國泰人壽
Cathay Life Insurance

國泰人壽保險股份有限公司資訊公開說明文件

項目：資通安全管理

依據：人身保險業辦理資訊公開管理辦法第 8 條第 1 項第 20 款

維護日期：民國 115 年 1 月 16 日

維護單位：資訊安全部

更新週期：年度終了三個月

一、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

(一)資通安全風險管理架構

本公司視資訊安全為永續經營之核心競爭力，自民國 107 年 4 月成立資訊安全專責部門以來，持續接軌國際標準並響應金管會「金融資安行動方案 2.0」，致力達成「安全、便利、營運不中斷」之金融服務目標。

1. 接軌國際框架：採用 NIST 網路安全框架（Cyber Security Framework），以識別（Identify）、保護（Protect）、偵測（Detect）、回應（Respond）、復原（Recover）五大核心構面為基礎，將資安風險管理全面融入事前預防、事中監控及事後應變之全生命週期。
2. 董事會層級監理：設立「資安管理委員會」，每半年定期審議資安執行成效；並於董事會下設「資安諮詢小組」，提供國際趨勢（如新興科技衝擊）諮詢與教育訓練，確保董事會能有效指導資安策略；並訂定涵蓋機密性、完整性、可用性及適法性之「資訊安全政策」，經董事會核定後公告實施，充分展現決策與監督之決心。
3. 國際標準認證：展現對雲端與數據安全之承諾，持續持有 ISO 27017（雲端服務資安管理）及 PCI DSS（支付卡產業資料安全）認證。更於 112 年率先於同業完成新版 ISO/IEC 27001:2022（資訊安全管理系統)轉版驗證，並於

114 年底完成全公司內勤部室擴大驗證，向客戶、合作夥伴與市場展現誠信與承諾，確保管理體系與時俱進。

(二) 前瞻性防禦與科技應用

面對新型態攻擊與數位詐欺，本公司採取「縱深防禦」與「自動化聯防」策略，主動識別並阻斷威脅：

1. 全時監控與演練：建置 7x24 小時資訊安全監控中心（SOC），即時掌握風險動態；定期執行白帽攻防、DDoS 攻擊及社交工程演練，驗證防禦機制之實戰有效性。

2. 智慧化威脅偵測：

(1) 外部偵測：導入外部偽冒偵測機制，針對偽冒網站及 APP 進行監控並即刻下架，保障客戶免受詐騙損害。

(2) 邊境與端點防護：建置次世代防火牆及進階網站應用程式防火牆（WAF），防禦機器人自動化攻擊；內部導入端點偵測與回應（EDR）防護與白名單系統，精準分析異常行為並防止系統遭不當異動。

（三）營運韌性與供應鏈管理

本公司重視風險轉移與供應鏈安全，建構具備韌性之資安生態系：

1. 供應鏈聯防：定期查核受委託處理客戶資訊之機構，確保委外廠商之合規性與風險控管能力，降低資料外洩風險。

2. 危機應變與保險：訂有「資訊安全事件通報暨應變作業辦法」並設置單一危機處理小組，定期演練以確保應變之即時性。同時，經審慎評估後持續每年

投保「資訊安全保險」，透過風險轉移機制確保穩健經營。

3. 公私協力聯防：與法務部調查局簽署「國家資通安全聯防與情資分享合作備忘錄」、與刑事警察局合作「金融阻駭反詐暨資安聯防」，更定期將內部偵測發現之威脅情資，主動回饋予「金融資安資訊分享與分析中心（F-ISAC）」。透過將自身防禦成果轉化為產業預警情資，供金融同業參考，以實際行動落實情資共享精神，建構資安聯防生態系。

（四）資源投入與績效檢視

1. 資源配置：114 年度資安類經費佔整體資訊經費約 9%，確保資安維護計畫擁有充足資源，並堅持在業務設計初期即導入資安防護需求（Security by Design）。

2. 具體成效：透過落實上述管控措施、定期電腦系統資安評估及 KPI 審查，114 年度及截至年報刊印日止，本公司未發生重大資訊安全事件。另委請獨立第三方機構評估整體執行情形，評估結果顯示本公司整體資安治理成效屬妥適有效。

（五）永續經營與數位信任

本公司以支撐永續經營與數位信任之關鍵基礎，將資訊安全融入公司 ESG 與公司治理架構中整體規劃。於治理面向，透過董事會層級之資安監督機制與專責單位運作，確保資安風險納入公司重大風險管理體系；於社會面向，持續強化客戶個人資料與交易資訊保護，維護金融消費者權益與信任；於環境與營運永續面向，藉由完善之資安防護與營運持續管理機制，降低資安事件

對營運穩定性之衝擊，確保關鍵金融服務之持續提供。除此之外，本公司亦積極回應主管機關近年監理與揭露趨勢，持續精進資安治理成熟度，聚焦零信任架構、第三方與供應鏈風險管理、關注 PQC 後量子密碼遷移議題，提升資安韌性與營運持續能力，強化利害關係人對公司數位治理、資料保護與永續經營之信賴。

二、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

114年度及截至年報刊印日止，本公司未發生重大資訊安全事件。另委請獨立第三方機構評估整體執行情形，評估結果顯示本公司整體資安治理成效屬妥適有效。

三、資通安全風險對公司財務業務之影響及因應措施

(一)精實防禦體系，維持營運穩健零事故；本公司已設立資訊安全專責單位，全面推動資安治理業務。面對外部威脅，我們採取主動防禦策略，定期執行各項系統安全檢測以強化防護能力，並透過持續性的教育訓練與各類資安應變演練，有效提升全體員工之資安意識，從內部降低駭客入侵與客戶機敏資料外洩之風險。經由上述嚴謹控管，近年來本公司未發生任何對財務或業務造成重大不利影響之資訊安全事件，具體展現風險控管之成效。

(二)強化數位韌性，前瞻佈局雲端合規；因應科技變革與數位金融快速發展所伴隨的資安挑戰，本公司已建立完善的資安風險評估機制及管理程序，並導入與營運持續相關之國際標準管理框架進行驗證，以確保並提升國泰人壽之資安韌性。此外，針對雲端服務廣泛應用之趨勢，本公司早於108年即取得「ISO 27017雲端服務資訊安全管理系統」國際標準驗證，確保雲端資安管理政策與措施之落實及完整性，有效支持公司數位轉型策略之推動。