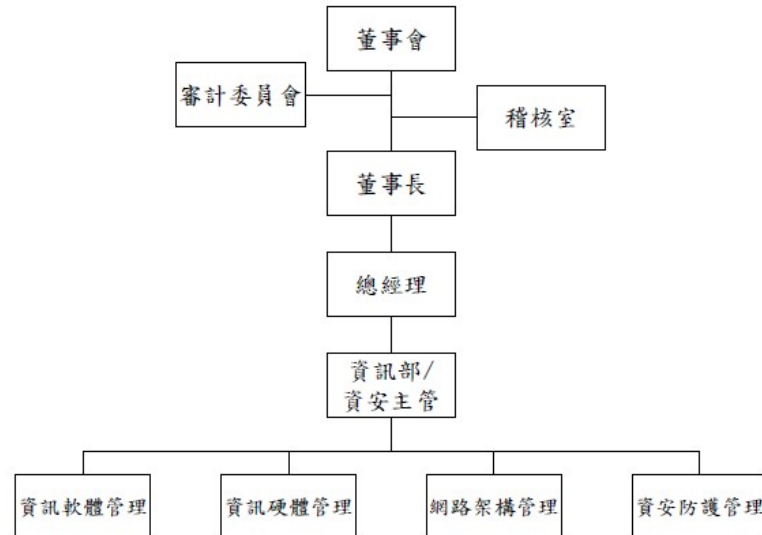


# 資通安全管理

## 1. 資通安全風險管理架構：

本公司設立資訊部門並由其專責資通安全管理，負責資安規劃及推動執行，以建構集團資安防禦能力及同仁良好之資通安全知識。



## 2. 資通安全政策：

- 以減少被攻擊的機率及提高入侵難度為主要手段。
- 以資料備份為基礎，加以管理措施減少資料外流的機會。
- 對各種作業流程建立內部稽核機制。

## 3. 具體管理方案：

- 減少不必要的被攻擊的標的：盡量減少放置在 Internet 的服務，比如 FTP 或是網站等。企業網站交由專業服務商代管，避免成為吸引企業網路被攻擊的標的。
- 建立從外部防火牆到內部防毒軟體、加密線路等的防禦機制，提高入侵難度
  - a. 不同地點的辦公室，採用硬體 Site to Site IPsec VPN 作為網路連線的方式，提高不同地點資料交換的安全性。
  - b. 在各營業據點架設防火牆，區隔內部跟外部網路，並以網路行為控制設備(AC)，以帳號權限方式管理使用者的網路行為。
  - c. 建立內部網路防毒管理中控制台，監控網域內電腦防毒軟體更新及部屬的情況，監控電腦中毒情況並即時採取必要的行動，避免災情擴大。
  - d. 郵件伺服器中建立 Mail SPAM 機制，並依實際情況做調整，建立 DNS SPF 規則，減少電子郵件網路詐騙發生的機率。
  - e. 建立 WSUS 機制，保持區網內作業系統更新狀況良好。
- 建立完整備份機制，分別針對 File server、DataBsase、重要服務建立備份還原機制以及異地備份。
- 以權限的方式管理使用者的網路使用，包含 E mail、即時通訊、一般網路瀏覽均需申請經過核決流程後，方得開放使用權限，並同時監控、記錄使用者的網路行為。
- 針對網路使用者做相關的教育訓練，若牽涉到個人資料部份，會進行個資法宣告，並經使用者確認無誤後，始得放行。
- 包含機房人員進出管制、伺服器維護紀錄、網路行為紀錄、網路帳號及各系統使用帳號權限申請、離職取消機制等，除年度內部稽核對資通安全項目進行查核，確認設備資安控制及系統復原測試執行是否確實，以確認各項機制可有效實施。

## 4. 投入資通安全管理之資源：

民國 110~111 年為完善備份機制及提高入侵的難度，分別陸續於新店機房投入一部 NAS，於桃園主機房室投入兩部 NAS，作為備份機制自動化及離線備份之用。

## 5. 資通安全管理原則：以所有資訊作業符合國內外法令的要求為目標，到目前為止從外部夥伴及客戶的回應，沒有發現有侵害顧客隱私或遺失顧客資料的事情發生。