富邦人壽

富邦人壽保險股份有限公司資訊公開說明文件

項目：公司治理-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 113 年 3 月 22 日

維護單位：資訊安全部

資通安全管理

項目	資訊內容
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 (1)本公司以 NIST CSF 為基礎，由下述五大面向組成八大核心業務，建構而成本公司之資通安全風險管理架構 A.風險識別：資安風險評估、資安弱點揭露、資安情資分析與處理 B.保護：企業資安文化推動、資安防護 C.偵測：資安警訊分析與監控 D.事件回應：資安事件回應 E.復原：營運持續計畫 (2)本公司已設置資訊安全專責主管及專責單位，設有處級組織資訊安全處，轄下資訊安全部、資安規劃科、資安維運科與資安數據分析科，共有資安專責人員 22 名(不含資訊安全長)。 (3)資訊安全管理會議辦理情形：定期於作業風險管理委員會呈報資安相關事項、與資訊單位進行技術弱點資安控管討論與議題協調、召開資安促進主管會議研議各部門資安作業之落實及分享資安新知與新興議題等會議。 2.資通安全政策 本公司資訊安全政策之資訊安全管理體系涵蓋以下之領域： (1)資訊安全之組織 (2)人力資源安全 (3)資產管理

項目	資訊內容
	(4)存取控制 (5)密碼學 (6)實體與環境安全 (7)運作安全 (8)通訊安全 (9)系統取得、開發及維護 (10)供應商關係 (11)資訊安全事故管理 (12)營運持續管理之資訊安全層面 (13)遵循性 3.具體管理方案 112 年度之具體行動任務說明： 管理面：制定「資安發展策略藍圖」、資訊安全管理制度 ISO 27001 驗證、資安成熟度評估、電腦系統資訊安全評估、加強培育資安人才、資通安全情資之評估及因應、辦理資安事件應變演練、企業資安文化之持續推動(包含董事/高階主管/中階主管/全體同仁之資安教育訓練、單位資安促進主管制度運行、全體同仁資安報你知宣導、客戶資安宣導)、資訊安全法令遵循風險督導。 技術面：行動 APP 資安檢測、網站年度資安檢測、資通安全威脅偵測管理(SOC)、備援演練、電子郵件社交工程演練、分散式阻斷服務攻擊(DDoS)演練、技術弱點揭露與管控、資安防禦系統建置與提升及聯防機制之建立。 4.投入資通安全管理之資源 本公司於 112 年度投入之資訊安全管理資源包含以下面向： (1)建置與提升資安防禦系統，如：分散式阻斷服務攻擊 DDoS 防禦、網路入侵偵測機制管理、防火牆、網頁防火牆防護、病毒與惡意程式偵測與阻擋、主機型入侵防禦機制管理、進階持續性威脅偵測系統

項目	資訊內容
	管理、原始碼掃描系統及資料外洩防護(DLP)等系統。 (2)強化 7x24 之資訊安全監控管理與聯防機制，如：資安事件監控分析、資安警訊與情資分析管理、加入金融資安聯防監控中心(F-SOC)會員等。 (3)辦理各項資訊安全評估與檢測，如：電腦系統資訊安全評估、行動應用程式資安檢測、網站安全漏洞檢測、沙箱掃描檢測、滲透測試、主機及物聯網設備弱點掃描、偽冒網站偵測、外部資安風險評級、資安成熟度評估、網路釣魚之防範等。 (4)執行各項資安演練，如：社交工程演練、分散式阻斷服務攻擊 DDoS 防禦演練、災害復原演練、紅藍攻防實戰演練、資安事件應變演練等。
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受之損失：無。 本公司於「作業風險事件通報辦法」已訂定資通安全事件通報、應變及演練相關機制，能即時掌控資通安全事件，並有效降低其所造成之損害
資通安全風險對公司財務業務之影響及因應措施。	本公司除以各項資安管控措施以降低各類資訊安全事件所可能帶來之衝擊與影響，並進一步於 112 年 12 月 27 日完成「資訊安全保障保險」續保，以利風險轉嫁、降低事故損失並確保公司聲譽與客戶權益。