中国太平洋财产保险公司厦门分公司文件

厦太保产发〔2025〕1号

关于印发《太平洋产险厦门分公司金融专网安全管理实施细则》的通知

各机构、各部（室）：

为强化金融专网安全管理，规范金融专网技术标准，防范网络安全风险、保障金融专网数据安全、信息系统安全，根据《中华人民共和国网络安全法》、《中国银保监会金融专网安全管理办法》、《中国人民银行金融城域网入网管理办法》（银办发〔2011〕158号）、《关于印发〈中国太平洋保险（集团）股份有限公司金融专网安全管理办法〉的通知》（太保发〔2024〕92号）文件规定，结合分公司实际，特制定本细则，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3日

太平洋产险厦门分公司金融专网安全管理实施细则

第一章　总则

第一条　为强化金融专网安全管理，规范金融专网技术标准，防范网络安全风险、保障金融专网数据安全、信息系统安全，根据《中华人民共和国网络安全法》、《中国银保监会金融专网安全管理办法》、《中国人民银行金融城域网入网管理办法》（银办发〔2011〕158号）、《关于印发〈中国太平洋保险（集团）股份有限公司金融专网安全管理办法〉的通知》（太保发〔2024〕92号）文件规定，特制定本细则。

第二条 本细则所称“金融专网”是指机构连接接入金融监管总局和国家金融监督管理总局厦门监管局的非涉密数据通信网络，用于采集传输保险业数据，主要满足保险业监管业务、政务服务等需要。

第三条　分公司金融专网按照产险总公司的规划进行建设和管理，并接入国家金融监督管理总局厦门监管局或中国人民银行厦门分行金融城域网。分公司以下单位原则上不建设金融专网，如有报送需求，应通过分公司金融专网进行报送，并做好网络隔离。

第四条　分公司全体员工应遵守保密义务，保护金融专网相关的数据安全，包括不限：业务数据、客户数据、交易数据、运营数据及各类衍生数据等。任何未经授权的披露、传输、使用或允许他人使用行为均被严格禁止。

第二章　职责分工

第五条　信息技术部负责牵头落实产险金融专网相关工作，履

行以下职责:

（一）建立健全金融专网安全管理实施细则与技术规范。

（二）制定并完善机构金融专网的管理机制、工作流程。

（三）遵照监管及集团与产险总公司管理要求，牵头落实金融专网的建设与运维工作，原则上分公司金融专网部署在分公司机房。

（四）牵头分公司金融专网资产台账的建立及维护工作包括:线路信息、网络设施、前置服务器、安全设施、人员信息等。

（五）配合产险总公司开展金融专网应急预案的制定，定期开展应急演练。

（六）对标产险总公司管理要求严格落实“专网专用、专机专用、专人管理”的金融专网管理要求，对接入本单位金融专网的设备加强运维监控和安全管理。

（七）每年第四季度开展本单位及辖内机构金融专网安全运维巡检与自查，并牵头落实各项整改措施；对于巡检与自查过程中，发现金融专网安全隐患、故障及安全事件，留存各环节记录佐证，并向产险总公司科技创新中心上报。

第六条　信息技术部负责牵头落实全辖金融专网管理要求，严格遵守“服务外包，责任不外包”的原则履行以下职责:

（一）按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”原则，明确和落实本单位金融专网的管理方、运维方、使用方;

（二）严格落实“专网专用、专机专用、专人管理”的金融专网管理要求，对标总部管理办法，建立健全本机构金融专网管理细则，责任落实到人。

（三）根据国家金融监督管理总局厦门监管局具体要求配合总部完善优化技术规范。

（四）负责本单位金融专网资产管理，包括：线路信息、网络设施、前置服务器、安全设施、终端信息、人员信息等，并按总部要求进行登记和更新;

（五）负责金融专网区域接入终端的日常安全管理，及时处置各类安全风险隐患，确保符合集团、产险总公司安全标准后接入金融专网。

（六）负责制定本单位金融专网应急预案，定期开展演练，确保每年至少一次演练并留存演练记录。

（七）每季度参照《金融专网安全自查清单》(附件1)，对全辖金融专网相关设施安全开展巡检与自查，并落实各项整改措施；对于巡检与自查过程中，发现金融专网安全隐患、故障及安全事件，应留存检查记录、整改佐证并及时向上级单位上报。

第三章　金融专网网络安全管理

第七条　金融专网不得直接或间接与公众互联网连通，应在网络边界上实施严格的安全隔离措施。

第八条　金融专网与其他网络之间应有清晰的网络边界，各网络之间必须严格隔离控制，专用终端所在VLAN应进行单独划分。

第九条　金融专网边界防火墙策略应按“最小必要”原则，以白名单方式进行双向访问控制，不得在无实际需求的情况下使用无关设备访问金融专网。除监管机构要求的访问目标地址和目标端口之外，应按最小化原则开放权限。

第十条　金融专网区域应部署入侵防御系统（IPS）等安全防护设备，对入侵金融专网的各类行为进行监控、预警、阻断，以防止未授权的访问和网络攻击，并定期更新威胁特征库正确启用策略确保其有效性，并按要求留存日志记录。

第十一条　应根据监管要求，对金融专网终端内网访问范围进行控制，在核心交换机、网关、本机防火墙等上实施访问控制策略，确保金融专网终端有限访问企业内网应用，若监管有其它规定的则遵照监管要求执行。

第十二条　金融专网终端、网络、安全等设备应开启日志记录功能，日志留存不得低于6个月，相关设备配置统一的NTP服务器以确保日志记录包含正确的时间，准确记录设备登录、维护操作等关键信息，确保维护操作可追溯。

第十三条　严禁在未经审批的情况下私自对涉及金融专网的网络区域、终端设备、网络设备等进行任何形式的安全扫描。

第四章　金融专网终端安全管理

第十四条　金融专网终端应落实专机专用不得用作与监管无关的工作，不得擅自改变使用用途，应使用固定IP地址，禁止随意变更。

第十五条　终端不允许访问互联网，应在代理服务器或防火墙上对专用终端进行技术性限制，禁止其访问。

第十六条　终端禁用不必要的网络服务、禁止公用账户、设置高强度密码策略等。

第十七条　终端须对移动存储介质进行管控，应只可访问授权

的移动存储介质设备。严禁未授权的、带有病毒或恶意程序的移动存储设备接入。存储介质专用，专人保管，不允许传递非金融专网工作相关资料，禁止在与报送工作无关的办公终端以及非公司终端中使用。

第十八条　终端应严格按照集团终端安全管理要求进行标准化安装，接入交换机启用DOT1X强准入功能，对接入终端进行严格控制，准入条件包括不限：联软、防病毒、DLP、域控等。若机构采取纯物理隔离方式的，准入方式可选择使用MAC/IP地址绑定等控制措施。

第十九条　金融专网终端应禁止附带或使用无线接入功能，严禁备使用双网卡或跨网接入金融专网。

第二十条　金融专网敏感数据的存储应采用加密措施，防止未授权访问和数据泄露。定期对存储系统进行安全检查和维护，确保其安全性和可靠性。

第二十一条　金融专网的应用软件采取白名单管理，分公司所有安装的非白名单应用软件须通过分管领导审批，禁止安装无关软件、禁止存放无关资料文档。

第二十二条　金融专网终端和服务器设备须安装统一的防病毒、日志审计等安全防护软件，及时更新防病毒软件引擎和特征库，防病毒策略不得随意更改，并定期对设备的安全配置进行审查和更新，以应对新的安全威胁。若采用物理隔离方式的，应通过离线方式定期对金融专网区域的终端、服务器、安全设施等进行特征库更新、扫描、加固。

第五章　金融专网前置服务器管理

第二十三条　根据要求设置金融专网前置服务器，应落实专机专用，不得用作与监管无关的工作，不得擅自改变使用用途，应使用固定IP地址，禁止随意变更。

第二十四条　前置服务器必须放置于分公司机房中。且前置服务器不允许访问互联网，禁止附带或使用无线接入功能，严禁使用多网卡或跨网，必须置于金融专网防火墙DMZ区中。

第二十五条　前置服务器应严格遵循金融专网安全技术基线标准，包括禁用不必要的网络服务、禁止公用账户、设置高强度密码策略等。

第二十六条　前置服务器禁止使用任何移动存储介质。且前置服务器不得存放数据。

第二十七条　前置服务器应使用正版windows server或统信UOS server版操作系统。前置服务器如安装window server操作系统，应严格按照集团、产险总公司终端安全管理要求进行标准化安装，包括不限：联软、防病毒、DLP、域控等。并及时更新防病毒软件引擎和特征库，防病毒策略不得随意更改，并定期对设备的安全配置进行审查和更新，以应对新的安全威胁。

第二十八条　前置服务器如安装统信UOS系统，应只部署Nginx应用，按照金融专网Nginx前置机安装模板进行配置。按照前置机操作系统安装及配置文档进行加固。

第六章　附则

第二十九条　本细则由信息技术部负责解释和修订。

第三十条　本细则自颁布之日起施行。

中国太平洋财产保险公司 厦门分公司办公室	2025年1月3日 印发
编录：曾秀玲	校对：邱丹丹