資訊安全

資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源：

1. 資通安全風險管理架構

   本公司由資訊室專責擬定年度資訊安全策略，整合及執行年度資訊安全計畫，不定期針對資訊安全相關議題向總經理討論彙報，落實資訊安全管理措施的有效性。

2. 資通安全政策

   針對資訊系統，由外部顧問協助，確認資訊作業流程符合產業標準及營運實際需要，並取得正式合規認證。

3. 具體管理方案

   3.1 採用專業軟體，定期進行內外部弱點掃描及滲透測試，針對掃描出的弱點以最快的速度進行更新，避免產生危害資訊安全事件。

   3.2 公司加入 TWCERT/CSIRT 資安聯盟(台灣電腦網路危機處理暨協調中心)，與聯盟成員共享資安相關訊息及最新消息，提升國家整體資安聯防能量，共同維護臺灣整體網路安全。

   3.3 建立自動化監控系統，隨時記錄系統運行狀態，並收集相關紀錄，有異常發生時會即時發出告警給相關人員，並視事態嚴重情形呈報至總經理(含)以下層級，確保系統發生狀況時能有最迅速的處理。

   3.4 與外界網路連接時，系統設置防火牆及防毒軟體，以加強資訊管理系統安全。

   3.5 加強宣導避免員工收發或下載與業務無關之郵件或軟體,杜絕電腦病毒感染機會。

   3.6 非經權責主管授權，禁止將公司相關資訊經由電子郵件對外傳送。

   3.7 重要之軟體或檔案加密處理，並定期更新密碼，以避免遭挪用或剽竊。

   3.8 員工如需要裝置其他網路服務應提出申請,呈權責主管核准並經 MIS 評估後始可安裝開放。

   3.9 定期更新偵測防毒軟體版本之防毒軟體,並訓練所有人員開啟防毒軟體及實戶功能，監控掃描所有進出電腦之資料檔案。

4. 投入資通安全管理之資源

   不定期進行資訊安全宣導，並進行相關測驗，確保同仁能隨時保有資安意識與相關知識。112年度透過趨勢科技股份有限公司資訊安全工程師進行公司內部弱點掃描，花費金額5萬元(未稅)，目前設置資安主管及資安人員各1名，並已編列民國113年適當預算強化資訊技術及安全防護。