# 紀錄編號： 填表日期：　　年　　月　　日

| 項次 | 量測項目 | 目標水準 | 量測方式 | 量測結果 | 差異說明 |
| --- | --- | --- | --- | --- | --- |
| A.5 | 資訊安全政策 | (1)資訊安全政策審查次數 | ≧1次/年 | 召開審查會議 | □　符合□不符合 |  |
| (2)資訊安全政策宣導次數 | ≧1次/年 | 會議、教育訓練 | □　符合□不符合 |  |
| A.6 | 資訊安全組織 | (1)有否確實簽署保密協議 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| (2)管理審查會議召開次數 | ≧1次/年 | 審查會議紀錄 | □　符合□不符合 |  |
| A.7 | 人力資源安全 | (1)檢查資通安全受訓時數 | 主　管≧3小時資訊人員≧6小時資安人員≧12小時一般人員≧3小時 | 教育訓練紀錄 | □　符合□不符合 |  |
| (2)離退人員帳號確實刪除 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| A.8 | 資產管理 | (1)資訊資產清單是否定期更新 | ≧1次/年 | 更新紀錄 | □　符合□不符合 |  |
| (2)資訊資產清單符合分級與標示規定 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| A.9 | 存取控制 | (1)定期審查重要系統存取權限（帳號清查） | ≧2次/年 | 清查紀錄 | □　符合□不符合 |  |
| (2)帳號申請是否依規定填寫表單 | 不符≦1件 | 稽核結果 | □　符合□不符合 |  |
| (3)系統稽核日誌是否已開啟 | 不符≦1件 | 稽核結果 | □　符合□不符合 |  |
| A.10 | 密碼學 | (1)管理者、使用者密碼長度及複雜度應符合規範 | 不符≦0件 | 稽核結果 | □　符合□不符合 |  |
| A.11 | 實體與環境安全 | (1)檢查有否遵守機房門禁規定 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| (2)檢查消防器材與UPS有否定期保養 | 不符≦1件 | 稽核結果 | □　符合□不符合 |  |
| A.12 | 運作安全 | (1)定期監控重要伺服器執行作業之系統容量（例如CPU、RAM、硬碟） | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| (2)病毒爆發次數（年） | ≦3次/年 | 事件紀錄 | □　符合□不符合 |  |
| (3)檢查病毒碼是否即時更新 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| (4)弱點掃瞄次數 | ≧1次/2年 | 掃瞄報告 | □　符合□不符合 |  |
| (5)定期備份重要系統資料 | 不符≦2件 | 稽核結果 |  |  |
| A.13 | 通訊安全 | (1)定期監控網路資源使用率（例如連外頻寬） | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| (2)連外網路斷線次數（年） | ≦3次/年 | 事件紀錄 | □　符合□不符合 |  |
| (3)檢查重要系統時間是否同步 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| (4)檢查防火牆設定是否與防火牆進出規則申請表資料相符 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| A.14 | 系統獲取、開發和維護 | (1)重要系統更新/上線前經測試 | 不符≦0件 | 稽核結果 | □　符合□不符合 |  |
| (2)重要系統開發或變更時應更新系統文件 | 不符≦2件 | 稽核結果 | □　符合□不符合 |  |
| A.15 | 供應者關係 | (1)合約書資通安全條款的訂定 | 不符≦1件 | 稽核結果 | □　符合□不符合 |  |
| A.16 | 資訊安全事故管理 | (1)發生資安事件未依規定通報之件數 | 不符≦1件 | 稽核結果 | □　符合□不符合 |  |
| (2)檢查資通安全事件通報單，是否重複發生相同資安事件件數 | 重複≦1件 | 通報單 | □　符合□不符合 |  |
| A.17 | 營運持續管理之資訊安全層面 | (1)業務永續運作計畫演練活動 | ≧1次/2年 |  | □　符合□不符合 |  |
| A.18 | 遵循性 | (1)合法軟體之安裝 | 不符≦0件 | 清查紀錄、稽核結果 | □　符合□不符合 |  |
| (2)矯正預防措施於規定時間內改善完成 | 逾期≦2件 | 稽核結果 | □　符合□不符合 |  |