

電信事業資通安全管理辦法總說明

本辦法係依電信管理法第十五條規定，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，應訂定資通安全維護計畫並依該計畫實施，並授權主管機關訂定辦法之規定，研擬相關具體實施規定，俾利電信事業遵行，落實資通安全防護，以提升電信事業持續營運能力，保障用戶通信權益。本辦法重點如下：

- 一、主管機關公告適用電信事業之考量因素（第二條）
- 二、資通安全維護計畫之提報、分級處理、管理驗證基準及執行方式。（第三條至第五條）
- 三、電信事業之聯防應變及通報措施（第六條）
- 四、資通安全維護計畫有修正時之處理方式（第七條）
- 五、設置電信設備機房之門禁管理之安全要求（第八條）
- 六、電信設備機房維運管理之特別規定（第九條）
- 七、電信事業委外設計、維運之管理要求（第十條）
- 八、電信事業辦理現場稽核作業及未能配合稽核時之處理方式（第十一條）
- 九、資通安全維護計畫實施情形之稽核小組之組成相關事項及稽核結果與改善（第十二條至第十三條）
- 十、施行日期（第十四條）

電信事業資通安全管理辦法

條文	說明
第一條 本辦法依電信管理法第十五條第三項規定訂定之。 本辦法未規定者，適用其他有關法令之規定。	一、明定本辦法訂定依據。 二、本辦法為資通安全管理法之特別規定，故於第二項明定，本辦法未規定者，適用其他有關法令之規定。有關法令包括資通安全管理法之授權子法規，如資通安全管理法施行細則、資通安全責任等級分級辦法、資通安全事件通報及應變辦法、特定非公務機關資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法及國家通訊傳播委員會所管特定非公務機關資通安全管理作業辦法等。
第二條 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。 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與應變辦法規定之第三級資通安全事件以上者。	明定主管機關公告應訂定資通安全維護計畫之電信事業之考量因素。
第三條 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。 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。 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、明定電信事業應提報資通安全維護計畫之時點，爰訂定第一項規定。 二、為確保資通安全計畫之完整性，於第二項明定資通安全維護計畫應載明項目不完備時之處理程序。 三、明定資通安全維護計畫之資通安全管理範圍應包含之項目，爰於第三項規定。 四、於第四項明定資通安全維護計畫之各項

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。 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。	資通訊系統防護分級處理方式應依主管機關公告之資通訊系統防護等級分級原則辦理。
第四條 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。 前項驗證範圍應於驗證前報請主管機關核准，變更時亦同。 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與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。 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。	一、為強化電信事業之資通安全防護能量，爰明定第一項規定，要求電信事業通過一定標準之資通安全管理驗證。 二、為確保國家資通安全防護，瞭解電信事業資通安全管理情形，爰於第二項明定資通安全管理驗證範圍於驗證前及驗證範圍變更時，應報請主管機關核准。 三、審酌電信事業即使經主管機關核准其應通過資通安全國際驗證之實施作業範圍，並通過國際驗證後，仍可能發生重大資通安全事件，或有危害國安、資安等情事，為督促電信事業再行檢視其系統資通安全漏洞並修正應通過資通安全國際驗證範圍，有效降低資安風險，爰於第三項明定資通安全管理驗證範圍修正之相關規定。 四、為因應資通安全風險發生預期以外突然升高之情形，爰於第四項明定國家安全或資通安全有關機關知會主管機關得通知電信事業縮減其通過資通安全管理驗證之期程。
第五條 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。	一、第一項明定電信事業資通安全維護計畫執行方式應載明之事項。 二、電信事業之電信基礎設施經主管機關指定為關鍵基礎設施者，因其資通安全之重

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。 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。	要性大為提高，故電信事業之資通安全維護計畫執行方式，除第一項所訂事項外，另增加九款應載明事項。
第六條 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。 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。 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。	一、為使電信事業建立資通安全事件之通報、處理、回報及聯防等應變措施，俾強化其資通安全事件之應處能力，爰明定第一項規定。 二、第二項係規範電信事業依主管機關通報資通安全事件之處理及相關紀錄保存之規定。 三、第三項明定電信事業被指定為關鍵基礎設施提供者之應變措施。
第七條 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。 前項計畫應載明事項有不完備者，電	一、第一項明定電信事業修正其資通安全維護計畫時之處理程序。 二、第二項明定資通安全維護計畫應載明項

信事業應於主管機關通知之期限內完成補正。	目不完備時之處理程序。
第八條 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。 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。 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。 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。 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。 前項第五款管理紀錄應至少保存六個月。 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。 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。	一、為使電信事業之電信設備機房空間設置時，與其他非電信事業之機房、設備採實體隔離方式辦理，以減少因相連而於資通安全事件發生時之損害擴大，爰訂定第一項規定。 二、電信設備機房應設置各出入口之門禁及監控設施，並將監視紀錄保存一定期間，俾強化門禁安全，爰訂定第二項。 三、第三項明定電信設備機房以原則禁止例外許可方式管理人員進出。 四、第四項至第六項明定電信事業應訂定電信設備機房安全管理作業規定、其含括要項及管理紀錄保存期限，並報主管機關備查。 五、為使電信事業之電信設備機房安全管理與時精進，第七項明定主管機關得視電信事業實施狀況要求電信事業變更其電信設備機房安全管理作業規定。 六、第八項規定為確保電信事業依第二項所自行訂定並經主管機關備查之電信設備機房安全管理作業規定能確實執行，爰規定主管機關得派員查核之。

第九條 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。	為避免電信設備機房等國家重要之基礎設施，因具危害國家安全疑慮之人員進入，而遭受破壞或致生重大資通安全事件，爰訂定本條。
第十條 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。 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。	一、考量委外辦理資通系統軟體設計開發、系統維運，可能會增加外力滲透入侵或破壞資通系統之風險，為利於主管機關監督管理，爰於第一項明定電信事業委外進行資通系統軟體設計開發、系統維運時，應先報請主管機關備查。另為留存紀錄以備日後查考，同項亦明定維運作業監控及紀錄保存期限規定。 二、第二項明定電信事業不得委託具危害國家安全疑慮之人員進行資通系統軟體設計及開發、連線維運及測試作業之規定。
第十一條 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。 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。 前項申請，除有不可抗力之事由外，以一次為限。 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。	一、第一項明定電信事業應依主管機關之擇定，辦理資通安全維護計畫實施情形稽核作業之時程、備妥相關資料及佐證，以供現場查閱。 二、第二項明定電信事業如未能於主管機關指定時間配合稽核者之變更稽核日期申請時限。 三、第三項明定電信事業向主管機關提出變更稽核日期申請之限制條件。 四、第四項明定主管機關辦理實地稽核前，得先訪談受稽核之電信事業。
第十二條 主管機關為辦理前條第一項之稽核，得組成稽核小組。 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。 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、第一項明定主管機關為辦理電信事業資通安全維護計畫稽核，得成立稽核小組。 二、第二項明定稽核小組之成員組成。 三、第三項明定稽核小組成員之迴避規定。 四、第四項明定主管機關應與稽核小組成員書面約定利益衝突之迴避事項及執行稽核之保密義務，以確保稽核作業公正與保密。

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。 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。	
第十三條 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。 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。	一、第一項明定電信事業收受主管機關之稽核結果，該稽核結果已指明有缺失或待改善者之改善報告提出時限。 二、第二項明定電信事業改善報告之執行情形補充程序，及主管機關亦得主動要求電信事業說明或改善。
第十四條 本辦法自中華民國一百零九年七月一日施行。	明定本辦法施行日期。