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)

二、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。

本則命令之總說明及對照表請參閱行政院公報資訊網（http://gazette.nat.gov.tw/）。