資訊安全政策及管理方案

2021.12.15

本公司為強化資訊安全管理，以確保資訊資產之機密性、完整性及可用性，特訂定本政策，以實施推行資訊安全管理作業。

一、資訊安全風險管理架構

1. 本公司資訊安全組織以『資訊部』為主要權責單位，並依公司現行管理規章依循 PDCA 原則進行作業規劃、執行、檢查、審查。
2. 資訊安全風險跨部門組織，如下圖示：

部門	權責
知識中心	統籌公司內外部企業風險掌控及管制
法務智權	制定營業秘密及機敏資料保護法及推行作業
資訊部	制定資安管理辦法及推行作業
稽核室	稽核管理辦法落實情況並向董事會報告

二、資訊安全政策及具體管理方案

1. 本公司資安政策有下列相關構面

構面	說明
資訊系統政策原則	系統權限管理、系統存取管理、備份管理
作業執行原則	軟體/設備安全管理、網路使用管理等
人員培訓作業原則	實施新進人員資訊安全教育訓練實務課程，並建置線上學習 (E-Learining) 資訊安全課程，藉以提昇內部人員資安知識與專業技能。
資安事件處理作業程序	發生重大事項依據 5W1H 原則，並經過資訊主管確認影響範圍及重大情況向上報告。

2. 本公司具體管理方案

構面	具體管理方案說明
資訊系統政策原則	■ 定期帳號及權限盤點 ■ 同仁存取權限之授權、審查及管控措施 ■ 資料備份及備援措施
作業執行原則	■ 實體及環境安全

資訊安全政策及管理方案

2021.12.15

	■ 軟硬體使用盤點 ■ 防毒及作業系統的更新作業 ■ 系統及網路狀態監控 ■ 定期營業機密及機敏資訊盤點及查核 ■ 定期個人資料盤點及查核 ■ 資安宣導 ■ 機敏資訊及隱私權管理宣導
人員培訓作業原則	■ 新人線上訓練必修課程 ■ 舉行面授教育訓練 ■ 機敏資訊及隱私權管理教育訓練
資安事件處理作業程序	■ 事件處理報告 ■ 公告重大資安訊息

鑒於資安保險為新興保險類別，考量其保險範圍、理賠鑑識及鑑識機制等資格議題成效上，本公司經評估後，暫不投保資安保險，但因資訊安全所面臨的挑戰，如 APT 進階持續性攻擊、DDOS 阻斷式攻擊 、Ransomware 勒索病毒、Social engineering 社交工程及 BEC 郵件詐騙攻擊等資安議題，已採取以下策略

1. 每年執行資訊安全性檢測（資安健診)
2. 持續關注內外部資安環境變化趨勢，對內宣導及公告防護機制及方案
3. 透過現行防毒系統、郵件防護系統及資安網通設備進行防護與記錄以期能事先防護及第一時間偵測並降低業務的影響。

資安通報作業程序：請參考下頁圖

資訊安全政策及管理方案

2021.12.15