

# 資訊安全風險管理

## 資訊安全目的與對象：

**目的：**為確保公司電子文件檔案資料之安全性、正確性、保密性及妥善的處理

**對象：**適用於本公司所有電子文件管理及系統使用者。資訊使用者係包含正式員工、聘僱人員、業務維運之相關人員、使用資訊資源之外部單位、服務提供廠商及其他經授權使用人員。

## 資訊安全風險管理架構：

1. 本公司由台灣辦事處為本公司電腦系統、設備安全管理之督導單位。
2. 內部稽核負責內部資安執行狀況，每年稽核一次。

## 資訊安全政策：

1. 確保公司所保管的資訊資產之機密性、完整性與可用性，並保障人員資料隱私。
2. 資訊安全政策應定期檢測評估。
3. 定期檢視資訊業務執行符合相關法令或法規要求之活動運作。
4. 定期對資訊設備進行安全評估，確定其遵守資訊安全政策及相關規定。

## 資訊安全具體方案：

資訊安全管理類型	相關作業
系統可用性	專人負責定期維護保養 設置『備份紀錄表』，並定期覆核及試讀 強化電腦軟、硬體設備設(放)置處、所防護措施
存取控管	賦予使用者適當之系統存取權限 管制資訊檔案存取 重要資料依規定加密
預防外部入侵	設置防火牆及防毒軟體 防毒程式病毒碼應定期更新 使用合法版權軟體
預防資料外洩	輸出資料妥善保存或銷毀 列印或瀏覽需取得同意 可攜帶儲存媒體納入管理

## 資訊安全事件：

2021 年度迄今無任何重大資安事故發生