資通安全管理運作情形(2023 年)

- **資通安全風險管理架構：**

本公司設置 IT 處負責公司資訊發展策略、資訊安全政策以及資訊系統之管理與改善，並由稽核人員定期執行資訊安全稽核作業，檢視存取權限及資訊安全管理制度之落實情形，以確保資訊系統及業務維持運作正常。並於 2022 年設置資通安全專責單位，持續強化資安防護能力，降低資通安全風險。

- **資通安全政策：**

為落實資通安全管理，本公司訂有”電腦化資訊處理控制制度”、”對外指定網站電子資訊存取系統使用規則”及”網域帳號、email 帳號及 MIS/PIS 帳號管理規定”等資訊安全規章，嚴格控管資訊資產之機密性/完整性、網際網路管控、及防止未經授權之資料修改或系統存取等，確保公司資通安全。

- **具體管理方案及投入資通安全管理之資源：**

(1)網際網路資安管控：IT 部門即時監控網路狀態、防止未經授權之存取，且定期檢視及評估網際網路可能之安全性弱點，以採取防護措施。

(2)資料存取管控：系統密碼定期更新、存取權限管控、列印輸出資料管制、資訊設備進出管制、禁止使用 USB 儲存裝置等。

(3)新進員工入職時皆需先進行電子郵件及資訊系統相關基本訓練後始核發帳號，以確保資通安全觀念融入日常作業中。

(4)於 2020 年委任外部專業機構執行資訊安全健檢及成熟度評估並向董事會報告。

(5) 2022 年設置資安長及資安專責單位。

- **2023 年資通安全管理執行情形**

(1) 加入指派資訊安全人員至中國、越南、印度與印尼地區工廠進行實地稽查。除確保資訊作業之合規性，也教導工廠 IT 人員日常檢查的重點，宣導「說、寫、做一致」與「持續改善」之資安精神，持續強化集團 IT 人員於資訊安全之專業性與能力。

(2) 集團總部增加培訓 1 名專責人員取得 ISO27001 資安稽核員認證，共參與 4 次外部資安教育訓練/研討會，並對集團 IT 部門人員加強資安教育訓練，提升人員資安職能。

(3) 定期更新「資安宣導專區」，發佈 52 則資安新聞、14 則釣魚郵件案例與 10 則宣導影片，以提升員工於資訊安全之意識。

(4) 第二季開始執行釣魚郵件測試，隨機寄送超過 2,600 封釣魚郵件給集團總部員工，共 1,557 人 參與，約 96% 之同仁通過測試。且未通過之同仁須接受額外教育訓練並通過測驗，以確保提升其資安意識。

(5) 持續更新外部資安威脅情資，追蹤集團 IT 人員及時修補具威脅之弱點。

(6) 每季執行集團伺服器與系統弱點掃描，追蹤修補 89 個中、高風險弱點，以確保系統安全性。
(7) 追蹤集團電腦皆安裝防毒軟體與病毒碼更新，以降低攻擊風險。
(8) 不定期稽查集團電腦軟體盤點清冊，確保軟體使用之合規性與安全性。
(9) 不定期稽查電腦帳號權限設置，避免權限不當使用風險。
(10) 定期稽查電腦化資訊處理控制制度與資訊安全維護作業落實執行,以防止未經授權的資料存取。