適用指標	418：客戶隱私
重大議題	• 資訊安全
衝擊說明	• 強化資訊安全的可支持系統的數據保護，確保環境績效資料的準確性和完整性，同時有助於保護公司免受網絡攻擊和數據洩露的損失，維護企業聲譽和經濟利益，並保護個人隱私和敏感數據，符合對個人資料保護的人權要求
政策與承諾	• 預計於 2025 年提出資安政策，確保組織內部資訊的保密性、完整性和可用性，以強化資訊安全管理。這項政策將涵蓋資安訓練、事件響應計劃及持續監控等關鍵領域，以應對不斷演變的資安威脅
權責單位	• 資訊部
因應措施與管理行動	• 持續優化端點防護措施，確保所有設備於接入網路時均能受到有效的保護 • 強化網路管控策略，實施訪問控制和流量監控，以防範潛在的資安威脅 • 定期安排資安健檢，對現有的資安架構進行全面評估，識別潛在的漏洞和風險，並提出改進建議
評核機制	• 資訊會議：每月舉行，報告進展，並針對各專案根據其特性進行評估，以確認推動情況，不定期於公司朝會中與全體員工分享最新資訊
申訴機制	• 內部匿名信箱
2024 年目標與達成情形	• 2024 年未發生資安相關事故
短期目標（1 年）	• 透過定期的宣導活動，提升員工資安意識 • 強化端點防護機制，以確保所有終端設備能有效抵禦各類資安威脅，降低潛在風險
中期目標（3~5 年）	• 優化資安防護架構，整合最新的資安技術和最佳實踐，建立一個靈活且高效的防護體系
長期目標（5 年以上）	• 企業的整體戰略中融入資安考量，以確保資安目標與業務目標的一致性

✓資訊管控

為了加強資訊安全的管理，將捷制定了一系列的策略和措施。首先，因公司重視網路架構的設計，為確保其符合嚴格的資安標準；定期邀請外部專家進行滲透測試和安全檢查，以有效識別系統中的潛在漏洞，並及時進行修補。此外，本公司每半年進行災害演練，以檢驗應急計畫的有效性，並提前識別可能的風險，從而增強整體的安全防護能力。在資訊安全的運作中，將捷同樣重視員工的資安意識培訓，透過持續的宣導和和訓練，希望每位員工都能於日常工作中落實資安規範。

✓資安管理機制

項目	內容說明
規劃網路架構	根據公司的業務擴展需求，持續優化網路架構，包括定期評估現有的網路設計，針對潛在的安全漏洞進行調整，並引入最新的技術和標準，藉以提升整體的防護能力。
滲透測試及健檢	2024 年執行滲透測試及社交工程演練，評估資訊系統的安全性，透過模擬潛在的攻擊情境，發現系統中的弱點，並制定相應的修補措施。
災害演練計畫	每半年執行資訊系統災害復原演練，檢驗應急計畫的有效性、提前識別可能的風險，確保在發生災害時，團隊能迅速有效地因應，以減少業務中斷的影響。

✓資安相關教育訓練

將捷計劃實施一系列的資安訓練和宣導活動，讓員工能夠在實際情境中學習如何識別和應對潛在的資安風險，內容涵蓋資安基本知識、常見的網路威脅、資料保護措施以及應對資安事件的應變流程等。此外，將定期發送資安相關的資訊和提示，幫助員工隨時保持警覺，並建立良好的資安習慣，以確保公司的資訊資產得到有效的保護。

✓資安事件因應流程（通報、處理、檢討機制等）

於應對資安事件時，將捷遵循既有的緊急事件應變作業程序進行通報與處理作業程序，以確保事件能夠迅速且有效地處理。

項目	內容說明
通報	於資安事件發生時，各公司現場處理人員應立即執行必要的緊急處置措施，及時通報權責主管。依據集團緊急事件應變作業程序之資通安全事件之定義，進行通報，通報層級依據事件嚴重程度判斷。
處理	資訊部將根據事件的風險層級進行後續處理，各層級的主管需根據事件的性質和影響程度，做出判斷並執行相應的處置措施。
檢討	所有處理結果將在事件結束後進行檢討，以持續改善我們的資安防護能力和應變流程。