

本公司『資訊安全風險管理委員會』由總經理擔任召集人，負責審視各業務單位之資訊安全政策之治理、規劃、督導及執行情形，以建構資訊安全防衛能力及同仁良好資訊安全意識，並於112年11月設置1名資安專責主管及1名資安專責人員。資訊安全主管每年定期向董事會報告。

【資安治理】：

- 確保資訊系統之可用性、抵抗外部威脅並落實權限及存取控管。

【具體管理措施】：

- 確保系統可用性
 - 集團總部及各分點建置4G 備援線路，確保系統可用性並降低營運中斷風險。
 - 資料異地備援系統，確保資訊復原及減少損害。
 - 定期災害復原演練。
- 抵抗外部威脅
 - 偵測病毒及惡意攻擊程式。
 - 系統主機定期檢測及更新。
 - 防護並過濾可疑及垃圾郵件。
 - 電信線路入侵防護及阻擋。
- 權限及存取控管
 - 營運系統權限管理。
 - 檔案存取權限控管。

【112 年度執行情形】：

- 總公司設置1名資安專責主管及1名資安專責人員。
- 本年度集團重要營運主機及系統持續於遠傳IDC機房（7級耐震並通過ISO 27001資訊安全管理認證）穩定運作。
- 本年度完成建置各營運分點與IDC機房之4G 備援線路（MDVPN），有效提昇線路及系統之可用性與穩定性，並大幅降低營運分點因線路故障導致之作業中斷風險。
- 本年度完成集團各點終端設備及老舊作業系統汰換逾150台。
- 本年度完成德安資料庫（Oracle）及老舊作業系統（Windows 2003）升級汰換，升級為Oracle 19C及Windows 2022。
- 本年度即時監控系統（PRTG），持續穩定運作，並提供主機及線路即時健康狀況回報。
- IDC 機房防火牆（FortiGuard）升級資安入侵防護IPS及ATP服務。
- 資安端點防護系統（WithSecure）提供各終端設備病毒偵測保護及每週防護報告。
- 集團各分點行政上網採用中華電信企業防駭及IPS入侵防護服務，以協助阻絕來自於網際網路的病毒、蠕蟲及駭客入侵攻擊，並提供每週線路入侵防護及阻擋報告。
- 每日重要資料庫系統異地備份。

- 本年度執行4次主機作業系統更新。
- 本年度執行1次營運系統升級作業。
- 本年度執行1次營運系統帳號清查作業。
- 本年度執行1次災害復原演練。