機關進行情資分享。

第四條 情資有下列情形之一者，不得分享：

- 一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人

民生命、身體、健康有必要，或經當事人同意者，不在此限。

二、其他依法規規定應秘密或應限制、禁止公開之情形。

情資含有前項不得分享之內容者，得僅就其他部分分享之。

第五條 公務機關或特定非公務機關（以下簡稱各機關）進行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。

第六條 各機關應就所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。

第七條 各機關進行情資整合時，得依情資之來源、接收日期、可用期間、類別、威脅指標特性及其他適當項目與內部情資進行關聯分析。

公務機關應就整合後發現之新型威脅情資進行分享。

第八條 各機關應就所接收之情資，採取適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。

第九條 各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。

各機關因故無法依前項規定方式進行情資分享者，分別經主管機關或中央目的事業主管機關同意後，得以下列方式之一為之：

- 一、書面。
- 二、傳真。
- 三、電子郵件。

四、資訊系統。

五、其他適當方式。

第十條 未適用本法之個人、法人或團體，經主管機關或中央目的事業主管機關同意後，得與其進行情資分享。

主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享，應以書面與其約定應遵守第四條至前條之規定。

第十一條 本辦法施行日期，由主管機關定之。

公務機關所屬人員資通安全事項獎懲辦法

第一條 本辦法依資通安全管理法（以下簡稱本法）第十五條第二項及第十九條第二項規定訂定之。

第二條 公務機關就其所屬人員辦理業務涉及資通安全事項之獎懲，得依本辦法之規定自行訂定獎懲基準。

第三條 有下列情形之一者，予以獎勵：

- 一、依本法、本法授權訂定之法規或機關內部規範，訂定、修正及實施資通安全維護計畫，績效優良。
- 二、稽核所屬或監督機關之資通安全維護計畫實施情形，或辦理資通安全演練作業，績效優良。
- 三、配合主管機關、上級或監督機關辦理資通安全維護計畫實施情形之稽核或資通安全演練作業，經評定績效優良。
- 四、辦理資通安全業務切合機宜，防止資通安全事件之發生，避免本機關、其他機關或人民遭受損害。
- 五、主動發現新型態之資通安全弱點或入侵威脅，並進行資通安全情資分享，防止資通安全事件之發生或降低其損害。
- 六、積極查察資通安全維護之異狀，即時發現重大資通安全事件，並辦理通報及應變，防止其損害擴大。
- 七、對資通安全業務提出具體建議或革新方案，並經採行。
- 八、辦理資通安全人才培育事務，有具體貢獻。
- 九、辦理資通安全科技之研發、整合、應用、產學合作或產業發展事務，有具體貢獻。

十、辦理資通安全軟硬體技術規範、相關服務及審驗機制發展等事務，有具體貢獻。

十一、辦理資通安全政策、法制研析或國際合作事務，有具體貢獻。

十二、辦理其他資通安全業務有具體功績。

第四條 有下列情形之一者，予以懲處：

一、未依本法、本法授權訂定之法規或機關內部規範辦理下列事項，情節重大：

(一)資通安全情資分享作業。

(二)訂定、修正及實施資通安全維護計畫。

(三)提出資通安全維護計畫實施情形。

(四)辦理資通安全維護計畫實施情形之稽核。

(五)配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出改善報告。

(六)訂定資通安全事件通報及應變機制。

(七)資通安全事件之通報或應變作業。

(八)提出資通安全事件調查、處理及改善報告。

二、辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。

三、其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。

第五條 公務機關辦理其所屬人員之平時考核，應審酌前二條所定獎勵及懲處情形，依事實發生之原因、經過、行為之動機、目的、手段、表現、所生之影響等因素為之；其所屬人員為聘用人員、約僱人員或其他與機關有僱傭關係之人員者，其獎勵及懲處之情形並應納入續聘之參考。

第六條 公務機關對所屬人員作成第四條各款情形之懲處前，應給予當事人申辯之機會；必要時，得就所涉資通

安全專業事項，徵詢相關專家學者之意見。

第七條 本辦法之施行日期，由主管機關定之。