更新日期:2026 年 3 月 維護單位:安全管制部

資通安全管理

項目	說明
資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源等。	● **資通安全風險管理架構** 為確保本公司所面臨之資通安全風險得以有效控管，本公司已參照 ISO 27001 與 ISO 31000 國際標準建立資通安全風險管理程序，每年由資安專責單位依據組織目標、需求、內外部議題執行資通安全風險評鑑作業，針對公司已知或潛在的資通安全風險進行風險識別、風險分析，並依風險發生可能性與損害程度評估威脅等級，若評估結果發現風險威脅已超過本公司可接受程度，則立即擬訂風險處理措施與計畫進行因應。資安專責單位每年負責向高階管理階層報告資通安全風險評鑑執行成果及風險處理狀況，以利高階管理階層有效掌握公司資通安全風險狀況，此外，資安專責單位亦定期檢討資通安全風險評鑑作業程序及可接受風險值，維持本公司資通安全風險管理作業之適用性與有效性。 ● **資通安全政策** 本公司已制定「資訊安全暨個人資料保護管理政策」作為全公司資通安全與個人資料保護管理作業的最高指導準則，目的為強化與持續改善各項資通安全與個人資料保護管理機制，落實資料、系統、設備及網路之保護，與遵循我國「個人資料保護法」、「資通安全管理法」及主管機關相關規範，同時確保資訊作業之機密性、完整性、可用性、適法性及保障個人資料當事人之權利。政策內容每年定期檢視，以確實反映政府法令、公司業務目標及資訊技術發展狀況。 ● **具體管理方案及投入資通安全管理之資源** 本公司已成功導入ISO 27001資訊安全管理系統(ISMS)國際標準並通過驗證，全公司由上而下均採用「Plan-Do-Check-Act」(PDCA) 之循環運作模式辦理資通安全各項管理作業，此外，本公司每年依照「保險業辦理資訊安全防護自律規範」之規定，委託外部專業機構辦理資通安全評估作業，主動發現資安威脅與弱點，持續改善並提升網路與資通訊系統安全防護能力。另為有效推行資通安全與個人資料保護管理工作，並確保資通安全與個人資料保護管理政策之落實，本公司已成立「資訊安全暨個人資料保護管理審查會」，負責推動、協調、督導及改善本公司資通安全

	與個人資料保護管理制度之運作。審查會委員由本公司各處級主管擔任，依規定每年至少召開一次管理審查會議，監督公司資通安全與個人資料保護各項作業辦理情形、協調資源運用及確認相關風險管控機制運作是否有效。本公司亦已依「保險業內部控制及稽核制度實施辦法」之規定成立資安專責單位，負責資通安全政策推動，規劃及執行各項資通安全管理作業，並就公司資安目標、需求及因應資安風險之目的建置及強化資安監控機制與防護設備。資安專責單位每年定期向董事會及高階管理階層報告公司資通安全整體執行情形，以增進公司經營階層掌握資安情勢及瞭解公司資通安全各項議題。
最近年度因重大資通安全事件所遭受之損失、可能影響及因應措施，如無法合理估計者，應說明其無法合理估計之事實及原因。	無此情形。
資通安全風險對公司財務業務之影響及因應措施。	資通安全風險對公司財務面影響，可能因保戶個資或公司敏感性資料被盜取而遭受罰款或需負連帶賠償相關損失之責任，也可能因發生重大資安事件影響公司商譽，不利業務推展，故在因應措施上，本公司除不斷投入資源強化資安防護措施外，每年也定期執行各項資通安全演練，並委託外第三方單位辦理資安評估作業，以使資安風險降至最低。