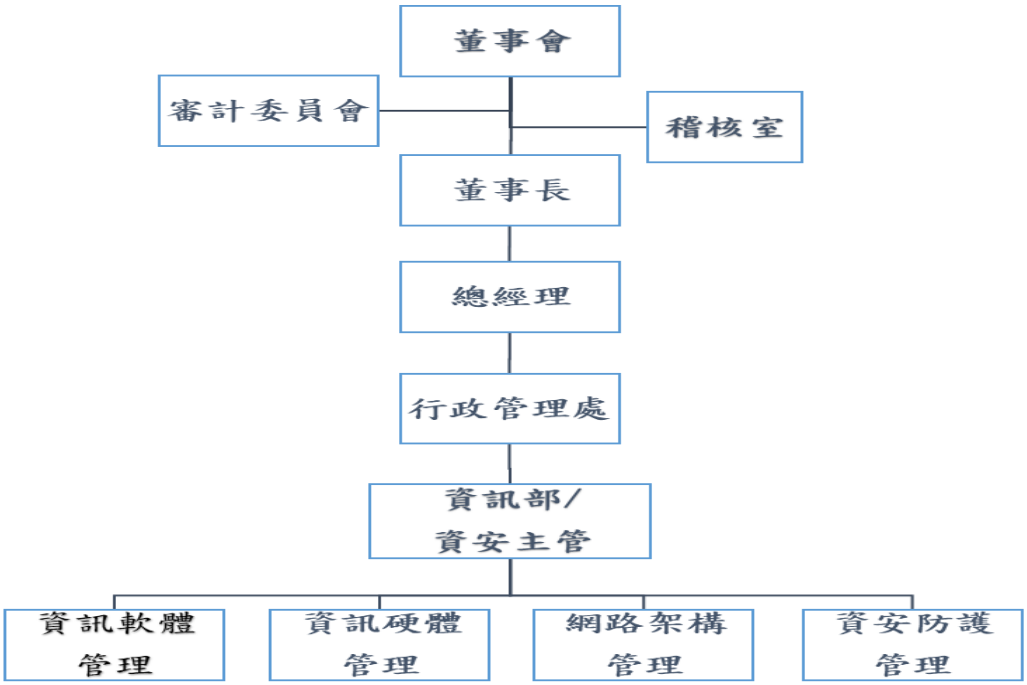
資通安全管理架構

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。



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

網路安全

以減少被攻擊的機率及提高入侵難度為主要手段

1. 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。
2. 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：

- 不同地點的辦公室，採用 MPLS VPN 作為網路連線的方式，提高不同地點資料交換的安全性。
- 在大陸跟台灣的辦公地點架設防火牆，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。
- 建立內部網路防毒管理中控台，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。
- 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。

建立主動防禦的能力，持續觀察對手的惡意網路行為並分析其發動攻擊之目的

1. 增設內部防火牆，把伺服器群與其內部網路跟電腦做區隔，並實時監控進出的網路流量，分析異常。
2. 實時更新分析網路異常行為的特徵碼，並加入雲端安全威脅知識庫，分享並取得最新的安全威脅資訊。

資料安全

以資料備份為基礎，加以管理措施減少資料外流的機會。

1. 建立完整備份機制，分別針對 File server、DB、重要服務建立備份還原機制以及異地備份。
2. 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後，經過核決流程後，方得開放使用權限，同時監控、記錄使用者的網路行為。
3. 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。
4. 傳統的主機式機房架構整改為超融合架構，提高整體架構的可靠性，減少因為硬體或軟體故障的停機風險，搭配虛擬機備份系統，提高備份跟還原的效率。

近期資通安全資源投入

1. 2021 年為完善備份機制及提高入侵的難度，分別於台灣辦公室投入一部 NAS，於大陸廠區投入兩部 NAS 作為備份機制自動化及離線備份之用。
2. 2022 年底規劃總部機房架構從傳統式主機架構升級為超融合架構。
3. 2023 年規劃導入內部防火牆，將伺服器群與其他辦公電腦做區隔，減少伺服器群暴露的風險。
4. 2022 年同仁參加資安相關教育訓練課程 10 人次共 28 小時。

資通作業規範

對各種作業流程建立內部稽核機制，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\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，將查核結果報告董事會(111.12.23)外，並引入外部稽核，如 ISO 及會計師年度稽核等，以確認各項機制可有效實施。