中国太平洋财产保险公司厦门分公司文件

厦太保产发〔2025〕6号

关于印发《太平洋产险厦门分公司科技风险管理实施细则》的通知

各机构、各部（室）：

为进一步加强分公司科技风险管理，根据国家金融监督管理总局《银行保险机构操作风险管理办法》（2023年第5号）、《关于印发修订后〈中国太平洋保险（集团）股份有限公司操作风险管理办法〉的通知》（太保发〔2024〕78号）、《关于印发修订后〈中国太平洋财产保险股份有限公司操作风险管理办法〉的通知》（太保产发〔2024〕205号）等相关规定，结合经营实际，特制定《太平洋产险厦门分公司科技风险管理实施细则》，现予以印发，请遵照执行。

特此通知。

中国太平洋财产保险股份有限公司

厦门分公司

2025 年 1 月 14 日

太平洋产险厦门分公司科技风险管理实施细则

第一章　总则

第一条　依据

为进一步加强分公司科技风险管理，根据《银行保险机构操作风险管理办法》《关于印发修订后〈中国太平洋保险（集团）股份有限公司操作风险管理办法〉的通知》（太保发〔2024〕78号）、《关于印发修订后〈中国太平洋财产保险股份有限公司操作风险管理办法〉的通知》（太保产发〔2024〕205号）等相关规定，制定本细则。

第二条　科技风险定义

本细则所称科技风险是由于信息科技系统存在问题以及网络安全事件造成损失的风险，包括法律风险，但不包括战略风险和声誉风险。

第三条　科技风险管理定义

本细则所称操作风险管理，是指根据分公司确立的科技风险管理目标，明确科技风险管理组织架构的设置与职责分工，各部门和岗位运用系统化、标准化的风险管理方法、工具和程序，对科技领域的操作风险进行识别、评估、控制和缓释、监测、报告的全过程。

第四条　科技风险管理目标

科技风险管理是全面风险管理体系的重要组成部分，目标是有效防范操作风险，降低损失，提升对内外部事件冲击的应对能力，为业务稳健运营提供保障。

第五条　科技风险管理基本原则

科技风险管理遵循以下基本原则:

（一）审慎性原则。科技风险管理坚持风险为本的理念，充分重视风险苗头和潜在隐患，有效识别影响风险管理的不利因素，配置充足资源，及时采取措施，提升前瞻性。

（二）全面性原则。科技风险管理覆盖各业务条线、各分支机构，覆盖所有部门、岗位、员工和产品，贯穿决策、执行和监督全部过程，充分考量其他内外部风险的相关性和传染性。

（三）匹配性原则。科技风险管理体现多层次、差异化的要求，管理体系、管理资源应当与机构发展战略、经营规模、复杂性和风险状况相适应，并根据情况变化及时调整。

（四）有效性原则。分公司应当以风险偏好为导向，有效识别、评估、控制和缓释、监测、报告所面临的科技风险，将操作风险控制在可承受范围之内。

第六条　适用范围

本细则是分公司科技风险管理的基本制度，适用于分公司辖下各单位。

第二章　科技风险治理和管理责任

第七条　管理架构

分公司建立与科技风险特点相适应的科技风险管理工作组，总经理为组长，信息科技分管领导为副组长，信息技术部、和财务部负责人为组员。

第八条　科技风险管理工作组职责

分公司科技风险管理工作组在总经理室授权下，负责组织实施

科技风险管理工作。主要职责包括:

（一）制定科技风险管理基本制度和管理细则;

（二）明确界定各单位的科技风险管理职责和报告要求，督促各单位履行科技风险管理职责，确保科技风险管理体系正常运行;

（三）全面掌握科技风险管理总体状况，特别是重大科技风险事件;

（四）为科技风险管理配备充足财务、人力和信息科技系统等资源;

（五）完善科技风险管理体系，有效应对科技风险事件;

（六）制定科技风险管理考核评价与奖惩机制;

（七）其他与科技风险管理相关职责。

第九条　信息技术部管理职责

信息技术部是分公司信息科技工作日常管理部门，是科技风险管理（数据安全管理除外）和网络安全工作的牵头部门和责任部门，具体承担以下职责:

（一）设立信息科技风险专职管理岗位及配备充足的资源，该岗位职责包括：根据公司信息安全管理规范制度及流程管理分公司产险专属应用系统的信息安全保障工作；负责分公司网络安全及应用安全管理工作，包括网络安全风险及漏洞隐患的识别、上报和处置；负责分公司业务运营安全（终端安全、数据安全、访问控制等）及应用系统全生命周期安全管理；协助总公司进行护网演练、攻防对抗实战演练、灾备演练等。

（二）负责制定网络安全和管理制度，履行网络安全保护义务，

执行网络安全等级和关键信息基础设施保护制度要求，采取必要的管理和技术措施，监测、防御、处置网络安全风险和威胁，有效应对网络安全事件，保障网络安全、稳定运行，防范网络违法犯罪活动。

（三）统筹科技风险管理，建立集中管理、分级负责的科技风险管理体系和汇报机制;

（四）跟踪科技风险监管政策与要求，拟定科技风险管理制度与规范，组织推动落实;

（五）统筹建立与优化科技风险管理平台，采集科技风险监测指标和数据，完善科技风险监测体系，防范科技风险。

（六）在科技架构规划、应用研发、项目管理、运行保障等科技工作中注意防范与化解科技风险。

第十条　财务部管理职责

财务部是科技风险管理中数据安全管理牵头部门，具体承担以下职责:

（一）负责制定数据安全管理制度，组织推动开展数据安全分类分级管理工作;

（二）组织推动各职能部门依据数据安全定级结果制定数据安全策略，采取差异化措施保护数据免遭篡改、破坏、泄露、丢失或者被非法获取、非法利用;

（三）组织开展数据安全相关法律法规、制度、流程执行情况的检查与评估工作。

第十一条　业务和管理部门职责

业务和管理部门加强各类业务系统授权和权限管理，并加强本部门员工行为管理，重点关注关键岗位员工行为。

第十二条　人力资源部职责

应明确各部门间职责分工，避免利益冲突；加强不相容岗位管理，有效隔离重要业务部门和关键岗位。

第十三条　法律合规部职责

法律合规部对科技风险管理进行日常监督。

第三章　科技风险管理流程和方法

第十四条　风险识别与评估

信息技术部根据科技风险偏好，识别内外部固有风险，评估控制和缓释措施的有效性，分析剩余风险发生的可能性和影响程度，划定科技风险等级，确定接受、降低、转移、规避等应对策略，有效分配管理资源。

第十五条　重大变更评估

信息技术部应组织相关业务管理部门参照科技风险自评估标准，建立并执行科技风险的事前识别、评估流程，并将有关情况纳入科技风险管理报告:

（一）开发新业务、新产品;

（二）新设附属机构;

（三）拓展新业务范围、形成新商业模式;

（四）管理制度、业务流程、信息科技系统等发生跨机构、跨部门的管理职责变更;

（五）组织架构调整或部门职能变更;

（六）其他重大变更情形。

第十六条　业务连续性计划

信息技术部根据分公司相关工作部署，结合突发事件总体应急预案制定与业务规模和复杂性相适应的信息系统保障业务连续性计划，有效应对导致业务中断的突发事件，最大限度减少业务中断影响。按照相关应急预案组织开展突发应急预案演练评估，验证应急预案及备用资源的可用性，提高员工应急意识及处置能力，测试关键服务供应商的持续运营能力，确保业务连续性计划满足业务恢复目标，有效应对内外部威胁及风险。

第十七条　科技外包管理

信息技术部在涉及科技外包时应当明确与科技外包有关的风险管理要求，确保有严谨的科技外包合同和服务协议，明确各方责任义务，加强对外包方的监督管理。

第四章　科技风险信息沟通与报告

第十八条　一般科技风险事件

一般科技风险事件是指由科技风险引发，导致分公司发生实际或者预计损失的事件。

一般科技风险事件，最晚应在事件发生或发现次月 10 日前由信息技术部汇总上报总经理室及总公司科技创新中心。

第十九条　重大科技风险事件

分公司建立重大科技风险事件报告机制，及时向总经理室及总公司科技创新中心报告重大科技风险事件。

信息技术部应当知悉以下重大科技风险事件后，及时向总经理

室报告，并在24小时内报告总公司科技创新中心。分公司在知悉或者应当知悉以下重大科技风险事件5个工作日内，按照监管职责归属向国家金融监督管理总局厦门监管局报告:

（一）重要信息系统出现故障、受到网络攻击，导致营业网点、电子渠道业务中断3小时以上;

（二）重要网络设备故障、受到网络攻击，导致营业网点、电子渠道业务中断3小时以上;

（三）其他需要报告的重大科技风险事件。

第二十条　责任追究

各单位责任人对管辖范围内的科技风险负责，对违反科技风险管理办法相关规定，或者已经造成损失或影响的，根据公司规定追究相关责任，并对责任人、责任机构予以问责。

第五章　附则

第二十一条　印发与解释修订

本细则由信息技术部负责解释和修订，自印发之日起施行。

中国太平洋财产保险公司
厦门分公司办公室　　2025年1月14日 印发

编录：曾秀玲　　校对：邱丹丹