資通安全管理

■ 資通安全風險管理架構

(1)公司於 112 年 12 月 4 日設置資訊安全長，由總經理室陳榮貴協理擔任。資訊安全由資訊部門負責推動管理相關事項之計畫、執行、稽核與溝通協調，並辦理相關之教育訓練及宣導，以確保人員熟悉業務執行所負之安全責任，並定期檢討資安政策，且每年一次向董事會彙報資安治理議題

(2)民國 114 年資通安全報告:本公司資訊安全長已於 114 年 11 月 07 日向董事會報告 114 年資通安全執行狀況。

■ 資通安全政策

(1) 文件資安政策：

透過文件加密系統，提供外發文件給供應商時進行加密，限制開檔次數、列印、修改及文件有效期限。

(2) 主機資安政策：

A. 主機定期備份及檔案異地備份。

B. 主機定期自動更新病毒碼及自動掃描防制病毒。

C. 主機定期自動更新作業系統修補(Patch)。

(3) 上網資安政策：

A. 所有外部電腦及資訊設備，需經資訊單位審核方能連接內部網路。

B. 導入惡意網站及廣告阻擋系統，對可疑網站進行封鎖限制。

C. 防火牆僅開放特定網路埠號，提供特定的服務使用。

(4) 用戶端資安政策：

A. 電腦自動更新修補程式至最新版及系統定期強制更新。

B. 用戶限制自行安裝軟體，需透過資訊部門審核軟體後安裝。

C. 外點設計人員導入終端作業雲桌面，相關工程資料都存放於機房內。

■ 網路安全風險管理具體方案

(1) 透過防火牆進行內外網路區隔，內部透過虛擬網路區隔各單位。

(2) 導入入侵防禦系統，並定期向管理階層提報資安報告。

(3) 定期對同仁宣導資安認知及教育訓練，並搭配每年內部定期稽核資訊安全政策及風險評估。

■ **投入資通安全管理之資源**

(1) 企業容災管理：定期依據系統備份週期進行本機備份、異機備份、異地備份，每年進行主機備份檔案還原演練與資料驗證。

(2) 加入 TWCERT/CC 台灣資安聯盟，提升公司資安情資分析與獲取強化資安韌性。

(3) 本公司於 112 年 11 月上市，遂於同年 12 月設置「資訊安全專責單位」由資訊部門擔任，負責規劃、監控及執行資訊安全管理作業，該單位由資訊安全長陳榮貴協理綜理資訊安全政策推動及資源調度事務，並配置 1 名資訊安全主管及 2 名資訊安全人員以推動資通安全策略。

(4) 每月向管理高層報告資訊安全實施情形，進行相關資安風險評估識別及緩解潛在的安全威脅。

(5) 本公司已定期辦理社交工程演練，藉由模擬釣魚郵件與社交詐騙情境，提升員工對駭客攻擊手法之辨識能力與資安意識，強化人員防護層面的資安防線。

(6) SecurityScorecard 評鑑獲得外部防禦能力 90 分以上，相關評鑑結果由資訊部定期追蹤並檢視，作為後續資安持續改善之依據。

(7) 預計 2025 年第 4 季開始導入 ISO27001，確保公司資訊資產的機密性、完整性與可用性，提升整體資訊安全成熟度。

(8) 預計 2025 年底前成立 ERC 組織，以提升公司面對資安威脅與突發事件的應變能力與持續營運韌性。