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：114/02

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，並每年於董事會提報前一年度資訊安全整體執行情形。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 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，並因應 ISO 27001 之更新，資訊安全部已完成 113 年度之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，順利於 114 年 1 月 7 日以無不符合事項之成果通過 ISO 27001:2022 資訊安全管理系統 (ISMS) 轉版驗證。 3. 具體管理方案及投入資通安全管理之資源 基於資訊安全政策及業務目標、保護本公司的核心資產和客戶資料之目的，本公司持續投入資源於資安管理，113 年度本公司資安類經費占整體資訊經費之比例約為 13%，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，本公司於 113 年度無發生重大資通安全事件。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，未來本公司持續從各面向精進各項資訊安全防護措施，以確保公司業務所需資訊環境安全無虞： (1) 治理面向 A. 本公司依據國際資安管理框架導入措施，持續取得 ISO 27001 國際標準認證，每年透過兩次資訊安全委員會，由高階管理階層定期執行管理審查活動，確保相關資安管控措施之有效性，持續精進管理作業並提供必要之資源，113 年度已依規劃分別於 6 月及 12 月完成上下半年之資訊安全委員會。基於資訊安全與資訊管理為密切相關之作業，本公司透過定期舉辦之資安與資訊體系定期溝通會議進行資安管控措施與資訊業務執行間之溝通與協調，確保相關資訊作業執行均有妥善之資安管控規劃，於 113 年度共計舉行 9 次會議。 B. 為提升對個人資料保護的管理能力，本公司已導入個人資料管理制度並取得 BS 10012 認證，以確保客戶的權益得到最佳的保障。為

	了確保資訊安全及應變能力，本公司亦投入相當資源於資訊安全預算及人員配置，導入 ISO 22301 框架的營運持續管理機制並取得認證，以定期執行異地辦公演練、系統異地備援演練、資料回存測試、備份還原測試等演練並推動異地備援中心的優化改善，確保資訊安全能夠持續地得到強化。 C. 資訊安全部已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。針對董監事成員及高階管理階層辦理資安教育訓練「資訊安全治理規範剖析下的金融業人工智慧應用發展」，以強化董監事及高階管理階層了解資訊安全與人工智慧治理的相關要求；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的資訊安全教育訓練；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。另於 113 年度本公司偕同金控及各子公司資安單位共同舉辦資安月活動，透過 6 場研討會邀集外部資安專家進行資安相關議題說明與宣導；辦理之資訊安全相關教育訓練共計參與人次為 2,838 人，總完訓時數共計約 8,700 小時，未來將持續提供多面向的資訊安全教育訓練，藉以提升公司人員之資安意識與資安能力。 D. 本公司已針對營業秘密訂定相關規定，包含核心政策、權責單位、保密義務及相關權利與獎懲，以持續管理、維護及運用本公司之營業秘密相關資料及智慧財產權。 (2) 技術面向 本公司基於美國國家標準技術研究院 (NIST) 發布之「網路安全框架 (Cybersecurity

	Framework)」，透過其核心的 5 大構面：識別(Identify)、保護 (Protect)、偵測 (Detect)、回應(Respond) 與復原 (Recover)，作為建構資訊安全防護的基礎，持續投入資訊安全預算強化資訊安全防禦架構。並持續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： A. 情資整合並加強安全資訊與事件管理(Security Information and Event Management, SIEM) 系統功能：定期蒐集並分析外部威脅情報，提前預警潛在的資安風險，協助更精準地判斷事件性質與嚴重性，並作出及時應對。同時擴充 SIEM 系統功能，整合更多資料來源(如日誌、網絡流量、行為分析等)，提高資安事件偵測的準確性，並建立高風險事件快速反應流程，縮短從偵測到解決的資安事件響應時間，以有效降低事件帶來的影響。作為事件偵測與分析的核心，SIEM 系統將與情資蒐集、偽冒網站下架服務及零信任架構導入等專案緊密結合，實現資安威脅的全方位監控。 於 113 全年度，資訊安全部達成偵測及回應資安事件的時間皆不超過 12 小時。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。 B. 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，本公司每年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。113 年度更增加辦理紅隊攻防演練及參與主管機關主辦之金融重大資安事件應變情境演練，藉以發現本公司資訊安全防禦機制的缺漏及資安事件應變程序的完整性，其中因本公司於金融重大資安事件應變情境演練表現積極並提供金融同業經驗分享，獲主管機關之感謝狀肯定。 C. 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」，為利用凱基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凱基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，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。 D. 金管會於 111 年 12 月發布「金融資安行動方案 2.0」，將「鼓勵零信任網路部署、強化連線驗證與授權管控」列為推動重點之一，並於 113 年 7 月 15 日發布「金融業導入零信任架構參考指引」供金融機構做為零信任架構導入之重要指引。金管會推動所有金融機構均須挑選高風險場域導入零信任架構，並於 113 年 12 月完成零信任導入規劃。由於本公司獲選為重點推動對象，將負責分享相關規劃及實施進程予金融同業；本公司規劃以高風險場域為核心之風險與衝擊評

	估方法論，並盤點公司資源存取路徑(身分、設備、網路、應用程式、資料)，制定其導入架構規劃藍圖，由外而內縮小攻擊表面並增進防禦深度、由內而外擴大防護表面，以期逐步符合主管機關對零信任架構各支柱之成熟度要求，並強化本公司資訊安全治理機制，確保提供顧客創新、安心、便利與穩定的金融保險服務環境。本公司於 113 年度完成研訂零信任網路導入規劃，並提報董事會通過，以確保該機制順利推動運作。
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。	最近年度因重大資通安全事件所遭受之損失：無；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。	1. 面臨複雜的資訊安全風險環境，本公司自 107 年度起持續投保電子商務及資訊安全保障責任保險，以降低重大資安事件發生後所遭受到的損失與公司承擔的風險。 2. 資訊安全是公司永續經營的重要基石。本公司透過建立多層次的資安防護體系，從事前的預防、事中的察覺、事後的處理三個面向全面提升資安防護能力，並從資訊安全治理面、技術面不斷精實強化，形成公司進行數位轉型的保護傘。透過零信任架構的導入、強化資安事件應對機制，並持續改善資安管理，我們將能有效降低資安風險，保障客戶資料的安全，並維護企業的聲譽與市場競爭力。這一系列資安策略的實施，不僅是對當前資安風險的應對，也是為公司長期穩健發展奠定堅實的基礎。