《金融信息协同平台建设安全管理规范》
团体标准编制说明

一、立项的意义

（一）填补监管空白，响应创新需求

金融信息协同平台涉及跨机构数据共享与系统联动，传统国标/行标制定周期长，难以及时覆盖新技术（如跨境数据流动、多方安全计算等）。团体标准凭借快速响应机制，能率先建立安全基线，为平台架构设计、数据加密、访问控制等提供规范指引，避免市场无序发展。例如，明确数据分级（核心/重要/一般数据）与脱敏要求，可衔接《银行保险机构数据安全管办法》的合规需求。

（二）促进行业协同，降低协作成本

当前金融机构间存在技术壁垒与信任成本。该标准通过统一安全接口与责任划分（如数据共同处理时的权责协议），推动建立跨机构“安全防火墙”，减少重复开发与兼容性问题。同时，为中小金融机构提供可落地的安全框架，缓解其技术能力不足的痛点，提升全行业协同效率。

（三）强化风险防控，提升安全水位

金融信息协同场景中，数据泄露、非法访问等风险突出。标准通过全生命周期安全管理要求（如数据加密传输、审计监控、应急响应等），系统性防控风险。

二、本标准适用范围及概要

（一）适用范围

本标准适用于指导金融信息协同平台建设的安全管理工作，主要面向由金融机构搭建，用于实现内部及相互间、与客户间信息交互、业务协同处理，涵盖数据传输、存储、处理等功能模块，支持多种金融业务开展的金融信息协同平台。

（二）概要

本标准围绕金融信息协同平台建设的安全管理，从管理原则、平台使用安全、权限管理、数据管理、系统维护与升级、安全处理等方面提出具体要求，旨在保障平台安全合规运行，促进金融业务协同高效开展。具体内容如下：

（一）管理原则

1.合规性原则

严格遵守国家金融监管规定、法律法规及地方金融政策，确保平台数据全生命周期符合《个人信息保护法》，定期开展合规审计并动态跟踪监管政策。

2.安全性原则

构建“技术+管理”双重防护体系，技术层面采用系统互联技术。系统部署在长三角数字金融数据中心；管理层面建立全员安全责任制度，明确数据泄露、系统漏洞等风险的应急响应流程，定期开展攻防演练。

3.高效性原则

通过流程自动化（如智能审批引擎）、数据标准化（统一接口规范）及系统性能优化（服务器负载均衡等）提升协同效率。

4.适应性原则

根据金融行业发展、技术进步以及苏州市金融市场特点，每年对平台安全策略进行全面评审，适时调整和完善平台管理规范。

（二）平台使用安全要求

1.账号管理

创建与激活：专人创建账号，双人复核激活，账号命名规则统一，合作机构账号绑定内部对接人并及时删除。

密码设置：强制修改初始密码，要求高强度密码（8位以上、多类型字符），定期更换，异常时及时重置。

账号保护：设备绑定与异常登录预警，禁止转借账号，泄露需承担责任。

2.登录与操作

登录限制：限制同一账号登录终端数量，连续三次输错密码自动锁定。

操作规范：按流程操作，关键操作双人复核，日志保存不少于5年。

操作时限：业务审批（紧急1小时、一般24小时）设置时效要求。

3.信息发布与共享

发布审核：智能检测敏感内容，三级审核机制（部门初审、负责人复审、合规部门终审）。

内容安全：确保信息真实合法，禁止发布虚假、涉密信息。

（三）权限管理

1.权限分类与设置

功能权限：按最小化原则分配，细分基础、高级、管理功能，建立权限互斥规则。

数据权限：按绝密、机密、秘密、公开分级，对应不同访问与操作权限（如绝密级仅限高管在线查看）。

2.权限申请与审批

线上申请流程，智能审批引擎区分风险等级，中高风险需人工逐级审批，审批失误追责。

3.权限变更与回收

岗位变动及时调整权限，离职/调岗立即回收账号，退休人员保留部分查询权限。

（四）数据管理

1.数据分类与分级

围绕数据分类分级的原则、具体分级标准、动态调整的触发条件与流程、权限更新方式等内容进行扩展，使数据分类分级管理更具系统性和可操作性。

2.数据存储与备份

敏感数据加密存储，每周全量备份、每日增量备份，定期测试恢复。

3.数据安全与保密

建立泄露溯源机制，构建多层级的数据追踪体系。在数据产生环节，为每一份数据赋予唯一的数字标识，包含数据创建者、创建时间、敏感等级等元信息，如同为数据贴上专属“身份证”；数据传输过程中，采用加密隧道与访问控制技术，在网关、防火墙等网络节点部署流量监测探针，实时记录数据流向、访问请求与传输路径；存储阶段，对数据库操作进行细粒度审计，完整记录数据的增删改查操作，精确到操作人、操作时间和具体操作内容。

（五）系统维护与升级

1.日常维护

实时监控系统的架构搭建、监控指标细化、每日巡检的具体流程、故障分级标准以及不同级别故障处理的详细流程等方面展开扩写，让监控运维体系更完善；详细说明系统监控和故障处理的各环节。

2.系统升级

升级前从兼容性、风险等维度评估，制定含时间节点与责任人的计划及回退方案；升级后按功能、性能等维度全面测试，确保系统稳定

3.用户响应

问题需24小时内响应，按分级限时解决：一级问题2小时内处理，复杂问题根据实际情况明确解决时限，确保问题妥善处理。

（六）安全处理要求

1.违规行为界定

分为技术安全、数据合规、协同操作三类违规，按情节轻重划分为轻微、严重、重大等级，便于精准处置各类违规行为。

2.处理措施

轻微违规警告整改，严重违规处罚通报，重大违规追究法律责任并赔偿。

三、国内外相关标准情况

（一）国内标准

信息安全等级保护相关标准：国家标准《信息安全技术网络安全等级保护基本要求》（GB/T 22239）是信息安全等级保护的基础标准。金融行业也有自己的等级保护标准，如JR/T 0071—2012《金融行业信息系统信息安全等级保护实施指引》、JR/T 0072—2012《金融行业信息系统信息安全等级保护测评指南》和JR/T 0073—2012《金融行业信息安全等级保护测评服务安全指引》，对金融行业信息系统的安全建设、测评等进行了规范。

数据安全相关标准：国家标准《数据安全技术 数据分类分级规则》（GB/T 43697—2024）为数据分类分级提供了指导。行业标准《个人金融信息保护技术规范》（JR/T 0171—2020）则针对个人金融信息的保护提出了具体要求。

金融信息服务相关标准：GB/T 36618—2018《金融信息服务 安全规范》针对金融信息服务提供商的内部管理及安全技术提出了基本要求，包括准确性、完整性、可用性等方面。

（二）国外标准

信息技术安全性评价通用准则（CC）：由美国国家安全局和国家技术标准研究所联合加、英、法、德、荷等国编制，是国际上广泛认可的信息技术安全评估标准，为信息系统和产品的安全性评估提供了通用的框架和方法。

信息保障技术框架（IATF）：由美国国家安全局（NSA）发布，强调从人员、技术和操作三个层面，采用多层防御的策略来保障信息系统的安全，对金融信息协同平台的安全体系建设具有一定的参考价值。

欧盟《通用数据保护条例》（GDPR）：对数据主体的权利、数据控制者和处理者的义务、数据保护的原则等方面做出了详细规定，在数据保护方面要求严格，对于涉及欧盟市场的金融信息协同平台，需要遵循该条例的相关要求。。

四、标准编制原则和主要技术内容确定的依据

（一）标准编制原则

合规性原则：严格遵循国家及金融监管部门颁布的法律法规，如《数据安全法》《个人信息保护法》以及《网络数据安全管理条例》等，确保团体标准在合法合规的框架内制定，使金融信息协同平台的安全管理要求与国家法律规定保持高度一致，为金融机构落实安全责任提供坚实法律支撑。同时，充分参考现有国家标准、行业标准，像GB/T 22239《信息安全技术 网络安全等级保护基本要求》、JR/T 0071—2012《金融行业信息系统信息安全等级保护实施指引》等，保证本团体标准与上位标准体系的兼容性和连贯性。

全面性原则：从金融信息协同平台建设的全生命周期出发，涵盖规划、设计、开发、部署、运营、维护到废弃等各个阶段，对平台涉及的人员、技术、管理、流程等所有方面进行系统规范。无论是数据的采集、传输、存储、使用，还是平台基础设施安全、网络安全、应用安全等，均制定全面且细致的安全管理要求，避免出现安全管理漏洞与盲区，确保平台整体安全防护的完整性。

风险导向原则：深入分析金融信息协同平台面临的各类安全风险，如网络攻击、数据泄露、内部人员违规操作等，基于风险评估结果确定安全管理的重点领域与关键环节。针对高风险场景，制定更为严格、针对性强的安全控制措施，优先解决对平台安全影响最大的风险问题，合理分配安全资

源，实现以最小成本获取最大安全效益，提升平台抵御安全风险的能力。

实用性与可操作性原则：在标准制定过程中，广泛调研金融机构、科技企业等实际参与平台建设运营的主体，充分吸纳其在实践中积累的成熟经验与有效做法，使标准内容紧密贴合行业实际业务需求。标准条款避免过于抽象、笼统，力求具体明确、易于理解和执行，通过详细的操作流程、技术指标、责任界定等，为金融信息协同平台安全管理工作提供切实可行的指导，确保标准能够在实际工作中落地实施。

先进性与前瞻性原则：关注金融科技、信息安全领域的前沿技术与发展趋势，如人工智能、区块链在安全防护中的应用，以及新兴的网络安全威胁态势。将具有前瞻性、引领性的技术和理念融入标准，鼓励金融机构采用先进的安全技术与管理方法，提升平台安全防护水平，使标准不仅能够满足当前平台安全管理需求，还能为未来一定时期内平台安全建设的发展提供方向，保持标准的时效性与适应性。

（二）主要技术内容确定的依据

法律法规与政策文件：《数据安全法》明确了数据安全保护义务、数据安全管理职责等，为数据安全相关技术内容提供法律依据，促使标准对金融信息在平台中的全生命周期安全管理提出严格要求，包括数据分类分级、加密传输、存储安全等方面。《个人信息保护法》着重规范个人信息处理

活动，保障个人信息权益，基于此，标准确定了个人金融信息在协同平台中的特殊保护技术措施，如去标识化、匿名化处理要求，以及个人信息主体权利保障技术手段。《网络数据安全管理条例》细化了数据安全管理规范，促使标准在平台数据安全管理流程、安全评估技术方法等方面做出明确规定。

现有相关标准：借鉴GB/T 22239《信息安全技术 网络安全等级保护基本要求》中关于物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复等层面的技术要求，结合金融信息协同平台特点进行针对性调整与补充，确保平台安全技术防护符合等级保护基本规范。参考JR/T 0171—2020《个人金融信息保护技术规范》，确定个人金融信息在平台中的采集、传输、存储、使用、共享等环节的技术保护措施，如信息加密算法要求、访问控制技术手段等，保障个人金融信息安全。GB/T 43697—2024《数据安全技术 数据分类分级规则》为金融信息在协同平台中的分类分级提供了方法依据，标准以此为基础，结合金融行业数据特点，制定适用于平台的详细数据分类分级技术标准，为后续差异化安全管理奠定基础。

行业实践经验：金融机构在长期信息系统建设与运营中，积累了大量关于网络安全防护、数据安全管理的实践经验。例如，部分银行在内部信息协同平台建设中，采用了多因子

身份认证技术保障用户登录安全，在标准制定中可将此类成熟技术纳入身份鉴别技术要求；一些金融科技公司在数据共享过程中，通过区块链技术实现数据溯源与不可篡改，标准可参考其做法，确定在金融信息协同平台数据共享环节的区块链应用技术规范。同时，对行业内频发的安全事件进行深入分析，如某金融信息平台因数据接口安全漏洞导致数据泄露，针对此类问题，在标准中明确数据接口安全技术标准，包括接口访问控制、数据校验、安全审计等技术要求，以防范类似安全风险。

技术发展趋势：随着人工智能技术在安全领域的应用日益广泛，如利用机器学习算法进行异常行为检测、入侵防范等，标准充分考虑这一趋势，在安全监测与预警技术内容中，纳入人工智能技术应用规范，鼓励平台采用先进的智能安全技术提升安全防护能力。区块链技术凭借其去中心化、不可篡改等特性，在保障数据真实性、完整性及可信共享方面具有独特优势，标准据此确定在金融信息协同平台数据存储、共享环节的区块链技术应用框架与技术指标。云计算技术在金融行业的普及，使平台建设与运营模式发生变化，标准结合云计算特点，制定基于云计算架构的金融信息协同平台安全技术要求，如云平台租户隔离技术、云服务安全评估技术等，适应金融信息协同平台的技术发展潮流。

五、技术保障及工作进度计划

（一）技术保障

1.组建专业技术团队

汇聚金融机构信息安全专家、高校科研人员、网络安全企业技术骨干及行业协会代表，构建跨领域技术团队。金融机构专家提供平台建设运营的实际安全需求与痛点；高校科研人员凭借理论优势，分析前沿安全技术可行性；网络安全企业分享成熟的安全防护技术与解决方案；行业协会协调各方资源，确保团队高效协作，为标准制定提供全面的技术智慧支撑。

2.引入先进技术与方法

积极引入人工智能等前沿技术。利用人工智能算法对金融信息协同平台的安全数据进行智能分析，实现异常行为的实时精准识别与风险预警。

3.建立技术交流与反馈机制

定期组织技术研讨会、专家咨询会，邀请国内外金融信息安全领域专家参与，对标准制定过程中的技术难点、争议问题进行深入探讨。同时，建立线上反馈渠道，收集金融机构、相关企业在标准试用阶段的意见建议，及时跟踪行业技术发展动态，持续更新标准中的技术内容，保持标准的先进性与适应性。

（二）工作进度计划

1.筹备阶段（第1-2个月）

成立标准编制工作组，明确各成员职责分工；开展广泛的行业调研，收集国内外相关标准、政策法规及金融信息协同平台安全管理实践案例；组织专家研讨，确定标准编制的总体框架、基本原则与主要技术方向，形成标准草案大纲。

（二）草案编制阶段（第3-5个月）

依据大纲，分章节撰写标准草案内容，重点明确平台建设安全管理的技术要求、管理流程、人员职责等。编制过程中，加强团队内部沟通协作，定期召开内部评审会，对草案内容进行讨论修改，确保草案内容的完整性、准确性与逻辑性。

（三）征求意见阶段（第6-7个月）

将标准草案发送至金融机构、行业协会、科研院所、相关企业等广泛征求意见。通过线上问卷、线下座谈会等多种形式，收集各方反馈意见，并对意见进行分类整理、分析研究，根据合理建议对草案进行修改完善，形成标准征求意见稿。

（四）技术审查阶段（第8个月）

组织召开标准技术审查会，邀请行业权威专家组成审查委员会，对标准征求意见稿进行全面审查。专家从标准的合规性、科学性、实用性、可操作性等方面提出审查意见，编制工作组根据审查意见进一步修改完善标准，形成标准送审稿。

（五）批准发布阶段（第9个月）

将标准送审稿提交团体标准归口管理部门审批，根据审批意见进行最后的修改完善，完成标准的批准发布工作，并组织开展标准宣贯培训活动，推动标准在行业内的实施应用。

六、其他需要说明的内容

无。