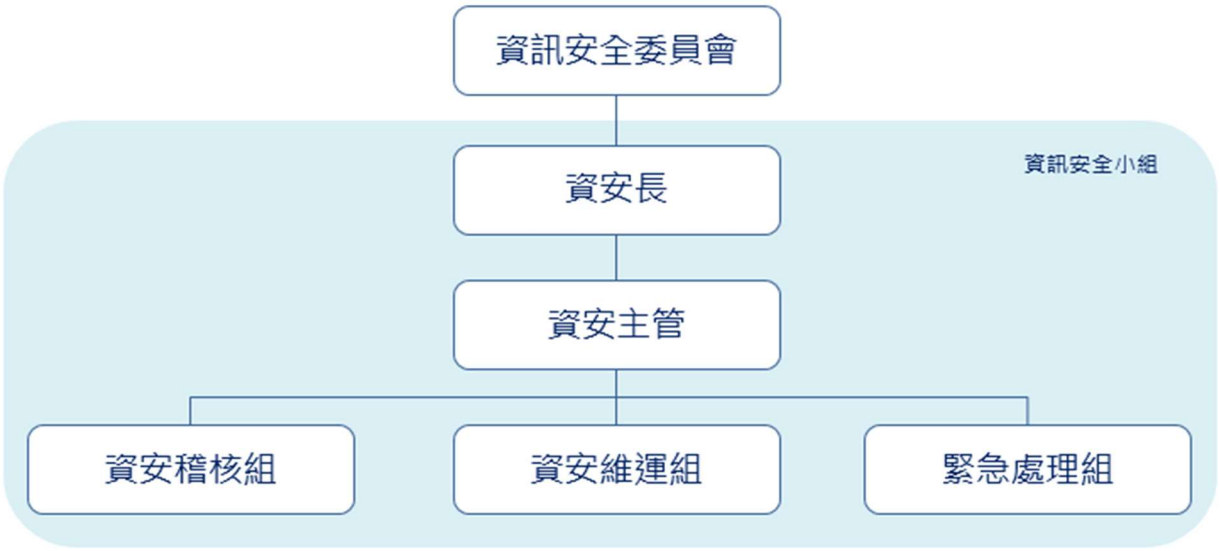
九、資通安全管理

● 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，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。



● 風險管理機制

執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊系統控制存取等管理。

● 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」。本公司已於 2016 年導入 ISO 27001 資訊管理系統，並定期取得 ISO 27001 認證，目前證書之有效期為 2022 年 8 月至 2025 年 8 月。透過 ISO 27001 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。

資訊安全具體管理方案

項目	具體管理措施
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。
資安險	本公司客戶主要為企業客戶，無消費者個資保管風險，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，但因應資訊安全所面臨的挑戰， 已導入相關軟硬體,例如防火牆、防毒、入侵防護系統…等，並持續關注資訊環境變化趨勢，並強化公司同仁資安危機意識及資安處理人員應變能力。

● 緊急通報程序

當發生資訊安全事件時，發生單位通報資訊安全小組-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。

● 因重大資通安全事件所遭受之損失、可能影響及因應措施:無此情形