資通安全政策

為防止本公司資通訊系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性、完整性及可用性，制訂資通安全作業規範等內部規章及資訊安全管理目標以資遵循。本公司預計導入 ISO 27001 資訊安全管理系統標準，讓資訊安全管理達到最大效益，在所有可能的風險內做好預先的規劃與防範，確保資訊安全與穩定性，同時減少資安運行過程的疏漏點，讓本公司營運不中斷，達到經營永續目標。

資通安全風險管理架構

鑒於近年來資通安全危害事件頻傳，為確保本公司資料、設備及資訊系統之安全，保障本公司及利害關係人權益，本公司於推動永續發展架構中，設有資通安全管理小組，為負責本公司資通安全之權責單位，統籌資訊安全事件管理、制定資通安全政策、資訊安全宣導等相關事務，並定期檢視資通安全政策與管控措施，落實資通安全管理的有效性。

資訊安全管理目標

- 維護資訊系統正常運作與企業永續經營。
- 防止駭客、病毒等惡意程式入侵及破壞。
- 防止人為意圖不當及不法使用。
- 避免人為疏失意外。
- 維護實體環境安全。

資訊安全管理具體方案

- 人員管理及教育訓練
  - 嚴格控管資訊服務處人員適任性，防範不法及不當行為制衡機制。
  - 即時取消離職、停職、退休人員系統使用權限。
  - 進行資訊安全宣導，提升員工資安意識。
  - 軟體下載之控管措施，新進員工於報到當日即簽署不得使用非法軟體同意書。
- 網路安全
  - 公司網路與外界網路連接的網點加裝防火牆，藉以控管資料傳輸與資源的存取。
  - 安裝防毒軟體自動偵測病毒，以確保系統資料安全性。
  - 電子郵件控管機制。
- 資料及設備管理
  - 電腦機房環境監控及進出管理措施。
  - 系統文件、軟體版權及電子檔案之保存、備援、授權及銷毀管控措施。
- 風險管理及事件應變演練

- 電腦當機、服務中斷及資料損毀等資訊事件原因分析管理及防止類似事件再發生之補救措施。
- 訂定網路設備與系統之備援機制及定期演練。
- 網路入侵之緊急處理程序。

近年來網路攻擊事件頻傳，勒索病毒尤為猖獗，資訊安全感脅日新月異，本公司關注國內外重大資安事件，除了加強系統防護機制外，也不定期以 E-mail 方式宣導資訊安全，讓同仁建立自我良好的資訊安全概念與習慣。另外，本公司將依據實務需要，評估投保資安險。

本公司 112 年進行三次共 488 人次的資訊安全宣導。

宣導日期	宣導事項	宣導人次
112.02.06	● 惡意人士冒用中央健康保險署的網址，大量寄發謊稱「健保費扣費明細」，並夾帶惡意程式附件的惡意郵件，提醒同仁提高警覺。 ● 資訊安全威脅日新月異，除透過系統建立防護機制外，也需建立自我良好的資訊安全概念與習慣。 ● 重申維護智慧財產立場與加強個人資訊安全防護之應遵守事項。	170
112.09.19	● 惡意人士以「商務電子郵件入侵」手法(變臉詐欺)，冒用公司主管名義寄發要求財務交易的需求，提醒同仁提高警覺，若有任何異常時，也請務必以其他管道與當事人再次確認。 ● 資訊安全威脅日新月異，除透過系統建立防護機制外，也需建立自我良好的資訊安全概念與習慣。 ● 重申維護智慧財產立場與加強個人資訊安全防護之應遵守事項。	160
112.10.03	● 新型態的 QR Code 釣魚信攻擊，提醒同仁提高警覺。	158

本公司於 112 年 12 月設置 1 名資訊安全主管及 1 名資訊安全人員。