資訊安全風險管理

資安風險管理架構

本公司於 2023 年 3 月 16 日申報設置資訊安全主管及一位資訊安全人員，負責推動、協調、監督本公司資安管理事項；並每年定期於董事會彙報資安管理成效資安相關議題及方向；由稽核室每年就內部控制制度 - 資訊循環，進行資安查核，評估公司資訊作業內部控制之有效性。

資安政策

為落實資安管理，並依據公開發行公司建立內部控制制度處理準則第 8 條、第 9 條規範應訂定個人資料保護之管理及電腦化資訊系統相關控制作業，本公司業已訂定資訊循環及其他管理環境（含資通安全檢查及電腦處理個人資料保護控制作業）之內部控制制度與相關作業規範，並於 2023 年 3 月 16 日頒布「資通安全管理政策聲明」，據以執行資安工作，嚴格管理資料之利用與安全維護，建置防火牆及設定使用者權限，以降低公司資安風險。

具體管理方法

網際網路資安管控	資料存取管控	應變復原機制	宣導及檢核
• 架設 VPN 伺服器	• 電腦設備應有專人保管，並設定帳號與密碼	• 定期檢視緊急應變計畫	• 隨時宣導資安全資訊，提升員工資安意識
• 架設防火牆	• 依據職能分別賦予不同存取權限	• 每年定期演練系統復原	• 每年定期執行資通安全檢查，由稽核室查核
• 定期對電腦系統及資料儲存媒體進行病毒掃瞄	• 調離人員取消原有權限	• 建立系統備份機制，落實異地備份	
• 各項網路服務之使用應依據資安政策執行	• 設備報廢前應先將機密性、敏感性資料及版權軟體移除或物理性破壞	• 定期檢討電腦網路安全控制措施	
• 定期覆核各項網路服務項目之系統日誌，追蹤異常之情形	• 遠端登入管理資訊系統應經核准		

2023 年執行狀況:

- 2023/9 執行網路安全意識宣導作業

- 本公司目前無重大資安事件導致營業損害之情事。

  持續落實資安管理政策目標，並定期實施復原計畫演練，保護公司重要系統與資料安全。
- 已於 2023/11/08 向董事會報告資安風險情形。