证券期货业网络安全管理办法
（征求意见稿）

第一章　总则

第一条　为了保障证券期货业网络安全，保护投资者合法权益，促进证券期货业稳定健康发展，根据《证券法》、《证券投资基金法》、《网络安全法》、《数据安全法》、《个人信息保护法》、《期货交易管理条例》、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条　核心机构和经营机构在中华人民共和国境内建设、运营、维护和使用网络及信息系统，信息技术服务机构为证券期货业务活动提供产品或者服务的网络安全保障，以及证券期货业网络安全的监督管理，适用本办法。

第三条　核心机构和经营机构应当遵循保障安全、促进发展的原则，建立健全网络安全防护体系，提升网络安全保障水平，确保网络安全与信息化工作同步推进，促进本机构相关工作稳妥健康发展。

信息技术服务机构应当遵循技术安全、功能合规的原则，为证券期货业务活动提供产品或者服务，与核心机构、经营机构共同保障行业网络安全，促进行业信息化发展。

第四条　核心机构和经营机构应当依法履行网络安全

保护义务，对本机构网络安全负责，相关责任不因其他机构提供产品或者服务进行转移或者减轻。

信息技术服务机构应当勤勉尽责，对提供产品或者服务的合规性、安全性承担责任。

第五条 中国证监会依法履行以下监督管理职责：

（一）组织制定并推动落实证券期货业网络安全和信息化发展规划、监管规则和行业标准；

（二）负责证券期货业网络安全的监督管理，对证券期货业关键信息基础设施进行监管；

（三）负责证券期货业网络安全重大技术路线、重大科技项目管理；

（四）组织开展证券期货业数据安全统筹管理；

（五）负责证券期货业网络安全应急演练、应急处置和事件报告与调查处理；

（六）指导证券期货业网络安全促进与发展；

（七）法律法规规定的其他网络安全监管职责。

第六条 中国证监会建立集中管理、分级负责的证券期货业网络安全监督管理体制。中国证监会科技监管部门统一对证券期货业网络安全实施监督管理。中国证监会其他部门配合开展相关工作。

中国证监会派出机构对本辖区经营机构和信息技术服务机构网络安全实施监督管理。

中证信息技术服务有限责任公司在中国证监会指导下，为证券期货业网络安全监督管理提供专业协助和支撑。

第七条 中国证券业协会、中国期货业协会、中国证券投资基金业协会等行业协会（以下统称行业协会）依法制定行业网络安全自律规则，对经营机构网络安全实施自律管理。

第八条 核心机构依法制定保障市场相关主体与本机构信息系统安全互联的技术规则，对与本机构信息系统和网络通信设施相关联主体加强指导，督促其强化网络安全管理，保障相关信息系统和网络通信设施的安全平稳运行。

第二章 网络安全运行

第九条 核心机构和经营机构应当具有完善的信息技术治理架构，健全网络安全管理制度体系，建立内部决策、管理、执行和监督机制，确保网络安全管理能力与信息化发展水平相匹配。

信息技术服务机构应当建立网络安全管理制度，配备相应的安全、合规管理人员，建立与提供产品或者服务相适应的网络安全管理机制。

第十条 核心机构和经营机构应当明确主要负责人为本机构网络安全第一责任人，分管科技工作的负责人为直接责任人。

核心机构和经营机构应当建立网络安全工作协调和决

策机制，保障网络安全第一责任人和直接责任人履行职责。

第十一条 核心机构和经营机构应当指定网络安全工作牵头部门或者机构，负责管理重要信息系统和相关基础设施、制定网络安全应急预案、组织应急演练、认定网络安全关键岗位等工作。

第十二条 核心机构和经营机构应当配备网络安全专职人员，保障技术人员数量和资金投入与业务活动规模及复杂程度相适应，网络安全专职人员应当具备与履行职责相匹配的专业知识和职业技能。

第十三条 核心机构和经营机构应当确保信息系统和相关基础设施具备合理的架构，足够的性能、容量、可靠性、扩展性和安全性，并保证相关安全技术措施与信息化工作同步规划、同步建设、同步使用。信息系统的性能容量不得低于历史峰值的两倍。

第十四条 核心机构和经营机构应当落实网络安全等级保护制度，依法履行网络安全等级保护义务，按照国家和证券期货业定级标准和定级要求，向公安机关办理备案和变更。

核心机构和经营机构应当按照相关要求，将网络安全等级保护定级、变更和日常工作开展情况及时报告中国证监会及其派出机构。

第十五条 核心机构和经营机构新建上线、运行变更、下线移除重要信息系统的，应当进行风险评估并开展充分测试，制定应急处置和回退方案；可能对证券期货市场安全平稳运行产生较大影响的，应当提前向中国证监会及其派出机构报告。

第十六条 核心机构和经营机构暂停或者终止借助网络向投资者提供服务前，应当履行告知义务，合理选取公告、定向通知等方式告知投资者相关业务影响情况、替代方式及其他应对措施。

第十七条 核心机构和经营机构应当建立健全网络安全监测预警机制，设定监测指标，持续监测信息系统和相关基础设施的运行状况，及时处置异常情形，对监测机制执行效果进行定期评估并持续优化。

核心机构和经营机构应当全面、准确记录并妥善保存生产运营过程中的业务日志和系统日志，确保满足故障分析、内部控制、调查取证等工作的需要。业务日志保存期限不得少于二十年，系统日志保存期限不得少于六个月。

第十八条 核心机构和经营机构应当建立同城和异地数据备份设施，至少每天备份数据一次，每季度至少对数据备份进行一次有效性验证。

核心机构和经营机构应当建立信息系统的故障备份设施和灾难备份设施，根据信息系统的重要程度和影响范围，

确定恢复目标，保证业务活动连续。灾难备份设施应当通过同城或者异地灾难备份中心的形式体现。

核心机构和经营机构采取双活或者多活架构部署重要信息系统的，确保业务连续运行能力不低于前款规定的前提下，任一数据中心可以视为其他数据中心的灾难备份设施。

第十九条 核心机构和经营机构应当至少每半年开展一次重要信息系统压力测试，根据系统技术特点和承载业务类型，制定压力测试方案，设定测试场景，从系统处理能力、网络冗余、灾备建设等方面设置测试指标，有序组织测试工作，测试完成后形成压力测试报告存档备查。

核心机构和经营机构应当按照有关要求，参加中国证监会组织开展的全行业重要信息系统压力测试，并根据测试情况及时整改；暂时无法整改的，应当制定切实可行的整改计划。

第二十条 信息技术服务机构应当依法向中国证监会备案，并按照有关业务规则为证券期货业务活动提供信息技术产品或者服务。

核心机构和经营机构应当建立健全内部管理机制，完善信息技术产品和服务准入标准，审慎采购并持续评估相关产品和服务的质量，加强保密管理，及时改进风险管理措施，健全应急处置机制，保障本机构网络安全和相关业务的安全平稳运行。

第二十一条 核心机构和经营机构应当加强自主研发能力建设，持续提升自主可控能力，并按照国家及中国证监会有关要求开展信息技术应用创新相关工作。

第二十二条 核心机构和经营机构应当按照知识产权相关法律法规，制定知识产权保护策略和制度，采取有效措施保护本机构自主知识产权，不侵犯他人的知识产权。

第三章 数据安全统筹管理

第二十三条 核心机构和经营机构应当履行数据安全管理责任，包括但不限于以下方面：

（一）建立健全数据安全管理制度体系，完善数据运营和管控机制；

（二）健全数据安全管理组织架构，明确数据安全管理权责机制；

（三）依据行业相关数据标准，制定覆盖本机构全部业务数据的相关标准，实施与业务特点相适应的数据分类分级管理；

（四）建立数据权限管理策略，按照最小授权原则设置数据访问权限，定期排查清理，并对数据访问记录进行留痕审计；

（五）构建数据质量评估框架，建立质量管控和追责机制；

（六）法律法规及中国证监会规定的其他事项。

第二十四条 核心机构和经营机构处理重要数据、核心数据的，应当依法明确数据安全负责人，指定数据安全管理机构或者部门。

核心机构和经营机构处理重要数据的信息系统原则上应当满足三级以上网络安全等级保护要求，处理核心数据的信息系统依照有关法律法规从严保护。

第二十五条 核心机构和经营机构应当综合采取网络隔离、用户认证、访问控制、数据加密、病毒防范、非法入侵检测和网络安全态势感知等技术手段，及时识别、阻断和溯源相关网络攻击，保障数据安全。

第二十六条 核心机构和经营机构应当遵循合法、正当、必要和诚信原则处理投资者个人信息，依法履行投资者个人信息保护义务，包括但不限于下列要求：

（一）收集个人信息，应当告知投资者个人信息处理的目的、方式和范围，并取得个人同意；

（二）采取必要的安全技术措施存储、传输个人信息，防止个人信息泄露、篡改、丢失；

（三）合理确定个人信息使用策略和操作权限，不得滥用个人信息；

（四）处理证券期货账户等敏感个人信息、向他人提供或者公开个人信息的，应当取得个人的单独同意。

为履行法定职责、法定义务或者监管要求所必需，核心机构和经营机构可以在未取得个人同意的情况下，处理个人信息。

第二十七条 核心机构和经营机构应当建立信息发布审核机制，加强对本机构和用户发布信息的管理，发现违反法律法规和有关监管规定的，应当立即停止发布传输，采取必要的处置措施，防止信息扩散，积极消除负面影响，并及时向中国证监会及其派出机构报告。

信息技术服务机构为证券期货业务活动提供产品或者服务的，应当按照前款规定执行。

第二十八条 任何机构和个人不得违规开展证券期货业重要信息系统认证、检测、风险评估等活动，不得违规向社会发布证券期货业系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息。

第二十九条 中国证监会可以指定相关机构建设证券期货业战略备份数据中心，开展行业数据的集中备份和管理工作，持续提升证券期货业重大灾难应对能力。

核心机构和经营机构应当按照规定及时向证券期货业战略数据备份中心报送数据，报送的数据必须真实、准确、完整。

第四章　网络安全应急处置

第三十条　核心机构和经营机构应当建立网络安全风险监测预警机制，加强日常监测，定期开展漏洞扫描、安全评估等工作。核心机构、经营机构和信息技术服务机构发现网络安全产品或者服务存在安全缺陷、系统漏洞等风险隐患的，应当及时核实并加固整改；可能对证券期货业网络安全产生较大影响的，应当向中国证监会及其派出机构报告。

中国证监会及其派出机构可以就相关安全缺陷、系统漏洞等风险隐患开展行业通报，核心机构、经营机构和信息技术服务机构应当及时排查并采取风险防范措施。

第三十一条　核心机构和经营机构应当根据业务影响分析情况，建立健全网络安全应急预案，明确应急目标、应急组织和处置流程，应急场景应当覆盖网络安全事件和自然灾害突发、重大人事变动、信息技术服务机构退出等情形。

第三十二条　核心机构应当组织与本机构信息系统和网络通信设施相关联主体开展网络安全应急演练，频率不低于每年一次，并于演练后15个工作日内将相关情况报告中国证监会。

核心机构和经营机构应当定期开展网络安全应急演练，并形成应急演练报告存档备查。

第三十三条　核心机构和经营机构应当建立网络安全应急处置机制，及时处置网络安全事件，尽快恢复信息系统

的正常运行，保护事件现场和相关证据，向中国证监会及其派出机构进行应急报告，不得瞒报、谎报、迟报、漏报。

信息技术服务机构应当协助开展信息系统故障排查、修复等工作，并及时告知使用同类产品或者服务的核心机构和经营机构，配合开展风险排查和整改工作。

第三十四条 核心机构和经营机构应当在网络安全事件应急处置结束、系统恢复正常运行后组织内部调查，认定并追究事件责任，按照有关规定报告中国证监会及其派出机构。

核心机构和经营机构应当配合中国证监会及其派出机构，对网络安全事件进行调查处理，尽快完成整改。

第三十五条 核心机构和经营机构发生网络安全事件的，应当及时通过官方网站、自媒体等渠道公示相关方可以采取的替代方式或者其他应急措施，提示相关方防范和应对可能出现的风险。

核心机构和经营机构发生网络安全事件，损害投资者合法权益的，中国证监会及其派出机构可以要求其履行投资者告知义务。

第五章 关键信息基础设施网络安全

第三十六条 运营关键信息基础设施的核心机构和经营机构（以下简称证券期货业关基单位）应当按照法律法规

及中国证监会有关规定，开展关键信息基础设施安全保护工作，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第三十七条 证券期货业关基单位应当将关键信息基础设施安全保护情况纳入网络安全第一责任人、直接责任人和相关人员的责任考核机制。

证券期货业关基单位应当指定专项工作领导机构或者部门负责关键信息基础设施安全保护，配备至少五名网络安全专职人员，为每个关键信息基础设施指定一名网络安全管理责任人，并明确岗位职责和分工。网络安全专职人员履职前，证券期货业关基单位应当依法开展安全背景审查，相关人员不适合岗位要求的，应当及时调整。

第三十八条 证券期货业关基单位对关键信息基础设施实施运行变更或者下线移除，可能对证券期货市场安全平稳运行产生较大影响的，应当在遵守本办法第十五条的前提下，组织来自监管部门、行业机构、外部专业机构的专家开展专项评审；未通过评审的，证券期货业关基单位原则上不得实施运行变更、下线移除等操作。

证券期货业关键信息基础设施停止运营或者发生较大变化，可能影响认定结果的，相关机构应当及时将相关情况报告中国证监会及其派出机构。

第三十九条 证券期货业关基单位应当每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，网络安全检测和风险评估的内容包括但不限于：关键信息基础设施的运行情况、面临的主要威胁、风险管理情况、应急处置情况等。

第四十条 证券期货业关基单位采购网络产品和服务的，应当按照有关要求开展风险预判工作，评估投入使用后可能对关键信息基础设施安全保护、金融安全和国家安全带来的风险隐患，形成评估报告报送中国证监会及其派出机构，并依法开展网络安全审查。

第四十一条 证券期货业关基单位应当对关键信息基础设施的安全运行进行持续监测，定期开展压力测试，发现系统性能和网络容量不足的，应当及时采取系统升级、扩容等处置措施，确保系统性能容量不低于历史峰值的三倍，网络带宽不得低于历史峰值的两倍。

第四十二条 证券期货业关基单位应当在符合本办法第十八条规定的基础上，建设同城和异地灾难备份中心，实现数据同步保存。

证券期货业关基单位采取双活或者多活架构部署关键信息基础设施的，确保业务连续运行能力不低于前款规定的前提下，任一数据中心可视为其他数据中心的灾难备份设施。

第六章　网络安全促进与发展

第四十三条　鼓励核心机构、经营机构和信息技术服务机构在依法合规的前提下，积极开展网络安全技术应用工作，运用新技术提升网络安全保障水平。

第四十四条　核心机构和经营机构组织开展行业信息基础设施建设的，应当在保障本机构网络安全的前提下，为行业统筹提供服务，提升信息技术资源利用和服务水平。

第四十五条　核心机构和经营机构参加资本市场金融科技创新机制的，应当遵守有关规定，在依法合规、风险可控的前提下，有序开展金融科技创新与应用，借助新型信息技术手段，提升本机构证券期货业务活动的运行质量和效能。

信息技术服务机构参加资本市场金融科技创新机制的，应当遵守有关规定，持续优化技术服务水平，增强安全合规管理能力。

第四十六条　核心机构可以申请国家专业资质，开展证券期货业网络安全认证、检测、测试和风险评估等工作。相关核心机构应当保障充足的资源投入，完善内部管理制度和工作流程，保证工作专业性、独立性和公信力。

中国证监会定期对核心机构前款工作开展情况开展评估，评估通过的，可以将其作为证券期货业网络安全监管支撑单位，相关工作开展情况可以作为中国证监会及其派出机构实施监督管理的参考依据。

第四十七条 核心机构和经营机构应当加强网络安全人才队伍建设，建立与网络安全工作特点相适应的人才培养机制，确保网络安全人才的资质、经验、专业素质及职业道德符合岗位要求。

行业协会应当制定网络安全培训计划，定期组织培训交流，提高证券期货从业人员网络安全意识和专业素养。

第四十八条 核心机构和经营机构应当加强本机构网络安全宣传与教育，每年至少开展一次网络安全教育活动，提升员工网络安全意识。

经营机构应当定期组织开展面向投资者的网络安全宣传教育活动，结合网上证券期货业务活动的特点，揭示网络安全风险，增强投资者风险防范能力。

第四十九条 行业协会应当鼓励、引导网络安全技术创新与应用，增强自主可控能力，组织开展科技奖励，促进行业科技进步。

行业协会应当引导信息技术服务机构规范参与行业网络安全和信息化工作，促进市场公平竞争。

第七章 监督管理与法律责任

第五十条 中国证监会及其派出机构可以要求核心机构、经营机构和信息技术服务机构提供证券期货业网络安全

管理相关信息和数据。相关机构应当配合，及时、准确、完整提供相关资料。

第五十一条 核心机构和经营机构应当于每年4月30日前，完成对上一年网络安全工作的网络安全专项评估，编制网络安全管理年报，报送中国证监会及其派出机构，年报内容包括但不限于网络安全治理情况、人员情况、投入情况、风险情况、处置情况和下一年度工作计划等。

核心机构和经营机构报送网络安全管理年报时，可以与中国证监会要求的信息技术管理专项报告等其他年度信息技术类报告合并报送。

证券期货业关基单位应当将关键信息基础设施网络安全检测和风险评估情况纳入网络安全管理年报。

第五十二条 中国证监会及其派出机构可以委托国家、行业有关专业机构采用渗透测试、漏洞扫描及信息技术风险评估等方式，协助对核心机构、经营机构和信息技术服务机构开展监督、检查。

第五十三条 中国证监会可以根据国家有关要求或者行业工作需要，组织开展证券期货业重要时期网络安全保障。中国证监会派出机构负责督促本辖区经营机构和信息技术服务机构落实相关工作要求。

证券期货业重要时期网络安全保障期间，核心机构和经营机构应当遵循安全优先的原则，加强安全生产值守工作，

严格落实信息报送要求，原则上不得对重要信息系统和门户网站开展运行变更、下线删除等操作。

第五十四条 核心机构违反本办法规定的，中国证监会可以对其采取监管谈话、责令限期整改等监管措施；对有关高级管理人员给予警告、记过、诫勉谈话、通报批评、撤职等行政处分，并责令核心机构对其他责任人给予纪律处分。

经营机构和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对其采取责令改正、监管谈话、出具警示函等监管措施；对直接责任人和其他责任人员采取责令改正、监管谈话、出具警示函等监管措施；情节严重的，对相关机构及责任人员单处或者并处警告、十万元以下罚款，涉及金融安全且有危害后果的，并处二十万元以下罚款。

第五十五条 经营机构违反本办法规定，反映机构治理混乱、内控失效或者不符合持续性经营规则的，中国证监会及其派出机构可以依照《证券公司监督管理条例》第七十条、《证券投资基金法》第二十四条、《期货交易管理条例》第五十五条规定，采取责令暂停借助网络开展部分业务或者全部业务、责令更换董事、监事、高级管理人员或者限制其权利等监管措施。

信息技术服务机构违反本办法规定，未履行备案义务的，中国证监会及其派出机构可以依照《证券法》第二百一十三条规定予以处罚。

第五十六条 核心机构、经营机构和信息技术服务机构违反本办法第九条、第十条、第十七条、第十八条、第二十三条、第二十五条、第三十条、第三十一条、第三十三条规定，未履行网络安全保护义务，或者应急管理存在重大过失的，中国证监会及其派出机构可以依据《网络安全法》第五十九条第一款规定予以处罚。

第五十七条 核心机构和经营机构违反本办法第十六条、第三十五条规定，擅自暂停或者终止借助网络向投资者提供服务的，或者未按照规定及时告知投资者，中国证监会及其派出机构可以依照《网络安全法》第六十条规定予以处罚。

第五十八条 核心机构和经营机构违反本办法第二十六条规定，违规处理个人信息，或者处理个人信息未履行个人信息保护义务的，中国证监会及其派出机构可以依照《网络安全法》第六十四条、《个人信息保护法》第六十六条规定予以处罚。

第五十九条 核心机构和经营机构违反本办法第二十七条规定的，对法律法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，中国证监会及其派出机构可以依照《网络安全法》第六十八条第一款、第六十九条规定予以处罚。

第六十条 核心机构、经营机构和信息技术服务机构拒绝、阻碍中国证监会及其派出机构行使监督检查、调查职权的，中国证监会及其派出机构可以依法予以处罚。

第六十一条 核心机构和经营机构参加资本市场金融科技创新机制或者信息技术应用创新机制，相关项目发生网络安全事件，相关机构处置得当，积极消除不良影响的，中国证监会及其派出机构可以予以从轻或者减轻处罚，未对证券期货市场产生不良影响的，可以免于处罚。

第八章 附则

第六十二条 本办法中下列用语的含义：

（一）核心机构，是指证券期货交易场所、证券登记结算机构、期货保证金安全存管监控机构等承担证券期货市场公共职能、承担证券期货业信息基础设施运营的机构及其下属机构。

（二）经营机构，是指证券公司、期货公司和基金管理公司等证券期货经营机构。

（三）信息技术服务机构，是指为证券期货业务活动提供重要信息系统的开发、测试、集成、测评、运维及日常安全管理等产品或者服务的机构。

（四）证券期货业网络安全，是指核心机构、经营机构和信息技术服务机构采取必要措施，对内外部网络攻击、入

侵、干扰和破坏进行有效识别、监测、防范和处置，保障承载证券期货业务活动的信息系统安全平稳运行，确保相关网络数据的完整性、保密性和可用性。

（五）重要数据、核心数据，是指按照《数据安全法》、国家和证券期货业有关数据分类分级保护制度，确定的重要数据、核心数据。

（六）双活或者多活架构，是指在同城或者异地的两个或者多个数据中心同时对外提供服务，当其中一个或者多个数据中心发生灾难性事故时，可以将原先由其承载的服务请求划拨至其他正常运作的数据中心，保障业务连续运行。

（七）以上，是指本数以上（含本数）。

第六十三条 本办法规定的核心机构、经营机构和信息技术服务机构相关报告事项，是指依照监管职责，核心机构应当向中国证监会报告；除中国证监会另有要求的，经营机构和信息技术服务机构原则上应当向属地中国证监会派出机构报告。

第六十四条 国家对存储、处理涉及国家秘密信息的网络安全管理另有规定的，从其规定。

第六十五条 境内开展证券公司客户交易结算资金第三方存管业务、期货保证金存管业务的商业银行，证券投资咨询机构，基金托管机构和从事基金销售支付、份额登记、估值、评价等基金服务业务的机构，借助信息系统从事证券

期货业务活动的经营机构子公司，借助自身运维管理的信息系统从事证券投资活动且存续产品涉及投资者人数合计一千人以上的私募证券投资基金管理人，区域性股权市场运营机构，应当根据相关信息系统网络安全管理的特点，参照适用本办法。

第六十六条 本办法自2022 年 月 日起施行。2012 年11 月1 日公布的《证券期货业信息安全保障管理办法》（证监会令第82 号）同时废止。