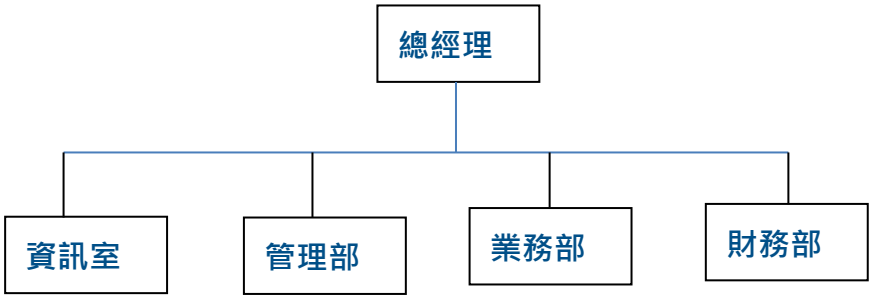
資安風險管理

資訊安全組織架構

本公司資訊安全之權責單位為資訊室，該單位設置資訊主管乙名及資訊安全人員一名，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及委外公司與同仁間之溝通協調，並定期向董事會報告公司資安治理概況。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，若有查核後發現缺失，旋即要求受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。



資訊安全政策

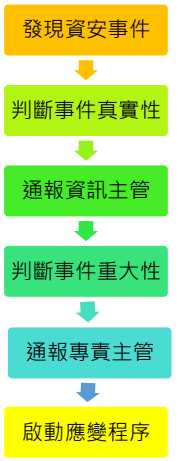
(一)制度規範：訂定公司資訊安全管理制度，規範人員作業行為。
(二)科技運用：建置資訊安全管理設備，落實資安管理措施。
(三)人員訓練：進行資訊安全教育訓練，提升全體同仁資安意識。

資訊安全具體管理方案

當資訊系統遭受來自內、外部人員不當使用或蓄意破壞，依下列程序進行障礙排除

1.由資訊室主管召集會議，由各相關部門主管參加
2.技術性相關事宜由資訊室資訊人員提出解決方案與後續預防改善措施
3.並由稽核室定期進行內部稽核。

資訊系統遭受外部侵害之應變流程



針對外在與內在的風險管理

(1)各級人員公務接觸任何公司資料都必需遵守保密規定，不得洩露資料給他人。
(2)若因公務所需資料涉及他人個資或機密資料，必須經由權責主管同意才能提供。
(3)重要文件與合約須妥善保管，若有文件要傳遞資料夾封口須緊閉，
避免未經授權人員取得查看。
(4)電腦密碼須每半年更換一次，禁止使用相同的密碼，避免張貼密碼在容易洩漏的地方。
(5)若離開座位達五分鐘以上，須將電腦帳號鎖定或登出，避免電腦讓他人自行操作。
(6)電腦禁止安裝非授權軟體，若涉及任何法律行為須由該電腦使用者自行負責。
(7)來路不明的軟體、檔案與網站常為散播病毒的來源，為確保電腦使用安全，不得安裝及使用。
(8)電腦系統及資料安全須由使用者自我管理與維護，若有任何系統中毒或異常情況，應須立即告知資訊室人員處理。
(9)各項資料應定期備份存放，避免因設備故障或人為因素造成的資料損毀影響業務。
(10)下班時，重要文件妥善保管，並關閉不須使用之電腦系統暨其週邊設備。

投入資通安全管理之資源

資訊安全已為公司營運重要議題，對應資安管理事項及投入之資源方案如下：

- 專責人力：設有專職之「資訊室」，負責公司資訊安全規劃事項，以維護及持續強化資訊安全。
- 客戶滿意：無重大資安事件，也未有接獲侵犯客戶隱私或遺失客戶資料的投訴。
- 投入資源：2025 年度共執行二次主機弱點掃瞄測試。

  2025 年 12 月委託中華資安國際公司利用系統自動化工具，結合其之專業知識、資訊安全技術，對於本公司內部伺服器主機進行弱點掃描，並提供專屬測試報告及系統補強建議。本次作業針對本公司使用之 ERP 系統進行弱點掃描，並將測試結果提供給相關單位參考，並提出個別修補建議。
- 教育訓練：2025 年度針對一般員工，透過線上課程，共完成 10 人次/小時的資訊安全訓練課程，主要的課程內容為個人隱私資訊概念、網路攻擊威脅、個人隱私資訊保護應有之認知等。