法規名稱：資通安全管理法

修正日期：民國 114 年 09 月 24 日

當次沿革：中華民國 114 年 9 月 24 日總統華總一義字第 11400095391 號令修正公布全文 35 條；依第 35 條規定：施行日期，由行政院定之

中華民國 114 年 12 月 1 日行政院院臺安字第 1141033966 號令發布定自 114 年 12 月 1 日施行

第 一 章 總則

第 1 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 2 條

本法之主管機關為數位發展部。

資通安全業務之執行，由數位發展部指定資安專責機關辦理。

第 3 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，或其他情形影響其機密性、完整性或可用性。

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或保護措施失效之狀態發生，影響資通系統機能運作。

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、特定財團法人或受政府控制之事業、團體或機構。

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，經行政院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，並報行政院核定者。

九、特定財團法人：指符合財團法人法第二條第二項、第三項或第六十三條第一項、第四項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者。

十、受政府控制之事業、團體或機構：指銓敘部依公務人員退休資遣撫卹法第七十七條第一項第二款第三目及第四目公告之事業、團體或機構，具資通安全重要性，經中央目的事業主管機關指定，並經主管機關核定者；其受地方政府控制者，應經地方主管機關同意後，主管機關始得核定。

十一、危害國家資通安全產品：指經主管機關認定，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、服務或產品。

第 4 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、相關服務及審驗機制之發展。

五、協助民間處理、因應及防範重大資通安全事件。

前項相關事項之推動，由主管機關擬訂國家資通安全發展方案，報請行政院核定後實施。

第 5 條

為落實國家資通安全政策，各政府機關、中央及地方間，應致力配合推動執行國家資通安全措施，共同建構國家資通安全環境。

為辦理國家資通安全政策、應變機制與重大計畫之諮詢審議，協調各政府機關、中央及地方間之資通安全相關事務，行政院應定期召開國家資通安全會報，由行政院院長或副院長擔任召集人，得邀請專家學者及民間團體代表出席，必要時得召開臨時會議，其幕僚作業由主管機關辦理。

前項國家資通安全會報決議事項，相關政府部門應予執行，由主管機關定期追蹤管考，並得辦理績效評核。

第二項國家資通安全會報之組成、任務、議事程序及其他相關事項之辦法，由行政院定之。

第 6 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，並應每年公布國家資通安全情勢報告、資通安全維護計畫實施情形稽核概況報告及國家資通安全發展方案。

前項情勢報告、實施情形稽核概況報告及國家資通安全發展方案，應由主管機關送立法院備查。

第 7 條

公務機關及特定非公務機關，應按其業務重要性與機敏性、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，報由主管機關核定或備查其資通安全責任等級。

公務機關及特定非公務機關應符合資通安全責任等級之要求，並自管理、技術、認知及訓練等面向，辦理資通安全防護措施。

前二項資通安全責任等級之區分基準、核定或備查程序、變更申請、資通

安全防護措施辦理項目、內容、專職人員之資格條件與配置及其他相關事項之辦法，由主管機關定之。

第 8 條

主管機關得定期或不定期稽核公務機關及特定非公務機關之資通安全維護計畫實施情形。

前項稽核後，發現受稽核機關資通安全維護計畫實施情形有缺失或待改善者，受稽核機關應提出改善報告，公務機關送交依第十四條規定收受其實施情形之機關、特定非公務機關送交中央目的事業主管機關審查後，由該審查機關送交主管機關。

前項收受改善報告之機關認有必要時，得要求受稽核機關進行說明或調整。

前三項資通安全維護計畫實施情形之稽核頻率、內容與方法、改善報告之提出及其他相關事項之辦法，由主管機關定之。

第一項稽核由主管機關擬訂年度計畫，報請行政院核定後辦理，年度計畫及年度成果報告應送交國家資通安全會報備查。

第 9 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 10 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，應選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。

前項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公正第三方驗證。

公務機關或特定非公務機關辦理第一項委外業務，應與受託者簽訂書面契

約，載明雙方之權利義務及違約責任。

公務機關及特定非公務機關，應配合主管機關之規劃辦理資通安全演練作業，並視需要導入第三方協力機制；演練內容及其他相關事項，由主管機關定之。

第 二 章 公務機關資通安全管理

第 11 條

公務機關不得下載、安裝或使用危害國家資通安全產品；其自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，亦同。但因業務需求且無其他替代方案者，經該機關資通安全長及依第十四條規定收受其實施情形之機關資通安全長核可，函報主管機關核定後，得以專案方式使用，並列冊管理。

公務機關發配供業務使用之資通訊設備，不得下載、安裝或使用危害國家資通安全產品，並應遵守相關法令規範。但因業務需求且無其他替代方案者，準用前項但書規定辦理。

前二項有關危害國家資通安全產品之審查程序、風險評估、情資分享、使用限制及其他相關事項之辦法，由主管機關會商有關機關擬訂，報請行政院核定之。

第 12 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 13 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 14 條

公務機關應每年向上級機關或監督機關提出資通安全維護計畫實施情形；

無上級機關或監督機關者，其資通安全維護計畫實施情形應依下列各款規定辦理：

一、總統府、國家安全會議及五院，向主管機關提出。

二、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會，向主管機關提出。

三、直轄市山地原住民區公所、直轄市山地原住民區民代表會，向直轄市政府提出；鄉（鎮、市）公所、鄉（鎮、市）民代表會，向縣政府提出。

第 15 條

公務機關應稽核其所屬、所監督之公務機關、所轄鄉（鎮、市）公所、直轄市山地原住民區公所及鄉（鎮、市）民代表會、直轄市山地原住民區民代表會之資通安全維護計畫實施情形。

第 16 條

受稽核機關之資通安全維護計畫實施情形有缺失或待改善者，應向稽核機關提出改善報告，並由稽核機關連同稽核結果依指定之方式送交主管機關。

稽核機關或主管機關認有必要時，得要求受稽核機關進行說明或調整。

前三條及第一項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、結果之交付、改善報告之提出及其他相關事項之辦法，由主管機關定之。

第 17 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，應向第十四條規定收受其實施情形之機關及主管機關通報。

公務機關應向前項受通報機關提出資通安全事件調查、處理及改善報告。

前三項通報與應變機制之必要事項、通報內容、報告之提出、演練作業及

其他相關事項之辦法，由主管機關定之。

第二項受通報機關知悉重大資通安全事件時，得提供公務機關相關協助；於適當時機並得公告與事件相關之必要內容及因應措施。

第 18 條

公務機關應符合其資通安全責任等級之要求，設置資通安全專職人員，辦理資通安全業務及應變處理；所屬人員辦理資通安全業務績效優良者，應予獎勵。

主管機關應妥善規劃推動專職人員之職能訓練，增進其資通安全專業知能；遇有重大資通安全事件，主管機關得調度各級機關資通安全人員支援之。

前二項人員獎勵、職能訓練、調度支援、績效評核及其他相關事項之辦法，由主管機關定之。

第 19 條

公務機關於必要時，得對所屬資通安全專職人員之適任性進行查核。

主管機關得於資通安全人員任用考試榜示後，對錄取人員之適任性進行查核。

拒絕查核或前二項查核結果經用人機關認定未通過者，不得辦理涉及國家機密、軍事機密及國防秘密之資通安全業務。

前項人員職務得由用人機關基於內部管理及業務運作需要，依法進行調整。

第一項及第二項查核紀錄，由用人機關依相關規定保密處理，並妥為保管，不得移作他用；違反者，視情節予以議處。

有關查核權責機關、應受查核人員、查核程序、內容及其他相關事項之辦法，由主管機關會商有關機關定之。

第 三 章 特定非公務機關資通安全管理

第 20 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，送由主管機關報請行政院核定，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，設置資通安全專職人員，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綜合考量所管關鍵基礎設施提供者業務之重要性與機敏性、資通系統之規模、性質、資通安全事件發生之頻率、程度及其他與資通安全相關之因素，定期稽核其資通安全維護計畫之實施情形。

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，應向中央目的事業主管機關提出改善報告。

中央目的事業主管機關應依指定之方式將稽核結果及改善報告送交主管機關。

第 21 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，設置資通安全專職人員，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。

中央目的事業主管機關應依指定之方式將稽核結果及改善報告送交主管機

關。

第 22 條

前二條資通安全維護計畫之必要事項、實施情形之提出、稽核之頻率、內容與方法、結果之交付、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，報由主管機關核定。

第 23 條

特定非公務機關應置資通安全長，由特定非公務機關之代表人、管理人、其他有代表權人或其指派之適當人員擔任，負責推動及監督機關內資通安全相關事務。

第 24 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。

前三項通報與應變機制之必要事項、通報內容、報告之提出、送交、演練作業及其他應遵行事項之辦法，由主管機關定之。

中央目的事業主管機關或主管機關知悉重大資通安全事件時，應提供必要之協助；於適當時機並得公告與事件相關之必要內容及因應措施。

第 25 條

中央目的事業主管機關為調查特定非公務機關發生之重大資通安全事件，得依下列程序辦理：

一、通知當事人或關係人到場陳述意見。

二、通知當事人及關係人提出獨立第三方機構出具之鑑識或調查報告。

三、派員、委任或委託其他機關（構）前往當事人及關係人之處所實施必要之檢查。

前項所定關係人，以該項特定非公務機關委託辦理資通系統之建置、維運或資通服務提供之受託者，且與重大資通安全事件相關者為限。

當事人或關係人對於中央目的事業主管機關依第一項所為之調查，不得規避、妨礙或拒絕。

執行調查之人員應出示有關執行職務之證明文件；其未出示者，受調查者得拒絕之。

第一項第三款受委任或委託之機關（構）對於辦理受任或受託事務所獲悉特定非公務機關之秘密，不得洩漏。

第 26 條

特定非公務機關對於所屬人員辦理資通安全業務績效優良者，應予獎勵。

第 27 條

中央目的事業主管機關對特定非公務機關下載、安裝或使用危害國家資通安全產品，得予以限制或禁止；特定非公務機關自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，亦同。但因業務需求且無其他替代方案者，經該特定非公務機關資通安全長核可，函報中央目的事業主管機關核定後，得以專案方式使用，並列冊管理。

前項對特定非公務機關限制或禁止使用危害國家資通安全產品之管控措施，由中央目的事業主管機關訂定，報主管機關備查。

第 四 章 罰則

第 28 條

公務機關所屬人員未依本法規定辦理者，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。

特定非公務機關所屬人員未依本法規定辦理，情節重大者，由特定非公務機關依規定予以懲處。

第 29 條

特定非公務機關未依第二十四條第二項規定，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一千萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。

第 30 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五百萬元以下罰鍰：

一、未依第二十條第二項或第二十一條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第二十二條所定辦法中有關資通安全維護計畫必要事項之規定。

二、未依第二十條第三項或第二十一條第二項規定，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，或違反第二十二條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、未依第八條第二項、第二十條第五項或第二十一條第三項規定，提出改善報告送交中央目的事業主管機關，或違反第二十二條所定辦法中有關改善報告提出之規定。

四、未依第二十四條第一項規定，訂定資通安全事件之通報及應變機制，或違反第二十四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、未依第二十四條第三項規定，向中央目的事業主管機關提出或向主管機關送交資通安全事件之調查、處理及改善報告，或違反第二十四條第四項所定辦法中有關報告提出、送交之規定。

六、違反第二十四條第四項所定辦法中有關通報內容、演練作業之規定。

第 31 條

違反第二十五條第三項規定，規避、妨礙或拒絕調查者，由中央目的事業主管機關處新臺幣十萬元以上一百萬元以下罰鍰。

第 五 章 附則

第 32 條

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

前項受委託之公務機關、法人或團體，不得洩露辦理相關事務過程中所知悉之秘密。

特定非公務機關之業務涉及數個中央目的事業主管機關之權責，主管機關得協調指定其中一個或數個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 33 條

本法所定資通安全事件，涉及個人資料外洩時，公務機關及特定非公務機關應另依個人資料保護法及其相關法令規定辦理。

第 34 條

本法施行細則，由主管機關定之。

第 35 條

本法施行日期，由行政院定之。