ICS 03.060
CCS A 11

T/SZFCC

苏州市金融业商会团体标准

T/XXX XXXX—XXXX

金融信息协同平台建设安全管理规范

Security management specifications for the construction of financial information collaboration platforms

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

苏州市金融业商会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

金融信息协同平台建设安全管理规范

1 范围

本文件规定了金融信息协同平台建设的管理原则、平台使用安全要求、权限管理、数据管理、系统维护与升级及安全处理等要求。

本文件适用于指导依法设立的金融机构（包括银行、证券、保险、信托、期货、基金等）及经监管部门批准的金融科技合作机构建设、运维和使用金融信息协同平台的安全管理工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 39786 信息安全技术 密码应用基本要求

JR/T 0197 金融数据安全 数据安全分级指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

金融信息 financial information

在金融业务开展及协同过程中产生、传输、存储的各类数据与信息。

3.2

金融信息协同平台 financial information collaboration platform

基于分布式计算框架（Hadoop、K8s）和加密传输协议（TLS1.3），集成数据脱敏引擎、电子签章系统、操作日志审计系统等组件，实现内部及跨机构、客户间信息交互与业务协同的金融信息系统。

注：金融信息协同平台协同场景包括金融机构内部部门间的信息交互与业务协同；不同金融机构之间（如银行与保险、证券与基金）的跨机构业务协同；金融机构与客户（个人客户、企业客户）之间的信息交互与服务协同。

4 管理原则

4.1 合规性原则

4.1.1 严格遵守国家金融监管规定、法律法规及苏州市地方金融政策，确保平台数据采集、存储、传输、使用各环节符合《个人信息保护法》要求。每季度开展 1 次合规性审计，建立监管政策动态跟踪机制（更新频率≥每月 1 次），及时调整平台功能与流程。数据传输采用国密算法（SM4）加密，个人信息处理通过隐私计算技术（如联邦学习）实现 “数据可用不可见”。

4.1.2 数据传输应采用国密算法(SM4)加密，个人信息处理通过隐私计算技术实现“数据可用不可见”，定期通过自动化合规检测工具验证是否符合《个人信息保护法》。

4.2 安全性原则

4.2.1 构建“技术+管理”双重防护体系。技术层面采用系统互联技术，部署下一代防火墙（NGFW）、入侵防御系统（IPS）及 Web 应用防火墙（WAF），系统应部署在满足国家 A 级或金融行业标准要求的安全数据中心；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，每半年开展 1 次攻防演练，每月更新 1 次安全漏洞库。

4.2.2 金融信息协同平台建设涵盖底层技术架构（如分布式集群、云原生部署）、数据安全技术（如加密算法、脱敏技术）、访问控制技术（如零信任架构）、安全运维技术（如日志审计、漏洞扫描）等

技术领域的管理要求，技术实现应满足金融行业三级等保 GB/T 22239 相关技术指标。

4.3 高效性原则

4.3.1 通过流程自动化（智能审批引擎，响应时间≤30 min）、数据标准化（如统一接口规范，接口调用成功率≥99.9%）提升协同效率。

4.3.2 采用容器化部署（Docker+K8s）实现资源动态调度，通过 API 网关（Spring Cloud Gateway）集成流量控制技术（限流阈值：单接口每秒≤1000 次请求），促进金融业务顺畅开展。

4.4 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。通过安全技术评估工具检查现有加密算法、认证方式与新型威胁（如AI驱动的钓鱼攻击）的适配性，确保安全策略技术落地有效性。

4.5 协同治理原则

参与各方应签署协同安全协议，明确各方在数据提供、使用、销毁等环节的权利、义务和责任，并建立争端解决和联合应急响应机制。

5 平台使用安全要求

5.1 账号管理

5.1.1 账号创建

5.1.1.1 新账号创建需通过“人脸+工卡”双因子核验对接机构统一身份认证系统 IAM，合作机构人员账号应关联数字证书（X.509 标准），指定专门的系统管理员负责平台账号的创建。新员工入职或合作机构人员需使用平台时，由指定的系统管理员统一创建平台账号。

5.1.1.2 合作机构人员账号应绑定金融机构内部对接人，对接人承担账号使用监督责任；合作终止后 2 个工作日内，系统管理员须删除账号，删除操作日志保存期≥7 年。

5.1.2 密码设置

5.1.2.1 用户首次登录平台后，须在 10 min 内修改初始密码。新密码需满足：长度≥8 位，包含大写字母、小写字母、数字及特殊字符（≥1 种），不包含连续字符或重复字符。

5.1.2.2 应新增“密码强度可视化提示”功能，实时显示强度等级（低/中/高），密码存储采用 PBKDF2 算法加盐哈希处理（盐值长度≥16 位），每 90 d 强制更新 1 次密码。

5.1.2.3 密码存储采用 PBKDF2 算法加盐哈希处理（盐值长度≥16 位），系统定期（每 90 天）强制密码更新，通过密码爆破模拟工具验证密码抗破解能力，应符合 GB/T 39786 的要求。

5.1.3 账号保护

5.1.3.1 应启用设备绑定功能，后续登录若检测到异常设备，异常设备检测采用设备指纹技术（采集硬件 UUID、浏览器指纹），二次认证集成时间同步令牌（TOTP，如 Google Authenticator），账号操作全程关联数字签名（防抵赖）。

5.1.3.2 用户对个人账号和密码承担严格保管责任，不得转借他人。若因个人原因致使账号密码泄露，须在发现后 1 h 内告知系统管理员进行密码重置，并承担因账号泄露引发的所有风险与责任。

5.2 登录与操作

5.2.1 登录限制

5.2.1.1 平台应设置登录限制，同一账号最多允许 2 个终端同时在线，登录环境应通过终端安全基线检测，连续错误登录触发后，系统自动记录攻击 IP 并加入临时黑名单（24 h）。

5.2.1.2 用户应在工作场所或经授权的网络环境下登录平台，禁止在公共网络或不安全环境中操作。连续 3 次输入错误密码后，账号自动锁定 24 h 时，用户应联系系统管理员解锁，解锁操作记录实时同步至审计系统。

5.2.2 操作规范

5.2.2.1 用户在使用平台过程中，应严格按照系统提示和既定的业务流程进行操作。不应进行任何可能影响平台正常运行、破坏数据完整性或违反金融法规的操作。对于复杂业务操作或涉及重要数据变更的操作，系统应提供操作记录和审核功能，以便追溯和审计。
5.2.2.2 对于复杂业务操作或涉及重要数据变更的操作，系统应提供操作记录和审核功能（审核通过率≥99%）。系统自动生成《操作日志》，包含操作时间、IP 地址、功能模块、数据变动前后值等 10 项字段，日志采用区块链存证（联盟链架构），确保不可篡改。
5.2.2.3 操作记录采用区块链存证（联盟链架构），确保日志不可篡改；复杂操作（如批量数据修改）启用操作前风险提示（基于历史风险数据的 AI 预警）。

5.2.3 操作时限

5.2.3.1 对于一些涉及时效性的业务操作，平台应设置合理的操作时限。用户应在规定的时间内完成相应操作，具体要求如下：
5.2.3.2 业务审批类操作,紧急事项（如风险预警处置）应在 1 小时内完成审批，对于自动化处置的风险,应及时处置。一般事项审批时限为 24 h，超期未处理系统自动触发逐级催办提醒；通过定时任务调度系统触发催办提醒，紧急事项超时未处理自动推送至应急指挥平台（联动短信、企业微信）；。

5.3 信息发布与共享

5.3.1 发布审核

5.3.1.1 应采用智能内容检测工具对发布信息自动扫描（基于 BERT 预训练模型），敏感词、违规表述及涉密内容识别准确率≥99.5%，误报率≤0.1%；检测不通过的信息无法提交审核。
5.3.1.2 智能检测工具采用 NLP 深度学习模型（BERT 预训练模型），支持多语种敏感词识别（含金融黑话、监管禁忌词），检测精度需≥99.5%，误报率≤0.1%。
5.3.1.3 在平台上发布的信息，应经过严格审核流程，发布前由信息发布者提交所在部门负责人或指定审核人员审核，审核通过后方可发布；涉及重大金融政策解读、重要业务信息或可能影响金融市场稳定的信息，还须经金融机构高级管理层审核（审核时限≤48 h）。

5.3.2 内容安全

5.3.2.1 发布的信息应真实、准确、完整，语言表达清晰、规范，不应发布虚假信息、误导性信息、涉及商业机密、客户隐私及违反法律法规和监管要求的信息。
5.3.2.2 信息发布者对所发布信息的真实性和合法性负责，发布信息嵌入隐形数字水印（基于内容特征的鲁棒水印），3 年内支持泄露溯源至发布人。

5.3.3 共享权限

5.3.3.1 根据信息的敏感程度和适用范围，设置不同共享权限：一般性公开信息设为全体用户可见；涉及特定业务部门或群体的信息，设置相应访问权限，确保信息仅在授权范围内共享。
5.3.3.2 引入动态权限管理模型（基于 ABAC 模型），根据用户所属机构类型、岗位职级、业务场景，实时匹配信息访问权限（响应时间≤1 s）。
5.3.3.3 应设置临时共享权限设置，因特殊业务需要共享敏感信息时，应填写《信息共享申请表》（注明共享对象、内容、期限，最长 7 d），审批通过后采用一次性加密链接传输（SM2 非对称加密），链接 24 h 后自动销毁数据，访问日志保存期≥1 年，链接应具备访问密码保护或二次身份验证机制。

6 权限管理

6.1 权限分类与设置

6.1.1 功能权限

6.1.1.1 根据机构业务流程和岗位职责，为用户分配功能权限，权限设置遵循最小化原则，确保用户仅能执行与其工作相关的操作。

6.1.1.2　按业务场景细分权限颗粒度：

a)　基础功能：文件预览、评论、版本追溯；

b)　高级功能：流程发起、电子签章、数据导出；

c)　管理功能：账号创建、权限分配、系统配置。

6.1.1.3　建立权限互斥规则，通过系统触发器强制实现岗位制衡，规则执行准确率≥100%。

6.1.1.4　权限颗粒度通过 RBAC+ABAC 混合模型管理，权限配置存储于加密数据库，权限互斥规则通过系统触发器强制校验。

6.1.2　数据权限

6.1.2.1　根据数据的敏感性和重要性进行划分，包括查看、修改、删除等权限。对于涉及客户核心信息等敏感数据，应设置严格的访问控制，仅授予特定岗位和人员相应权限。同时，数据权限应与功能权限相互匹配，避免权限冲突。

6.1.2.2　数据分级技术标签采用元数据管理工具，敏感数据访问需通过动态脱敏，绝密级数据访问全程启用屏幕录像。

6.1.2.3　数据分级与权限映射表见表 1。

表 1　数据分级与权限映射表

数据级别	典型数据类型	访问权限	操作权限
绝密级	客户生物特征数据	仅限公司高管+加密终端	不应导出，仅限在线查看
机密级	客户交易流水	部门负责人+审批流程	导出的数据文件须加密，解密密钥通过带外方式发送给审批通过的接收人
秘密级	普通客户联系方式	业务经办岗+基础认证	可导出至指定安全邮箱
公开级	机构联系方式	全体用户	自由访问
注：本表为数据分级与权限映射的基本示例。各机构应依据相关法律法规和自身业务风险，制定并动态维护更详细的数据分类分级目录和权限映射策略，并确保技术上严格执行。			

6.2　权限申请与审批

6.2.1　申请流程

6.2.1.1　用户因工作需要申请权限变更时，应填写《平台权限申请表》，详细说明申请权限的原因、所需权限的具体内容以及预计使用期限等信息。申请表应提交给所在部门负责人进行初审。

6.2.1.2　应开发权限智能审批引擎，系统自动识别申请权限的风险等级，低风险权限可触发“即申即批”自动化流程，中高风险权限，需人工逐级审批，对于中高风险权限的自动化审批,其审批规则和算法应经过独立的安全评估和审计并保留完整的、不可篡改的自动化决策日志。

6.2.1.3　智能审批引擎集成风险评分模型（基于申请权限敏感度、申请人历史操作风险），低风险权限自动审批响应时间≤5 min，中高风险权限需关联电子签章审批。

6.2.2　审批流程

6.2.2.1　涉及重要功能或敏感数据的权限申请，应提交公司高级管理层进行最终审批。审批结果应在3～5 个工作日内反馈给申请人。

6.2.2.2　审批链采用链式加密存储，审批意见通过哈希值校验防篡改，审批责任追溯对接机构审计系统（如 IBM QRadar）。

6.2.2.3　应建立审批责任追溯机制，审批人应在审批意见中明确理由，因审批失误导致权限滥用的，审批人承担连带管理责任。

6.3　权限变更与回收

6.3.1　权限变更

6.3.1.1　岗位调动权限调整通过 API 对接人力资源系统（HRM），自动触发权限模板匹配（基于岗位-权限映射库），旧权限回收采用“逻辑删除+数据归档”双机制（归档数据加密存储）。

6.3.1.2 当用户的岗位职责发生变动或业务需求发生变化时，所在部门应及时通知系统管理员进行权限变更。系统管理员应在接到通知后的 2 个工作日内完成权限调整，并确保用户权限与新的工作要求相匹配。
6.3.1.3 岗位调动时，系统自动触发权限体检，根据新岗位职责匹配权限模板，旧权限自动回收，新权限需重新走审批流程，整个过程需在 3 个工作日内完成。
6.3.1.4 应按“最小必要”原则授予临时权限，借调期结束前 2 天系统自动提醒回收，借调期间操作记录单独归档。

6.3.2 权限回收

6.3.2.1 员工离职账号处理通过工单系统联动，冻结账号时自动清理会话缓存，删除账号前强制备份操作日志（加密压缩存储，保存期≥7 年）。
6.3.2.2 员工离职、岗位调动或合作关系终止时，所在部门应及时通知系统管理员回收其平台账号及相应权限。对于因特殊原因需临时保留部分权限的，应明确保留期限和使用范围，并在到期后及时收回。
6.3.2.3 人力资源部门需在员工离职申请提交时，同步系统管理员冻结账号。离职审批流程完成后，立即删除账号并清除所有关联数据。
6.3.2.4 对于退休人员，保留其历史操作记录查询权限，但禁止任何新增、修改、删除操作，权限保留期限为退休后 3 年。

7 数据管理

7.1 数据分类与分级

7.1.1 数据分类

7.1.1.1 根据机构的业务特点和数据性质，将平台数据分为客户信息数据、业务交易数据内部管理数据等类别。
7.1.1.2 建立数据资产目录，每季度更新数据分类清单，标注数据所有者、存储位置、共享范围等属性，通过数据治理平台实现可视化管理。数据资产目录采用自动化扫描工具，每季度扫描新增数据资产并标注敏感属性（基于预设规则库），支持可视化图谱展示。

7.1.2 数据分级

7.1.2.1 对各类数据进行分级管理，应符合 JR/T 0197 的要求，分为绝密、机密、秘密和公开四个级别，具体要求如下：

a) 绝密级数据包括客户核心隐私信息、核心商业机密等；
b) 机密级数据包括重要业务数据、财务数据等；
c) 秘密级数据包括一般客户信息、日常业务记录等；
d) 公开级数据为可对外公开的一般性信息。

7.1.2.2 设定数据分级变更触发条件，客户信息因业务升导致敏感程度提升，系统应具备数据分级动态评估能力。当触发分级变更条件时，应自动生成变更审批工单，由数据安全官或相关负责人审核后执行变更。系统通过数据内容识别引擎自动检测敏感程度变化，分级变更后实时同步至权限管理系统（延迟≤1 min）。
7.1.2.3 公开级数据原则上不可升级为敏感级，敏感级数据需经合规部门评估确认无风险后，方可降级为公开级。

7.2 数据存储与备份

7.2.1 存储要求

7.2.1.1 存储设备应支持硬件加密（SED 自加密硬盘），敏感数据采用“传输加密（TLS 1.3）+存储加密（SM4）”双层保护，存储介质退役前需通过数据擦除工具（符合 DoD5220.22-M 标准）处理。
7.2.1.2 平台数据应存储在符合金融行业安全标准的存储设备和系统中，采用冗余存储技术，确保数据的可靠性和可用性。对于敏感数据，应进行加密存储，加密算法应符合国家相关标准和行业要求。

7.2.2 备份策略

7.2.2.1 制定完善的数据备份策略，定期对平台数据进行全量备份和增量备份。全量备份应每周进行一次，增量备份应每天进行。全量备份采用增量快照技术（如 ZFS 快照），备份数据需通过校验码（SHA-256）验证完整性，异地灾备采用异步复制（RPO≤15 min，RTO≤1 h）。
7.2.2.2 定期对备份数据进行恢复测试，确保备份数据的完整性和可恢复性。数据安全与保密。

7.2.3 安全防护

7.2.3.1 建立健全数据安全防护体系，采用防火墙、入侵检测系统、防病毒软件等安全技术手段，防范网络攻击、病毒感染等安全威胁。加强对平台系统的安全漏洞管理，及时更新系统补丁，确保系统安全稳定运行。
7.2.3.2 防火墙应支持应用层深度包检测（DPI），入侵检测系统（IDS）规则库每周更新，漏洞管理采用自动化扫描工具（Nessus），高危漏洞修复时间≤24 h。

7.2.4 保密措施

7.2.4.1 严格遵守数据保密制度，员工不应私自将平台数据带出工作场所或泄露给无关人员。在数据共享和传输过程中，应采取加密传输等安全措施，对于违反数据保密规定的行为，应严肃追究相关人员的责任。
7.2.4.2 应采用数字水印、数据探针或行为分析(UEBA)等技术手段，建立数据泄露溯源机制，通过数字水印技术，实现泄露数据的快速定位，结合操作日志分析锁定责任人。数字水印采用空域嵌入算法（LSB），支持抗裁剪、旋转攻击；数据泄露溯源通过日志关联分析（ELK Stack），定位泄露路径时间≤2 h。

8 系统维护与升级

8.1 日常维护

8.1.1 监控与巡检

8.1.1.1 系统管理员应建立日常监控机制，实时监测平台的运行状态，包括服务器性能、网络连接等。每日对平台进行巡检，及时发现并处理潜在的问题和故障。同时，记录系统运行日志，分析和追溯系统运行情况。
8.1.1.2 监控工具采用 Prometheus+Grafana，实时采集服务器 CPU/内存/磁盘（阈值：CPU≥80%、内存≥85%触发告警）、网络流量（异常流量≥100Mbps 自动限流），巡检报告自动生成并加密归档。

8.1.2 故障处理

8.1.2.1 制定完善的故障处理流程，平台出现故障时，系统管理员应立即启动应急预案，尽快恢复平台正常运行。对于一般性故障，应在 2 h 内解决；对于重大故障，应在 4 h 内给出解决方案，并及时向相关部门和用户通报故障处理进展情况。故障处理完成后，应进行故障原因分析和总结，采取相应的改进措施，防止类似故障再次发生。
8.1.2.2 故障定位采用分布式追踪工具（Jaeger），一般性故障通过自动化运维工具（Ansible）修复，重大故障启用热备切换（RTO≤30 min），故障根因分析采用鱼骨图+日志关联技术。

8.2 系统升级

8.2.1 升级评估

8.2.1.1 升级前通过漏洞扫描工具检测兼容性风险，性能影响评估采用压力测试工具（JMeter，模拟 10 万用户并发），升级计划需包含回退触发条件（如心功能故障率≥1%）。
8.2.1.2 平台供应商发布系统升级版本，应及时对升级内容进行评估，包括功能改进、安全漏洞修复、性能优化等方面。结合机构的实际业务需求和系统现状，分析升级对现有业务流程和数据的影响，制定详细的升级计划。

8.2.2 升级实施

8.2.2.1 升级计划应包括升级时间、升级步骤、回退方案等内容。在升级实施前，应提前通知相关部门和用户，告知升级时间和可能对业务造成的影响。采用灰度发布，先在10%节点验证，无异常后全量推送；升级后通过自动化测试工具（Selenium）验证核心功能（通过率≥99.9%）。
8.2.2.2 升级过程中，应严格按照升级操作手册进行操作。升级完成后，应进行全面的系统测试，满足业务需求和安全要求。若升级过程中出现问题，应立即启动回退方案，将系统恢复到升级前的状态，并及时与平台供应商沟通解决。

8.3 响应用户

8.3.1 用户在平台使用过程中反馈的问题，系统管理员应在接到反馈后的24h内做出响应，具体要求如下：

a) 一般性问题，应在24 h内解决；
b) 较为复杂的问题，应在3个工作日内制定出解决方案，并向用户明确告知解决时间节点。

8.3.2 问题处理对接工单系统（Jira），一级问题自动分配至应急工程师（SLA计时），问题解决后通过用户满意度调研（嵌入平台）验证效果，问题分类模型定期通过机器学习优化（提升自动派单准确率）。
8.3.3 平台运营方应建立并发布清晰的问题分级处理服务水平协议(SLA)，并确保有效执行。推荐的处理时限如下：

a) 一级问题（如系统登录失败）：2 h内解决；
b) 二级问题（如数据显示异常）：4 h内解决；
c) 三级问题（如业务流程阻断）：8 h内解决；
d) 需协调供应商的复杂问题：明确告知用户预计解决时间。

9 安全处理要求

9.1 违规行为界定

9.1.1 违规类型要求如下：

a) 技术安全违规：擅自接入未经认证的设备或软件、故意制造系统漏洞；
b) 数据合规违规：超范围采集客户信息、跨境传输敏感数据；
c) 协同操作违规：在平台外泄露协同办公中获取的第三方机构商业信息。

9.1.2 量化违规等级要求如下：

a) 轻微违规：首次账号未定期更换密码、非敏感信息发布未审核；
b) 严重违规：越权访问机密级数据、未加密传输敏感信息；
c) 重大违规：故意泄露绝密级数据、利用平台实施金融违法犯罪。

9.2 警告与整改

初次发现的轻微违规行为，应由系统管理员或所在部门负责人对违规人员进行口头警告，并责令其立即整改。整改完成后，应提交整改报告，经审核通过后，视为处理完毕；整改未通过的，升级为严重违规处理。

9.3 处罚与通报

对于多次出现轻微违规行为或一次出现较严重违规行为的，金融机构应视情节轻重给予相应的处罚，如扣减绩效奖金、降低岗位等级、暂停平台使用权限等。同时，在金融机构内部进行通报批评，以起到警示作用。

9.4 法律责任追究

9.4.1 对于因违规行为给金融机构造成重大经济损失、声誉损害或违反法律法规的，金融机构将依法追究相关人员的法律责任，并要求其承担相应的赔偿责任。
9.4.2 相关证据链（操作日志、违规记录等）采用区块链存证（时间戳+哈希值），确保具备司法效力（符合《民事诉讼法》电子证据要求），证据保存期≥7 年。

参 考 文 献

[1] 《中华人民共和国网络安全法》
[2] 《数据安全法》
[3] 《个人信息保护法》