（機關名稱）所管特定非公務機關資通安全管理作業辦法（範本）

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）第二十二條規定訂定之。

（中央目的事業主管機關另得依本法第二十七條第一項規定，要求所管特定非公務機關限制或禁止使用危害國家資通安全產品。）

第二條

本辦法所稱關鍵基礎設施提供者，指○○（以下簡稱【本○】）依本法第二十條第一項規定指定，送由主管機關報請行政院核定者。

第二章 資通安全維護計畫必要事項及實施情形之提出

範例一

第三條

【本○】所管特定非公務機關（以下簡稱特定非公務機關）之資通安全維護計畫，除依本法施行細則第九條第一項規定外，並應包含下列事項：（由各中央目的事業主管機關依所管特定非公務機關之特殊需要臚列）

一、……

二、……

特定非公務機關依本法第二十條第三項或第二十一條第二項規定提出資通安全維護計畫實施情形，除依本法施行細則第九條第二項規定外，並應包括前項各款之執行成果及相關說明。

範例二

第三條

【本○】所管特定非公務機關（以下簡稱特定非公務機關）之資通安全維護計畫，應依本法施行細則第九條第一項規定辦理。

特定非公務機關依本法第二十條第三項或第二十一條第二項規定提出資通安全維護計畫實施情形，應依本法施行細則第九條第二項規定辦理。

第四條

關鍵基礎設施提供者應依【本○】指定之方式提出資通安全維護計畫。

關鍵基礎設施提供者以外之特定非公務機關，經【本○】要求提出資通安全維護計畫者，應於收受【本○】通知後○個月內，依【本○】指定之方式提出。

（本條請各中央目的事業主管機關視自身需求斟酌是否要求所管特定非公務機關定期或依通知再行提出資通安全維護計畫）

第五條

關鍵基礎設施提供者應於每年○月前，依【本○】指定之方式提出資通安全維護計畫實施情形。

關鍵基礎設施提供者以外之特定非公務機關，經【本○】依本法第二十一條第二項規定要求提出資通安全維護計畫實施情形者，應於收受【本○】通知後○個月內，依【本○】指定之方式提出。

有特殊情形無法依前二項指定之方式提出者，得經【本○】同意以其他適當方式為之。

第六條

【本○】所管【下列（如非對於所管特定非公務機關一體適用者，建議可自行依據考量分別列舉）】特定非公務機關不得下載、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，經評估下載、安裝或使用該危害產品可能風險及敘明因應之管控措施，並經該特定非公務機關資通安全長核可，函報【本○】核定後，得以專案方式使用。

經前項核定以專案方式使用危害國家資通安全產品之特定非公務機關，應遵守所核定之資通安全管控措施。

（各中央目的事業主管機關可參酌危害國家資通安全產品審查辦法第七條公務機關專案使用危害國家資通安全產品應採取之措施，並依該領域業務獨特性及政策性質，自行訂定相關資通安全管控措施；且依本法第二十七條第二項規定，函報主管機關備查。）

特定非公務機關接收危害國家資通安全產品情資後，應採取下列措施：

一、盤點其資通系統、服務、產品及發配供業務使用之資通訊設備，以確認是否有下載、安裝或使用該危害國家資通安全產品。

二、有下載、安裝或使用該危害國家資通安全產品者，應立即移除、解除安裝或停止使用。但因業務需求且無其他替代方案者，得依第一項但書規定辦理。

（本條適用於中央目的事業主管機關業依本法第二十七條第一項規定，要求所管特定非公務機關限制或禁止使用危害國家資通安全產品。）

第三章　資通安全維護計畫實施情形之稽核

第七條

範例一

【本○】應定期擇定關鍵基礎設施提供者，並得納入關鍵基礎設施提供者以外之特定非公務機關，以實地稽核或其他適當之方式，稽核其資通安全維護計畫實施情形。（第一項範例一，適用於管理之特定非公務機關包含關鍵基礎設施提供者之中央目的事業主管機關）

範例二

【本○】得定期擇定特定非公務機關，以實地稽核或其他適當之方式，稽核其資通安全維護計畫實施情形。（第一項範例二，適用於管理之特定非公務機關不含關鍵基礎設施提供者之中央目的事業主管機關）

【本○】為辦理前項稽核，應訂定稽核計畫，其內容包括稽核之依據與目的、稽核範圍、作業期程、稽核小組組成方式、保密義務、受稽核之特定非公務機關（以下簡稱受稽核機關）遴選原則、稽核基準、稽核方式及項目等與稽核相關之事項。

【本○】訂定前項稽核計畫時，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。

【本○】依第一項規定擇定受稽核機關時，應綜合考量其業務之重要性與機敏性、資通系統之規模及性質、資通安全事件發生之頻率及程度、資通安全演練之成果、歷年受主管機關或【本○】稽核之頻率及結果或其他與資通安全相關之因素。

第八條

【本○】辦理前條第一項之稽核，應於一個月前以書面通知受稽核機關。

受稽核機關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【本○】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。

第九條

【本○】辦理第七條第一項之稽核，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、證明資料供稽核小組查閱，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、實地稽核或其他適當之稽核方式。

受稽核機關依法律有正當理由，未能為前項說明、協力或提出資料供稽核小組查閱者，應以書面敘明理由，向【本○】提出，【本○】收受書面後，應進行審核。

【本○】進行前項審核，認有理由時，應將審核之依據及相關資訊記載於稽核結果報告，並得停止稽核作業之全部或一部；認無理由時，應要求受稽核機關依第一項規定辦理。經停止稽核作業者，【本○】得擇期續行辦理，並於十日前以書面通知受稽核機關。

第十條

【本○】為辦理第七條第一項之稽核，應依第七條第四項所定考量因素，就各受稽核機關分別組成三人以上之稽核小組。

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四分之一。

【本○】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，與受稽核機關或其代表人、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，與受稽核機關或其代表人、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曾任職之機關（構）或單位，曾為受稽核機關之輔導，其輔導項目與受稽核項目相關。

四、其他足認擔任稽核小組成員，將對稽核結果之公正性造成影響。

第十一條

【本○】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、第九條第二項所定受稽核機關未能為說明、協力或提出資料供稽核小組查閱之情形、理由與同條第三項所定稽核機關審核結果，及其他與稽核相關之必要內容。

第十二條

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【本○】交付稽核結果報告後一個月內，依本法施行細則第六條第一項規定及【本○】指定之方式，向【本○】提出改善報告。

受稽核機關提出改善報告後，應依本法施行細則第六條第二項規定，提出改善報告之執行情形送交【本○】。

【本○】認有必要時，得要求該受稽核機關就前二項之改善報告、改善報告之執行情形進行說明或調整。

第四章　附則

第十三條

本辦法所定資通安全維護計畫之必要事項與實施情形之提出、資通安全維護計畫實施情形之稽核及其他相關事項，【本○】得委任所屬公務機關辦理。

第十四條

本辦法自發布日施行。

註：本辦法引用資通安全管理法施行細則及參考資通安全維護計畫實施情形稽核辦法內容部分，依子法調修內容調整。