資通安全管理

維護單位：資訊安全部
更新週期：每年
最近維護日期：113/03

項目	說明
敘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。	1. 資通安全風險管理架構 由於經營環境日趨複雜、全球網路攻擊與金融資安事件影響甚鉅，為確保公司資通訊的安全並保障顧客及員工權益，以及符合主管機關法令規定，本公司設立「資訊安全委員會」負責審視公司資訊安全管理制度，監督制度運作情形。於 107 年度成立獨立專責之資安單位「資訊安全部」，負責規劃、監控及執行資訊安全管理作業，並依法規指派綜理資訊安全政策推動及資源調度事務之副總經理層級主管擔任資訊安全長。秉持維護本公司作業環境之資訊安全理念，持續提高資訊安全事件監控及防護水準、建立標準化及文件化之資訊安全控制作業流程，以及提升全公司的資安認知及資安職能。在落實維護公司整體資訊安全的責任下，規劃公司整體資訊安全藍圖，尋求資訊安全風險管理與公司營運效益中之最佳平衡點。 2. 資通安全政策 在符合法令法規要求之前提，為維護資訊作業正常且安全穩定的運作，提供可信賴之資訊服務，並確保本公司資訊資產之機密性、完整性、可用性，避免遭受內、外部蓄意或意外之威脅以降低資訊作業風險，爰衡酌本公司之業務需求，訂定本公司資訊安全政策，作為公司整體資訊安全管理之最高指導原則。 本公司資訊安全管理制度之運作為依照 ISO 27001:2013 標準，採用「Plan-Do-Check-Act」(PDCA)之循環運作模式，建立資訊安全管理制度，並維繫其有效運作與持續改進。資訊安全管理系統 (ISMS) 預定之相關計畫均已完成，並順利於 112 年 12 月 19 日以無

	不符合事項之成果通過 ISO 27001:2013 資訊安全管理系統（ISMS）年度驗證。 3. 具體管理方案及投入資通安全管理之資源 隨著網路犯罪集團的全球攻擊態勢以及新興科技的演變而引起的風險，未來本公司持續藉由持續強化資訊安全防護架構及資訊安全管理制度、資安威脅防禦與應變，以確保公司業務所需資訊環境安全無虞： (1) 治理面向 除了藉由外部顧問公司的審查確認本公司資訊安全管理作業有效運作外，資訊安全部持續優化資訊安全管理制度，針對現有資訊安全內部控制文件進行確認與分析，建置全公司之資訊安全組織架構及應遵循之資安制度，於各部門設立資訊安全人員，將資訊安全管理作業推展至全公司。並因應 ISO 27001 之更新，本公司已規劃資訊安全管理制度轉版計畫(轉版至 ISO 27001:2022)，藉由新增的控制措施提升本公司資訊安全管理制度之完整性，預計於 113 年底完成轉辦驗證作業。 針對公司全員辦理資訊安全教育訓練與宣導，以加強資訊安全認知。一般同仁經由本公司員工學習網接受三小時、部門資訊安全人員則接受六小時之的資訊安全教育訓練，且透過資安試題以驗證同仁的資安認知及觀念正確與否；資安專責單位同仁則透過自辦教育訓練課程、國內受訓課程、研討會及國外受訓課程等方式，完成至少十五個小時的教育訓練時數。民國 112 年全公司參與測驗及通過比率為 100%。另於 112 年度本公司偕同金控資安處共同舉辦資安月活動、安排外部資安公司進行 16 場次資訊安全相關課程，藉以持續提升公司同仁之資安意識與資安能力。 (2) 技術面向 持續投入資訊安全預算強化資訊安全防禦架構，並透過資訊安全威脅情資之蒐集、網路流量監控、

	資訊安全評估檢測作業，掌握公司面臨的資訊安全風險，對資安防護機制進行更正確且有效的規劃與投資。持續精進本公司的資訊安全防護能力： i. 建立資安監控中心(SOC)：本公司設有資安監控中心(SOC)，進行每日 24 小時 (7x24) 全天候即時監控、偵測與發現資安事件並主動封鎖外部持續性攻擊，以提升資安事件監控的能量。整合本公司資安監控平台與相關資安設備、網路設備等設備之日誌，進行多維度關聯分析，經由專業的 SIEM 資安分析人員進行研判與建議，以達到精準的資安事件即時通報與預警之效益。資安事件的即時通報將大幅提升後續追蹤與應變處理的有效性，落實資安事件妥善處理，降低資安事件的危害程度。 此外，資訊安全部持續監控本公司網路資安風險管理之分數與評比，112 年期間本公司網路資安風險管理之分數均維持在同業前三名，112.07~112.11 期間更位於同業第一名，足可證明本公司於資訊安全投入之心力及成果。 ii. 辦理資安相關演練：為因應外部多變的攻擊手法並降低遭遇突發緊急危難或異常事故所可能造成資訊作業中斷之衝擊，本公司定期辦理核心資訊系統災難備援演練、DDoS 演練、電腦系統資訊安全評估、對外網站滲透測試及全公司社交工程演練，以確保公司資訊設施的安全並保護機敏資料與顧客個人資料。 iii. 因應資安情勢之日益嚴峻與情資來源的多元化及金管會推動之「金融資安行動方案」，為利用開發金控集團內資源整合及相互支援之運作優勢，本公司已建立內部跨單位資安威

	脅事件處理小組並加入開發金控建立之電腦資安事件應變小組，俾利即時掌握及支援集團內成員資安事件之應變處置，降低事件損害。另外重大資安事件往非僅影響單一機構，現行本公司已加入 F-ISAC 資安情資關聯分析平台，並透過壽險公會與法務部調查局建立資通安全聯防與情資分享合作機制，透過機構間之聯防機制強化體系風險控管，提升跨機構或跨領域之橫向通報應變與支援協處之運作機制與能力，以降低重大事件之體系災損。
列明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。	本公司於 112 年度無發生重大資通安全事件。另委請獨立第三方評估資訊安全整體執行情形，未發現有影響本公司資訊安全整體執行情形之重大異常情事。
資通安全風險對公司財務業務之影響及因應措施。	面臨複雜的資訊安全風險環境，本公司於 113 年度持續投保資訊安全保險，俾降低重大資安事件發生後公司之法律、財務承擔責任及受影響客戶的索賠等損失，強化公司風險承擔能力。