資通安全管理運作情形(2024 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、資通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。

- **2024 年資通安全管理執行情形：**

(1)集團進一步強化供應鏈風險、軟硬體設備、數位資料存取、電腦機房、帳號與網路權限的管理，並修訂相關管理制度，以落實資訊安全「最小權限」與「僅知」原則。

(2)集團定期進行資訊安全稽查，並向工廠 IT 人員宣導日常檢查的重點，培養「說、寫、做一致」與「持續改善」的資安精神。同時，集團致力於提升 IT 人員的專業能力，嚴格遵循法規要求，並於越南區增設資安主管加強管控，確保資訊資產的機密性、完整性與可用性，並以達成零資安事件為目標。

(3)集團總部 2 名資安人員均取得 ISO27001 資安稽核員認證，共參與 5 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。

(4)定期更新「資安宣導專區」，發佈 113 則外部資安情資與資安新聞、14 則釣魚郵件案例與資安小百科，以提升員工於資訊安全之意識。

(5)對全集團員工執行電子郵件社交工程演練，2024 年度隨機寄送 7,305 封釣魚測試郵件，約 96% 的員工通過測試，對於未通過之同仁加強宣導，以確保提升其資安意識.

(6)導入特權帳號管理系統，管控高權限帳號與留存使用軌跡，防止越權操作。
(7)強化供應商設備的掃毒與資安檢查規定，防範設備中毒或版權誤用，降低供應鏈資安風險。
(8)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。
(9)每季執行集團伺服器與系統弱點掃描，共修補 761 個高、中風險弱點，以確保系統安全性。
(10)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。
(11)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。
(12)不定期稽查電腦帳號權限設置，避免權限不當使用風險。
(13)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。