4-20 資通安全管理【資料日期：113.12.31】

更新頻率：年度終了後三個月內更新

一、資通安全風險管理架構

(一)法規遵循依據

1.「保險業內部控制及稽核制度實施辦法」第六條

遵循情形：業已編定對應之資訊管理及資訊安全政策。

2.「保險業內部控制及稽核制度實施辦法」第六條之一

遵循情形：

(1)已任務指派經管資安業務之副總經理為資安長，並設置資訊安全專責單位。

(2)已協同外部顧問公司彙整各年度資訊安全整體執行情形。

(3) 113年度相關人員已經完成對應之教育訓練。

3.同業相關自律規範範圍

遵循情形：已依照業務情形遵循保險業相關自律規範及作業原則。

(二)執行方法

1.本公司資安管理組織

(1)依據本公司資訊安全管理組織實施要點。

(2)資訊安全推行小組：負責統籌資訊安全政策、計畫、資源調度等事宜之協調及研議。

(3)資訊安全執行小組：負責資訊安全管理各項活動事務之跨單位協調工作，以推動與協調資訊安全管理工作之執行。

(4)資安長：負責督導本公司資通安全相關業務。

(5)資訊安全專責單位：

A.本公司設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。

B.負責訂定、修正及實施資通安全維護計畫。

C.負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，依本公司內部控制制度第五條規定提報董事會。

2.資安相關規章

本公司資訊安全相關管理實施要點。

3.資安治理

本公司於106年取得ISO 27001資訊安全管理制度(ISMS)認證，其後每年由公正第三方機構定期審查、每三年重審換證，持續維持認證之有效性，逐步發展落實資安治理，藉由領導與控制組織及資訊安全活動流程，以確保與維繫各階層人員進行有效地溝通，並遵循與維繫規劃(Plan)、執行(Do)、檢查(Check)、行動(Act)之有效運作與持續改善模式，深化資訊安全管理作業。

113年辦理活動包含：通過ISO 27001定期審查維持證照持續有效、資訊資產盤點、風險評鑑、資訊作業營運持續管理、資安稽核作業、召開資訊安全會議、資安治理成熟度制度評估作業、電腦系統資訊安全評估作業及完成資通安全責任等級B級之特定非公務機關應辦事項。

(三)年度查察作業

1.金融監督管理委員113年資通安全實地稽核

2. 金控稽核處113年度上半年專案查核
3. 金控稽核處113年度下半年專案查核
4. 113年電腦系統資訊安全評估服務
5. 113年ISMS外部稽核
6. 113年資訊安全外部查核(ISMS內部稽核)
7. 內部查核：一般、專案及資通安全專案自行查核共3次

二、資通安全政策

本公司資訊安全政策係依據「資通安全管理法」、「資通安全管理法施行細則」及「金融監督管理委員會所管特定非公務機關資通安全管理作業辦法」訂定，主要係為強化資訊安全管理，確保資料、系統、設備、網路安全及保障客戶權益，特訂定本政策，並至少每年經「資訊安全推行小組」評估一次，以符合相關法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

三、具體管理方案

(一)防護演練

透過演練及通報作業，早日發現資安威脅與弱點，亦可強化組織內同仁資訊安全意識，藉以防範資訊安全的威脅與平衡組織所面臨資訊安全的挑戰，進一步有效遵循保險業內部控制及稽核制度實施辦法之第六條第十項電腦病毒擴散及網路駭客入侵之防範控制及第十一項系統復原計畫、災變備援計畫及測試程序之控制之要求。113年度辦理活動包含：防範惡意電子郵件社交工程演練作業、各應用系統回復演練作業、分散式阻斷式服務(DDoS)攻防演練、資通安全通報演練及資訊安全評估作業。

(二)教育訓練

本公司每年依據資訊安全整體發展趨勢，規劃資訊安全教育訓練課程，例如：防範惡意電子郵件社交工程、淺談物聯網之資安防護、大數據時代下的資訊安全、機器人流程自動化的安全挑戰及風險、後疫情時代遠距辦公、雲端服務應用的資安挑戰級防護等，另為加強同仁資訊安全觀念，每月進行資安宣導。113年辦理活動包含一般使用者與主管計3小時資訊安全宣導課程與通過課程評量、資通安全專責人員(113年配置3人)資通安全專業課程訓練15小時以上、資訊人員資通安全專業課程訓練3小時以上。現行資通安全專責人員共持有5張資安國際證照或職能證照。

(三)資安觀念及設施強化

為強化網站弱點掃描管理，有效掌控公司各類網站弱點掃描修復進度，本年度新建網站弱點黑箱掃描工具平台及弱點報告追蹤管理系統管理模組。為強化資安聯防時效，即時掌握金融機構分享之情資，本年度完成F-ISAC情資訊息與公司弱點報告追蹤管理系統串接之整合作業，完成SOC資安監控通報與F-SOC金融資安聯防監控系統界接設定。

(四)投入資通安全管理之資源

除前述措施，另列與機房維運、網路設備維運、防火牆、入侵防禦系統、弱點掃描修補追蹤及資安顧問等相關經費，113年投入資通安全管理金額約12,822千元。