

## 資訊安全風險管理

### 1. 資訊安全政策：

本公司制定資訊安全政策作為資訊安全管理之指導準則，聚焦個人資料檔案之安全維護與管理、營業秘密檔案管理及資訊系統安全三大面向，並持續落實資訊安全管理，強化人員、設備、系統、資料及網路等資訊資產之安全管理，免於因外在威脅或內部人員不當的管理，遭受洩密、破壞或遺失等風險。

### 2. 資訊安全組織架構：

- (1) 本公司設置「資訊安全委員會」，負責資訊安全推動等相關事宜。
- (2) 「資訊安全委員會」下設個人資料保護管理、營業秘密管理及資訊系統安全管理等小組，負責執行相關管理作業。
- (3) 由稽核室稽核資訊安全作業。
- (4) 全體員工及協力廠商等資訊使用者遵行本公司資訊安全要求。

### 3. 管理階層支持：

109年3月已向董事會報告108年資訊安全管理執行狀況。

### 4. 資訊安全具體管理方案：

- (1) 建置防火牆系統防止非法入侵、破壞或竊取資料，以保障資料安全，109年未發生重大的網路攻擊或事件。
- (2) 建置垃圾郵件過濾系統，109年過濾95%以上的垃圾信件。
- (3) 每台電腦安裝防毒軟體，定期掃毒，以提供同仁安全的作業環境。
- (4) 定期下載漏洞修補程式更新作業系統，以防止駭客或病毒攻擊。
- (5) 每日、每月定期進行備份作業，並將備份資料異地存放。
- (6) 109年5月進行ERP系統異地還原演練，確保備份資料正確及有效。
- (7) 資料存取權限須經權責主管核可後，方由資訊單位設定。
- (8) 109年度人員到職、異動、離職時，均依作業要求進行權限變更。
- (9) 應用系統軟體之變更，由使用部門填具「電腦作業變更申請單」經權責主管核准，並依程式開發及設計程序辦理。

### 5. 資安與網路風險之評估：

- (1) 109年資訊風險評鑑作業，依程序執行風險鑑別、風險分析、界定風險等級、風險評價，評鑑結果並無重大影響營運風險事項。
- (2) 109年勤業眾信聯合會計師事務所進行資訊作業內部控制之有效性查核，並無重大之風險問題。
- (3) 109年委由外部廠商進行網路安全檢測2次，並未發現重大之網路資安問題。

### 6. 資安事件：

近三年度未發生任何重大資安事件，致對公司業務及營運產生不利影響。