证券基金经营机构信息技术管理办法（2021 修订）

发 文 机 关：中国证券监督管理委员会

发 布 日 期：2021.01.15

生 效 日 期：2021.01.15

证券基金经营机构信息技术管理办法（2021 修订）

（2017 年 3 月 31 日中国证券监督管理委员会 2017 年第 2 次主席办公会议审议通过，根据 2021 年 1 月 15 日中国证券监督管理委员会《关于修改、废止部分证券期货规章的决定》修正）

第一章 总则

第一条 为加强证券基金经营机构信息技术管理，保障证券基金行业信息系统安全、合规运行，保护投资者合法权益，根据《证券法》、《证券投资基金法》、《证券公司监督管理条例》等法律法规，制定本办法。

第二条 证券基金经营机构借助信息技术手段从事证券基金业务活动，信息技术服务机构为证券基金业务活动提供信息技术服务，适用本办法。

第三条 本办法所称证券基金经营机构，是指经中国证监会批准在境内设立的证券公司和管理公开募集基金的基金管理公司（以下简称基金管理公司）。

本办法所称信息技术服务机构，是指为证券基金业务活动提供信息技术服务的机构。信息技术服务的范围如下：

（一）重要信息系统的开发、测试、集成及测评；

（二）重要信息系统的运维及日常安全管理；

（三）中国证监会规定的其他情形。

以上机构统称证券基金经营与服务机构。

第四条 证券基金经营机构是从事证券基金业务活动的责任主体，应当保障充足的信息技术投入，在依法合规、有效防范风险的前提下，充分利用现代信息技术手段完善客户服务体系、改进业务运营模式、提升内部管理水平、增强合规风控能力，持续强化现代信息技术对证券基金业务活动的支撑作用。

第五条 中国证监会及其派出机构依法对证券基金经营与服务机构借助信息技术手段从事证券基金业务活动或提供相关服务实施监督管理。

中国证券业协会及中国证券投资基金业协会依照本办法制定和完善相关自律规则，对证券基金经营机构借助信息技术手段从事证券基金业务活动或提供相关服务实施自律管理。

中证信息技术服务有限责任公司（以下简称中证信息）在中国证监会指导下制定相关配套业务规则，协助开展信息技术相关备案、监测、检测和检查等工作。

第二章 信息技术治理

第六条 证券基金经营机构应当完善信息技术运用过程中的权责分配机制，建立健全信息技术管理制度和操作流程，保障与业务活动规模及复杂程度相适应的信息技术投入水平，持续满足信息技术资源的可用性、安全性与合规性要求。

第七条 证券基金经营机构董事会负责审议本公司的信息技术管理目标，对信息技术管理的有效性承担责任，履行下列职责：

（一）审议信息技术战略，确保与本公司的发展战略、风险管理策略、资本实力相一致；

（二）建立信息技术人力和资金保障方案；

（三）评估年度信息技术管理工作的总体效果和效率；

（四）公司章程规定的其他信息技术管理职责。

第八条 证券基金经营机构经营管理层负责落实信息技术管理目标，对信息技术管理工作承担责任，履行下列职责：

（一）组织实施董事会相关决议；

（二）建立责任明确、程序清晰的信息技术管理组织架构，明确管理职责、工作程序和协调机制；

（三）完善绩效考核和责任追究机制；

（四）公司章程规定或董事会授权的其他信息技术管理职责。

第九条 证券基金经营机构应当在公司管理层下设立信息技术治理委员会或指定专门委员会（以下统称信息技术治理委员会）负责制定信息技术战略并审议下列事项：

（一）信息技术规划，包括但不限于信息技术建设规划、信息安全规划、数据治理规划等；

（二）信息技术投入预算及分配方案；

（三）重要信息系统建设或重大改造立项、重大变更方案；

（四）信息技术应急预案；

（五）使用信息技术手段开展相关业务活动的审查报告以及年度评估报告；

（六）信息技术治理委员会委员提请审议的事项；

（七）其他对信息技术管理产生重大影响的事项。

信息技术治理委员会应当由高级管理人员以及合规管理部门、风险管理部门、稽核审计部门、主要业务部门、信息技术管理部门等部门负责人组成，可聘请外部专业人员担任信息技术治理委员会委员或顾问。

第十条 证券基金经营机构应当指定一名熟悉证券、基金业务，具有信息技术相关专业背景、任职经历、履职能力的高级管理人员为首席信息官，由其负责信息技术管理工作，并具备下列任职条件：

（一）从事信息技术相关工作十年以上，或者在证券监管机构、证券基金业自律组织任职八年以上；

（二）最近三年未被金融监管机构实施行政处罚或采取重大行政监管措施；

（三）中国证监会规定的其他条件。

第十一条 证券基金经营机构应当设立信息技术管理部门或指定专门机构（以下统称信息技术管理部门）负责实施信息技术规划、信息系统建设、信息技术质量控制、信息安全保障、运维管理等工作。

第三章 信息技术合规与风险管理

第十二条 证券基金经营机构应当将信息技术运用情况纳入合规与风险管理体系，为合规管理部门和风险管理部门配备与业务活动规模、复杂程度相适应的信息技术资源，并建立相应的审查、监测和检查机制，确保合规与风险管理覆盖信息技术运用的各个环节。

第十三条 证券基金经营机构借助信息技术手段从事证券基金业务活动的，应当在业务系统上线时，同步上线与业务活动复杂程度和风险状况相适应的风险管理系统或相关功能（以下统称风险管理系统），对风险进行识别、监控、预警和干预。

第十四条 证券基金经营机构借助信息技术手段从事证券基金业务活动前，应当开展内部审查，验证下列事项并建立存档记录：

（一）业务系统的流程设计、功能设置、参数配置和技术实现应当遵循业务合规的原则，不得违反法律法规及中国证监会的规定；

（二）风险管理系统功能完备、权限清晰，能够与业务系统同步上线运行；

（三）具备完善的信息安全防护措施，能够保障经营数据和客户信息的安全、完整；

（四）具备符合要求的信息系统备份及运维管理能力，能够保障相关系统安全、平稳运行。

第十五条 证券基金经营机构应当识别借助信息技术手段从事证券基金业务活动的各类风险，建立持续有效的风险监测机制。证券基金经营机构应当及时、稳妥处置发现的风险问题，并至少每年开展一次风险监测机制及执行情况的有效性评估。

第十六条 证券基金经营机构应当定期开展信息技术管理工作专项审计，频率不低于每年一次，确保三年内完成信息技术管理全部事项的审计工作，包括但不限于信息技术治理、信息技术合规与风险管理、信息技术安全管理、应急管理。

证券基金经营机构应当委托外部专业机构开展信息技术管理工作的全面审计，频率不低于每三年一次；未能有效实施信息技术管理被采取行政处罚措施、监管措施或者自律管理措施的，应当在三个月内完成对有关事项的专项审计。

证券基金经营机构应当跟踪审计发现问题的整改情况，相关问题未能及时整改的，应当说明理由，并将审计报告提交信息技术治理委员会审议。证券基金经营机构应当妥善保存审计报告，保存期限不得少于二十年。

第十七条 除法律法规及中国证监会另有规定外，证券基金经营机构应当通过自身运营管理的信息系统直接接收客户交易指令，并记录客户交易指令接收时间。

第十八条 证券基金经营机构应当按照中国证监会有关规定采集、记录、存储、报送客户交易终端信息，并采取有效的技术措施，保障相关信息真实、准确、完整。

证券基金经营机构借助专业化交易信息系统向特定客户提供交易服务的，应当要求客户登记交易终端信息；信息发生变更的，应当要求客户履行变更程序，确保客户真实使用的客户交易终端信息与登记内容一致。

第十九条 证券基金经营机构使用电子合同从事证券基金业务活动的，应当将电子合同存储在指定的信息系统，并提供可供投资者及合同其他相关方查询、下载的公开渠道。

第二十条 证券基金经营机构从事证券交易相关业务，应当按照监管规定及自律管理规则的要求，确保风险管理系统具备审查账户资金及证券是否充足、监控交易及资金划转是否异常等功能。

第四章 信息技术安全

第一节 信息系统安全

第二十一条 证券基金经营机构应当建立独立于生产环境的专用开发测试环境，避免风险传导；开发测试环境使用未脱敏数据的，应当采取与生产环境同等的安全控制措施。

证券基金经营机构在生产环境开展重要信息系统技术或业务测试的，应对测试流程及结果进行审查。

第二十二条 证券基金经营机构重要信息系统上线或发生重大变更的，应当制定专项实施方案，并对信息系统上线或变更操作行为进行审查、确认和跟踪。

证券基金经营机构重要信息系统计划停止使用的，应当开展技术和业务影响评估，制定完整的系统停用和数据迁移保管方案，并组织必要的评审及停用后的安全检查。

第二十三条 证券基金经营机构应当结合公司发展战略、市场交易规模等因素定期对重要信息系统开展压力测试和评估分析，确保其容量满足业务开展需要。

第二十四条 证券基金经营机构应当建立健全信息系统安全监测机制，设定监测指标并持续监测重要信息系统的运行状况。

证券基金经营机构应当指定专人跟踪监测发现的异常情形，及时处置并定期开展评估分析。

第二十五条 证券基金经营机构应当妥善保存信息系统开发、测试、上线、变更及运维过程中产生的文档，并根据业务开展情况以及信息系统的重要程度建立与监测工作相适应的日志留痕机制，确保满足应急处置和审计需要。

第二十六条 证券基金经营机构重要信息系统部署以及所承载数据的管理，应当遵循法律法规等规定。

第二十七条 证券基金经营机构可以在安全、合规的前提下为子公司提供机房、通信网络及其他信息技术基础设施，并协助开展相关运维工作。

证券基金经营机构为其子公司提供信息技术服务的，应当充分评估信息技术基础设施的支撑能力与冗余程度，并与子公司签订服务协议，明确合作双方的权利义务，以及建立日常协作、业务隔离和应急管理机制，防范基础设施共用产生的新增风险。

证券基金经营机构可以设立信息技术专业子公司，为母公司提供信息技术服务。信息技术专业子公司经中国证监会备案后可为其他金融机构提供信息技术服务。

第二十八条 证券基金经营机构应当确保重要信息系统具备可审计功能，并可以根据监管部门的要求转换、提供数据。

第二节 数据治理

第二十九条 证券基金经营机构应当结合公司发展战略，建立全面、科学、有效的数据治理组织架构以及数据全生命周期管理机制，确保数据统一管理、持续可控和安全存储，切实履行数据安全及数据质量管理职责，不断提升数据使用价值。

第三十条 证券基金经营机构应当将经营及客户数据按照重要性和敏感性进行分类分级，并根据不同类别和级别作出差异化数据管理制度安排。

第三十一条 证券基金经营机构应当完善网络隔离、用户认证、访问控制、数据加密、数据备份、数据销毁、日志记录、病毒防范和非法入侵检测等安全保障措施，保护经营数据和客户信息安全，防范信息泄露与损毁。

第三十二条 证券基金经营机构应当遵循最少功能以及最小权限等原则分配信息系统管理、操作和访问权限，并履行审批流程。合规管理和风险管理部门应当对权限管理制度和操作流程进行合规审查及风险控制。

证券基金经营机构应当建立对信息系统权限的定期检查与核对机制，确保用户权限与其工作职责相匹配，防止出现授权不当的情形。

证券基金经营机构应当对重要信息系统的开发、测试、运维实施必要分离，保证信息技术管理部门内部岗位的相互制衡。

第三十三条 证券基金经营机构应当记录经营数据和客户信息的使用情况，并持续监督信息技术服务机构等相关方落实保密协议的情况。

证券基金经营机构发现其他机构、个人违规存储或使用自身经营数据和客户信息的，应当排查数据泄露途径、评估影响范围，采取合理可行的整改措施，及时处置风险隐患，并按照中国证监会规定履行报告和调查处理职责。

证券基金经营机构发现信息技术服务机构等相关方违规存储或者使用自身经营数据和客户信息的，应当责令其立即改正并销毁已获取的经营数据和客户信息；信息技术服务机构等相关方拒绝配合整改的，证券基金经营机构应当立即停止与其合作，并采取措施维护自身及客户的合法权益。

第三十四条 证券基金经营机构应当建立健全数据安全管理制度，不得收集与服务无关的客户信息，不得购买或使用非法获取或来源不明的数据。在收集使用客户信息之前，证券基金经营机构应当公开收集、使用的规则和目的，并征得客户同意。

除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。

第三十五条 证券基金经营机构应当充分挖掘、梳理和分析数据内容，提高管理精细化程度，在业务经营、风险管理与内部控制中加强数据应用，实现同一客户、同类业务统一管理，充分发挥数据价值。

第三节 应急管理

第三十六条 证券基金经营机构借助信息技术手段从事证券基金业务活动的，应当建立信息技术应急管理的组织架构，确定重要业务及其恢复目标，制定应急预案，配置充足资源，稳妥处置信息技术突发事件，并积极开展应急演练和信息技术应急管理的评估与改进。

第三十七条 证券基金经营机构应当落实下列应急管理职责：

（一）信息技术管理部门为信息技术应急管理的牵头组织部门，组织开展信息技术应急预案的制定、演练、评估与改进工作，并负责信息系统的应急响应与恢复；

（二）各业务部门负责评估本业务条线信息技术突发事件相关风险，开展业务影响分析，确定并实施重要业务恢复目标和恢复策略；

（三）风险管理部门负责评估信息系统与相关业务恢复目标和恢复策略制定的合理性，确保与公司整体风险管理策略保持一致。

第三十八条 证券基金经营机构应当制定并持续完善应急预案，包括应急管理建设目标、备份信息系统建设和恢复机制、备份数据恢复机制、业务恢复或替代措施、应急联系方式、与客户沟通方式、向监管部门及有关单位的报告路径、应急预案披露与更新机制等内容。

证券基金经营机构应急预案应当充分考虑重要信息系统故障、相关信息技术服务机构无法继续提供服务、证券基金经营机构信息技术高管或重要技术团队发生重大变动以及自然灾害等可能影响重要信息系统平稳运行的事件。

第三十九条 证券基金经营机构应当根据系统变更、业务变化等情况，持续更新应急预案。

证券基金经营机构应当根据应急预案定期组织关键岗位人员开展应急演练，演练频率不低于每年一次，并确保应急演练在两年内覆盖全部重要信息系统。应急演练应当形成报告，保存期限不得少于五年。

第四十条 证券基金经营机构应当在公司网站、客户交易终端等渠道公示信息技术突发事件发生时客户可采取的替代交易方式等信息，提示客户防范和应对可能出现的风险。

第四十一条 证券基金经营机构应当确保备份系统与生产系统具备同等的处理能力，保持备份数据与原始数据的一致性。重要信息系统应当符合下列信息系统备份能力等级要求：

（一）实时信息系统、非实时信息系统的数据备份能力应当达到第一级；

（二）非实时信息系统的故障应对能力应当达到第二级；

（三）证券公司实时信息系统的故障应对能力应当达到第四级，基金管理公司实时信息系统的故障应对能力应当达到第三级；

（四）实时信息系统、非实时信息系统应当具备灾难及重大灾难应对能力，相关技术指标应当分别达到灾难应对能力第五级、重大灾难应对能力第六级；

（五）灾难应对能力可以通过重大灾难应对能力体现，但重大灾难应对能力相关技术指标应当达到灾难应对能力第五级。

第四十二条 证券基金经营机构应当按照中国证监会有关规定，建立信息安全事件的分级响应机制，明确内部处置工作流程，确保相关信息系统及时恢复运行。

第五章 信息技术服务机构

第四十三条 证券基金经营机构借助信息技术手段从事证券基金业务活动的，可以委托信息技术服务机构提供产品或服务，但证券基金经营机构依法应当承担的责任不因委托而免除或减轻。

证券基金经营机构应当清晰、准确、完整的掌握重要信息系统的技术架构、业务逻辑和操作流程等内容，确保重要信息系统运行始终处于自身控制范围。除法律法规及中国证监会另有规定外，不得将重要信息系统的运维、日常安全管理交由信息技术服务机构独立实施。

第四十四条 证券基金经营机构委托信息技术服务机构提供服务，应当按照本办法第十四条的规定对信息技术服务机构及相关信息系统进行内部审查，并向中国证监会及其派出机构报送审查意见及相关资料。

证券基金经营机构应当在选择信息技术服务机构之前，制定更换服务提供方的流程及预案，确保在特定情况下可更换服务提供方。

第四十五条 证券基金经营机构应当与信息技术服务机构签订服务协议和保密协议，明确各方权利、义务和责任，约定质量考核标准、持续监控机制、异常处理机制、服务变更或者终止的处置流程以及现场服务人员保密要求等内容，并持续监督信息技术服务机构及相关人员落实服务协议和保密协议的情况。

证券基金经营机构应当参照本办法第三条在服务协议中列明委托信息技术服务机构提供的服务范围、服务方式、涉及信息系统及相关证券基金业务活动类型。

第四十六条 信息技术服务机构出现异常情形的，证券基金经营机构应当按照应急预案开展内部评估与审查；信息技术服务机构保障能力不足，导致相关产品或服务的可用性、完整性或机密性丧失的，应当及时更换信息技术服务机构。

第四十七条 信息技术服务机构应当向中国证监会备案，具体规定由中国证监会另行制定。

第四十八条 基金信息技术服务机构备案材料应当包括本机构基本情况、信息技术服务情况、服务对象情况、内部控制情况等相关资料。备案内容发生变更的，基金信息技术服务机构应当及时更新备案材料。

基金信息技术服务机构备案材料不完整或者不符合规定的，应当根据中国证监会要求及时补正。

第四十九条 为证券公司、证券投资咨询机构提供信息技术服务的机构（以下简称证券信息技术服务机构）可以自愿接受中证信息业务指导，并遵守相关业务规则。

第五十条 信息技术服务机构应当健全内部质量控制机制，定期监测相关产品或服务，在提供服务过程中出现明显质量问题的，应当立即核实有关情况，采取必要的处理措施，明确修复完成时限，及时完成修复工作。

第五十一条 信息技术服务机构为证券基金业务活动提供信息技术服务，不得有下列行为：

（一）参与证券基金经营机构向客户提供业务服务的任何环节或向投资者、社会公众等发布可能引发其从事证券基金业务误解的信息；

（二）截取、存储、转发和使用证券基金业务活动相关经营数据和客户信息；

（三）在服务对象不知情的情况下，转委托第三方提供信息技术服务；

（四）提供的产品或服务相关功能、操作流程、系统权限及参数配置违反现行法律法规；

（五）无正当理由关闭系统接口或设置技术壁垒；

（六）向社会公开发布信息安全漏洞、信息系统压力测试结果等网络安全信息或泄露未公开信息；

（七）法律法规及中国证监会禁止的其他行为。

第六章 监督管理

第五十二条 证券基金经营机构新建或更换重要信息系统所在机房、证券基金交易相关信息系统，应当在开展相关业务活动的五个工作日内向中国证监会报送有关资料，包括内部审查意见、机房基本信息、技术架构设计、操作流程、信息安全管理资料、业务制度、合规管理及风险管理制度等。

第五十三条 证券基金经营机构应当在报送年度报告的同时报送年度信息技术管理专项报告，说明报告期内信息技术治理、信息技术合规与风险管理、信息技术安全管理、信息技术审计等执行本办法规定的情况。

信息技术服务机构提供信息技术服务时，应当按照中国证监会要求定期报送相关资料。

证券基金经营与服务机构提交报告的内容应当真实、准确、完整。

第五十四条 证券基金经营机构应当按照中国证监会有关规定履行信息安全事件报告和调查处理职责。

第五十五条 信息技术服务机构出现下列情形的，应当立即报告住所地中国证监会派出机构：

（一）人员、财务、技术管理等方面发生重大变化，可能无法持续为证券基金经营机构提供信息技术服务；

（二）提供的信息技术服务存在明显缺陷，可能导致所服务的三家及以上证券基金经营机构发生信息系统运营异常、数据泄露、遭受网络攻击等情形；

（三）其他可能对投资者合法权益、证券期货市场造成严重影响的事件。

第五十六条 中国证监会及其派出机构在对证券基金经营与服务机构信息技术管理及服务活动的监管过程中，可以采用渗透测试、漏洞扫描及信息技术风险评估等方式开展现场检查及非现场检查。证券基金经营与服务机构应当予以配合，如实提供有关文件、资料，不得拒绝、阻碍或隐瞒。

第五十七条 证券基金经营机构违反本办法规定的，中国证监会及其派出机构可以依法对其采取责令改正、暂停业务、出具警示函、责令定期报告、责令增加合规检查次数、公开谴责等行政监管措施；对直接负责的主管人员和其他责任人员采取责令改正、监管谈话、出具警示函、公开谴责等行政监管措施。

第五十八条 证券基金经营机构违反本办法规定，反映公司治理混乱、内控失效的，中国证监会及其派出机构可以按照《证券投资基金法》第二十四条、《证券公司监督管理条例》第七十条的规定，采取责令暂停部分或全部业务、责令更换董事、监事、高级管理人员或者限制其权利等行政监管措施。

第五十九条 信息技术服务机构违反本办法规定的，中国证监会及其派出机构可以要求其提交说明材料，并采取责令改正、监管谈话、出具警示函等行政监管措施，情节严重的，中国证监会及其派出机构可以对信息技术服务机构及其直接负责的主管人员和其他直接责任人员单处或者并处警告、三万元以下罚款。

第七章 附则

第六十条 证券基金专项业务服务机构借助信息技术手段从事证券基金业务活动的，参照本办法执行。

从事证券公司客户交易结算资金存管活动的商业银行、从事公开募集基金的基金托管机构、证券基金经营机构在境内依法设立的子公司及其下设机构借助信息技术手段从事相关证券基金业务活动的，参照本办法执行。

第六十一条 证券基金专项业务服务机构违反本办法规定的，中国证监会及其派出机构可以对证券基金专项业务服务机构及其直接负责的主管人员和其他直接责任人员单处或者并处警告、责令停止基金服务业务或三万元以下罚款等行政监管措施。

第六十二条 证券基金经营机构、证券基金专项业务服务机构应当按照本办法第五十二条规定，在本办法实施之日起半年内将已投产的重要信息系统所在机房、证券基金交易相关信息系统等相关情况报送中国证监会。

本办法实施前，已提供相关服务的基金信息技术服务机构应当按照本办法规定，在本办法实施之日起半年内向中国证监会备案。

本办法实施前，已从事相关业务活动且不符合本办法第十七条规定的，证券基金经营机构应当妥善处理相关问题，并在本办法实施之日起半年内完成整改；整改未完成前，不得借助违规接收客户交易指令的信息系统增加新客户或提供新服务。

第六十三条 本办法中下列用语的含义：

（一）证券基金专项业务服务机构，是指从事公开募集基金的销售、销售支付、份额登记、估值、投资顾问、评价等基金服务业务的机构和证券投资咨询机构。

（二）重要信息系统，是指支持证券基金经营机构和证券基金专项业务服务机构关键业务功能、如出现异常将对证券期货市场和投资者产生重大影响的信息系统。包括集中交易系统、投资交易系统、金融产品销售系统、估值核算系统、投资监督系统、份额登记系统、第三方存管系统、融资融券业务系统、网上交易系统、电话委托系统、移动终端交易系统、法人清算系统、具备开户交易或者客户资料修改功能的门户网站、承载投资咨询业务的系统、存放承销保荐业务工作底稿相关数据的系统、专业即时通信软件以及与上述信息系统具备类似功能的信息系统。

（三）重大变更，是指经证券基金经营机构、证券基金专项业务服务机构自行评估，可能影响业务合规和信息系统安全稳定运行的系统变更，包括但不限于信息技术服务机构更换、技术架构重大调整、主要功能变化等。

（四）专业化交易信息系统，是指除网上交易系统、移动终端交易系统等标准化交易系统外，证券基金经营机构向具有个性化需求并且符合规定条件的特定客户提供服务的交易系统。

（五）证券基金经营机构信息系统备份能力、数据备份能力、故障应对能力、重大灾难应对能力、实时信息系统、非实时信息系统以及备份能力等级相关定义参见中国证监会关于信息系统备份能力相关行业标准。

第六十四条 本办法自 2019 年 6 月 1 日起实施。《证券投资基金销售机构通过第三方电子商务平台开展业务管理暂行规定》（证监会公告〔2013〕18 号）同时废止。