資訊安全風險管理

為保護公司核心業務相關資訊資產之安全，確保業務資訊依規定正當使用、保存與管理，防範因人為疏失或蓄意破壞而對公司營運造成影響及財務損失，本公司已制定「資訊安全政策」，並要求全體員工遵循。此外，公司亦不定期舉行資訊安全宣導活動，以提升員工對資訊安全風險的認識及防護意識。

資訊安全風險管理架構

本公司資安管理權責單位為行政部資訊組，設有專業資訊主管及 1 名專業資訊人員，負責制定企業內部資訊安全政策，規劃與執行資訊安全防護措施，並推動資安相關政策，確保企業資訊系統之有效運作。

同時，本公司稽核室為資訊安全之查核單位，負責檢視公司內部資安執行狀況。如經查核發現缺失，稽核室將要求資訊組提出具體改善計畫及可行之措施，以有效降低內部資訊安全風險，同時提升資安管理效能。

本公司採用循環式管理與定期稽核之組織運作模式，確保持續強化資訊系統之安全管理，實現穩健可靠之營運目標。

具體管理方案

- **訂定資訊安全作業與制度規範**
  訂定各類資訊作業與資安系統制度辦法，以規範本公司人員資訊安全行為並檢視相關系統 與制度是否符合營運資安之需求並適時調整，積極宣導資訊安全相關應用與規範，藉以提昇公司同仁資訊安全知識。

- **新式技術與防護系統建置**
  依據營運需求引進新式技術，佈建監控設備與防護系統，實施異地備援(備份)機制，提昇整體資訊環境之安全性，降低各項風險發生率，以保障客戶、合作夥伴、利害關係人之利益。

- **落實資訊安全與個人資訊保護**
  依據《個人資料保護法》，以及本公司《資通安全管理作業規範》、《資訊系統管理作業辦法》等相關規定，審慎處理並保護個人資訊及相關系統之安全。落實資訊安全稽核，確保各項資安政策之遵循，以利資安管理制度有效執行與持續運作。

投入資源

本公司為有效防範各種內部及外部資安威脅，除採用多層式網路架構設計外，積極建置多項資安防護系統，以全面提升整體資訊環境之安全性。114 年度針對個資系統防護之資安設備投入金額為新台幣 260,000 元。現有之資安防護資源與控管系統包括：

- 網路防火牆
- 核心網路堆疊交換器
- 網路入侵偵測防護系統
- 電子郵件閘道防護系統
- 電腦病毒防護軟體
- 企業網域控制系統

重大資訊安全事件因應措施及日常防護

重大資訊安全事件因應措施

- 資安事件之損害控制與通報作業。
- 資安事件所造成損害之復原作業。
- 資安事件相關檢視及其他調查作業。
- 資安事件後續發展及與其他事件關聯性之檢測作業。
- 其他資通安全事件應變之相關事項。

日常防護

- 加強宣導與教育訓練，提高同仁資安風險意識。
- 依現況調整網路資安防護等級與添購設備。

114 年度執行情形

- 管理與決策：召開 8 次資安工作會議，追蹤個資改善進度與策略調整。
- 意識培育：辦理 3 場員工資安教育訓練(宣導)，有效提升同仁對個資保護與風險辨識之能力。
- 外部協作：正式加入「台灣電腦網路危機處理暨協調中心(TWCERT/CC)」，藉由外部情資共享，全面強化預警、通報及應援能量。