|  |
| --- |
| **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113年3月5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**

1. 資通安全風險管理架構

本公司資訊安全管理策略，採行「NIST:Cyber Security Framework」安全框架，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，將資訊安全風險對應到事前、事中與事後的所有環節，以提供完善且全面的管理策略，因應急速變化的資安威脅。

1. 資通安全政策、具體管理方案及投入之資源
2. 因應金管會推動之「金融資安行動方案2.0」，持續精進與強化資訊安全防護能力，達成安全、便利、營運不中斷的金融服務。
3. 考量制度管理、管控措施、風險預警、危機管理四個面向，完善本公司資訊安全治理框架：
4. 制度管理
5. 設有資安管理委員會，負責規劃、監控及執行資訊安全管理作業，委員會每半年召開一次資安管理審查會議，由資訊安全部門定期提報資安管理業務執行報告供委員會審議。。
6. 設置董事會資安諮詢小組，提供資安相關分享及諮詢，並針對國際資安趨勢及新興科技衝擊等議題專設教育訓練課程。每年於董事會提報前一年度資訊安全整體執行情形。
7. 以機密性、完整性、可用性、適法性與營運持續等多面向訂定「資訊安全政策」，經董事會核決後，公告於員工網站。
8. 持續取得「ISO27017雲端服務資訊安全管理系統」、「PCI　DSS支付卡產業資料安全標準」國際標準認證，並於112年完成新版ISO/IEC 27001:2022資訊安全管理系統驗證。
9. 管控措施
10. 訂定資訊安全監控指標並定期審查檢視適切性及目標達成情形。
11. 定期針對處理客戶資訊之受委託機構進行查核，確認其風險及合規性，強化數據安全並降低數據外洩之風險。
12. 每年執行電腦系統資訊安全評估案，追蹤系統安全狀況並實行改善措施。
13. 風險預警

建立７ｘ２４資訊安全監控中心，即時掌握資訊安全風險提早進行因應，並定期執行白帽攻防演練、ＤＤｏＳ攻擊演練、社交工程演練等，以驗證防禦、監控機制之有效性及應變即時性。

1. 危機管理
2. 訂定「資訊安全事件通報暨應變作業辦法」，並設有資安事件應變小組，定期執行重大資安事件應變演練，以即時因應各類資訊安全事件。
3. 強化資安管理機制，並期許精實資安作業韌性，本公司亦審慎評估後投保資安保險，確保本公司穩健經營，落實資安風險管理。
4. 面對與日俱增的新型態攻擊，著重投入資源在有效的邊境偵測與攔阻，與強化內部自動化防護機制：
5. 透過使用外部資安風險監控機制與資安情資蒐集暨處理，了解公司對外曝露的資安風險程度，即時修補暴露之弱點。
6. 因應詐騙、釣魚網站及APP氾濫，導入外部偽冒偵測機制，期能在造成損害前，即刻下架偽冒之網站及APP。
7. 建置次世代防火牆與進階網站應用程式防火牆，強化加密連線的解析與機器人自動化攻擊的防護。
8. 導入端點APT與白名單系統，分析端點異常活動行為並保護系統遭到不當異動。
9. 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」、內政部警政署刑事警察局簽署「金融阻駭反詐暨資安聯防」，透過政府民間通力合作，建立資安聯防生態系，落實資安及國安的目標。
10. 112年度資安類經費占整體資訊經費之比例約為5%，考量資訊安全政策及目標，提供建立、實行、維持及持續改善資訊安全維護計畫所需之資源，並於資訊業務設計時，一併規劃資安防護需求。

**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**

112年度及截至年報刊印日止國泰人壽未發生重大資訊安全事件；另委請獨立第三方評估資訊安全整體執行情形，結果亦尚屬妥適。

**三、資通安全風險對公司財務業務之影響及因應措施**

1. 本公司由資訊安全專責單位負責推動資訊安全業務，定期經由各項資訊安全檢測，改善及強化資訊系統安全防護能力，並透過資訊安全教育訓練、各項資安應變演練，提升員工資訊安全意識，降低駭客入侵攻擊與客戶機敏資料外洩之風險，近年未發生對公司重大不利影響之的資訊安全事件。
2. 隨著科技改變與數位金融之快速發展所帶來的資通安全風險，本公司已制定完善資安風險評估、因應措施及管理程序，並借資安與營運持續之相關國際標準管理框架之驗證，確保提升國泰人壽之資安韌性。另隨著雲端服務之廣泛應用，本公司亦已於108年取得「ISO27017雲端服務資訊安全管理系統」國際標準驗證，確保本公司之雲端資訊安全管理政策與措施之落實及完整性。