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。