資通安全風險管理架構

本公司於2023年3月15日經董事會通過委任自4月1日起，由吳文哲經理擔任本公司資安長，並已成立資安專責單位負責資安相關工作。

資訊安全政策揭露

本公司資安的管理透過專門的資安管理平台及團隊，讓本公司及子公司能以最佳方式運用資源、適度及適性集中管理、升級及更新既有之資安網路設備與機制，使資訊安全防護與時俱進。

資訊安全政策

本公司資訊安全政策聚焦於科技運用與資安治理，透過人與機器、軟體與硬體之交互配合與制衡，建構資安管理網絡，透過這些網絡落實執行法規及政策。

具體管理方案

- 防火牆設置：
    1. 「資料存取」:「人員」、「事件」、「時間」、「如何執行」、「來源地目的地」與「存取物件」進行有效安全管控。
    2. 「威脅檢測」: 入侵檢測與防禦、病毒、蠕蟲等得到有效控管。
    3. 「軌跡紀錄」: 包含誰，到哪裡，存取了資料。
- 資訊機房管理：
    1. 「一級資訊機房」: 落實執行實體及環境安全之各項標準。
    2. 「不斷電UPS系統」: 避免因電源失效而導致設備毀損、資料遺失及服務中斷。
    3. 「空調冷卻系統」: 滿足電腦高密度機櫃的散熱需求。
    4. 「火災偵測及自動滅火消防系統」: 符合相關消防法規並定期維護。
    5. 「門禁管制」: 實體硬體設施均建置，防止重要資訊硬體設備損毀與破壞。
    6. 「錄影監控」: 24小時運作，避免未經授權之出入，落實資料資產安全維護。
- 異地備援: 機房設施及備份媒體。
- 使用者資安管理：
    1. 個人電腦權限設定。

2. 電腦系統安全性定時更新。
3. 郵件防護。
4. 企業端點防毒。
5. 端點偵防安全。
6. 外部網路存取。
7. 內部系統管控。
8. 「集團電子化文件線上控管作業」政策及機制。
9. 「資訊安全管理規範」

- 災難演練: 資安管理單位每年不定時進行，確保復原計劃可正常運作，提升資安緊急應變功能與復原能力。
- 廠區資安管理：
    1. 定期研討: 與各廠資安管理同仁討論每年廠區資訊安全之問題、趨勢及相關強化措施。
    2. 教育訓練: 優化各廠同仁有關資訊安全環境維護及提升風險意識水準。
- 教育訓練：說明資安犯罪手法與須注意事項，主動提高員工資安知識，提升同仁資安意識
    1. 寄發資安宣導信件
    2. 實體資安課程講座。

未來重點

- 強化企業網路安全防護。
- 提高同仁資訊安全風險意識。
- 遵循政府資安政策法規及公司相應之內規。
- 落實日常資安管理工作。

量化數據

- 每月一次召開資安月會，檢討及追蹤資安相關工作。
- 每年至少委外資安專業廠商進行一次資安健檢及一次弱點掃描等重要資安工作。
- 申請加入「台灣資安聯盟(TWCERT)」。
- 每月發佈「資訊安全月報」及每半年實施一次資安社交工程演練，強化資安意識，防範資安風險.。
- 2023年資安專責人員完成12小時以上資安專業課程；使用資訊系統之一般員工完成2小時資安通識課程。
- 2023/9月取得政府認可之資通安全專業證照1張。