固定通信業務管理規則部分條文修正總說明

為提升固定通信業務經營者之資通安全管理、災害重大事故之通報及關鍵基礎設施防護能量，以保障電信用戶資料與電信網路安全，爰修正「固定通信業務管理規則」部分條文，其修正重點如下：

一、增訂電信基礎設施之定義。（修正條文第二條）

二、增訂因災害或重大事故導致電信機線設備發生故障時，經營者應辦理通報作業、揭露障礙情形及造成使用者損害處理方式之規定。（修正條文第五十條之一）

三、增訂提報關鍵基礎設施防護計畫規定。（修正條文第五十條之二）

四、增訂經營者報請修正資通安全管理驗證實施作業範圍之規定。（修正條文第七十四條之二）

五、增訂電信設備機房或網路資料中心機房以原則禁止例外許可方式管理人員進出。（修正條文第七十四條之三）

六、移列有關經營者設置網路資料中心機房提供其他電信事業置放電信設備提供電信服務之規定。（修正條文第七十四條之四）

七、增訂禁止具危害國家安全疑慮之人員進入電信設備機房或網路資料中心機房之規定。（修正條文第七十四條之五）

八、移列有關委外進行資通系統軟體設計、系統維運、測試作業之限制規定。（修正條文第七十四條之六）

固定通信業務管理規則部分條文修正條文對照表

修正條文	現行條文	說明
第二條　本規則用詞定義如下： 一、固定通信系統：指利用有線或其他經主管機關核准之傳輸方式連接固定發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備，以及二者之附屬設備所組成之通信系統。 二、固定通信網路：指由固定通信系統所組成之通信網路。 三、固定通信：指利用固定通信網路發送、傳輸或接收語音、數據、影像、視訊、多媒體或其他性質訊息之通信。 四、固定通信業務：指經營者利用固定通信網路提供固定通信服務之業務。 五、經營者：指經主管機關特許並發給執照經營固定通信業務者。 六、管線基礎設施：指為建設市內、長途及國際通信所需之架空、地下或水底電信線路、電信引進線、電信用戶設備線路，及各項電信傳輸線路所需之管道、人孔、手孔、塔臺、電桿、配線架、機房及其	第二條　本規則用詞定義如下： 一、固定通信系統：指利用有線或其他經主管機關核准之傳輸方式連接固定發信端與受信端之網路傳輸設備、與網路傳輸設備形成一體而設置之交換設備，以及二者之附屬設備所組成之通信系統。 二、固定通信網路：指由固定通信系統所組成之通信網路。 三、固定通信：指利用固定通信網路發送、傳輸或接收語音、數據、影像、視訊、多媒體或其他性質訊息之通信。 四、固定通信業務：指經營者利用固定通信網路提供固定通信服務之業務。 五、經營者：指經主管機關特許並發給執照經營固定通信業務者。 六、管線基礎設施：指為建設市內、長途及國際通信所需之架空、地下或水底電信線路、電信引進線、電信用戶設備線路，及各項電信傳輸線路所需之管道、人孔、手孔、塔臺、電桿、配線架、機房及其	一、為明確本規則所定電信基礎設施適用範圍，爰增訂第二十二款之定義。 二、其餘未修正。

他附屬或相關設施。 七、固定通信業務市場主導者：指依第一類電信事業資費管理辦法第十條所規定之經營者。 八、用戶：指與經營者訂定契約，使用該經營者提供之固定通信服務者。 九、使用者：指用戶及其他使用經營者提供之固定通信服務者。 十、公用電話：指由經營者設置以投幣、簽帳卡、信用卡或預付卡付費，供公眾使用之電話。 十一、緊急電話：指火警、盜警及其他緊急救援報案之電話。 十二、國際海纜系統：指鋪設於海洋中之國際海底電纜及附屬設施組成之通信系統。 十三、國際海纜登陸站：指連接國際海纜與內陸鏈路設施，將國際通信所收發之電信轉接至該海纜或鏈路設施，對境內或境外進行傳輸之電信設備與附屬設施。 十四、內陸介接站：指設置於內陸以介接國際海纜電路與公眾電信網路之電信設備與附屬設施。 十五、內陸鏈路設施：指連接國際海纜登陸站與內陸介接站或任一經營者	他附屬或相關設施。 七、固定通信業務市場主導者：指依第一類電信事業資費管理辦法第十條所規定之經營者。 八、用戶：指與經營者訂定契約，使用該經營者提供之固定通信服務者。 九、使用者：指用戶及其他使用經營者提供之固定通信服務者。 十、公用電話：指由經營者設置以投幣、簽帳卡、信用卡或預付卡付費，供公眾使用之電話。 十一、緊急電話：指火警、盜警及其他緊急救援報案之電話。 十二、國際海纜系統：指鋪設於海洋中之國際海底電纜及附屬設施組成之通信系統。 十三、國際海纜登陸站：指連接國際海纜與內陸鏈路設施，將國際通信所收發之電信轉接至該海纜或鏈路設施，對境內或境外進行傳輸之電信設備與附屬設施。 十四、內陸介接站：指設置於內陸以介接國際海纜電路與公眾電信網路之電信設備與附屬設施。 十五、內陸鏈路設施：指連接國際海纜登陸站與內陸介接站或任一經營者	

公眾電信網路交換設備間之高容量內陸傳輸鏈路及附屬設備。	公眾電信網路交換設備間之高容量內陸傳輸鏈路及附屬設備。	
十六、多媒體內容傳輸平臺服務：指市內網路業務經營者設置互動媒介平臺，供用戶藉由寬頻接取電路及用戶機上盒，接取該平臺上由內容服務提供者所提供之多媒體內容服務。	十六、多媒體內容傳輸平臺服務：指市內網路業務經營者設置互動媒介平臺，供用戶藉由寬頻接取電路及用戶機上盒，接取該平臺上由內容服務提供者所提供之多媒體內容服務。	
十七、多媒體內容服務：指頻道節目內容服務或其他多媒體內容服務提供者利用多媒體內容傳輸平臺提供之語音、數據及視訊等內容服務。	十七、多媒體內容服務：指頻道節目內容服務或其他多媒體內容服務提供者利用多媒體內容傳輸平臺提供之語音、數據及視訊等內容服務。	
十八、頻道節目內容：指視聽內容以節目為單元，依內容服務提供者事先安排之播放次序及時間，於傳輸平臺頻道播放，並由用戶經由電子選單表選購收視之內容。	十八、頻道節目內容：指視聽內容以節目為單元，依內容服務提供者事先安排之播放次序及時間，於傳輸平臺頻道播放，並由用戶經由電子選單表選購收視之內容。	
十九、內容服務提供者：指利用多媒體內容傳輸平臺，提供頻道節目內容或多媒體內容服務之業者。	十九、內容服務提供者：指利用多媒體內容傳輸平臺，提供頻道節目內容或多媒體內容服務之業者。	
二十、電信設備機房：指經營者設置用以控制機械、器具、線路及其他相關設備，以提供電信服務之機房。	二十、電信設備機房：指經營者設置用以控制機械、器具、線路及其他相關設備，以提供電信服務之機房。	
二十一、網路資料中心機房：指經營者設置機櫃、電力、空調及消防等設	二十一、網路資料中心機房：指經營者設置機櫃、電力、空調及消防等設	

施，出租、代管或提供用戶自行架設資通設備之機房。 二十二、電信基礎設施：指電信設備及其管線基礎設施。	施，出租、代管或提供用戶自行架設資通設備之機房。	
第五十條之一　因災害或其他重大事故導致電信機線設備發生故障，有下列各款情形之一，經營者應依第二項規定辦理通報作業，並依第四項規定向使用者揭露障礙情形及造成使用者損害處理方式： 一、市內網路業務用戶一萬戶以上中斷服務達三十分鐘以上者。 二、長途電路一千路以上中斷服務達三十分鐘以上者。 三、本島與離島間、國際間之海纜系統中斷服務達三十分鐘以上者。 經營者依前項規定辦理通報作業時，應依下列通報程序辦理： 一、前項各款情形發生後十五分鐘內，以簡訊通報障礙情形。 二、前項各款情形發生後二小時內，將障礙情形及修復進度登錄主管機關之通訊傳播重大災害災損通報系統；並於故障排除		一、本條新增。 二、審酌固定通信業務包含綜合網路、市內網路、長途網路、國際網路及電路出租等業務，現階段主管機關因應災害防救需要，需掌握市內網路業務之市話語音、數據通信，及長途電路、海纜之網路狀態，為強化經營者對於災害或其他重大事故發生時之因應能力，並利於主管機關適時監督經營者之災損復建情形及確保消費者權益，爰於第一項明定經營者於發生災害或重大事故，導致無法提供服務之情形嚴重者，應依規定辦理通報作業，並向用戶揭露障礙情形及損害處理方式。 三、第一項第一款考量市內網路業務經營者確認市話或數據網路故障原因，至少約需十五分鐘以上，且核心網路與城鎮區域網路所需時間不同，另市話交換機門號數一般市話局約二萬戶

前，每三小時更新障礙情形及修復進度。但障礙情形有重大變化時，應隨時通報。 經營者無法依前項規定通報時，得以傳真、電話、電子郵件或其他方式通報。 第一項各款情形發生後一小時內，經營者應利用廣播、電視或網際網路等電子媒體向使用者揭露障礙情形，包含障礙原因、障礙影響區域及預計修復提供服務時間；經營者並應於第一項情形完成修復提供服務後一小時內，向使用者揭露第五十條第二項第五款所規定之處理方式。 經營者積極執行災害防救工作經政府評定績效優良者，主管機關得予以獎勵或補助。		為單位，規劃以其半數用戶障礙為通報要件，爰以市內網路業務一萬用戶斷訊逾三十分鐘之條件作為業者通報門檻；第二款審酌市話撥打長途電話將使用長途路由，一條長途路由可收納多路市內電話通訊，且長途電路故障時係以路由調度方式因應，爰以一千路斷訊達三十分鐘以上之持續性障礙作為經營者通報門檻；第三款審酌本島與離島間、國際間之海纜通信均為重要之對外通訊路由，雖然故障時得以路由調度方式因應，惟導致斷訊達三十分鐘以上已屬持續性障礙，爰訂為通報門檻。 四、第二項以複式通報之原則明定通報程序，以利經營者辦理通報作業。 五、第三項明定無法透過網路至主管機關系統登錄時之替代通報方式，俾經營者遵循辦理。 六、第四項明定經營者應向使用者揭露障礙情形及補償措施之方式，俾保障消費者權益。 七、電信事業係屬災害防救法施行細則第三條所規範之公共事業，為提升

		經營者辦理防災、應變、減災及救災等業務之意願，爰於第五項明定對於積極辦理防救災且經政府評定績效優良者予以獎勵或補助。
第五十條之二　經營者應於主管機關通知之日起三個月內，依附表一盤點其各項電信基礎設施，盤點結果如列為電信關鍵基礎設施者，應辦理電信關鍵基礎設施自評，並檢具附表二至四陳報主管機關核定其關鍵基礎設施之項目及級別。 前項經營者檢具之附表資料應載明基礎設施項目不完備者，經營者應於主管機關通知之期限內完成補正。 經營者應於主管機關核定關鍵基礎設施項目及其級別之日起三個月內，依下列規定完成關鍵基礎設施防護計畫： 一、屬一級關鍵基礎設施者，應提報主管機關核定。 二、屬二級關鍵基礎設施者，應報主管機關備查。 三、屬三級關鍵基礎設施者，應自行列管。 前項經營者提報之一級或二級關鍵基礎設施		一、本條新增。 二、第一項明定經營者應於主管機關通知後一定期限內盤點電信基礎設施，同時針對盤點結果符合一定規模之設施自評電信關鍵基礎設施級別，並檢具自評之相關資料，陳報主管機關，由主管機關核定其關鍵基礎設施之項目及級別，以配合辦理關鍵基礎設施防護工作。 三、第二項明定經營者自評資料不完備之補正規定。 四、第三項明定經營者應配合完成關鍵基礎設施防護計畫之期限，及不同級別關鍵基礎設施防護計畫之列管方式。 五、為確保經營者提報關鍵基礎設施防護計畫之合理性及完整性，爰為第四項規定。 六、為確保經營者落實執行關鍵基礎設施防護計畫，爰於第五項明定經營者應定期演練，並作成書面紀錄保存。

防護計畫應載明事項(如附件一)不完備者,經營者應於主管機關通知之期限內完成補正。 經營者應依關鍵基礎設施防護計畫定期自行辦理演練，並作成書面紀錄，該紀錄應保存五年。 主管機關得指定經營者依其關鍵基礎設施防護計畫辦理演練，並由主管機關就演練情形予以評核；評核結果有待改善事項者，經營者應依主管機關之通知限期改善。		七、為督促經營者確實辦理關鍵基礎設施定期演練事宜，爰為第六項規定，透過指定演練及評核措施，要求經營者改善關鍵基礎設施防護計畫之缺失，以強化關鍵基礎設施韌性。
第七十四條之二　經營者應於取得特許執照之日起一年內建立資通安全防護與偵測設施，並於二年內通過下列資通安全管理驗證： 一、CNS 27001 國家標準或 ISO/IEC 27001 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/IEC 27011 增項稽核表。 本規則中華民國一百零四年十一月十三日修正之條文施行前，已取得特許執照之經營者，應自修正施行之日起一年內建立資通安全防護與偵測設施，並於二年內通過前項資通安全管理驗證。	第七十四條之二　經營者應於取得特許執照之日起一年內建立資通安全防護與偵測設施，並於二年內通過 ISO/IEC 27001 國際標準及主管機關公告之電信事業資通安全管理手冊 ISO/IEC 27011 增項稽核表之資通安全管理驗證。 本規則中華民國一百零四年十一月十三日修正之條文施行前，已取得特許執照之經營者，應自修正施行之日起一年內建立資通安全防護與偵測設施，並於二年內通過 ISO/IEC 27001 國際標準及主管機關公告之電信事業資通安全管理手冊 ISO/IEC 27011 增項稽核表之資通安全管理驗證。	一、經查經濟部標準檢驗局一〇三年四月二十四日公告 CNS 27001「資訊技術-安全技術-資訊安全管理系統－要求事項」國家標準，CNS 27001 係參考二〇一三年最新版 ISO/IEC 27001 國際標準修訂，爰酌為修正第一項及第二項文字。 二、審酌經營者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，仍可能發生重大資安事件，或有危害國安、資安等情事，為督促經營者再行檢視其系統資通安全漏洞並擴大應通過資通安

前二項驗證之實施作業範圍與資通安全偵測防護設施，應先報請主管機關核准。 經營者有下列情形之一，應依主管機關通知，修正第一項及第二項驗證之實施作業範圍，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、系統發生資通安全事件達國家資通安全通報應變作業綱要規定之影響等級第三級以上者。 二、有危害國家安全或資通安全之虞，經有關機關通知者。 第一項及第二項期間，經國家安全或資通安全有關機關通知，主管機關得命經營者縮減之。 經營者應定期進行滲透測試、弱點掃描及修補作業，且應依主管機關公告之資通安全應變作業程序，建立資通安全事件之通報、處理、回報等聯防應變措施。 資通安全事件發生後，經營者應依主管機關通報之資安事件，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。	前二項驗證之實施作業範圍與資通安全偵測防護設施，應先報請主管機關核准。 第一項及第二項期間，經國家安全或資通安全有關機關通知，主管機關得命經營者縮減之。 經營者應定期進行滲透測試、弱點掃描及修補作業，且應依主管機關公告之資通安全應變作業程序，建立資通安全事件之通報、處理、回報等聯防應變措施。 資通安全事件發生後，經營者應依主管機關通報之資安事件，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。	全國際驗證之實施作業範圍，有效降低資安風險，爰增訂第四項規定。 三、原條文第四項移列為第五項。 四、原條文第五項移列為第六項。 五、原條文第六項移列為第七項。

第七十四條之三　經營者設置電信設備機房或網路資料中心機房，均應以實體隔離方式設置，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或網路資料中心機房，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。 經營者應按其設置之電信設備機房或網路資料中心機房，分別訂定機房安全管理作業規定，並報主管機關備查。 前項電信設備機房或網路資料中心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：包含進出機房之員工、協力廠商、參訪人員或網路資料中心之客戶等人員之姓名、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	第七十四條之三　經營者設置電信設備機房或網路資料中心機房，均應以實體隔離方式設置，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。 經營者應按其設置之電信設備機房或網路資料中心機房，分別訂定機房安全管理作業規定，並報主管機關備查。 前項電信設備機房或網路資料中心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：包含人員（員工、協力廠商、參訪人員或網路資料中心之客戶等）身分識別（至少包含進出人員姓名、身分證統一編號或護照號碼）、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	一、增訂第三項，明定電信設備機房或網路資料中心機房以原則禁止例外許可方式管理人員進出。 二、第四項移列至第五項，第二款並酌作文字調整。 三、第六項及第七項移列至增訂條文第七十四條之四。 四、第八項及第九項項次遞移，分別移列至第七項及第八項，並酌作文字調整。

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，主管機關得視經營者實施狀況要求經營者變更之。 經營者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。	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。 經營者設置網路資料中心機房提供其他電信事業置放電信設備提供電信服務時，其出租予其他電信事業之空間，應以實體隔離方式設置，並具備獨立出入口。 經營者設置網路資料中心機房已出租予其他電信事業置放電信設備不符前項規定者，應於本規則一百零四年十一月十三日修正之條文施行之日起一年內改正，無法於期限內改正者，得於期限屆滿前敘明理由向主管機關申請展期。展期最長不得逾六個月，並以一次為限。 第三項機房安全管理作業規定，主管機關得視經營者實施狀況要求經營者變更之。 經營者應落實執行第三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。	
第七十四條之四　經營者設置網路資料中心機房提供其他電信事業置放電信設備提供電信服務時，其出租予其他電信事業之空間，應以實體隔離方式設置，並具備獨立出入口。 經營者設置網路資料中心機房已出租予其他電信事業置放電信設備不符前項規定者，應於本規則中華民國一百零四年十一月十三日修正之條文施行之日起一年內改正。無法於期限內改正者，得於期限屆滿前敘明理由向主管機關申請展期；展期最長不得逾六個月，並以一次為限。		一、本條新增。 二、由現行條文第七十四條之三第六項及第七項移列，並酌作文字調整。
第七十四條之五　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，經營者應依主管機關通知，禁止該人員進入電信設備機房或網路資料中心機房。		一、本條新增。 二、比照第二類電信事業管理規則第三十一條之二第四項規定，明定禁止具危害國家安全疑慮之人員進入電信設備機房或網路資料中心機房，以防止國家重要之電信基礎設施遭受破壞或入侵。
第七十四條之六　經營者如委託他人設計涉及網路系統資源、用戶個人資料及通信內容相關之資通系統		一、本條新增。 二、由現行條文第七十四條之四移列，內容未修正。

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。 經營者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、遠端系統連線維運及測試作業。		

附表一

電信關鍵基礎設施影響因子評量表

設施名稱	風險因子	風險等級
	影響用戶數(人)	□非常高(10 萬人以上)
		□高(1 萬人以上 未達 10 萬人)
		□中(1 千人以上 未達 1 萬人)
		□低(未達 1 千人)
	經濟(營運)損失(NT$)	□非常高(2 億 5 千萬元以上)
		□高(2 千 5 百萬元以上 未達 2 億 5 千萬元)
		□中(1 千萬元以上 未達 2 千 5 百萬元)
		□低(未達 1 千萬元)
	本設施失效時，其他電信基礎設施對本設施功能替代性	□高(無法藉由其他設施替代本設施服務功能 70%以上)
		□中(僅有 1 至 2 個其他設施可替代本設施服務功能 70%以上)
		□低(有 2 個以上其他設施可替代本設施服務功能 70%以上)
	總分	**各項風險因子中有任 1 項風險等級達中級以上者** 列為電信關鍵基礎設施

附表二

電信事業關鍵基礎設施基本資料

填表日期：　　年　　月　　日

填報單位資料				
部會	單位	聯絡人姓名	聯絡人電話	聯絡人電子郵件

風險評量資料(依附表三風險評量得分填列)							
屬性	相依性	脆弱性	關鍵性	民心士氣	復原力	替代性	風險評量總分

相關採購、安裝與維護有無涉及外(陸)資或人員	
說明（無則填「無涉及」）	

(一)設施概述	
編號	
名稱	
主部門與次部門	主部門： 次部門：
設施級別	
機密等級	
設施財產擁有單位	
設施地址(位置)	縣市/地址/郵遞區號： 位置經度： 位置緯度：
設施擁有單位聯絡電話	
設施保管人	
設施保管人連絡電話	辦公室： 住家： 行動電話：
代理人	
代理人聯絡電話	辦公室： 行動電話：
設施自有警衛人數	
設施民防組織	
設施警監、安全裝備	
設施消防裝備	
避難引導權責單位	
減災防護權責單位	
避難容留場所	
(二)核心功能概述	
相關核心功能	

設施毀損時，對核心功能維持之影響	
設施毀損時，對軍事作戰之影響	
設施毀損時，對全民防衛動員之影響	
設施及民生機能或金融秩序之關係	
(三)相依性描述	
設施毀損時，對其他關鍵基礎設施之影響	
那些關鍵基礎設施毀損時，會影響本設施	
(四)過去五年內曾遭遇之破壞(脆弱性)	
遭人為攻擊之次數及情況	
遭網路攻擊之次數及情況	
遭天然災害破壞之次數及情況	
(五)消防與救護規劃	
消防救護派遣單位	
可派遣人力	
主要裝備	
抵達所需時間	
聯絡方式	(每支援機關列出 2 隻聯絡電話)
救護優先醫院	(每支援機關列出 2 隻聯絡電話)
其他支援消防單位	
消防、救護特別注意事項	(如輻射線、毒化物、易燃品等)
(六)資安防護計畫	
設施資安維護人員	
聯繫電話	辦公室： 行動電話：
資安防護計畫	
資安建議	
(七)搶救復原計畫	
搶修負責單位	
搶修負責單位聯絡人	
聯絡人電話	辦公室：

	行動電話：
搶修計畫	（以維持基本運作為主）
搶修所需人力	
搶修所需機具	
搶修評估時效	
搶修預期之困難	
復原規劃	（以恢復基本運作為主）
復原、評估時效	
復原預期之困難	
(八)替代性 1.設施毀損時本單位有何替代性設施	
替代性設施名稱	
替代性設施位置	
替代性設施聯絡人	
聯絡人電話	辦公室： 行動電話：
(八)替代性 2.設施毀損時他單位有何替代性設施可供支援	
替代性設施名稱	
替代性設施位置	
替代性設施聯絡人	
聯絡人電話	辦公室： 行動電話：
(九)演練計畫	
演練項目	
演練目標	
演練時程	
演練方式及想定	
演練人員	
(十)其他	
防護建議或其他要求事項	
有無相關防護計畫書（如有，請列附件）	

備註：

「(一)設施概述」之設施級別，應依該關鍵基礎設施之「(二)核心功能概述」及附表三「電信事業關鍵基礎設施風險評量表」評量結果評定級別為「一級、二級、三級」。

附表三

電信事業關鍵基礎設施風險評量表

填表日期：　　年　　月　　日

	條件定義	配分	得分	小計
A 屬性（複選）	□該設施為部會遂行指管之節點	1-10		
	□該設施為產生重要資訊之節點	1-5		
	□該設施與支援軍事作戰相關	1-5		
	□該設施為執行全民防衛動員之必要節點	1-5		
	□該設施與民生必需機能或金融秩序相關	1-5		
I 相依性	與其他部門關鍵基礎設施間之相依性，例如斷電斷水將影響其他設施效能及運作(未與其他設施相依者為 1 分，每增加 1 座相依設施則加計 1 分)	1-10		
V 脆弱性	遭爆炸之防護能力 □0 分-無設施□1 分-特殊結構□2 分-運作結構分散或鋼結構□3 分-混凝土/石材硬化結構□4 分-存有易燃物/炸藥或木頭結構□5 分-無安全設計	0-5		
	遭生物性/化學性攻擊之防護能力 □0 分-無設施□1 分-具防恐計畫且員工訓練完善□2 分-空調進口有過濾及保護□3 分-郵件/包裹自由傳遞□4 分-大眾自由進出□5 分-無保護措施	0-5		
	遭網路攻擊之防護能力 □0 分-無設施□1 分-具資安防護計畫且演訓完善□2 分-具資安防護計畫但已二年以上未曾演訓□3 分-具資安防護計畫但已三年以上未曾演訓□4 分-具資安防護計畫但無演訓□5 分-無資安防護計畫	0-5		
	遭天然災害之防護能力 □0 分-無設施□1 分-具防災計畫且演訓完善□2 分-具防災計畫但已二年以上未曾演訓□3 分-具防災計畫但已三年以上未曾演訓□4 分-具防災計畫但無演訓□5 分-無防災計畫	0-5		

C 關鍵性	經濟損失與重建經費(單位：新臺幣元) □0 分-無□0.5 分-未達 1 千萬元□1 分-1 千萬元以上未達 2 千 5 百萬元□1.5 分-2 千 5 百萬元以上未達 5 千萬元□2 分-5 千萬元以上未達 1 億元□2.5 分-1 億元以上未達 2 億 5 千萬元□3 分-2 億 5 千萬元以上未達 5 億元□3.5 分-5 億元以上未達 7 億 5 千萬元□4 分-7 億 5 千萬元以上未達 1 兆元□4.5 分-1 兆元以上未達 25 兆元□5 分-25 兆元以上	0-5		
	設施遭破壞 72 小時內直接影響人數 □0 分-無□0.5 分-未達 1 千人□1 分-1 千人以上未達 1 萬人□1.5 分-1 萬人以上未達 2 萬 5 千人□2 分-2 萬 5 千人以上未達 5 萬人□2.5 分-5 萬人以上未達 10 萬人□3 分-10 萬人以上未達 50 萬人□3.5 分-50 萬人以上未達 100 萬人□4 分-100 萬人以上未達 250 萬人□5 分-250 萬人以上	0-5		
	預估死亡人數 □0 分-無□0.5 分-未達 10 人□1 分-10 人以上未達 50 人□1.5 分-50 人以上未達 100 人□2 分-100 人以上未達 250 人□2.5 分-250 人以上未達 500 人□3 分-500 人以上未達 1 千人□3.5 分-1 千人以上未達 5 千人□4 分-5 千人以上未達 1 萬人□4.5 分-1 萬人以上未達 5 萬人□5 分-5 萬人以上	0-5		
E 民心士氣	對民心士氣之影響(複選，每項 1.25 分) □基本生存機能□地方標的物□政府標的物□國家標的物□國際標的物□歷史標的物□社會尊嚴□民族尊嚴	1-10		
Y 復原力	□該設施在受損程度 50%時，無法於 72 小時內恢復正常運作	1		
	□該設施在受損程度 50%時，能於 24 小時至 72 小時間恢復正常運作	0.9		
	□該設施在受損程度 50%時，能於 24 小時內恢復正常運作	0.5		
Z 替代性	□無法藉由其他設施以替代該設施之 70%以上之功能	1		
	□僅有 1 至 2 個其他設施可替代該設施之 70%以上之功能	0.9		

	□具有 2 個以上其他設施可替代該設施之 70%以上之功能	0.5	

風險評量總分　（A＋V＋I＋C＋E）＊Y＊Z　=	

備註：本表如有更新，以行政院下達之最新版本為準。

附表四

電信事業關鍵基礎設施風險評量及設施級別自評表

公司有無涉及外資情形？ -------------------　　　　填報單位：公司全名

公司有無涉及陸資情形？ -------------------

編號											
公司別	項次	次部門	重要元件設施		資產名稱	地點	風險評量總分	設施級別	理由	機房有無網管系統等	機房有無其他重要資訊系統

備註：

1.本表每一列之自評資料應依附表二之基本資料填列。

2.「公司別」欄位：請以2至4字簡稱公司名稱

3.「理由」欄位：需摘要敘明評定該設施級別之理由。

4.「機房有無網管系統等」欄位：係指與CI直接關聯之網管維運系統、網域名稱解析系統、主控播出系統、數位訊號加擾及授權管理系統。

5.「機房有無其他重要資訊系統」欄位：係指與CI營運有關之帳務及用戶管理系統。

附件一

○○公司○○業務電信關鍵基礎設施防護計畫(參考格式)

壹、依據

貳、願景及目標

一、 機房安全防護願景

(依照營運需要、相關法律與法規，敘明管理階層對安全防護之指示與支持)

二、 機房安全防護目標

(安全防護的系列政策應明訂出來，受管理階層核准、發布並傳達給員工與相關的外部團體)

參、機房人力及防護編組

(明確建立具有管理能力之組織框架，以辦理、管理機房安全防護實施和操作)

一、機房人力

(明訂組織架構、人力編制及工作職掌等，安全防護責任亦應予明確分配)

三、 防護編組

(編組時應注意相互衝突的職務與責任領域應加以區隔，以降低組織資產遭未經授權或非故意的修改或誤用之機會)

肆、機房資產管理

(應鑑別組織資產與明訂適當保護責任；確保資產依照其對組織的重要性受到適切等級的保護；防止資產被未經授權的揭露、移除或破壞)

一、系統及網路架構

(架構圖與說明、連外傳輸路由及空間配置圖)

二、機房設備盤點

(機房設備清單：設備之名稱、數量、容量、功能、所在位置、適用業務別)

伍、機房風險評鑑

(明訂定期風險評鑑或發生重大變更時重新評鑑，以確保其持續的適用性、充分性與有效性)

一、風險識別

（應明確識別所有資產，並製作與維持所有重要資產的清冊；識別前應經由定期蒐集與量測有關於災難、意外事件、社會現象等導致電信設備失效與網路壅塞之相關資訊並彙集關鍵知識）

二、風險估計

三、風險評估

（評估潛在的天然災害、恐怖攻擊及網路攻擊等，所造成各種直接與間接的危害風險，以及分析機房在各種危害威脅下之脆弱性）

四、風險處理

陸、機房實體及環境安全防護

（防護規劃應儘可能的防止機房內部設施遭未經授權的存取、損害及干擾；防止資產的遺失、損害、竊盜或破解，同時防止機房運作遭到中斷）

一、機房安全邊界

（訂定資產管理規範、實體及環境安全規範；應界定與使用安全邊界，藉以防護敏感的或是重要的資訊與資訊處理設施之區域）

二、門禁管理

（訂定人員進出管制措施；安全區域應藉由適當的入口控制措施加以保護，以確保只有經授權人員方可允許進出；應規劃並實施辦公室、房間及設施的實體安全）

三、環境安全措施

（訂定消防安全、水源供應、電力供應、耐震性及空調等之安全措施；明訂對外部與環境威脅的保護規範，包含要求在安全區域內工作、收發與裝卸區、設備安置與保護、支援的設施、佈纜的安全、設備維護、資產的攜出、駐外設備的安全、設備的汰除或再使用之安全、無人看管的用戶設備、桌面淨空與螢幕淨空政策等）

四、人力資源安全管理

（訂定員工、承包商、第三方之角色責任及須遵循之安全規範及管理，內容包含資訊系統獲取、開發及維護、行動設備的政策、遠距工作、聘僱前之管理、聘僱期間管理、聘僱終止與變更之管理、使用者責任之管理、供應商關係的資訊安全管理、供應商服務交付管理、通報資訊安全弱點等）

柒、機房網路維運管理

一、機房作業機制

（機房設備之各項作業程序及活動，是否文件化並適當維護，並訂定組織資訊安全管理規範，內容包含通信與作業管理、存取控制、資訊系統之獲取、開發及維護、存取控制的營運要求、使用者存取管理、系統與應用系統的存取控制、密碼控制措施、作業之程序與責任、防範惡意程式、備份、存錄與監控、作業軟體的控制、技術脆弱性管理、資訊系統稽核考量、網路安全管理、資訊轉換、資訊系統的安全要求、開發與支援過程的安全、測試資料等）

二、機房依賴性

（機房服務對象之重要性，並建立災害搶修對象之優先順序）

三、備援機制

（系統、網路及電力損害之備援機制，內容並包含資訊系統獲取、開發及維護、資訊安全的持續性、複式配置等）

捌、救援規劃及通報應變

（應與相關權責機關維持適當聯繫；應與各特殊利害相關團體或其他各種專家安全性論壇及專業協會維持適當聯繫）

一、救援資源規劃

（內部資源：人力配置、聯絡辦法；外部資源：消防、警戒人力及救護規劃）

二、通報應變作業

（災前：設備整備、偵測及預防；災中：通報、災情蒐集及通訊確保之應變及處理；災後：復原及檢討，並訂定資訊安全事故與改進的管理）

玖、安全防護教育訓練、演練及檢討

一、安全防護教育訓練

（教育員工熟悉災害及資安事故之通報及處理程序）

二、安全防護演練及事故檢討

（訂定演練計畫，並定期演練；建立事故後管理會議，從相關經驗中進行成效評估，從資訊安全事故中學習，作為後續檢討與改善之依據；應評鑑資訊安全事件，並決定是否歸類為資訊安全事故）

備註：業者撰寫電信關鍵基礎設施防護計畫時，請參考 CNS27001 及 CNS27011 之相關規定。