資通安全管理法及子法彙編

行政院

中華民國 108 年 9 月

目次

壹、 法規條文

一、資通安全管理法

總統令　　中華民國 107 年 6 月 6 日
華總一義字第 10700060021 號

茲制定資通安全管理法，公布之。

總　　統　蔡英文
行政院院長　賴清德

資通安全管理法

中華民國 107 年 6 月 6 日公布

第一章 總則

第一條　為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。

第二條　本法之主管機關為行政院。

第三條　本法用詞，定義如下：

一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、資通安全：指防止資通系統或資訊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，以確保其機密性、完整性及可用性。

四、資通安全事件：指系統、服務或網路狀態經

鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

五、 公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。

六、 特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

七、 關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。

八、 關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關指定，並報主管機關核定者。

九、 政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。

第四條　為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：

一、 資通安全專業人才之培育。

二、 資通安全科技之研發、整合、應用、產學合作及國際交流合作。

三、 資通安全產業之發展。

四、 資通安全軟硬體技術規範、相關服務與審

驗機制之發展。

前項相關事項之推動，由主管機關以國家資通安全發展方案定之。

第五條　主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。

前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。

第六條　主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。

前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。

第七條　主管機關應衡酌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；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之。

主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。

特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。

第八條　主管機關應建立資通安全情資分享機制。

前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。

第九條　公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

第二章　公務機關資通安全管理

第十條　公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

第十一條　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

第十二條　公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。

第十三條　公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。

受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。

第十四條　公務機關為因應資通安全事件，應訂定通報及應變機制。

公務機關知悉資通安全事件時，除應通報上

級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。

公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。

第十五條　公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。

前項獎勵事項之辦法，由主管機關定之。

第三章特定非公務機關資通安全管理

第十六條　中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。

關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。

中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。

關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關。

第二項至第五項之資通安全維護計畫必要事

項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。

第十七條　關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。

中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。

前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。

第十八條　特定非公務機關為因應資通安全事件，應訂定通報及應變機制。

特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。

特定非公務機關應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。

前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由主管機關定之。

知悉重大資通安全事件時，主管機關或中央目的事業主管機關於適當時機得公告與事件相關之必要內容及因應措施，並得提供相關協助。

第四章 罰則

第十九條　公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。

前項懲處事項之辦法，由主管機關定之。

第二十條　特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰：

一、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫必要事項之規定。

二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。

三、未依第七條第三項、第十六條第五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條第六項或第十七條第四項所定辦法中有關改善報告提出之規定。

四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八條第四項所定辦法中有關通報及應變

機制必要事項之規定。

五、 未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。

六、 違反第十八條第四項所定辦法中有關通報內容之規定。

第二十一條　特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

第五章 附則

第二十二條　本法施行細則，由主管機關定之。

第二十三條　本法施行日期，由主管機關定之。

二、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。

三、資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定
中華民國 108 年 8 月 26 日行政院院臺護字第 1080184606 號令修正

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、資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、 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。

七、 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機關、監督機關或上開機關指定之公務機關兼辦或代管。

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、中央目的事業主管機關所管特定非公務機關或出資之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；特定非公務機關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；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。

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。

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。
	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。
	限制使用危害國家資通安全產品		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	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。
		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、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。

六、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。
	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。
	限制使用危害國家資通安全產品		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，且不得與業務網路環境介接。
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。
		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、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。

六、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。
	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。
	限制使用危害國家資通安全產品		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	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。
		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、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。

六、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。
	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。
	限制使用危害國家資通安全產品		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，且不得與業務網路環境介接。
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。
		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、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。

六、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；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。
	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。
	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。
	限制使用危害國家資通安全產品		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	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	
		目錄伺服器設定及防火牆連	

		線設定檢視	
	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	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。
		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，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、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。

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；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。
	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。
	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。
	限制使用危害國家資通安全產品		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，且不得與業務網路環境介接。
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	
		目錄伺服器設	

		定及防火牆連線設定檢視	
	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	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。
		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、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。

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
管理面	限制使用危害國家資通安全產品		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。
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資通安全通識教育訓練。

備註：

一、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。

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。

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
管理面	限制使用危害國家資通安全產品		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。
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。

備註：

一、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。

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。

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

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
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。 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。	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	一、執行「源碼掃描」安	一、應針對安全需求實作必要控制措施。

	展生命週期開發階段	全檢測。 二、具備系統嚴重錯誤之通知機制。 三、等級「中」及「普」之所有控制措施。	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護措施。	無要求。	無要求。
	資料儲	靜置資訊及相關具保護	無要求。	無要求。

	存之安全	需求之機密資訊應加密儲存。		
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，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、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。

四、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。

五、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。

六、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。

七、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。

貳、逐條說明

一、資通安全管理法

條　　文	說　　明
第一章　　總則	章名。
第一條　為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。	一、明定本法之立法目的。 二、隨著數位及其他資通科技(Information Communication Technology)應用之普及，資通安全議題日益受到重視。為有效規劃我國之資通安全管理政策，落實於公、私部門，以建構安全之資通環境，進而保障國家安全，維護社會公共利益，特制定本法。
第二條　本法之主管機關為行政院。	明定本法之主管機關為行政院。
第三條　本法用詞，定義如下： 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。 二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。 三、資通安全：指防止資通系統或資訊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，以確保其機密性、完整性及可用性。 四、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。 五、公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。	明定本法用詞定義，說明如下： 一、參考美國國家標準技術研究所（National Institute of Standards and Technology）SP800-60 Volume I: Guild for Mapping Type of Information and Information System to Security Categories 及經濟部標準檢驗局公布國家標準 CNS 27001「資訊技術－安全技術－資訊安全管理－要求事項」等文件，於第一款至第四款規定資通系統、資通服務、資通安全及資通安全事件之定義。 二、第五款及第六款規定公務機關及特定非公務機關。公務機關指依法行使公權力之中央、地方機關（構）或公法人，例如總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、公立社會教育機構、公立文化機構、公立醫療機構或行政法人等。另考量軍事機關及情報機關之性質特殊，其資通安

六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 七、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。 八、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關指定，並報主管機關核定者。 九、政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。	全管理宜由該等機關另行規定，故定明非屬本法所稱公務機關；該等機關之範圍，將於施行細則中規範。特定非公務機關則包括關鍵基礎設施提供者、公營事業及政府捐助之財團法人。其中政府捐助之財團法人之定義，則明定於第九款。 三、參考美國 31 CFR 800.208 所定關鍵基礎設施（critical infrastructure）、日本網路安全基本法（サイバーセキュリティ基本法）第三條所定重要社會基礎業者、韓國情報通信基礎保護法(정보통신기반보호법)第二條所定情報通信基礎設施等定義，於第七款明定關鍵基礎設施之內涵，並考量關鍵基礎設施因應環境與時代變遷，其範圍可能調整，故規定由行政院公告之。我國現行重要關鍵基礎設施所涉領域包括能源、水資源、通訊傳播、交通、金融、高科技園區等；以通訊傳播領域為例，目前該領域之一級關鍵基礎設施均為我國第一類電信業者；又以高科技園區為例，園區本身為關鍵基礎設施，而提供該園區正常運作之電力、電信及供水等設施者，即為關鍵基礎設施提供者，而位於園區內之廠商則為使用者，非關鍵基礎設施提供者。行政院為本款規定之公告時，將僅公告領域名稱(如通訊傳播、高科技園區)，並將公布該領域內為關鍵基礎設施提供者之組織名稱，而非公布該組織內之關鍵基礎設施具體設備。 四、考量關鍵基礎設施對國家安全、社會公共利益、國民生活及經濟活動有重大影響，然各維運關鍵基礎設施之特定非公務機關其屬性及重要性仍有不同，爰於第八款規定關鍵

	基礎設施提供者為由中央目的事業主管機關指定其中具重要性者，並報行政院核定之。另為合理及適切訂定關鍵基礎設施提供者範疇，中央目的事業主管機關於指定關鍵基礎設施提供者前，應徵詢相關公務機關、民間團體、專家學者之意見，事後並應以書面通知受核定者。 五、提供或維運關鍵基礎設施之全部或一部者，如屬本法所定義之公務機關，應遵循本法有關公務機關之規定；至其他關鍵基礎設施之提供者，則應遵循本法有關關鍵基礎設施提供者之規定。 六、非提供或維運關鍵基礎設施功能或重要元件設施，而僅提供關鍵基礎設施所需用之其他設備或服務者，雖非本法所稱關鍵基礎設施提供者，但如其係受關鍵基礎提供者委託辦理資通系統之建置、維運或資通服務之提供時，仍應依第九條規定，受委託者之監督。 七、本法係以風險管理概念界定規範對象，即經由風險評估程序，認其資通安全有相當風險者，始納入本法規範範疇；目前係以組織為規範對象，並非以個人為規範對象，且未及於所有民間企業、團體，須視其是否屬本法所定特定非公務機關之範疇而定，併予敘明。
第四條　為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項： 一、資通安全專業人才之培育。 二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。 三、資通安全產業之發展。 四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。 前項相關事項之推動，由主管機關以國家資通安全發展方案定之。	一、鑒於資通安全之提升須以全民重視為前提，並須佐以先進之資通安全技術、軟硬體、專業人才等資源，政府應與民間共同提升全民資通安全意識，以利先進資通安全技術、軟硬體、專業人才等之發展，爰參考日本網路安全基本法第十九條產業之振興及國際競爭力強化、第二十條研究開發之推動、第二十一條人才之確保等規定，為本

	條第一項規範，並於第二項明定本條相關事事項之推動，由行政院以國家資通安全發展方案定之。 二、 關於租稅優惠措施，因事涉國家稅收，且現行已有產業創新條例、科學技術基本法等法律相關規定可資運用，爰不另於本法規範，併予敘明。
第五條　主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。 前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。	一、 考量我國有關資通安全政策之推動所涉範圍甚廣，為利相關業務之推動，行政院應考量國家資通安全相關事務發展之需求，規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜。為使各界了解國家資通安全趨勢，行政院原則將每年公布國家資通安全情勢報告及對公務機關資通安全維護計畫實施情形稽核概況報告；另配合國家資通安全政策之推動，原則以四年為一期公布資通安全發展方案，逐年滾動檢討修正並公布，爰於第一項明定上開事項。 二、 為使立法院能掌握國家資通安全情勢、行政院對公務機關資通安全維護計畫實施情形之稽核概況及資通安全發展方案，爰於第二項明定第一項之報告及方案均應送立法院備查。
第六條　主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。 前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。	一、 除政策制定等本質上不宜委任或委託辦理之事務外，行政院為推動資通安全業務，如有需要，得依行政程序法第十五條或第十六條規定，委任或委託其他公務機關、法人或團體辦理。為利實務運作，爰為本條規範。又委外事務倘不涉及公權力之移轉，例如國際法規或國際政策之研析，或雖為資通安全整體防護或國際交流等事項而未有公權力移轉之情形時，則仍應依政

	府採購法等規定辦理。 二、 行政院依本條規定為委任或委託，因涉及公權力之移轉，應考量事務之性質、對象之屬性等事項，先行評估委任或委託辦理之適當性後，再行為之。 三、 為保障關鍵基礎設施提供者之秘密不因主管機關之委託或委任而有洩露的情形，明定被委託者在執行過程中就獲悉之秘密有保密之義務。
第七條　主管機關應衡酌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；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主管機關定之。 主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。 特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。	一、 考量公務機關與特定非公務機關之規模及業務性質不一，其應遵行之資通安全責任等級亦應有不同，此外，資通安全責任等級宜因機關調整、裁撤、業務變動或運用之資通系統發生重大變更等事由，而有所調整，以達到資通安全防護之最適效果。就此，目前有「政府機關（構）資通安全責任等級分級作業規定」可作為遵循之參考；於資通安全管理法制化後，上述諸事宜亦應加以規定，爰於第一項明定行政院應衡酌公務機關及特定非公務機關業務等事項，訂定資通安全責任等級之分級，並就其分級基準、等級變更申請、義務內容及專責人員之設置及其他相關事項，授權該院訂定辦法規範。 二、 為監督特定非公務機關實施資通安全維護計畫之情形，爰為第二項規定，並授權行政院訂定稽核頻率、內容與方法及其他相關事項之辦法。行政院依本項進行稽核時，應考量稽核對象之責任等級、其過往資通安全維護狀況、歷來接受行政院、中央目的事業主管機關稽核之頻率、結果及其他相關情形，決定最適之受稽核者名單。至於公務機關資通安全維護計畫實施情形

	之稽核，則於第十三條規範。 三、 考量特定非公務機關依第二項規定接受稽核後，經發現其資通安全維護計畫實施有缺失或待改善情形，宜由行政院及相關機關進行監督，確認改善之狀況，爰為第三項規定。
第八條　主管機關應建立資通安全情資分享機制。 前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。	一、為增進與改善我國境內面對資通安全威脅與風險之應變能力及策略擬定，應建立相關資通安全情資分享機制，爰為第一項規定。 二、第二項定明資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由行政院定之，以資遵循。
第九條　公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。	考量公務機關或特定非公務機關於本法適用範圍內委外辦理資通系統建置、維運或資通服務之提供時，應依所委外項目之性質與資通安全需求，選任適當之受託者，並就受託者之資通安全維護為監督，以確保國家安全、社會公共利益或個人權益，爰為本條規定。相關監督事項之技術性及細節性內容，將於施行細則中規定。
第二章　公務機關資通安全管理	章名。
第十條　公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。	一、 為確保公務機關之資通安全，避免因人為疏失、蓄意或自然災害等風險，致機關資通系統或資訊遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務，公務機關（包含總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府與其所屬或監督之各級公務機關及直轄市議會、縣（市）議會等）應符合第七條第一項所定資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，爰為本條規

	定。公務機關訂修及實施上開計畫，應衡酌機關資源之合理分配，並依循上級或監督機關之相關資通安全規定為之。 二、 有關資通安全維護計畫之內容，將由行政院訂定範本，提供各公務機關參考，以利執行。
第十一條　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。	為確保有效推動資通安全維護事項，公務機關應置資通安全長，由其成立相關推動組織及督導推動相關工作。考量資通安全長如由副首長擔任，更能提升資通安全於機關中之重要性，並參考美國二〇一四年聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014）§3554關於資訊長應指定資深資安專責人員負責相應事務規定之意旨，爰為本條規定。
第十二條　公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。	參考日本網路安全基本法第十二條有關促進地方公共團體確保網路資訊安全相關事項之規定，及同法第三十條規定相關行政機關之首長應適時提供與網路資訊安全相關之資料或資訊，以利執行所掌事務之精神，明定公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形，以確認其實施成效，並使上級或監督機關得了解及稽核所屬或受監督機關之年度資通安全維護情形。另因總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議會及縣（市）議會等公務機關無上級機關，爰規定無上級機關者應將資通安全維護計畫實施情形送交行政院。行政院收受上開計畫實施情形後將予以備查，並得視情形提供必要協助。
第十三條　公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。	一、 第一項規定公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。各公務機關對於其所屬或監督之各級公務機關，應依其機關層級、業務及其他相關情形，就稽核之基準、頻率、內容與方法訂定相關行政規則，以利執行。稽核時，宜考量受稽核者歷來接受行

	政院、上級或監督機關稽核之頻率與結果等因素，決定最適之受稽核者。 二、 第二項規定受稽核機關之資通安全維護計畫實施有缺失或待改善者，應向稽核機關及上級或監督機關提出改善報告，以確保資通安全維護計畫之落實及政府資通安全維護之強度。
第十四條　公務機關為因應資通安全事件，應訂定通報及應變機制。 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。 公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。	一、 為即時掌控資通安全事件，並有效降低其所造成之損害，爰於第一項規定公務機關應建立資通安全事件之通報及應變機制。資通安全事件之具體類型將於施行細則及本條第四項授權訂定之辦法中規範。 二、 參考日本網路安全基本法第十八條政府相關組織就有重大網路安全影響之虞之事件有相互合作、分享資訊並採取必要措施之義務之規定，於第二項明定公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院。另因總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議會及縣（市）議會等公務機關無上級機關，爰規定無上級機關者應通報行政院。 三、 考量公務機關於知悉資通安全事件後，應進行調查、處理及改善工作，爰於第三項規定公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交行政院，以利上級機關、監督機關或行政院監督，並得據以提供必要之協助。 四、 關於公務機關資通安全事件之通報及應變，目前有「國家資通安全通報應變作業綱要」可資遵循參考，於本法施行後，應檢視原有機制並依本法要求調整之，故第四項

	授權行政院訂定第一項至第三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，以利公務機關適用。
第十五條　公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。 前項獎勵事項之辦法，由主管機關定之。	為促進公務機關所屬人員對於資通安全工作之重視與投入，該等人員於踐行本法要求事項成果優良或卓越時，應予獎勵，其獎勵辦法由行政院定之，爰為本條規定。
第三章　特定非公務機關資通安全管理	章名。
第十六條　中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。 關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。 關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。 中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。 關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關。 第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。	一、 第一項規定關鍵基礎設施提供者之指定及其程序。關鍵基礎設施提供者之資通安全維護，乃現今國際針對資通安全保護所重視之議題，爰參考歐盟二〇一六年「網路與資訊系統安全指令」(The Directive on security of network and information systems)第五條關於關鍵服務營運商之清單、第十四條關於關鍵服務營運商用以提供關鍵服務之網路與資訊系統，如有影響其安全之事件，關鍵服務營運商須採取適當措施及最小化事件之影響，以確保服務之持續性、美國 6 USC §132 指定關鍵基礎設施保護計畫(Designation of critical infrastructure protection program)及第一三六三六號行政命令有關改善關鍵基礎設施網路安全（Executive Order 13636）、日本網路安全基本法第六條重要社會基礎業者之職責、韓國情報通信基礎保護法第八條中央行政機關長官有權指定主要資訊通信基礎設施及同法第五條主要資訊通信基礎設施保護措施之制定等立法例，將關鍵基礎設施提供者納入本法之適用範圍。 二、 因關鍵基礎設施涉及國家安全、社

	會公共利益、國民生活及經濟活動，爰於第二項規定關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並訂定、修正及實施資通安全維護計畫，以確保其資通安全。 三、 為使中央目的事業主管機關掌握所管關鍵基礎設施提供者之資通安全維護計畫實施狀況，爰於第三項規定關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形，以利中央目的事業主管機關監督，並適時提供相關建議或協助。 四、 為確保資通安全維護計畫之落實，於第四項規定中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。稽核時，宜考量受稽核者歷來接受行政院、中央目的事業主管機關稽核之頻率與稽核結果等因素，決定最適之受稽核者名單與頻率。 五、 第五項規定關鍵基礎設施提供者之資通安全維護計畫實施情形有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關，以確保資通安全維護計畫之落實。 六、 考量資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，其內容宜有一致性，以利關鍵基礎設施提供者適用與遵循，爰於第六項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。 七、 中央目的事業主管機關宜訂定特定非公務機關資通安全維護計畫之範本，以供非公務機關參考；行政院並得提供必要之協助。
第十七條　　關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬	一、 考量關鍵基礎設施提供者以外之特定非公務機關亦應負相當之資通安

資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。 中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。 前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。	全責任，仍應訂定安全維護計畫並提出計畫實施情形，爰參考日本網路安全基本法第三條賦予重要社會基礎業者配合政府資通安全政策之協力義務之規定，於第一項明定該等非公務機關應符合其所屬資通安全責任等級之要求，並修訂及實施資通安全維護計畫。 二、 鑒於資通安全維護事項與事業之經營管理關係密切，對於特定非公務機關資通安全維護之指導、監督、管理及稽核，宜由各特定非公務機關之中央目的事業主管機關執行，爰為第二項及第三項規定。 三、 考量資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，其內容宜有一致性，以利第一項之特定非公務機關適用與遵循，爰於第四項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。 四、 中央目的事業主管機關宜訂定特定非公務機關資通安全維護計畫之範本，以供特定非公務機關參考；行政院並得提供必要之協助。
第十八條　特定非公務機關為因應資通安全事件，應訂定通報及應變機制。 特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。 特定非公務機關應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由主管機關定之。 知悉重大資通安全事件時，主管機關或中央目的事業主管機關於適當	一、 為使中央目的事業主管機關、行政院即時掌握特定非公務機關之資通安全事件，監督及協助該等特定非公務機關進行緊急應變處置，並在最短時間內回復業務正常運作，爰參考歐盟二〇一六年「網路與資訊系統安全指令」第十四條事件通知、日本網路安全基本法第十四條促進重要社會基礎業者確保網路資訊安全、韓國情報通信基礎保護法第十六條於金融、通信等領域別之情報通信基礎設施業者得依法成立及運作情報共有、分析中心，作為有侵害事故時之即時警報與分析體系等

時機得公告與事件相關之必要內容及因應措施，並得提供相關協助。	規定，為第一項至第三項規定。重大資通安全事件之認定，將於施行細則中規範。 二、 第四項明定第一項至第三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由行政院定之，以利特定非公務機關依循。 三、 考量重大資通安全事件可能影響多數人民之生命、身體或財產安全，宜由行政院、中央目的事業主管機關於知悉後，分別或共同公告必要之內容(例如發生原因、影響程度及目前控制之情形等)及因應措施，並提供相關協助，以利防範、避免損害之擴大，爰為第五項規定。
第四章　罰則	章名。
第十九條　公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。 前項懲處事項之辦法，由主管機關定之。	對於公務機關所屬人員之懲戒、懲處本有公務人員考績法、公務員懲戒法等規定加以規範，惟為促進該等人員對於資通安全工作之重視與投入，爰於本條規定行政院應訂定懲處事項之辦法，對公務機關所屬人員未遵守本法規定者，按情節輕重予以懲處。
第二十條　特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰： 一、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫必要事項之規定。 二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。 三、未依第七條第三項、第十六條第	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為，制定有效罰則之意旨，並考量違反本法所定行政法上義務應受責難程度及其所生影響，針對特定非公務機關未依本法規定訂定、修正、實施資通安全維護計畫、提出資通安全維護計畫之實施情形、改善報告送交中央目的事業主管機關、訂定資通安全事件之通報及應變機制、向中央目的事業主管機關或行政院提出資通安全事件之調查、處理及改善報告，或違反資通安全事件通報內容之規定等情形，明定所課予之行政裁罰。

五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條第六項或第十七條第四項所定辦法中有關改善報告提出之規定。 四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八條第四項所定辦法中有關通報及應變機制必要事項之規定。 五、未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。 六、違反第十八條第四項所定辦法中有關通報內容之規定。	
第二十一條　特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為，制定有效罰則之意旨，並考量違反本法所定行政法上義務應受責難程度及其所生影響，針對特定非公務機關未依第十八條第二項規定，通報資通安全事件之情形，明定所課予之行政裁罰。
第五章 附則	章名。
第二十二條　本法施行細則，由主管機關定之。	本法施行細則之訂定機關。
第二十三條　本法施行日期，由主管機關定之。	本法施行日期，考量配套子法作業時程，並為周延法制，以落實本法規定之執行，爰授權由行政院定之。

二、資通安全管理法施行細則

條文	說明
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。	明定本細則訂定之依據。
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。	參考國家情報工作法及檢察機關辦理刑事案件與軍事機關聯繫要點之規定，明定本法第三條第五款所稱軍事機關及情報機關之範圍。
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。	明定公務機關或特定非公務機關（以下簡稱各機關）之資通安全維護計畫實施情形經稽核發現缺失或待改善時，所提改善報告應包含之內容，以及後續執行情形之提出，說明如下： 一、第一款及第二款為該缺失或待改善事項之具體項目與內容及發生原因。 二、第三款所定措施，係因應缺失或待改善項目所採取之機關組織、作業程序、應變機制、人員管考、教育訓練、實體或虛擬設備等管理、技術、人力或資源等層面之相關措施。 三、第四款所定預定完成時程及執行進度之追蹤方式，係因應缺失或待改善項目所規劃採行相關措施之時程評估，及為確認其效果所進行之追蹤、管考。
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。	一、依本法第九條規定各機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。為利執行，爰於第一項明定相關注意事項，說明如下： (一)為確保受託者辦理受託業務之程序及環境具安全性，並得妥善執行受託業務，爰為第一款及第二

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。	款規定。第一款所稱第三方，係指通過我國標準法主管機關委託機構認證之機構，其驗證標準可為國際、國家或團體標準。 (二)委託機關應依受託業務之性質，決定是否允許受託者就受託業務為複委託；如允許複委託，應注意得複委託之範圍與對象，及複委託之對象應具備之資通安全維護措施，爰為第三款規定。 (三)考量國家機密牽涉國家之安危或重大利益，應嚴加保護，爰於第四款明定受託業務涉及國家機密時，受託者辦理該項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，以利各機關謹慎審酌其辦理受託業務之合宜性及維護國家機密。 (四)為確保受託業務執行之適法性及安全性，受託業務如包含客製化資通系統之開發，應確保該資通系統之安全性，如委託金額達一定金額以上，或該資通系統為委託機關核心資通系統時，應由委託機關自行或委託公正之第三方進行安全性檢測之複測；且該業務如涉及利用非自行開發之系統或資源，受託者並應標示與揭露該系統或資源之內容與其來源，及提供授權證明，爰為第五款規定。所定委託金額達新臺幣一千萬元以上，係參考目前政府採購法勞務採購之查核金額定之。所稱第三方，同上開(一)之說明。 (五)受託者執行受託業務，有違反資通安全相關法令之情形，或知悉資通安全事件時，為避免損害擴大，應立即將相關情狀通知委託機關，並採行諸如啟動備援、回復運轉、損害管制等適當之補救措施，爰為第六款規定。 (六)為確保對於受託業務相關資料及

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。	系統之保護，受託者於委託關係結束時，應返還、移交、刪除或銷毀為履行契約所持有之資料，爰為第七款規定。 (七)委託機關就委外辦理之業務，得要求受託者依業務之性質及內容，調整其須具備之資通安全相關維護措施，爰為第八款規定。 (八)為確保受託業務執行之妥適性，委託機關應定期檢視執行狀況；於知悉受託者發生可能影響受託業務之資通安全事件時，亦應確認受託業務之執行情形，爰為第九款規定。 二、適任性查核之對象應包括受託者辦理該受託業務之人員及可能接觸該國家機密之人員。而查核之項目則應考量上開業務所涉及之機密等級、內容，於必要範圍內查核之。各機關於辦理受託業務之委外作業時，若有第一項第四款之情事者，應於招標公告、招標文件、委外契約中敘明受託者辦理該項受託業務之人員及可能接觸該國家機密之人員，應接受查核之項目，使其知悉並以書面同意。為使規範明確，以利執行，爰為第二項及第三項規定。
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。	明定本辦法及本法所定書面，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	一、 為利各機關訂定、修正及實施資通安全維護計畫，爰於第一項明定該計畫應包括之內容，說明如下： （一）各機關為有效落實其資通系統之安全管理，應釐清其核心業務，並說明該業務之重要性為何，爰為第一款規定。 （二）各機關依其業務性質推動資通安全維護事項，應建立資通安全政策，並應於各內部單位建立與資通安全政策一致之資通安全目標，爰為第二款規定。 （三）第三款至第五款明定計畫應包括

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。	機關內部推動資通安全事務之組織，與為達成資通安全政策及目標，所配置之專責人力及資源，公務機關並應配置資通安全長。 （四）各機關為有效推動資通安全管理，應盤點其資訊、資通系統，並應標示核心資通系統及相關資產，以利執行風險評估等作業，爰為第六款規定。 （五）第七款明定資通安全維護計畫之內容應包括資通安全風險評估相關之資訊，例如：機關應建立相關之風險評估機制，並了解諸如資訊儲存區域、組織面、實體面、技術面及作業面等資通安全風險；風險評估之範圍，包含第六款規定盤點之資訊、資通系統及相關資產。 （六）第八款明定資通安全維護計畫之內容應包括機關針對其資訊、資通系統及相關資產，應採取之防護及控制措施。 （七）第九款明定資通安全維護計畫之內容應包括機關資通安全事件通報、應變及演練相關機制。 （八）為強化各機關對於資通安全情資之應用，於第十款明定機關應訂定評估及因應之相關機制，例如於收受資通安全情資後，應評估情資之內容，據以決定是否就資通安全維護計畫、資通安全事件之通報、應變方式或其他資通安全維護事宜為調整及因應。 （九）第十一款明定資通安全維護計畫應載明委外辦理資通系統或服務時之管理措施，以利執行本法第九條所定對受託者進行之監督。 （十）公務機關所屬人員辦理業務涉及資通安全事項者，應適時予以考核，爰於第十二款明定資通安全維護計畫應包含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。

	（十一）第十三款明定資通安全維護計畫應包含該計畫與實施情形之持續精進及績效管理機制，例如計畫合宜性、適切性及有效性之持續改善方式，以及對於相關人員之績效管理機制。 二、為利各機關依本法規定提出資通安全維護計畫實施情形，爰於第二項明定其提出資料應包括之必要內容。 三、考量部分公務機關或特定非公務機關之人力等行政資源可能較為不足，其資通安全維護計畫之訂修、執行及實施情形之提出等事宜，倘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、中央目的事業主管機關所管特定非公務機關統一辦理，較符合行政效率；為符合實務執行需求，以利資通安全維護業務之推展，爰於第三項明定資通安全維護計畫之訂定、修正、實施及其實施情形之提出，除由各機關自行辦理外，亦得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辦理，或經中央目的事業主管機關同意後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	一、第一項明定第六條第一項第一款之核心業務之範圍。公務機關之核心業務，應視其組織法規之規定或業務是否係屬維運、提供關鍵基礎設施所必要進行判斷；於公營事業及政府捐助財團法人，則視其是否係屬主要服務或功能所在；各機關業務如涉關鍵基礎設施，則其維運、提供關鍵基礎設施所必要之業務，以及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，亦屬各機關之核心業務。另是否係屬核心業務，除由特定非公務機關自行認定外，中央目的事業主管機關

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。	亦得協助認定之，併予敘明。 二、第二項明定第六條第一項第六款之核心資通系統，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，以利各機關辦理本法及相關法令要求之事項，並強化各機關之資通安全防護。
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。	明定資通安全事件調查、處理及改善報告應包括之內容。
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。	為保障人民權益，明定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。	明定重大資通安全事件之定義。
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	為利相關機關辦理本法第十八條第五項重大資通安全事件之公告，使民眾了解其事件之必要內容及因應措施，並考量民眾權益之保護及公共利益之維護，爰明定公告時應載明之事項及不予公告之情形。

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。	考量特定非公務機關之業務性質可能涉及數個中央目的事業主管機關之權責，為避免發生該等中央目的事業主管機關就本法所定事宜權責不清之情形，爰明定主管機關得協調指定其中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。	明定本細則之施行日期，由主管機關定之。

三、資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定
中華民國 108 年 8 月 26 日行政院院臺護字第 1080184606 號令修正

部分條文修正條文對照表

修正條文	現行條文	說明
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	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	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。

或非常嚴重之影響。 七、屬公立醫學中心。	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、資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、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。 七、屬公立區域醫院或	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	一、序文、第二款及第三款未修正。 二、現行第一款所定「捐助」是否包含「資助」之情形，文義未盡清楚，為使規範更為明確，爰修正第一款，增訂「資助」之文字。所定「資助」，包含補助、委託或出資等方式。 三、考量公務機關之業務若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，具有相當之資通安全風險，爰增訂第四款，納入上開情形規定。 四、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，爰修正現行第四款並配合遞移款次為第五款，以保留彈性及符合實務需求。 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。

地區醫院。	響。 六、 屬公立區域醫院或地區醫院。	
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機關、監督機關或上開機關指定之公務機關兼辦或代管。 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、中央目的事業主管機關所管特定非公務機關或出資之公務機關兼辦或代管。	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。	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機關兼辦或代管，及特定非公務機關之全部資通業務由其出資之公務機關兼辦或代管者，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，爰修正第二款及第三款，將上開情形納入規定。
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；特定非公務機關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。	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。	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

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；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。	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。	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　本辦法之施行日期，由主管機關定之。	一、第一項未修正。 二、為明定本辦法修正條文之施行日期，爰增訂第二項規定。

資通安全責任等級分級辦法

中華民國 107 年 11 月 21 日行政院院臺護字第 1070213547 號令訂定

條文	說明
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。	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，	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。 二、基於尊重總統府、國家安全會議及行政院以外其他四院之權限，該等公務機關及其所屬、監督或所管之各機關（特定非公務機關部分，例如司法院所管之財團法人法律扶助基金會）之資通安全責任等級，宜由其自行認定，並於核定後送主管機關備查即可；至於行政院直屬機關與各地方自治團體之行政及立法機關，主管機關應督導或協助其辦理資通安全維護業務，該等機關及其所屬、監督或所管之各機關之資通安全責任等級，宜由主管機關核定，爰分別於第二項至第五項明定各機關資通安全責任等級之認定程序。 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

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。	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。	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。
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	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。

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。	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、	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，因業務機敏性、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，而有調整分級之必要。為利第三條第一項至第五項之公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。各機關資通安全責任等級之認定，原則應依第四條至第九條規定辦理，例外則得視實務狀況，依本條規定予以適當調

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。	整其等級。
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。	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。 二、 考量部分公務機關或特定非公務機關辦理附表一至附表八所定事項及附表十所定控制措施，可能因技術限制、個別資通系統之設計、結構或性質等因素而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，爰於第三項明定有該等情形者，經第三條第二項至第四項之等級提交機關或同條第五項之等級核定機關同意

	並報請主管機關備查後，得免執行該事項或控制措施。 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，由主管機關定之。	明定本辦法之施行日期，由主管機關定之。

附表一修正對照表

修正規定

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<u>或ISO 27001等</u>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，<u>並</u>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。
	<u>限制使用危害國家資通安全產品</u>		<u>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。</u> <u>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。</u> <u>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。</u>
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	

現行規定

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<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。
	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。

說明

一、於管理面之資訊安全管理系統之導入及通過公正第三方之驗證，配合實務需求明定包含ISO 27001等資訊安全管理系統標準，以資明確。

二、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

三、於認知與訓練中，針對資通安全及資訊人員資通安全教育訓練，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

		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。
		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：

	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。

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。

四、於備註增訂危害國家資通安全產品之定義，以資明確，並配合將現行第三點至第五點之點次遞移。

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。 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。 六、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

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<u>或ISO 27001等</u>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，<u>並</u>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。
	<u>限制使用危害國家資通安全產品</u>		<u>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。</u> <u>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。</u> <u>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。</u>
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	

現行規定

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<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。
	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	

說明

一、於管理面之資訊安全管理系統之導入及通過公正第三方之驗證，配合實務需求明定包含ISO 27001等資訊安全管理系統標準，以資明確。

二、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

三、於認知與訓練中，針對資通安全及資訊人員資通安全教育訓練，修正為資通安全專責人員每人每年至少接受十二小時以上之

		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。
		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、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	
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。

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。

四、於備註增訂危害國家資通安全產品之定義，以資明確，並配合將現行第三點至第五點之點次遞移。

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。 六、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

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<u>或ISO 27001等</u>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。
	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。
	<u>限制使用危害國家資通安全產品</u>		<u>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。</u> <u>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。</u> <u>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。</u>
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	

現行規定

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<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。
	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。

說明

一、於管理面之資訊安全管理系統之導入及通過公正第三方之驗證，配合實務需求明定包含ISO 27001等資訊安全管理系統標準，以資明確。

二、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

三、於認知與訓練中，針對資通安全及資訊人員資通安全教育訓練，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

		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。
		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。

	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。

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。

四、於備註增訂危害國家資通安全產品之定義，以資明確，並配合將現行第三點至第五點之點次遞移。

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。 六、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

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<u>或ISO 27001等</u>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。
	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。
	<u>限制使用危害國家資通安全產品</u>		<u>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，且不得與業務網路環境介接。</u>
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	

現行規定

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<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。
	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	

說明

一、於管理面之資訊安全管理系統之導入及通過公正第三方之驗證，配合實務需求明定包含ISO 27001等資訊安全管理系統標準，以資明確。

二、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

三、於認知與訓練中，針對資通安全及資訊人員資通安全教育訓練，修正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

		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。
		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、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。

六、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。

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。

四、於備註增訂危害國家資通安全產品之定義，以資明確，並配合將現行第三點至第五點之點次遞移。

五、其餘內容未修正。

附表五修正對照表

修正規定

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；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。
	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。
	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。
	限制使用危害國家資通安全產品		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	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	

現行規定

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	
		目錄伺服器設定及防火牆連線設定檢視	
	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	

說明

一、於管理面之資通系統分級及防護基準，刪除現行「系統等級為『高』者」之文字，以明確規範C級之公務機關針對自行或委外開發之各級資通系統，應完成附表十之控制措施之時間。

二、於管理面之資訊安全管理系統之導入，配合實務需求明定包含ISO 27001等資訊安全管理系統標準，以資明確。

三、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

四、於認知與訓練中，針對資通安全及資訊人員資通安全教

		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	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。
		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，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、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。

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。

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。

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、於認知與訓練中，針對資通安全專業證照，增訂應持續維持證照之有效性之規定，俾確保資通安全專職人員之專業性，並與附表一至附表四及附表六之規定一致。

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

修正規定

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；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。
	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。
	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。
	限制使用危害國家資通安全產品		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，且不得與業務網路環境介接。
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	

現行規定

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	
		目錄伺服器設定及防火牆連線設定檢視	
	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	

說明

一、於管理面之資通系統分級及防護基準，刪除現行「系統等級為『高』者」之文字，以明確規範C級之特定非公務機關針對自行或委外開發之各級資通系統，應完成附表十之控制措施之時間。

二、於管理面之資訊安全管理系統之導入，配合實務需求明定包含ISO 27001等資訊安全管理系統標準，以資明確。

三、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

四、於認知與訓練中，針對資通安全及資訊人員資通安全教育訓練，修正

		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	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。
		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、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。

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。

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。

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。

五、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點之點次遞移。

六、其餘內容未修正。

附表七修正對照表

修正規定

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
管理面	限制使用危害國家資通安全產品		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。
技術面	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。
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。

備註：

一、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。

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。

現行規定

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 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。
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。

說明

一、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。

二、於認知與訓練中，針對一般使用者及主管，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。

三、於備註增訂危害國家資通安全產品之定義，以資明確。

四、其餘內容未修正。

附表八修正對照表

<table>
<tr><th>修正規定</th><th>現行規定</th><th>說明</th></tr>
<tr>
<td>
附表八 資通安全責任等級E級之各機關應辦事項
<table>
<tr><th>制度面向</th><th>辦理項目</th><th>辦理項目細項</th><th>辦理內容</th></tr>
<tr><td>管理面</td><td colspan="2">限制使用危害國家資通安全產品</td><td>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。</td></tr>
<tr><td>認知與訓練</td><td>資通安全教育訓練</td><td>一般使用者及主管</td><td>每人每年接受三小時以上之資通安全通識教育訓練。</td></tr>
</table>
備註：
一、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。
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。
</td>
<td>
附表八 資通安全責任等級E級之各機關應辦事項
<table>
<tr><th>制度面向</th><th>辦理項目</th><th>辦理項目細項</th><th>辦理內容</th></tr>
<tr><td>認知與訓練</td><td>資通安全教育訓練</td><td>一般使用者及主管</td><td>每人每年接受三小時以上之一般資通安全教育訓練。</td></tr>
</table>
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。
</td>
<td>一、為強化各機關之資通安全防護，降低國家資通安全風險，爰於管理面中增訂限制使用危害國家資通安全產品之規定。
二、於認知與訓練中，針對一般使用者及主管，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。
三、於備註增訂危害國家資通安全產品之定義，以資明確。
四、其餘內容未修正。</td>
</tr>
</table>

附表九修正對照表

<table>
<tr><th>修正規定</th><th>現行規定</th><th>說明</th></tr>
<tr>
<td>
附表九 資通系統防護需求分級原則
<table>
<tr><th>防護需求等級
構面</th><th>高</th><th>中</th><th>普</th></tr>
<tr><td>機密性</td><td>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。</td><td>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。</td><td>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。</td></tr>
<tr><td>完整性</td><td>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。</td><td>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。</td><td>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。</td></tr>
<tr><td>可用性</td><td>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。</td><td>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。</td><td>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。</td></tr>
<tr><td>法律遵循性</td><td>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。</td><td>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。</td><td>其他資通系統設置或運作於法令有相關規範之情形。</td></tr>
</table>
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。
</td>
<td>
附表九 資通系統防護需求分級原則
<table>
<tr><th>防護需求等級
構面</th><th>高</th><th>中</th><th>普</th></tr>
<tr><td>機密性</td><td>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。</td><td>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。</td><td>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。</td></tr>
<tr><td>完整性</td><td>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。</td><td>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。</td><td>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。</td></tr>
<tr><td>可用性</td><td>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。</td><td>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。</td><td>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。</td></tr>
<tr><td>法律遵循性</td><td>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。</td><td>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。</td><td>其他資通系統設置或運作於法令有相關規範之情形。</td></tr>
</table>
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。
</td>
<td>本附表未修正。</td>
</tr>
</table>

附表十修正對照表

修正規定

附表十　資通系統防護基準

控制措施 \ 系統防護需求分級		高	中	普
構面	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。		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

現行規定

附表十　資通系統防護基準

控制措施 \ 系統防護需求分級		高	中	普
構面	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。		七、依規定時間週期及紀錄留存政策，保留稽核紀錄。 八、確保資通系統有稽核特定事件之

說明

本附表未修正。

				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。
	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	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。

				功能，並決定應稽核之特定資通系統事件。 九、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	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。

		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。		
	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。 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。		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。

		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。		
	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。 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。		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。 三、等級「中」及「普」之所有控制措施。	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護措施。	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。
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，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。	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。

	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。 三、等級「中」及「普」之所有控制措施。	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護措施。	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。
系統與資訊完整性	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。		系統之漏洞修復應測試有效性及潛在影響，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。	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。

		二、 等級「中」之所有控制措施。		
	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、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。

		二、 等級「中」之所有控制措施。		
	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、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。

四、資通安全事件通報及應變辦法

條文	說明
第一章　總則	章名。
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。	明定本辦法訂定之依據。
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	一、考量不同資通安全事件對公務機關或特定非公務機關（以下簡稱各機關）造成之影響或損害程度不同，爰以資通安全事件之性質及業務實際受影響之程度等因素作為判斷標準，將資通安全事件區分為四個等級，於第一項明定資通安全事件之分級，並於第二項至第五項分別規定第一級至第四級資通安全事件之情形。 二、所定核心業務，依資通安全管理法施行細則第七條第一項之規定認定；所定核心資通系統，依該細則第七條第二項之規定認定，併予敘明。 三、所稱一般公務機密，參考行政院訂定之文書處理手冊第五十一點規定，係指公務機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。 四、所稱敏感資訊，指包含個人資料等非一般公務機密或國家機密之資訊，如遭洩漏可能造成機關本身或他人之損害或困擾，而具保護價值之資訊。 五、所稱國家機密，依國家機密保護法第二條規定，指為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依該法核定機密等級者。

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。	為強化資通安全事件之管理、追蹤及加速處理之效率，爰明定各機關辦理資通安全事件通報作業之基本通報項目。
第二章　公務機關資通安全事件之通報及應變	章名。
第四條　公務機關知悉資通安全事件	一、第一項明定公務機關辦理資通

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。	安全事件之通報，應於知悉後一小時內依主管機關指定之方式及對象為之。 二、考量公務機關可能於辦理完成資通安全事件之通報後，始發現資通安全事件等級須變更，為確保其上級、監督機關或主管機關知悉該情事，並能對之為本辦法所定之審核、覆核及提供必要之協助，爰於第二項明定已依第一項規定通報之資通安全事件，如發生等級變更之情事，該公務機關應依第一項規定續行通報。 三、考量如有天災、事變或其他事故，可能發生網路或電力中斷等情形，致公務機關無法利用經指定之方式（例如通報應變網站）進行資通安全事件之通報，爰於第三項明定因故無法依指定方式通報時，公務機關應依其他適當方式進行通報，並註記說明阻礙通報之事由。 四、第四項明定公務機關於阻礙其依指定方式通報之事由解除後，仍應依主管機關指定之方式補行通報。
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	一、考量公務機關於進行資通安全事件之通報時，因受限於時間急迫或其他因素，就資通安全事件等級之判斷或有不適當之情形，爰於第一項明定主管機關對於其自身資通安全事件之審核，並於第二項規範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，通報資通安全事件後，依規定之時限完成對該資通安全事件等級之審核，並得依審核結

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。	果變更其等級。 二、為使主管機關得掌握資通安全事件之情況，以利適時提供必要協助，爰於第三項明定第二項之機關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及相關資訊通知主管機關，以利主管機關進行後續之覆核。 三、第四項明定總統府、國家安全會議、立法院、司法院、考試院、監察院及直轄市、縣（市）議會資通安全事件等級之審核及通知主管機關等程序。 四、第五項明定主管機關得就各公務機關資通安全事件之等級進行覆核。另考量部分資通安全事件之急迫性與時效性，及避免相關機關未能於規定時限內完成資通安全事件等級之審核致貽誤時效，爰明定主管機關認有必要，或第二項及第四項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	一、第一項明定公務機關於知悉資通安全事件後，應視該事件之等級，於時限內完成損害控制或復原作業及通知事宜。 二、為使公務機關對於資通安全事件儘速妥適處理，於第二項及第三項明定公務機關完成第一項所定資通安全事件之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，並應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；另得經其上級或監督機關及主管機關同意後延長上開時限。 三、為強化公務機關之資通安全管理，爰於第四項明定上級、監督機關或主管機關就第二項之調查、處理及改善報告認為有必

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。	要，或認有違法或不當等情事者，得要求該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。	一、考量公務機關執行資通安全事件之通報及應變作業時，依其所能使用之資源，可能無法適時完成各項要求，或有數公務機關同時發生類似之資通安全事件，需其上級、監督機關或主管機關協助應變之情形，爰於第一項明定總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應視情形提供資通安全事件通報及應變作業之必要支援或協助，並於第二項明定主管機關得視情形提供必要支援或協助，以利各公務機關順利完成相關作業。 二、考量第三級或第四級資通安全事件影響層面、可能發生之損害皆較嚴峻，爰於第三項明定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	一、考量資通安全演練作業係屬資通安全事件應變機制之一環，為使公務機關於資通安全事件發生時得妥適進行相關應對措施，爰於第一項明定總統府與中央一級機關之直屬機關及直轄市、縣（市）政府應規劃並辦理其自身、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及其所屬或監督之公務機關、前開鄉（鎮、市）、直轄市山地原住民區民代表會之資通安全演練作業，並於第二項明定資通安全演練作業之基本內容。 二、總統府與中央一級機關及直轄市、縣（市）議會，亦應辦理資

市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。	通安全演練作業，以利資通安全事件發生時得妥為應對，爰為第三項規定。
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。	為確保公務機關於知悉資通安全事件後，得依本辦法規定迅速進行通報及適當之處置，爰為本條規定。各公務機關訂定資通安全事件之通報作業規範時，應考量其機關特性、資源及其他需求等因素，依本條規定為之。
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。	為確保公務機關於發生資通安全事件後，得依本辦法規定迅速且確實進行資通安全事件之應變，爰為本條規定。
第三章　特定非公務機關資通安全事件之通報及應變	章名。
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	一、第一項明定特定非公務機關辦理資通安全事件通報之方式與時限。 二、考量特定非公務機關可能於辦理完成資通安全事件之通報後，始發現資通安全事件等級須為變更，為確保中央目的事業主管機關知悉該情事，並能對之為本辦法所定之審核及提供必要之協助，爰於第二項明定已依第一項規定通報之資通安全事件，如發生等級變更之情事，該特定非公務機關應依

該方式補行通報。	第一項規定續行通報。 三、考量如因天災、事變或其他因素，可能發生網路或電力中斷之情形，致特定非公務機關無法依經指定之方式（例如通報應變網站）進行資通安全事件之通報，爰於第三項明定因故無法依指定方式通報時，特定非公務機關應依其他適當方式通報中央目的事業主管機關，並註記說明阻礙通報之事由。 四、第四項明定特定非公務機關於阻礙其依指定方式通報之事由解除後，仍應依中央目的事業主管機關指定之方式補行通報。
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。	一、考量特定非公務機關於進行資通安全事件之通報時，因受限於時間急迫或其他因素，就資通安全事件等級之判斷或有不適當之情形，爰於第一項明定中央目的事業主管機關於特定非公務機關完成資通安全事件之通報後，應於規定時限內完成資通安全事件等級之審核。 二、為使主管機關得掌握資通安全事件之情況，以利適時提供必要協助，爰於第二項明定資通安全事件經中央目的事業主管機關判斷為第三級或第四級事件者，中央目的事業主管機關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送交主管機關；如判斷屬第一級或第二級事件者，則應定期彙整審核結果、依據及其他必要資訊送交主管機關，無須立即為之。 三、第三項明定主管機關接獲中央目的事業主管機關送交之資通安全事件審核資料後，得就資通安全事件之等級進行覆核，並為等級變更。
第十三條　特定非公務機關知悉資通安	一、第一項明定特定非公務機關於

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。	知悉資通安全事件後，應視該事件之等級，於時限內完成損害控制或復原作業及通知事宜。 二、為使特定非公務機關及其中央目的事業主管機關對於資通安全事件儘速妥適處理，爰於第二項及第三項明定特定非公務機關完成第一項所定資通安全事件之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，並應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；另得經中央目的事業主管機關同意後延長上開時限。 三、為強化特定非公務機關之資通安全管理，爰於第四項及第五項明定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；就第三級或第四級資通安全事件之調查、處理及改善報告，應於審查後送交主管機關，主管機關認有必要，或有違法或不當等情事者，得要求該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。	一、考量特定非公務機關執行資通安全事件之通報及應變作業時，依其所能使用之資源，可能無法適時完成各項要求，或有數特定非公務機關同時發生類似之資通安全事件，需中央目的事業主管機關或主管機關協助應變之情形，爰於第一項明定中央目的事業主管機關應視情形提供資通安全事件通報及應變作業之必要支援或協助，並於第二項明定主管機關得視情形提供必要支援或協助，以

	利各特定非公務機關順利完成相關作業。 二、考量第三級或第四級資通安全事件影響層面、可能發生之損害皆較嚴峻，爰於第三項明定特定非公務機關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。	為確保特定非公務機關於知悉資通安全事件後，得依本辦法規定迅速進行事件之通報及適當之處置，爰為本條規定。
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。	為確保特定非公務機關於知悉資通安全事件後，得依本辦法規定迅速且確實進行資通安全事件之應變，爰為本條規定。
第四章　附則	章名。
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。	考量第三級與第四級資通安全事件之影響範圍及資訊洩漏之情形較鉅，爰明定主管機關得針對各機關之第三級與第四級資通安全事件（即重大資通安全事件），邀集相關機關召開會議，就事件之損害控制、復原及其他相關事宜進行研商，以

	提升各機關對於重大資通安全事件之處理成效，避免類似事件再次發生。
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。	考量資通安全演練作業為資通安全事件應變之一環，為使公務機關對於資通安全事件之預防與應變更臻完備，爰明定公務機關應配合主管機關規劃、辦理之資通安全演練作業及相關項目。
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。	一、考量資通安全演練作業為資通安全事件應變之一環，為使特定非公務機關對於資通安全事件之預防與應變更臻完備，爰於第一項明定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及相關項目。 二、考量部分資通安全演練作業可能影響特定非公務機關之業務運作或造成資通系統損壞，而侵害其權利或正當利益，為保護特定非公務機關之權益，爰於第二項明定主管機關規劃、辦理該等演練作業，應先經特定非公務機關之書面同意，始得為之。 三、為提升行政效率，於第三項明定主管機關依第二項取得特定非公務機關之書面同意時，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，	一、考量目前部分公務機關之業務領域已具備完善之資通安全事件通報及應變機制，為有效利用行政資源，爰為第一項規定。特定非公務機關未依本項規定依該機制辦理資通安全事件之通報及應變，即屬違反本辦法所定資通安全事件通報及應變機制必要事項之情形，其中央目的事業主管機關得依本法第

應送主管機關重為核定。	二十條第四款規定裁罰之。 二、公務機關為因應業務或實務趨勢等內在或外在條件之改變，對於資通安全事件之通報及應變機制可能有配合調整之需求，其通報及應變機制經變更後，內容是否妥適，仍須由主管機關審視決定，爰為第二項規定。
第二十一條　本辦法之施行日期，由主管機關定之。	明定本辦法之施行日期，由主管機關定之。

五、特定非公務機關資通安全維護計畫實施情形稽核辦法

條文	說明
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。	明定本辦法訂定之依據。
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。	明定本辦法所定書面，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。	一、第一項明定主管機關稽核特定非公務機關資通安全維護計畫實施情形之頻率。 二、為有效利用稽核資源，提升稽核成效，爰於第二項明定主管機關擇定受稽核機關時應綜合考量之因素，以決定最適之受稽核機關名單。 三、第三項明定主管機關為辦理第一項之稽核，應訂定稽核計畫及其內容應包括之事項。 四、為使稽核作業能切合我國資通安全政策之規劃內容，並適時反映國內外資通安全相關趨勢，強化稽核資源分配與成效，爰於第四項明定主管機關於訂定稽核計畫，決定稽核之重點領域與基準及其項目時，應綜合考量之因素。
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。	一、為避免主管機關辦理稽核影響受稽核機關之日常業務，並使受稽核機關有充裕時間預為準備，以增進稽核效能，爰於第一項明定主管機關應於實際辦理稽核之一個月前，以書面通知受稽核機關。 二、考量受稽核機關可能有因業務因素或其他正當理由，難以依主管機關所定日期配合稽核之情形，爰於第二項及第三項明定於此情形，受稽核機關得於收受第一項通知後

	五日內，以書面敘明理由向主管機關申請調整稽核日期，其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。	一、 本法第七條第二項明定主管機關得稽核特定非公務機關之資通安全維護計畫實施情形，並授權主管機關就稽核之頻率、內容與方法及其他相關事項之辦法，依其立法說明，係為監督特定非公務機關實施資通安全維護計畫之情形。從上開法律規定及立法理由整體觀察，足認受稽核之特定非公務機關有配合主管機關辦理稽核之義務，主管機關並應就稽核之內容、方法等相關事項訂定規範，以利實務執行，爰於第一項明定主管機關辦理第三條第一項之稽核時得要求受稽核機關配合之事項，以利主管機關藉由稽核確認受稽核機關遵循本法之情形。 二、 受稽核機關如依法律有正當理由，不能為第一項之說明、配合措施或提供資料，例如提供資料將侵害第三人之權利或正當利益，此時受稽核機關應以書面敘明其理由，向主管機關提出，俾利主管機關審核及決定是否繼續該項作業，爰為第二項規定。 三、 第三項明定主管機關收受受稽核機關依第二項規定提出書面理由後之處理。受稽核機關對主管機關依本項第二款規定所為之決定不服者，得依訴願法及行政訴訟法等規定提起救濟，以維護自身權益。
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。	一、 為使主管機關對不同之特定非公務機關均得妥適辦理其資通安全維護計畫實施情形之稽核，爰於第一項明定主管機關應考量相關因素，就各受稽核機關分別組成稽核小組。 二、 考量稽核小組成員需具備之知能，於第二項明定主管機關組成稽核小組時應邀請之人員，以協助主管機關進行稽核及提供專業意見。另

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。	為確保稽核結果之公正性，明定公務機關代表不得少於稽核小組全體成員人數之三分之一。 三、為保障受稽核機關之權益，爰於第三項明定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。 四、為確保稽核結果之客觀性及避免爭議，爰於第四項明定第二項之公務機關代表或專家學者應主動迴避擔任稽核小組成員之情形。
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。	一、第一項明定主管機關應於每季所定受稽核機關之稽核作業均辦理完成後之一個月內，將稽核結果報告交付該季受稽核機關。 二、第二項明定稽核結果報告應記載之內容。
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。	依本法第七條第三項規定，特定非公務機關受主管機關稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。為利執行，爰於第一項明定受稽核機關應提出改善報告之期限及程序，並於第二項明定應提出改善報告之執行情形，俾利主管機關及中央目的事業主管機關進行後續之監督。有關改善報告應包括之內容，則係於本法施行細則第三條規範之，併予敘明。
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。	明定主管機關辦理第三條第一項之稽核時，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，以利順利執

	行稽核，並使中央目的事業主管機關亦得知悉受稽核機關之資通安全維護實施情形。
第十條　本辦法之施行日期，由主管機關定之。	明定本辦法之施行日期，由主管機關定之。

六、資通安全情資分享辦法

條文	說明
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。	明定本辦法訂定之依據。
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。	為使公務機關或特定非公務機關（以下簡稱各機關）得以知悉何種資通安全資訊具有進行分享之效益，以利進行資通安全情資分享，爰參考美國 Cybersecurity Information Sharing Act of 2015, SEC102(6)之規定，明定本辦法所稱資通安全情資之定義。其中第一款所定資通系統之惡意偵察 (malicious reconnaissance)或情蒐活動，包括進行資通系統之弱點、安全漏洞是否存在等資訊蒐集之異常活動；第四款所定與惡意程式相關之資訊，例如惡意指令、控制受害者、中繼站位址或連線資訊之方式等。
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。	一、考量目前資通安全之攻擊可能來自全球各地，為強化資通安全管理體系下之預警功能，於第一項明定主管機關應就資通安全情資分享進行國際合作。 二、第二項至第五項明定主管機關與其他公務機關及中央目的事業主管機關與特定非公務機關進行情資分享之規定，俾利各機關掌握情資，提升其資通安全維護能量，以適時調整資通安全應變機制，預防相關資通安全威脅之發生。 三、另各機關於知悉自身之資通安全事件時，應依本法及資通安全事件通報及應變辦法之規定進行通報及應變，已達情資分享之效，爰本辦法就該等情形不再另行規範，併予敘明。
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	為避免各機關進行情資分享時，可能影響其他個人、法人或團體之權益，或有其他依法規規定應秘密或應限制、禁止公開之情形，爰參考美國 Cybersecurity Information Sharing Act of 2015,

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。	SEC104(d)與政府資訊公開法第十八條第一項第七款及第二項規定，明定不得分享情資之範疇，並明定情資含有不得分享之內容者，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。	為督促各機關妥適管理及運用情資，及避免發生情資外洩、遭未經授權之存取或竄改，或其他侵害個人、法人或團體權益之情事，爰明定進行情資分享應就情資為分析及整合，並應規劃適當之資通安全維護措施，例如於分享前應遮蔽無關之個人資料或其他依法規應予保密或不得分享之資訊等。
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。	考量各機關於進行情資分析時，應辨識情資來源之可靠性與時效性以利及時研判潛在風險，並採取適當之預防或應變措施，爰為本條規定。
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。	各機關於辦理情資整合時，應針對情資之來源、時效、威脅指標類別、特性或其他性質，與內部情資進行關聯分析；公務機關於進行情資整合後，亦應就所發現之新型威脅情資進行分享，爰為本條規定。
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。	考量各機關於接收其他機關分享之情資後，應以適當方式確保情資之安全性，爰參考 Cybersecurity Information Sharing Act of 2015, SEC104(d)之規範意旨，為本條規定。
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。	一、 為確保情資分享之效率及正確性，進行資通安全情資分享之方式宜臻明確，爰於第一項明定各機關應遵循之資通安全情資分享方式。 二、 考量實務上可能發生各機關依規定應進行情資分享，惟因故無法依第一項規定方式辦理之情形，為使各機關適時掌握情資，仍應循其他方式進行情資分享，爰參考其他法規所定提供資料之方式，於第二項明定各機關於此情形得採取之情資分享方式。

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。	一、考量未適用本法之個人、法人或團體亦可能持有資通安全情資，或有資通安全情資分享之需求，爰於第一項明定該等個人、法人或團體經主管機關或中央目的事業主管機關同意後，得與其進行資通安全情資分享。 二、為確保第一項與主管機關或中央目的事業主管機關進行情資分享之個人、法人或團體處理情資符合本辦法相關規定，爰為第二項規定。
第十一條 本辦法施行日期，由主管機關定之。	明定本辦法施行日期，由主管機關定之。

七、公務機關所屬人員資通安全事項獎懲辦法

條文	說明
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。	明定本辦法訂定之依據。
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。	一、考量各公務機關之業務性質不同，及其上級或監督機關對於其資通安全業務具有監督管理權責，爰明定公務機關就其所屬人員辦理業務涉及資通安全事項之獎勵及懲處，得依本辦法之規定，自行訂定獎懲基準。 二、依公務人員考績法施行細則第十三條第二項規定「各主管機關得依業務特殊需要，另訂記一大功、一大過之標準，報送銓敘部核備。」同條第三項規定「嘉獎、記功或申誡、記過之標準，由各機關視業務情形自行訂定，報請上級機關備查。」公務機關自行訂定資通安全事項之獎懲基準後，仍應依上開規定辦理，併予敘明。
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	明定公務機關人員辦理業務涉及資通安全事項，應予獎勵之情形。

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，	明定公務機關人員辦理業務涉及資通安全事項，應予懲處之情形。

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。	一、為使公務機關就其所屬人員辦理資通安全業務之情形給予適當評價，並促進其所屬人員對於資通安全工作之重視與投入，爰為本條規定。 二、所定公務機關所屬人員，除具有公務員身分者外，並包含公務機關之聘用人員、約僱人員或技工、工友等其他與其有僱傭關係之人員。公務機關就不具公務員身分之所屬人員，仍應依本條規定，審酌其辦理業務涉及資通安全事項之具體情形，予以適當之獎勵或懲處，並納入續聘之參考。
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。	為保障當事人權益，明定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；如涉及資通安全專業事項，必要時得徵詢相關專家學者之意見，俾妥適判斷案件情節及當事人是否應予懲處。
第七條　本辦法之施行日期，由主管機關定之。	明定本辦法之施行日期，由主管機關定之。