建置資通安全風險管理架構：

1. 建置資通安全專責單位，配置主管 1 員；成員 1 員，共計 2 員專責人員。負責擬定資訊安全政策、實施，檢討調整現行資訊作業與資安政策。
2. 每月主管會議中報告資安政策與相關議題。

資安政策與具體作為：

1. 已加入 TWCert 聯防通報。
2. 制定『個人資料檔案安全維護計畫』公佈並實施。
3. 資訊安全管理系統(ISMS)擬定。
4. 每月至少一次全公司資安宣導。
5. 定期社交工程安全演練。
6. 定期災害復原演練。
7. 定期舉辦資安教育訓練課程。
8. 每月定時安全性修補，不定時資訊系統重大弱點修補。
9. 定時執行弱點掃描、滲透測試，並執行修補或虛擬修補。
10. 持續增強現有資訊安全系統韌性，佈建資安縱深防禦面向。建置高可用性網路防護系統，強化端點防護與資料洩漏偵測。
11. 定期資訊系統風險評估調整。
12. 落實資安人員持續教育訓練。

投入資通安全管理資源：

1. 設置資安專責人員 2 員。
2. 投入資安相關系統建置約 200 萬。
    - 防毒軟體。
    - 端點防護、資產管理、資料洩漏防護。
    - 設備存取控制系統(認證、授權、紀錄)。
3. 投入資安硬體升級約 100 萬。
    - 高可用性防火牆、IPS、WAF。
4. 資安人員持續教育訓練課程，課程總時數達 18 小時，完訓後測驗及格率皆為 100%。