

114年度資訊安全管理報告

本公司資訊安全之權責單位為資訊室，負責規劃、執行及推動資訊安全管理事項，隨時監控資安情況，並定期透過教育訓練提升員工的資訊安全意識。遇重大資安風險事件，及時向總經理報告。此外，公司每年由外部會計師派員進行資訊系統的定期查核，以確保資訊安全防護的完整性與有效性。

114年度執行情形如下：

一、 年度投入資訊安全費用相關共計約 226 萬元，細項如下：

| 內容 | 費用/年 | | | |
|--------|-------------|-------------|-------------|-------------|
| | 2022 | 2023 | 2024 | 2025 |
| 防毒軟體 | 113,333 | 113,333 | 103,333 | 103,333 |
| 郵件守門員 | 273,333 | 273,333 | 400,000 | 360,000 |
| 端點防護 | 810,000 | 810,000 | 800,000 | 780,000 |
| 多因子認證 | 150,000 | 150,000 | 150,000 | 136,666 |
| 安全威脅偵測 | 300,000 | 300,000 | 560,500 | 560,500 |
| 主機匿蹤 | | | | 325,000 |
| | \$1,646,666 | \$1,646,666 | \$2,013,833 | \$2,265,499 |

1. 防毒軟體：檢測並移除惡意軟體；透過網頁保護功能，提醒使用者避免進入有潛在危險的網站或下載可疑檔案。
2. 郵件守門員：阻擋垃圾郵件、郵件或附件中的病毒與惡意程式。
3. 端點防護：透過AI快速判斷事件，並自動執行隔離端點、封鎖惡意流量等動作，縮短事件處理時間。
4. 多因子認證：確保帳號安全，降低未經授權存取風險。
5. 安全威脅偵測：利用AI分析大量日誌與警示，過濾誤報，讓資安人員專注於高風險事件。
6. **主機匿蹤**：讓駭客難以判斷正確的攻擊目標，增加攻擊成本；與端點防護、安全威脅偵測結合，形成多層防禦。

二、 復原演練

完成年度資訊系統災難復原演練，培養災難應變能力，確保資訊系統持續營運不中斷。

| 系統名稱 | 負責人員 | MTPD | RPO | RTO | 衝擊說明 |
|--------------|------|----------|---------|--------|----------|
| | | 最大允許中斷時間 | 資料回復點目標 | 復原時間目標 | |
| ERP系統 | 葉庭彰 | 8 | 8 | 4 | 影響公司業務運作 |
| Vmware虛擬系統 | 葉庭彰 | 24 | 24 | 8 | 影響公司業務運作 |
| Exchange郵件系統 | 劉興弘 | 24 | 8 | 2 | 影響業務郵件收發 |
| 檔案伺服器 | 劉奕均 | 24 | 24 | 8 | 影響單位業務資料 |
| 電力系統 | 張誌袁 | 24 | N/A | N/A | 影響機房電力供應 |

三、 弱點補強

1. 委由協力廠商Team T5進行資安健診並依據建議完成修補。
2. 土耳其廠子公司進行弱點掃描，已完成修補並複查。

四、 教育訓練及認證

1. ISO 27001資訊安全管理系統(ISMS)改版，原2013改為2022。
2. 於本年度實施3次電子郵件社交工程演練，每次針對公司內2~300個使用者帳號進行模擬釣魚郵件測試，共713人次。針對未通過測試的員工，安排參與線上資安課程並完成相關測驗，以提升防範意識。
3. 本年度進行2次線上資訊安全教育訓練影片及測驗，共460人次。
4. 不定期資訊安全宣導，加強員工對於資訊安全風險之應變與警覺。

五、 今年2025/9/19(五)土耳其子公司遭受駭客攻擊，經啟動應變機制與隔離措施，成功阻止擴散，並於48小時內完成系統復原，無重大資料外洩或財務損失。

1. 受影響範圍：土耳其AD、備份主機。
2. 原因分析：疑似105廠無線網路管制有漏洞。
3. 改善措施：調整防火牆策略，加強資安宣導與社交工程演練。

115年度預計執行計畫：

1. 導入IIOT防護架構，預計100萬。
2. 因應越來越多的需求，需升級ERP主機，預計300萬。
3. 郵件主機改走0365方案。
4. 擴充端點防護與安全威脅偵測的AI偵測與事件回應能力，與協力廠商討論中。