資通安全

本公司於民國（下同）112 年 8 月 11 日董事會決議並公告設置一位資訊安全長及一位資安專責人員，負責推動、協調、監督本公司資通安全管理事項。
資訊安全執行成果已於 114 年 3 月 13 日董事會報告。

一、 資訊安全政策

1. 建立安全可信賴之資訊作業環境，確保公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。維持公司業務營運穩定，避免因系統中斷或資安事件造成營運損失。
2. 確保公司資訊之機密性、完整性與可用性。
   . 機密性：確保被授權之人員才可使用資訊。
   . 完整性：確保使用之資訊正確無誤、未遭竄改。
   . 可用性：確保被授權之人員能取得所需資訊。

二、 資訊安全管理架構

1. 資訊安全之目標:
   建立安全及可信賴之電腦化作業環境，確保公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。
2. 資訊安全管理辦法
   為強化公司內部資訊安全管理，即確保資訊的機密性、完整性與可用性，以及網路安全，訂定「電腦作業管理辦法」, 規範資訊資料之安全維護。對於各類機敏性資料的存取、產出、使用、保存等訂定管理制度，並規範員工執行業務使 用電腦資訊系統時須遵守之各項資訊安全行為。保護資訊資產免遭不當使用、洩漏、竄改、破壞等情事，確保資訊蒐集、處理、傳送、儲存及流通之安全。
3. 資訊安全之範圍
   (1)人員管理及資訊安全資訊宣導。
   (2)電腦系統安全管理。
   (3)網路安全管理。
   (4)郵件資料安全管理。
   (5)系統存取管制。
   (6)系統發展及維護安全管理。
   (7)實體及環境安全管理。
   (8)資訊安全稽核。

三、 資訊安全管理方案

1. 資訊安全具體方案
   (1)建立防火牆設定連線規則。
   (2)使用防毒軟體，降低病毒感染機會。

(3)郵件安全管控，防範不安全的郵件及垃圾郵件。

(4)資料備份:每日備份資料並異地儲存保障資料安全。

(5)資料復原:每年至少一次資料復原演練，以確保備援程序與資料有效性，以預防災難發生的風險，確保資訊系統能順利銜接。

2. 資訊安全稽核檢討

(1) 本公司每年有外部單位與內部稽核單位各執行乙次「資訊安全查核」及兩次「資訊系統內部控制自我評量」。

(2) 不定期於管理會議中提出檢討報告有關內部資訊應用系統、辦公室自動化、網路資訊及資訊安全防護措施等，提供營運、管理及決策有關工具，以降低資訊安全暨效益風險管理。

四、 投入資通安全管理之資源

.資通安全設備有防火牆、郵件防毒、垃圾郵件過濾等。

.每日由專責人員監控系統，預防駭客侵入及竊取公司資料。

.為強化資訊安全機制及與產業界資安情資交流，本公司於 114 年 3 月加入台灣電腦網路危機處理暨協調中心(TWCERT/CC)，以即時取得最新的資安威脅情資和防護資訊，並能立即採取行動來防禦資安攻擊。

.不定期針對各項資訊安全認知進行公告及宣導，提升員工資安意識。
114 年執行情形：資訊安全教育宣導共 12 次。

.不定期舉辦資通安全相關課程，提升員工資安認知。
114 年執行情形：資安人員培訓，共計 21 人次 50 小時。

.114 年啟動更新網路設備及優化電子郵件系統，加強網路安全防護。
預計於 115 年初完成系統及設備更新。