資通安全管理

1、資通安全風險管理架構

由資訊管理處負責統籌全公司資訊安全及相關事宜，並定期進行內部資訊安全檢查。

管理架構：

(1)資訊安全之權責單位為資訊管理處，本處設置資訊主管乙名，與專業資訊人員二名，負責訂定內部資訊安全政策、規劃暨執行資訊安全作業與資安政策推動與落實。

(2)本公司稽核室為資訊安全監理之督導單位，該室設置稽核主管乙名，負責督導內部資安執行狀況，若有查核發現缺失，即要求受稽查單位提出相關改善計畫與具體作為，且定期追蹤改善成效，以降低內部資安風險。

2、資通安全政策

(1)目的：

為有效管理公司內部電腦及網路運作環境，提高軟硬體使用效率及其檔案文件之安全，維持業務持續運作，降低資訊作業風險，保障資訊服務使用者之權益，建立資訊安全管理系統，規範本程序為最高指導方針，以達成資訊安全管理的目標。

(2)範圍：

本公司資訊安全管理範圍，包括本公司所屬各據點資訊作業之相關人員、管理制度、應用程式、資料、文件、媒體儲存、硬體設備及網路設施。

(3)目標：

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞，或當已遭受不當使用、蓄意破壞等緊急事故時，公司能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之經濟損害及營運中斷。

(4)程序：

執行資訊機房、網路安全、ERP 程式修改、資料安全、資訊保密、智慧財產權、資訊委外等管理。

(5)資通安全稽核管理實施：

資訊安全政策訂定、資訊安全組織與權責、人員安全與管理、資產分類與控管、實體及環境安全管理、通訊與操作管理、存取控制管理、系統開發與維護管理、永續運作管理、內部稽核及其他。

(6)資通安全稽核依稽核項目：

資通安全稽核依稽核項目逐項檢查，並得調閱有關資料、實地測試或檢查資訊軟、硬體設備使用情形，受稽核部門及人員應配合提供必要之說明及文件資料。稽核人員對稽核之文件應予保密。

3、具體管理方案及投入資通安全管理之資源

防火牆防護、防毒軟體、內外網管制、檔案存取管制、郵件安全管控、網站防護機制、資料備份機制、異地備份存放、檢修紀錄、資通安全宣導、作業系統更新、定期實施資訊安全稽核，落實資訊安全管理政策，確保資訊資料、系統、設備及網路安全。本公司資訊及資安人員共五名，每週固定召開會議討論管理資通安全，113 年編列 200 餘萬元用於設備更新、維護、弱掃等服務，降低資安風險。