羅昇企業股份有限公司
資訊安全管理運作情形

資通安全風險管理架構

本公司在資訊安全管控方面訂有「資訊安全政策」並將資訊安全檢查納入每年年度稽核項目中，本公司資訊部成員共4人，設有資安專責主管及資安專責人員各1人，資訊部負責主導及規劃並制訂資訊安全管理政策，各相關單位配合執行，以確認資訊安全管理運作正常並定期檢討修正。

資安專責單位於每季召開會議討論及檢討資安風險評估及預計改善方式，2023年度共計召開4次會議。並於2023/10/31 於董事會報告當年度資訊安全管理執行狀況。

資通安全政策

確保資訊資產(與資訊處理相關之硬體、軟體、資料、文件等)之機密性避免遭受內、外部蓄意或意外之威脅，以保障員工，供應商和客戶間之隱私權保護。

具體管理方案

(1)重要資訊系統或設備應建置適當之備援維持可用性。

(2)員工個人電腦安裝防毒軟體且定期確認病毒碼更新，並禁止使用未經授權軟體。

(3)員工帳號、密碼與權限應善盡保管與使用責任並定期更換。

(4)模擬各種資安攻擊事件並安排相關人員參與演練，確保事件發生時能啟動緊急流程，減少公司的損失。

投入資通安全管理之資源

(1)建置次世代防火牆以智慧型防護機制主動偵測各種網路與應用層攻擊並具備一般防火牆被動黑白名單防護/流量管控/即時監控等傳統功能。

(2)目前郵件系統為Microsoft Exchange On Line，採用微軟系統既有的防護政策並可自行訂定黑白名單及相關郵件策略，有效避免員工誤開惡意郵件。

(3)安裝企業防毒軟體並開啟系統的自動更新來防堵漏洞被外部攻擊，此外，重要檔案及內部主機及區域皆進行權限控管，避免被惡意程式操控危害重要的主機及竄改重要的檔案。

(4)遇到重大危害及毀損，可以藉由異地備援檔案，伺服器端可以最快的速度讓服務上線及營運，而使用者端加強宣導資安意識，建議個人日常要備份重要資料及檔案，以利遭遇系統毀損時可以快速復原使用。