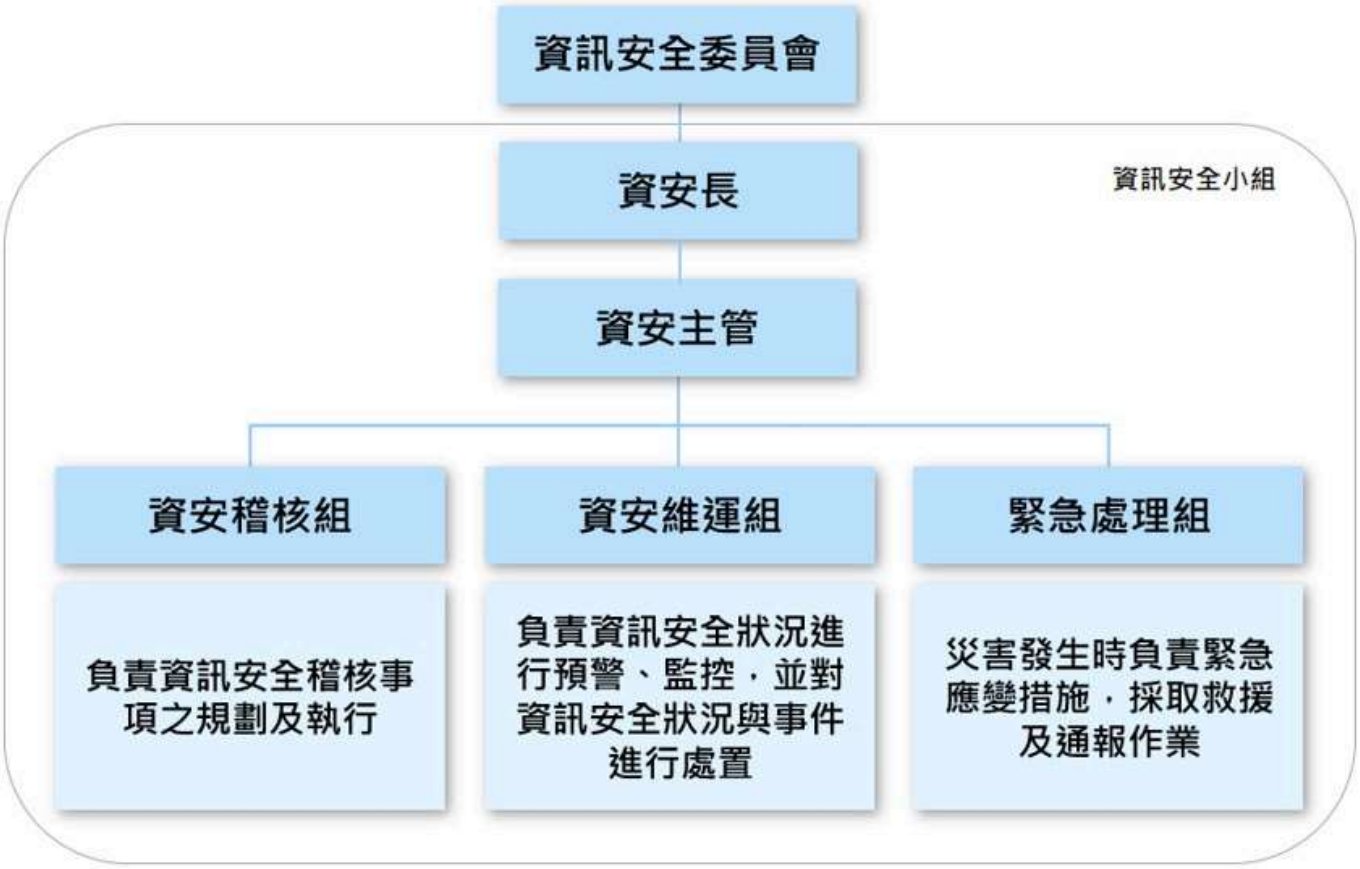
資訊安全風險管理組織

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊安全管理委員會，由資安長擔任資訊安全小組之召集人，且每年至少一次向董事會報告，資安長已於2024年11月4月向董事會報告。組織團隊包含資安維運組、緊急處理組與資安稽核組；資安維運組執行資訊安全系統建置，包含網路管理與系統管理；緊急處理組負責營運持續計劃規範及危機處理程序、執行危機應變措施與通報，並進行事後分析及防範之工作；資安稽核組配合公司稽核單位進行資訊安全稽核工作，包含內部稽核與外部稽核。



資訊安全政策

本公司資訊安全政策為「維護公司資訊之機密性、完整性、可用性與適法性，避免發生人為疏失、蓄意破壞與自然災害時，遭致資訊與資產不當使用、洩漏、竄改、毀損、消失等，影響本公司作業，並導致公司權益損害」。已於2016年導入資訊安全管理系統，並取得ISO 27001證書，及維持證書連續有效性。透過資訊安全管理系統之導入，強化資訊安全事件之應變處理能力，保護公司與客戶之資產安全。

資訊安全風險管理機制

項目	具體管理措施
資訊安全小組	由各功能代表所組織的團隊有19人，負責資訊安全推動與維運。每季至少召開一次資訊安全相關會議。
防火牆防護	1. 防火牆設定連線規則。 2. 如有特殊連線需求需經權責主管核准始能開放。
使用者上網控管機制	1. 使用自動網站防護系統控管使用者上網行為。 2. 自動過濾使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。

防毒軟體	使用防毒軟體，並自動更新病毒碼，降低病毒感染機會。
作業系統更新	作業系統自動更新，因故未更新者，由資訊中心協助更新。
郵件安全管控	1. 有自動郵件掃描威脅防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件，及擴大防止惡意連結的保護範圍。 2. 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
資料備份機制	重要資訊系統資料庫皆設定每日備份。
重要檔案上傳伺服器	公司內各部門重要檔案存放於伺服器，由資訊中心統一備份保存。
網路傳輸防護	1. 連線通道加密。 2. 資料內容加密 及 資料內容電子簽章驗證。
資料保存防護	1. 動態資料遮罩 : 僅能存取有權限的資料。 2. 內容加密儲存 : 機敏資料存入資料庫前，先行加密再做儲存，使用時須解密。
資安險	本公司客戶主要為企業客戶，無消費者機敏個資保管風險，於評估市面資安險種保險範圍、適用行業等項目後，暫不投保資安險。因應資訊安全所面臨的挑戰，持續關注資訊環境變化趨勢，並導入相關軟硬體，例如防火牆、防毒、入侵防護系統...等，強化公司同仁資安危機意識及資安處理人員應變能力。

數位資訊安全強化．客戶隱私升級

為使客戶資料獲得完善的保護，本公司建置客戶資料管理制度，從企業策略面著手定位組織管理與運作，透過業務流程與資訊系統的分析，檢視個人資料取得、處理、傳遞、儲存的存取控管，並在經銷商網站上揭露客戶資料之隱私權聲明，除承諾將保護客戶隱私外，並清楚說明客戶資料的使用與安全規範等，以保障顧客隱私權。2023 年，本公司無侵犯客戶隱私或遭客戶投訴隱私遭侵犯之情事發生。

緊急通報程序

建立資安事件通報機制，當發生資訊安全事件時，通報資訊安全小組-緊急處理組，判斷事件類型並找出問題點，即時處理並留下紀錄。