# 紀錄編號： 填表日期：　　年　　月　　日

| 控制目標 | 控制措施 | 適用Y/N | 適用/不適用理由 | 相關參考文件 |
| --- | --- | --- | --- | --- |
| A.5資訊安全政策 |
| A.5.1 | 資訊安全之管理指導方針 | A.5.1.1 | 資訊安全政策 | Y |  |  |
| A.5.1.2 | 資訊安全政策之審查 | Y |  |  |
| A.6資訊安全之組織 |
| A.6.1 | 內部組織 | A.6.1.1 | 資訊安全之角色及責任 | Y |  |  |
| A.6.1.2 | 職務區隔 | N | C級單位不適用 |  |
| A.6.1.3 | 與權責機關之聯繫 | Y |  |  |
| A.6.1.4 | 與特殊關注方之聯繫 | Y |  |  |
| A.6.1.5 | 專案管理之資訊安全 | N | C級單位不適用 |  |
| A.6.2 | 行動裝置及遠距工作 | A.6.2.1 | 行動裝置政策 | N | C級單位不適用 |  |
| A.6.2.2 | 遠距工作 | N | C級單位不適用 |  |
| A.7人力資源安全 |
| A.7.1 | 聘用前 | A.7.1.1 | 篩選 | N | C級單位不適用 |  |
| A.7.1.2 | 聘用條款及條件 | Y |  |  |
| A.7.2 | 聘用期間 | A.7.2.1 | 管理階層責任 | N | C級單位不適用 |  |
| A.7.2.2 | 資訊安全認知、教育及訓練 | Y |  |  |
| A.7.2.3 | 懲處過程 | Y |  |  |
| A.7.3 | 聘用責任之終止或變更 | A.7.3.1 | 聘用責任之終止或變更 | Y |  |  |
| A.8資產管理 |
| A.8.1 | 資產責任 | A.8.1.1 | 資產清冊 | Y |  |  |
| A.8.1.2 | 資產擁有權 | Y |  |  |
| A.8.1.3 | 資產之可被接受的使用 | Y |  |  |
| A.8.1.4 | 資產之歸還 | Y |  |  |
| A.8.2 | 資訊分級 | A.8.2.1 | 資訊之分級 | Y |  |  |
| A.8.2.2 | 資訊之標示 | Y |  |  |
| A.8.2.3 | 資產之處置 | Y |  |  |
| A.8.3 | 媒體處理 | A.8.3.1 | 可移除式媒體之管理 | N | C級單位不適用 |  |
| A.8.3.2 | 媒體之汰除 | Y |  |  |
| A.8.3.3 | 實體媒體傳送 | N | C級單位不適用 |  |
| A.9存取控制 |
| A.9.1 | 存取控制之營運要求事項 | A.9.1.1 | 存取控制政策 | N | C級單位不適用 |  |
| A.9.1.2 | 對網路及網路服務之存取 | N | C級單位不適用 |  |
| A.9.2  | 使用者存取管理 | A.9.2.1 | 使用者註冊與註銷 | Y |  |  |
| A.9.2.2 | 使用者存取權限之配置 | N | C級單位不適用 |  |
| A.9.2.3 | 具特殊存取權限之管理 | N | C級單位不適用 |  |
| A.9.2.4 | 使用者之秘密鑑別資訊的管理 | Y |  |  |
| A.9.2.5 | 使用者存取權限之審查 | N | C級單位不適用 |  |
| A.9.2.6 | 存取權限之移除或調整 | Y |  |  |
| A.9.3 | 使用者責任 | A.9.3.1 | 秘密鑑別資訊之使用 | Y |  |  |
| A.9.4 | 系統及應用存取控制 | A.9.4.1 | 資訊存取限制 | Y |  |  |
| A.9.4.2 | 保全登入程序 | Y |  |  |
| A.9.4.3 | 通行碼管理系統 | Y |  |  |
| A.9.4.4 | 具特殊權限公用程式之使用 | N | C級單位不適用 |  |
| A.9.4.5 | 對程式源碼之存取控制 | N | C級單位不適用 |  |
| A.10密碼學(加密控制) |
| A.10.1 | 密碼式控制措施(加密控制措施) | A.10.1.1 | 使用密碼式控制措施(加密控制措施)政策 | N | C級單位不適用 |  |
| A.10.1.2 | 金鑰管理 | N | C級單位不適用 |  |
| A.11實體及環境安全 |
| A.11.1 | 安全區域 | A.11.1.1 | 實體安全周界 | Y |  |  |
| A.11.1.2 | 實體進入控制措施 | N | C級單位不適用 |  |
| A.11.1.3 | 保全之辦公室、房間及設施 | N | C級單位不適用 |  |
| A.11.1.4 | 防範外部及環境威脅 | N | C級單位不適用 |  |
| A.11.1.5 | 於保全區域內工作 | N | C級單位不適用 |  |
| A.11.1.6 | 交付及裝卸區 | N | C級單位不適用 |  |
| A.11.2 | 設備 | A.11.2.1 | 設備安置及保護 | N | C級單位不適用 |  |
| A.11.2.2 | 支援之公用服務事業 | N | C級單位不適用 |  |
| A.11.2.3 | 佈纜安全 | N | C級單位不適用 |  |
| A.11.2.4 | 設備維護 | Y |  |  |
| A.11.2.5 | 財產之攜出 | Y |  |  |
| A.11.2.6 | 場所外設備及資產的安全 | N | C級單位不適用 |  |
| A.11.2.7 | 設備汰除或再使用之保全 | Y |  |  |
| A.11.2.8 | 無人看管之使用者設備 | N | C級單位不適用 |  |
| A.11.2.9 | 桌面淨空及螢幕淨空政策 | N | C級單位不適用 |  |
| A.12運作安全 |
| A.12.1 | 運作程序及責任 | A.12.1.1 | 文件化運作程序 | Y |  |  |
| A.12.1.2 | 變更管理 | N | C級單位不適用 |  |
| A.12.1.3 | 容量管理 | N | C級單位不適用 |  |
| A.12.1.4 | 開發、測試及運作環境之區隔 | N | C級單位不適用 |  |
| A.12.2 | 防範惡意軟體 | A.12.2.1 | 防範惡意軟體之控制措施 | Y |  |  |
| A.12.3 | 備份 | A.12.3.1 | 資訊備份 | N | C級單位不適用 |  |
| A.12.4 | 存錄及監視 | A.12.4.1 | 事件存錄 | N | C級單位不適用 |  |
| A.12.4.2 | 日誌資訊之保護 | N | C級單位不適用 |  |
| A.12.4.3 | 管理者及操作者日誌 | N | C級單位不適用 |  |
| A.12.4.4 | 鐘訊同步 | N | C級單位不適用 |  |
| A.12.5 | 運作中軟體之控制 | A.12.5.1 | 運作中系統之軟體安裝 | Y |  |  |
| A.12.6 | 技術脆弱性管理 | A.12.6.1 | 技術脆弱性管理 | N | C級單位不適用 |  |
| A.12.6.2 | 對軟體安裝之限制 | N | C級單位不適用 |  |
| A.12.7 | 資訊系統稽核考量 | A.12.7.1 | 資訊系統稽核控制措施 | Y |  |  |
| A.13通訊安全 |
| A.13.1 | 網路安全管理 | A.13.1.1 | 網路控制措施 | N | C級單位不適用 |  |
| A.13.1.2 | 網路服務之安全 | N | C級單位不適用 |  |
| A.13.1.3 | 網路之區隔 | N | C級單位不適用 |  |
| A.13.2 | 資訊傳送 | A.13.2.1 | 資訊傳送政策及程序 | Y |  |  |
| A.13.2.2 | 資訊傳送協議 | Y |  |  |
| A.13.2.3 | 電子傳訊 | N | C級單位不適用 |  |
| A.13.2.4 | 機密性或保密協議 | Y |  |  |
| A.14系統獲取、開發及維護 |
| A.14.1 | 資訊系統之安全要求事項 | A.14.1.1 | 資訊安全要求事項分析及規格 | N | C級單位不適用 |  |
| A.14.1.2 | 保全公共網路之應用服務 | N | C級單位不適用 |  |
| A.14.1.3 | 保護應用服務交易 | N | C級單位不適用 |  |
| A.14.2 | 作業系統存取控制 | A.14.2.1 | 保全開發政策 | N | C級單位不適用 |  |
| A.14.2.2 | 系統變更控制程序 | N | C級單位不適用 |  |
| A.14.2.3 | 運作平台變更後，應用之技術審查 | N | C級單位不適用 |  |
| A.14.2.4 | 軟體套件變更之限制 | N | C級單位不適用 |  |
| A.14.2.5 | 保全系統工程原則 | N | C級單位不適用 |  |
| A.14.2.6 | 保全開發環境 | N | C級單位不適用 |  |
| A.14.2.7 | 委外開發 | N | C級單位不適用 |  |
| A.14.2.8 | 系統安全測試 | N | C級單位不適用 |  |
| A.14.2.9 | 系統驗收測試 | N | C級單位不適用 |  |
| A.14.3 | 測試資料 | A.14.3.1 | 測試資料之保護 | N | C級單位不適用 |  |
| A.15供應者關係 |
| A.15.1 | 供應者關係中之資訊安全 | A.15.1.1 | 供應者關係之資訊安全政策 | N | C級單位不適用 |  |
| A.15.1.2 | 於供應者協議中闡明安全性 | Y |  |  |
| A.15.1.3 | 資訊及通訊技術供應鏈 | N | C級單位不適用 |  |
| A.15.2 | 供應者服務交付管理 | A.15.2.1 | 供應者服務之監視及審查 | Y |  |  |
| A.15.2.2 | 管理供應者服務之變更 | Y |  |  |
| A.16資訊安全事故管理 |
| A.16.1 | 資訊安全事故及改善之管理 | A.16.1.1 | 責任及程序 | Y |  |  |
| A.16.1.2 | 通報資訊安全事件 | Y |  |  |
| A.16.1.3 | 通報資訊安全弱點 | Y |  |  |
| A.16.1.4 | 資訊安全事件評估及決策 | Y |  |  |
| A.16.1.5 | 對資訊安全事故之回應 | Y |  |  |
| A.16.1.6 | 由資訊安全事故中學習 | Y |  |  |
| A.16.1.7 | 證據之收集 | Y |  |  |
| A.17營運持續管理之資訊安全層面 |
| A.17.1 | 資訊安全持續 | A.17.1.1 | 規劃資訊安全持續 | N | C級單位不適用 |  |
| A.17.1.2 | 實作資訊安全持續 | N | C級單位不適用 |  |
| A.17.1.3 | 查證、審查及評估資訊安全持續 | N | C級單位不適用 |  |
| A.17.2 | 多重備援 | A.17.2.1 | 資訊設備之可用性 | N | C級單位不適用 |  |
| A.18遵循性 |
| A.18.1 | 對法律及契約要求事項之遵循 | A.18.1.1 | 適用之法規及契約的要求事項之識別 |  |  |  |
| A.18.1.2 | 智慧財產權 |  |  |  |
| A.18.1.3 | 紀錄之保護 |  |  |  |
| A.18.1.4 | 個人可識別資訊之隱私及保護 |  |  |  |
| A.18.1.5 | 密碼式控制措施(加密控制措施)的監管 | N | C級單位不適用 |  |
| A.18.2 | 資訊安全審查 | A.18.2.1 | 資訊安全之獨立審查 |  |  |  |
| A.18.2.2 | 安全政策及標準之遵循性 |  |  |  |
| A.18.2.3 | 技術遵循性審查 | N | C級單位不適用 |  |