中国太平洋财产保险公司厦门分公司文件

厦太保产发〔2024〕37号

关于印发修订后的《太平洋产险厦门分公司信息系统账号权限管理实施细则》的通知

各机构、各部（室）：

为贯彻落实法律法规和监管要求，进一步规范公司信息系统用户管理工作，加强用户账号的集中管理和统一认证，现将修订后的《太平洋产险分公司信息系统账户权限管理细则》印发给你们，请学习并遵照执行。

特此通知。

中国太平洋财产保险股份有限公司

厦门分公司

2024年8月12日

太平洋产险厦门分公司用户账号权限管理实施细则

第一章　总则

第一条　为建立集中式的用户管理体系，对信息系统的用户账号权限规划、建设和管理提供指导和依据，明确管理原则，避免或降低用户管理缺陷带来的风险，使用户更安全、更高效地使用公司的信息系统资源，特制订本细则。

第二条　本细则适用于全司信息系统用户和权限管控。公司信息系统具体包括：各业务应用系统、主机（服务器操作系统/数据库/中间件）、网络设备（交换机/路由器/ACS等）、安全设备、云平台及云虚拟资源等。

第三条　公司信息系统用户管理工作遵循以下原则：

（一）实名制：用户的账号须做到实名制；

（二）必要性：用户权限管理需遵循最小权限原则；

（三）合理性：用户权限的设置需与岗位职责相匹配；

（四）有效性：离职转岗人员的账号须及时删除、失效或权限调整。

第二章　术语与定义

第四条　本细则涉及的术语与定义主要包括：

（一）用户：指使用公司信息系统的用户，包括内部员工、外勤人员和外部人员，不包括客户；

（二）内部员工：以个人身份和公司签订正式劳动合同，由人力资源部集中管理的人员，及在公司人力资源部正式注册的劳务派遣人员；

（三）外勤人员：指与公司签约保险服务合同，从事公司外部经营活动的人员。如同时和公司签订了劳务合同，账号管理视同内部员工;

（四）外部人员：未与公司签订劳动合同或保险服务合同，与公司有工作合作关系的人员。外部人员主要包括：外部供应商、外部合作伙伴、监管部门人员等;

（五）账号：指在信息系统中注册创建，具备对信息系统进行特定的访问操作权限的主体;

（六）主账号：指用户在公司信息系统中的身份管理标识，与实际人员一一对应;

（七）从账号：指用户具体使用某信息系统，具备特定的权限的主体，与用户主账号关联;

（八）权限：指用户通过账号能够访问的信息系统资源，以及在系统中能够进行的操作等;

（九）角色：是一个表达访问控制策略的语义结构，它可以表示承担特定工作的资格，一般一个角色是单个系统权限或者数个系统权限的组合;

（十）岗位职责：指用户在各业务部门中真实的工作内容或角色，各业务部门在人力资源部定义的岗位职责基础上根据实际的工作分配进行细化;

（十一）授权矩阵：体现用户及其对应的岗位职责关系的列表;

（十二）认证：通过有效的行为或流程操作来确认访问系统主体的身份真实性;

（十三）授权：通过有效的行为或流程操作来决定，访问系统主体按照相关岗位职责或制度被许可访问什么样的资源及进行什么样的操作。

（十四）账号权限管理员：由各部门指定账号权限管理人员，负责本部门的用户账号权限日常管理。

第三章　职责与分工

第五条　分公司信息技术部负责用户权限管理的规范，具体职责为:

（一）制定分公司信息系统账户权限管理制度;

（二）制定信息系统用户认证和授权相关的安全要求;

（三）组织分公司账号权限定期审阅工作

（四）负责分公司人员离职的账号注销。

第六条　各部门账号权限管理员负责本部门的用户管理和权限管理工作，具体职责包括:

（一）负责本部门内、外部人员的账号权限增、删、改任务的申请及审核;

（二）系统所属业务部门负责该系统权限的审阅工作，进行权限梳理、审核与反馈;

（三）系统所属业务部门负责建立和维护角色授权矩阵，负责根据内部控制要求建立和维护不相容职责矩阵。

第四章　用户集中管理规范

第七条　对于公司信息系统，用户账号管理分为以下内容:

（一）身份注册

用户身份注册需要遵循统一标准的流程进行相应操作。注册时用户须实名制，要提交必要的个人信息。内部员工和外勤人员的注册信息的内容至少包括：姓名，工号，身份证，手机号码。外部人员的身份信息的维护由其内部合作部门负责信息的完整性、准确性和及时性。

（二）用户账号创建

用户主账号与实际人员对应，每人一个。用户在集中认证系统（P13）中设定的账号是用户的主账号。针对应用系统，账号权限管理员需根据用户的工作部门和岗位，为用户在主账号下建立关联的从账号，主账号与从账号应建立严格的对应关系。主账号和从账号对应关系表须集中管理。

（三）用户身份标

1、每个系统的用户标识（例如User ID，证书）需能代表某个系统的用户。每个账号需要有一个所属人;

2、内部用户主账号命名符合以下的规则:

（1）身份标识基本规则为员工的姓名全名拼音;

（2）用户身份标识出现重名时，采用重名冲突规则解决。用户身份标识超长时，采用超长规避规则处理。

（四）账号口令管理

1、口令需满足《关于印发〈中国太平洋保险（集团）股份有限公司应用系统信息安全管理办法〉的通知》（太保发〔2022〕27号）中的密码相关要求;

2、确保口令的保密性，口令禁止共享。

（五）账号的使用

账号持有人应妥善保管和使用账号，因个人管理和使用账号不当原因造成的公司损失，由账号持有人承担。

第八条　信息系统用户访问系统资源前，必须经过用户认证。

（一）自建应用系统须接入集中认证管理系统，外购成品软件应优先考虑接入集中认证管理系统;

（二）对于已经纳入集中认证的业务系统，其认证由集中认证系统完成，应采用单点登录SSO的方式实现对应用资源的访问。同时对于有较高认证强度要求的系统，须根据用户访问的具体需要配置相应强度的认证方式（如双因素认证），整体实现分级认证;

（三）对于纳入集中认证的主机操作系统、数据库、中间件，其认证也由集中管理平台的认证模块完成;

（四）对于没有纳入集中认证的业务系统、主机操作系统、数据库、中间件、网络和安全设备等，其认证口令也必须满足公司信息安全技术标准中关于口令的安全要求。

第九条　用户权限管理遵循主管负责制、集中管理、授权标准化、最小化权限的原则。

（一）主管负责制是用户所在部门或机构对账号权限创建和分配的必要性、真实性、有效性负责;

（二）集中管理是自建应用系统的用户权限都须纳入集中权限平台进行统一管理;

（三）授权标准化是指公司应用系统的授权必须采用标准化管理，建立授权矩阵;

（四）最小化权限是指用户所在部门主管应根据岗位职责、业务实际需要分配权限，严格禁止权限滥用。

第十条　用户权限管理应当符合以下要求:

（一）公司须根据实际情况，对用户进行分类，并制定对应的管控策略。系统技术维护人员、公司内部审计人员、合规检查人员、外部检查人员及业务操作人员应在系统中具有不同的权限和管控要求;

（二）系统账号包括应用系统账号和基础设施账号。分为高权限账号及普通账号，高权限账号包括: 具有系统的参数变更、功能配置及所有业务操作权限的账号，即admin或super admin等系统管理员账号; 可对系统中普通账号、角色及权限进行维护操作的账号。普通账号为高权限账号以外的所有账号。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，并应由应用管理员负责维护，严禁未经许可给予他人使用。

（三）公司应用系统应建立岗位职责和应用系统角色、权限的对应关系，即授权矩阵“岗位-角色-权限”清单，由各应用系统所属业务部门建立和维护;

（四）用户的直接主管是用户权限申请的审批人和责任人;

（五）在用户权限发生变动时，原则上应通过“角色”的调整进行变更，而不可直接调整该用户角色对应的权限;

（六）在用户权限发生变动时，各应用系统所属业务部门应调整和维护不相容职责矩阵，通过系统角色授权予以限制。

（七）公司自建应用系统须接入账户权限管理系统，采用自动化的审批工作流完成用户账号和权限的相关申请及审批工作。外购成品软件应优先考虑接入账号权限管理系统;

（八）对于未纳入集中账号权限管理的主机操作系统、数据库、中间件、网络和安全设备等基础设施账号，相应的账号权限管理人员应确保用户权限的管理遵循安全要求，权限变动均应通过审批，并做到可追踪、可审计，确保系统中账号及权限的设置准确性。

第十一条　外部人员的账号权限管理还应当符合以下要求:

（一）申请账号权限，应由内部合作部门申请;

（二）申请必须注明账号使用期限（最长一年），并每年对外部人员账号进行回顾;

（三）外部供应商人员离岗、外部合作伙伴解除合作关系、监管部门人员工作完成时，公司内部合作部门应及时申请账号删除。

第五章　用户账号生命周期管理

第十二条　公司建立和维护用户账号生命周期管理机制，保障信息系统账号权限的安全管理。用户账号生命周期管理主要包括创建、变更、注销、审阅等环节和流程，具体步骤和规则按照《账号生命周期管理流程》（详见附件）执行。

第十三条　各部门用户账号创建应当落实以下安全管理要求:

（一）每个系统的业务所属部门须根据系统重要性和业务属性制定用户账号的审批流程;

（二）人力资源部应在各部门员工入司的第一时间完整注册用户信息，为其申请主账号;

（三）员工所在部门的账号权限管理员负责根据员工的岗位职责，进账号权限系统中申请相关权限;

（四）外部人员申请账号，须由内部合作部门申请，并明确告知信息技术部室外部人员使用。

第十四条　各部门用户账号变更、注销应当落实以下安全管理要求:

（一）各部门用户转岗，必须及时调整用户权限;

（二）公司内部员工、外勤人员离职，信息技术部账号权限管理员须对该员工各系统里的账号及权限进行检查后及时提请注销。

（三）外部人员结束在公司的服务工作时，内部合作部门的账号权限管理员应及时申请账号注销。

第十五条　分公司积极组织开展用户和权限的审计和审阅。

（一）用户日志审计。应用系统在用户管理过程应具备完备的日志审计功能，应用系统日志和审计要求按照《关于印发〈中国太平洋保险（集团）股份有限公司应用系统信息安全管理办法〉的通知》（太保发〔2022〕27号）执行。

（二）账号权限审阅。分公司应每年至少开展一次账号权限审阅工作。账号权限平台应具备自动化功能，对长期不活跃账号采取自动通知或冻结等措施，防止僵尸账号的产生。

第六章　附则

第十六条　机构和员工违反用户账号权限管理规定，存在违规行为的，按照分公司相关责任追究制度实施责任追究。

第十七条　本细则自发布之日起施行，《中国太平洋财产保险股份有限公司厦门分公司应用系统人员授权审批管理办法（2017年修订）》（厦产函〔2017〕-91号）即时废止。

第十八条　本细则由信息技术部负责解释及修订。

附件：账号生命周期管理流程

中国太平洋财产保险公司 厦门分公司办公室	2024年8月12日 印发
编录：曾秀玲	校对：邱丹丹