

資通安全管理

一、資通安全風險管理架構與資通安全政策：

本公司於民國 111 年 1 月設置資訊安全部及資訊安全部主管乙名，112 年 10 月設置資訊安全專責人員乙名，取得 1 張資訊安全專業證照，協助電資部門及電券部門並統籌資訊安全及訂定各項資通安全及災害回復等辦法為強化資訊通訊安全，防止之資訊系統及相關資料遭不當使用、洩漏、竄改、破壞等情事，並確保與網路連線之資訊系統及其資料的安全，並維護電腦運作順暢、設備及資料具安全性、完整性、隱密性，落實電腦資訊使用管理，維護電腦資源有效運用，以期整體資訊業務順利進行。持續針對重要資訊系統加強管理與提升防衛能力，以符合法規及資安要求，定期檢討及執行包含資訊安全措施、教育訓練及宣導等改善作為，以確保本公司重要機密資訊不外洩。

二、具體管理方案及投入資通安全之管理資源：

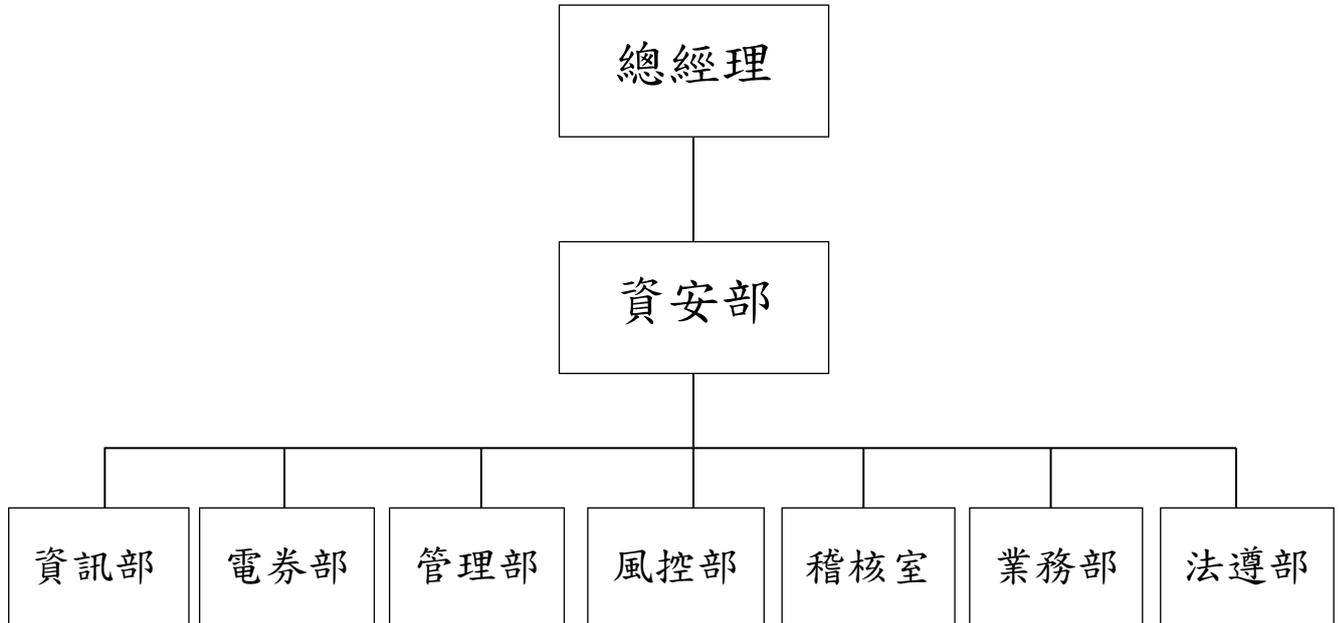
公司已建立全面網路與電腦相關資安防護措施，但無法保證其控管能完全避免來自任何第三方惡意軟體及駭客攻擊。為了預防惡意的駭客及降低此類攻擊所造成的傷害，落實相關改進措施並持續更新。

本公司因應 DDOS 攻擊，建置 ISP 流量清洗服務，以避免遭受攻擊。提供客戶使用之行動 APP，每年委由認證合格之第三方檢測實驗室進行資安檢測，並於簽訂之服務合約中，要求其遵守保密及網路安全規定，但不能保證每個第三方服務廠商都將嚴守這些義務。若發生重大資訊服務異常事件或資通安全事件時，依訂定之資安事件通報機制迅速辦理。投入於資通安全管理之資源係為 IT 人員薪資、軟硬體購置、維護等，已逐年編列預算執行。

112 年度舉辦 2 次資訊安全教育訓練課程,參加成員全體員工(約 210 名)；
並執行 2 次電子郵件社交工程釣魚郵件演練,演練人數超過 50 人。

三、資訊安全小組

(一)資安小組組織：



(二)資安小組工作職掌：

1. 負責執行資訊安全工作之推展與政策規劃。
2. 擬訂資訊安全政策及管理原則與作業標準。
3. 定期辦理有關資訊安全教育訓練。
4. 確認資訊資產的所有權與控制皆有適當的管理。
5. 監控、記錄與調查資訊安全事件。
6. 整理彙總年度執行資安風險狀況。
7. 資安諮詢。
8. 個人資料維護處理相關事項。

四、重大資通安全事件：

最近年度及截至年報刊印日止，並無因重大資通安全事件所遭受之損失、可能影響及因應措施。