中国太平洋财产保险公司厦门分公司文件

厦太保产发〔2021〕33号

关于印发《太平洋产险厦门分公司网络安全管理办法》的通知

各机构、各部（室）：

为加强网络安全工作统筹管理，压实网络安全主体责任，降低操作风险，根据总公司《关于印发〈中国太平洋财产保险股份有限公司网络安全管理办法〉的通知》（太保产发〔2020〕224号）文件要求，结合分公司实际，特制定《太平洋产险厦门分公司网络安全管理办法》，现印发给你们，请认真组织学习并遵照执行。

特此通知。

中国太平洋财产保险股份有限公司

厦门分公司

2021年9月15日

太平洋产险厦门分公司网络安全管理办法

第一章　总则

第一条　为规范网络信息安全工作，切实推行网络安全管理，积极预防风险，完善控制措施，根据总公司《关于印发〈中国太平洋财产保险股份有限公司网络安全管理办法〉的通知》（太保产发〔2020〕224号）文件要求，结合分公司实际，特制订本管理办法。

第二章　网络安全工作组织及职责

第二条　分公司党委对网络安全工作负主体责任。总经理为第一责任人，分管网络安全的班子成员为直接责任人。主要承担的网络安全责任包括:

（一）认真贯彻落实党中央和习近平总书记关于网络安全工作的重要指示精神、决策部署及市委工作要求，贯彻落实网络安全法律法规，明确分公司网络安全主要目标、基本要求、工作任务、保护措施。

（二）建立和落实网络安全责任制，把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力支持和保障力度。

（三）统一组织领导本机构网络安全保护和重大事件处置工作，研究解决重要问题。

（四）采取有效措施，为公安机关、国家安全机关依法维护国家安全，侦查犯罪以及防范调查恐怖活动提供支持和保障。

（五）组织开展网络安全宣传教育，采取多种方式培养网络安

全人才，支持网络安全技术产业发展。

第三条　信息技术部负责网络安全归口管理工作，履行信息系统安全管理职责，主要承担的网络安全责任包括:

（一）加强网络信息安全、数据安全、开发安全的管控。

（二）确保信息系统安全稳定运行。

（三）建立完善网络安全应急预案、灾难备份及恢复计划，确保业务的连续性。

（四）加强对外包风险的统筹管理，建立外包服务及采购管理制度。

（五）将信息安全建设整改、运行维护、日常管理、检查评估等网络安全工作经费纳入年度信息化工作预算，相关费用执行应按年度网络安全工作计划开展。

（六）设置相应安全岗位，该岗位专业技术人员每人每年教育培训时长不得少于3个工作日。信息安全从业人员的网络安全教育培训，每人每年教育培训时长不得少于1个工作日。

（七）建立信息技术制度执行情况内控检查监督机制，确保各项监管要求、管理制度和要求的落实执行。

（八）建立完善的系统技术架构评审和系统需求分析机制，以确保信息化战略规划与业务发展目标保持一致。

第四条　所有员工须参加并完成网络安全意识培训。

第五条　将网络安全相关违规问题纳入内部责任追究制度，明确网络安全违规问责标准。

第六条　强化安全评估与准入机制。在引入新技术、开源技术

应用前，加强科技创新、新技术应用的风险监测与处置，防止因业务创新而导致降低安全管控的标准。

第三章 网络信息安全管理

第七条　信息技术部须将新开发的APP项目接入统一身份认证平台进行身份认证。

第八条　审计、合规检查的账号须遵循使用时间最小化原则，账号有效期不超过3个月，且仅授予查询权限。

第九条　应用系统中高权限账号须由应用系统业务归属部门审批授权，并由管理员负责维护，严禁未经许可给予他人使用。

第十条　多个用户使用同一个账户（共享），须明确账号责任人和使用原因，且有效期不超过1年。

第十一条　严禁擅自拆装分公司配发的终端设备，不得自行添加、拆除、更换或升级硬件。

第十二条　移动终端须启用硬盘锁功能，所有办公终端设备的账号和密码，不得转借他人或共用。密码须按照更新周期要求进行定期修改，保证强密码要求。

第十三条　妥善保管存放分公司相关资料和信息的U盘、移动硬盘和笔记本，避免丢失、被盗和损坏。

第十四条　终端设备如需委托第三方进行数据恢复，申请人需经所在部门负责人及信息技术部门负责人审核通过后，并在信息技术部指定人员陪同下进行。第三方恢复机构须提供相关资质证明，并签署保密协议。

第十五条　存放分公司相关资料和信息的U盘、移动硬盘和笔

记本，在进行维修更换前，须进行消磁处理。设备下线或报废须严格遵循相关流程。

第十六条　信息技术部须定期对全司打印机设备的运行状态及网络接口进行安全检查，及时记录和管理桌面终端、服务器、存储、网络及安全等设备信息、设备位置、使用情况等内容，并定期进行回顾。

第十七条　分公司配发的笔记本办公设备，不能安装与工作无关的软件、黑名单软件或盗版软件，不得将破解操作系统管理权限的终端接入内网，移动终端用户须从分公司指定的安全平台上下载、安装公司企业移动应用。

第十八条　接入内网的所有办公终端须符合网络准入标准。安装安全防护系统，包括防病毒系统、数据防泄漏系统和域控系统及网络准入客户端、安全补丁等，不得自行关闭或卸载，并通过代理服务器访问互联网，电子政务系统专用办公电脑不得与互联网连接。

第十九条　所有员工须通过太保云盘、分公司网盘备份系统等对重要信息定期进行备份，不得在无任何安全防护的终端设备上备份重要敏感信息，同时用户须通过分公司通讯途径（如UCStar、邮件系统等）传输、共享工作文件，其他通讯途径不得进行敏感信息的传输、共享。

第二十条　除工作需要外禁止使用分公司邮箱注册第三方网站、论坛或者在线服务等第三方平台的行为。

第二十一条　IT外部人员、非正式员工须使用“云桌面”进行

日常办公和运维，不得拥有信息数据在本地或互联网交互的权限。

第二十二条　信息系统开发项目生命周期中的立项、可行性分析、需求制定、方案设计、程序开发、系统测试、系统验收、使用培训、操作和维护等各环节须加强管控力度。

第二十三条　员工不得将客户个人信息存放在个人电子设备或U盘等存储媒介中。未经脱敏、加密情况下，不得将客户个人信息提取到IT系统生产环境之外。

第四章　运营保障及业务连续性管理

第二十四条　网络边界防护设备应配置正确的日期与时间，并设置时间同步，用户认证须符合安全标准，内置账户不得存在缺省密码或弱口令。

第二十五条　网络边界防护设备须具有登录失败处理功能，如结束会话、登陆失败时阻断间隔、限制非法登录次数和登录连接超时自动退出等措施，同时定期对网络边界防护设备的配置进行备份，并妥善保存配置文件。

第二十六条　严格限制通信的IP地址、协议和端口，根据需求控制源主机能够访问目的主机和控制源主机不能访问目的主机。

第二十七条　须对全司系统采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定保存不少于六个月的相关网络日志。

第二十八条　加强对信息系统开发质量的改进，对被监管机构或第三方通报的漏洞情况进行集中管理（含漏洞统计、分析、整改），具体包括:

（一）加快修复系统漏洞，以强化系统安全稳定性，对中危及以上等级漏洞及时修复率开展考核。

（二）监管单位及第三方发现的漏洞应第一时间修复或下线处理，不得超过24小时。

（三）内部发现的高、中危漏洞应第一时间修复或下线，原则上高危漏洞修复时效不超过5天、中危漏洞修复时效不超过2周；通用型高危漏洞原则上5天内完成修复。

第二十九条　所有应用升级发布前必须完成安全检测，无高中危遗留漏洞才能发布上线。

第三十条　建立网站内容发布规范和第三方链接的备案制度，明确相关职能部门的职责和分工，对发布内容和链接进行审批和审核。

（一）内容发布应确保合法合规并符合集团管理规范，发布前应包括内容提交、业务确认、内容审核三个环节，并保留详细操作记录、操作人员信息等内容，以备审查和追溯。

（二）对第三方链接进行备案，全面落实网站内容和第三方链接的全生命周期管理。

（三）建立第三方链接长效管控机制，针对各类链接进行定期回顾，对各类无效的、变更的链接及时在CIMS中进行清理。

（四）对于业务营销、推广等活动所发布的外部链接，业务需求方应在活动结束后组织相关外部链接的下线工作。

第三十一条　互联网应用收集、使用客户数据须符合集团客户数据安全负面清单要求，且不得违反《中国太平洋保险（集团）股

份有限公司数据防泄漏管理办法》（太保发〔2017〕55号）。

第三十二条　建立完善网络安全应急预案，明确网络安全应急响应组织体系、职责分工和人员团队。

第三十三条　每年至少组织演练一次IT应急预案，演练方式包含桌面推演、实战演练，可按照由模拟到实际、从易到难、从局部到整体的原则进行测试和演练。

第五章　外包采购管理

第三十四条　加强对外包风险的统筹管理，充分识别科技外包风险，明确外包范围和责任边界，严守“安全管理责任不外包、安全标准不降低”的风险底线。

第三十五条　建立外包服务管理制度，明确外包服务管理的责任人或责任部门，规定外包服务机构选择、外包合同和保密协议订立、服务水平协议和服务水平监控、合同履约情况评价等要求。

第三十六条　加强对外包服务机构和人员的安全管理，严禁自带设备存储公司数据，防止重要信息或源代码等敏感信息外泄。

第三十七条　采购管理文档中，需包括网络产品和服务采购的完整记录，所采购的网络关键设备和网络安全专用产品，应按照相关国家标准的强制性要求，通过具备资格机构的安全认证或安全检测，同时须包括与网络产品和服务提供者签订安全保密协议。

第三十八条　驻点外包人员账号权限有效期不超过合同约定服务时间，为防止冒名顶替情况，应当定期进行抽查，注销僵尸账号。账号有效期不超过1年，如需继续使用须重新申请。

第三十九条　内部员工离职应及时删除或失效该用户的主账

号，其担保的外部人员账号应同时失效或变更担保人。

第六章　附则

第四十条　本办法由分公司信息技术部负责解释。

第四十一条　本办法自印发之日起施行。

内部发送：　总经理室。	
中国太平洋财产保险公司 厦门分公司办公室	2021年9月16日印发
编录：曾秀玲	校对：邱丹丹