全國法規資料庫
Laws & Regulations Database of The Republic of China

法規名稱：電信事業資通安全管理辦法

發布日期：民國 109 年 07 月 09 日

第 1 條

1 本辦法依電信管理法（以下簡稱本法）第十五條第三項規定訂定之。

2 本辦法未規定者，適用其他有關法令之規定。

第 2 條

1 設置使用電信資源之公眾電信網路之電信事業或其他經主管機關公告之電信事業（以下簡稱電信事業），應依本法第十五條第二項規定訂定資通安全維護計畫。

2 主管機關為前項之公告時，應考量下列情形：

一、具有關鍵電信基礎設施。

二、用戶數或網路達一定規模具有影響力、或經營控制權等因素認定有必要者。

三、有危害國家安全或資通安全之虞，經有關機關通知者。

四、發生資通安全事件達資通安全事件通報及應變辦法規定之第三級資通安全事件以上者。

第 3 條

1 電信事業應於主管機關通知之日起三個月內，訂定資通安全維護計畫，報請主管機關備查，並依該計畫實施。

2 前項電信事業提報之資通安全維護計畫不完備者，應於主管機關通知之期限內補正。

3 第一項資通安全維護計畫之資通安全管理範圍至少應包含下列項目：

一、電信網路之設備及功能元件、電信設備機房及網路管理中心機房等。

二、公眾電信網路維運系統，包含作業維運系統及業務維運系統。其中作業維運系統包括核心網路、接取網路等維運系統；業務維運系統包括用戶資料、客服與帳務等維運系統。

三、為保護前二款所設置之資通安全防護設施。

4 第一項資通安全維護計畫之各項資通訊系統防護分級處理方式，電信事業應依主管機關公告之資通訊防護等級分級原則辦理。

第 4 條

1 電信事業應於提供電信服務之日起二年內，通過下列資通安全管理驗證並維持其有效性：

一、CNS27001 國家標準或 ISO/IEC27001 國際標準。

二、主管機關公告之電信事業資通安全管理手冊 ISO/IEC27011 增項稽核表。

2 前項驗證範圍應於驗證前報請主管機關核准，變更時亦同。

3 電信事業有下列情形之一時，經主管機關通知後提出修正之驗證範圍，報請主管機關核准，並於主管機關指定期限內通過資通安全管理驗證：

一、發生資通安全事件達資通安全事件通報及應變辦法規定之第三級資通安全事件以上者。

二、有危害國家安全或資通安全之虞，經有關機關通知者。

4 第一項期間，經國家安全或資通安全有關機關通知，主管機關得命電信事業縮減之。

第 5 條

1 電信事業資通安全維護計畫執行方式應載明下列事項：

一、資通安全政策及目標。

二、核心業務及其重要性。

三、公眾電信網路資通安全維護範圍。

四、資通安全推動組織。

五、資訊及資通系統之盤點規劃。

六、資通安全風險評估。

七、資通安全防護及控制措施。

八、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。

2 前項電信事業經主管機關指定為關鍵基礎設施提供者時，其資通安全維護計畫執行方式除應載明前項各款外應包括下列事項：

一、專責人力及經費之配置。

二、資通安全長之配置。

三、資通安全事件通報、應變及演練相關機制。

四、資通安全情資之評估及因應機制。

五、資通系統或服務委外辦理之管理措施。

六、所屬人員辦理業務涉及資通安全事項之考核機制。

七、資通安全偵測與防護之建置及執行方案。

八、執行前款執行方案所蒐集、儲存、處理及利用用戶之隱私與個人資料安全保護措施。

九、通過資通安全管理驗證之執行方案。

第 6 條

1 電信事業應建立資通安全事件之通報、處理、回報及聯防等應變措施。

2 資通安全事件發生後，電信事業應依主管機關通報之資通安全事件，辦理緊急應變措施並保存紀錄，回報主管機關備查，該紀錄應至少保存六個月。

3 電信事業被指定為關鍵基礎設施提供者之應變措施，應依資通安全管理法第十八條第四項規定授權訂定之資通安全事件通報及應變辦法規定辦理。

第 7 條

1 電信事業之資通安全維護計畫內容變更時，應敘明理由報請主管機關備查。

2 前項計畫應載明事項有不完備者，電信事業應於主管機關通知之期限內完成補正。

第 8 條

1 電信事業應以實體隔離方式設置電信設備機房，並具備獨立出入口。

2 前項出入口應設置全天候入侵告警與錄影監控之門禁安全管理系統，告警與錄影紀錄至少應保存六個月。

3 第一項電信設備機房除設置、維護、監督或其他營運必要之目的外，禁止任何人進入機房。

4 電信事業設置之電信設備機房應訂定機房安全管理作業規定。

5 前項電信設備機房之安全管理作業規定至少包含下列項目：

一、權責劃分：包含安全維護區、負責單位、員工編制及職掌、員工進出機房權限等。

二、門禁管理：包含進出機房人員之姓名、身分證統一編號或護照號碼等身分識別、所屬機關（構）、進出時間、進入目的、複查人員之複查紀錄及物品進出機房等管理。

三、維運管理：包含員工維運或協力廠商維護機房設備等管理。

四、環境管理：包含消防、保全、電力及相關設施管理。

五、管理紀錄：包含門禁管理、維運管理及環境管理等紀錄。

六、查核作業：包含定期與不定期查核作業。

6 前項第五款管理紀錄應至少保存六個月。

7 第四項機房安全管理作業規定，主管機關得視電信事業實施狀況要求電信事業變更之。

8 電信事業應落實執行第四項機房安全管理作業規定，主管機關得定期或視需要派員查核之。

第 9 條

具危害國家安全疑慮之人員，經國家安全或資通安全有關機關知會主管機關，電信事業應依主管機關通知，禁止該人員進入電信設備機房。

第 10 條

1 電信事業委託他人設計、設置涉及網路系統資源、用戶個人資料及通信內容相關之資通系統軟體或維運系統者，應先報請主管機關備查。維運作業時應由電信設備機房員工全程監控，並將系統連線之操作指令完整記錄之，該紀錄檔應至少保存六個月。

2 電信事業不得委託具危害國家安全疑慮之人員進行涉及網路系統資源、用戶個人資料及通信內容相關之資通系統軟體設計及設置、遠端系統連線維運及測試作業。

第 11 條

1 電信事業經主管機關通知為稽核對象者，應於主管機關通知辦理現場實地稽核之日前，備妥資通安全維護計畫實施情形之相關說明及佐證資料，以供現場查閱。

2 電信事業未能依前項規定辦理或未能於主管機關指定之時間配合稽核者，得於收受前項通知後五日內，以書面敘明理由，向主管機關提出。

3 前項申請，除有不可抗力之事由外，以一次為限。

4 主管機關辦理第一項之實地稽核前，得先訪談受稽核之電信事業。

第 12 條

1 主管機關為辦理前條第一項之稽核，得組成稽核小組。

2 前項稽核小組成員三人至七人，由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；其中公務機關代表不得少於全體成員人數之三分之一。

3 前項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，與受稽核之特定非公務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，與受稽核之特定非公務機關或其負責人間，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，曾為受稽核之特定非公務機關進行與受稽核項目相關之顧問輔導。

四、其他足認擔任稽核小組成員將影響稽核結果公正性之情形。

4 主管機關應以書面與稽核小組成員約定利益衝突之迴避事項及執行稽核之保密義務。

第 13 條

1 電信事業之資通安全維護計畫實施情形，經稽核後認有缺失或待改善者，應於收受主管機關交付之稽核結果報告後一個月內，向主管機關提出改善報告。

2 前項受稽核之電信事業提出改善報告後，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；主管機關認有必要時，得要求該電信事業說明或改善。

第 14 條

本辦法自中華民國一百零九年七月一日施行。