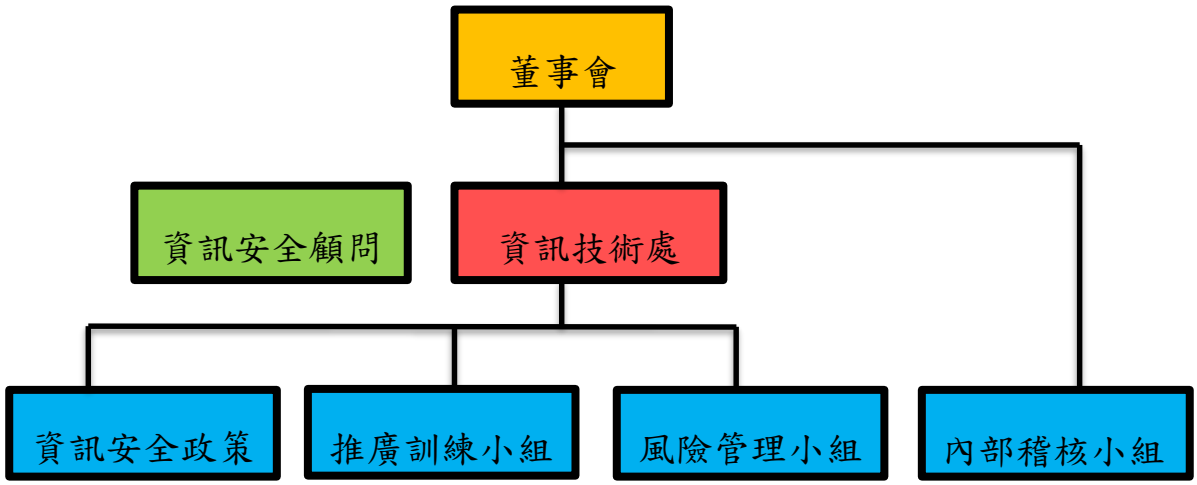
資安風險管理

有鑑於資訊安全風險逐年高升，網路攻擊不僅可能使公司暴露於資料外洩及勒索風險外，更可能面臨生產系統中斷而造成嚴重營運損失，影響企業的優良商譽。為保護資訊免受多種威脅的攻擊及確保公司營運可持續運作，將損失降至最低，故公司積極建立系統化管理資訊風險。

資安風險管理架構

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊安全委員會，並每年向董事會報告資訊安全政策執行情形。委員會由資訊技術處處長為召集人，組織團隊包含風險管理小組 1 人、推廣訓練小組 1 人與內部稽核小組 1 人；風險管理小組執行資訊安全系統建置，包含網路管理與系統管理；推廣訓練小組負責宣導資訊安全訊息，提升員工資安意識；內部稽核小組由稽核室每年就內部控制制度，進行資訊安全查核，評估公司資訊作業內部控制之有效性。



資訊安全政策

為落實資安管理，公司訂有內部控制制度—電腦化資訊處理循環、電腦資訊處理作業辦法及電腦資料與網路管理程序，期望達成下列政策目標：

- 確認資訊資產的所有權與控制皆有適當的管理。
- 確保依據部門職能規範資料存取。
- 監控、紀錄與調查資訊安全事件，以確保資訊系統之持續運作。
- 定期辦理資訊安全教育訓練及宣導，以提高員工資訊安全意識，並遵守資訊安全規定。
- 定期執行資安稽核作業，確保資訊安全落實執行。

資通安全管理

項目	具體管理措施
網路安全管理	● 防火牆，掌握網路流量且加以控制，自動過濾上網可能連結到有木馬病毒或惡意程式的網站。 ● 未經核准禁止使用即時通訊軟體、Web Mail、雲端硬碟空間、FTP 檔案傳輸等網路服務。
機房安全管控	● 機房進出有門禁系統，非經許可不得進入。 ● 每日執行機房環境監測，注意機房溫度及空調設備等之運轉狀況。 ● 不斷電系統，保護伺服器系統不因停電而故障。
防毒軟體	● 定時更新防毒軟體病毒碼，降低中毒風險。
存取控管	● 依據職能分別賦予不同存取權限。 ● 調離人員取消原有權限。 ● 遠端登入管理資訊系統應經適當之核准。
郵件安全管控	● 有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 ● 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。 ● 辦理社交工程模擬演練及教育訓練
資料備份機制	● 重要資訊系統資料庫建立系統備份機制，落實異地備份。 ● 辦理災難復原演練

112 年度投入及執行成果

本年度於董事會報告(共 1 次)資通安全管理現況及執行情形

- 進行社交工程演練，對全體員工進行社交工程演練之釣魚信件的點擊率由 111 年之 17%，112 年降低至 2%。
- 辦理災難復原演練，112 年 RD 伺服器故障排除及復原之時數相較 111 年縮短 21%。
- 現有資安防護方式(電腦 PC、網路連線、郵件收發、遠端連線及裝置管理)