# 4-20 資通安全管理【資料日期：112.12.31】

**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：已適用遵循並業已編定對應之資訊管理及資訊安全政策(說明如下)。

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)業已任務指派經管資安業務之副總經理為資安長並設置對應之資訊安全專責單位。

(2)業已與外部顧問公司合作彙整各年度之資訊安全整體執行情形。

(3)每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：保險業相關自律規範及作業原則等12項。

遵循情形：已依照業務情形適用遵循。

(二)執行方法：

1.本公司資安管理組織：

(1)依據：臺銀人壽保險股份有限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：臺銀人壽保險股份有限公司資訊安全相關管理實施要點等22項。

3.資安治理

本公司自104年開始導入資訊安全管理系統(ISMS)，並於110年03月25日取得ISO 27001驗證、於108年開始導入個人資訊管理系統(PIMS)，並於110年12月13日取得BS 10012 PIMS驗證、於110年開始導入營運持續管理系統(BCMS)，並於111年10月取得BS 22301 BCMS驗證，資安治理已逐步發展落實。臺銀人壽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)」有效之運作與持續改善模式，深化公司資訊安全管理制度作業，112年度辦理活動包含資訊安全執行小組會議及資訊安全推行小組會議，賡續通過國際標準ISO 27001：2013認證、資訊資產盤點作業、風險評鑑作業、營運持續管理作業、資安內稽作業、定期召開資訊相關會議以及政府機關(構)資通安全B級應辦事項執行等。

(三)年度查察作業：

1.金融監督管理委員會一般/專案實地稽核

2.金控稽核處上/下半年專案查核

3.董事會稽核室年度一般/資通安全專案查核
4.顧問會計師事務所年度資訊內控查核
5.審計部年度期中財務收支查核
6.資安顧問年度電腦系統資訊安全評估服務
7.顧問公司年度PIMS外部稽核
8.顧問公司年度ISMS外部稽核
9.內部查核：一般自行、專案及資通安全專案自行查核共3次

## 二、資通安全政策

本公司訂有臺銀人壽保險股份有限公司資訊安全政策，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

本公司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，並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。112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、「金融監督管理委員會及所屬機關(構)112年度資通安全通報演練計畫」演練作業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，委請專業資安講師親自講授相關課程，如「防範惡意電子郵件社交工程」、「淺談物聯網之資安防護」、「資訊作業營運持續管理」、「後疫情時代遠距辦公」、「數位轉型下資安新思維」及「近期資安新知分享」等，並提供同仁線上學習資訊安全教育訓練課程。另為加強同仁資訊安全觀念，每月進行資安宣導月報，112年度辦理活動包含一般使用者與主管計475人接受3小時線上資訊安全宣導課程並通過課程量、資通安全專責人員3人已完成資通安全專業課程訓練15小時以上、資訊人員(不含資通安全專責人員)已完成資通安全專業課程訓練3小時以上、董事長、總經理及副總經理完成「財政部112年主管人員資通訊安全宣導活動」課程以及每月電郵提供各單位資訊安全宣導月報，並統計資通安全專責人員共計有5張資安國際證照或職能證照。

(三)資安觀念及設施強化：

本公司鑑於近期網路攻擊威脅日益升高，為確保電腦系統具有一定之安全防護能力，需由機房、伺服主機、用戶設備、網路及電子郵件等各層面提升防護設施，藉以實施技術面與管理面相關控制措施，以改善並提升網路及資訊系統安全防護能力，並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十三項客戶及公司機密資料之保密及安全防範控制之要求。現行整體資訊安全防護設施包含：實體安全管理、伺服器安全管理、使用者端資訊安全管理；另，公司面對日新月異之新型態資安威脅，公司亦持續強化各面向之資安防護設施，以降低資

安風險，112年度執行並完成之專案包含: VMware軟體增購暨三年更新授權維護案、10G邊際交換器採購案、磁帶館暨磁帶加密管理系統汰換案等。。

113年度除承接前一年度專案外，預計啟動新專案包含：檔案交換管理平台、客戶身份辨識技術發展、數據中台及壽險系統轉換評估案等，另有專人隨時查看F-Isac相關資安訊息並適時分享以強化本公司資訊人員資安相關概念。

## 四、投入資通安全管理之資源

(一)資通安全管理之資源，除上述相關措施外，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之經常門(費用)支出，112年投入資通安全管理之金額約16,656千元。

(二)最近年度因重大資通安全事件所受之損失近3年度並無重大資通安全事件發生。

(三)資通安全風險對公司財務業務之影響及因應措施倘日後發生重大資通安全事件情事，將依本公司資通安全事件管理要點之處理、通報、處理改善等規範辦理。