证券期货业网络和信息安全管理办法

第一章　总则

第一条　为了保障证券期货业网络和信息安全，保护投资者合法权益，促进证券期货业稳定健康发展，根据《中华人民共和国证券法》（以下简称《证券法》）、《中华人民共和国期货和衍生品法》（以下简称《期货和衍生品法》）、《中华人民共和国证券投资基金法》（以下简称《证券投资基金法》）、《中华人民共和国网络安全法》（以下简称《网络安全法》）、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）、《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、使用网络及信息系统，信息技术系统服务机构为证券期货业务活动提供产品或者服务的网络和信息安全保障，以及证券期货业网络和信息安全的监督管理，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，建立健全网络和信息安全防护体系，提升安全保障水平，确保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。

信息技术系统服务机构应当遵循技术安全、服务合规的原则，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和信息安全，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和信息安全保护义务，对本机构网络和信息安全负责，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。

信息技术系统服务机构应当勤勉尽责，对提供产品或者服务的安全性、合规性承担责任。

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和信息安全发展规划、监管规则和行业标准；

（二）负责证券期货业网络和信息安全的监督管理，按规定做好证券期货业涉及的关键信息基础设施安全保护工作；

（三）负责证券期货业网络和信息安全重大技术路线、重大科技项目管理；

（四）组织开展证券期货业投资者个人信息保护工作；

（五）负责证券期货业网络安全应急演练、应急处置、事件报告与调查处理；

（六）指导证券期货业网络和信息安全促进与发展；

（七）支持、协助国家有关部门组织实施网络和信息安全相关法律、行政法规；

（八）法律法规规定的其他网络和信息安全监管职责。

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和信息安全监督管理体制。中国证监会科技监管部门对证券期货业网络和信息安全实施监督管理。中国证监会履行监管职责的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系统服务机构网络和信息安全实施日常监管。

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）依法制定行业网络和信息安全自律规则，对经营机构网络和信息安全实施自律管理。

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，督促其强化网络和信息安全管理，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 网络和信息安全运行

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，健全网络和信息安全管理制度体系，建立内部决策、管理、执行和监督机制，确保网络和信息安全管理能力与业务活动规模、复杂程度相匹配。

信息技术系统服务机构应当建立网络和信息安全管理制度，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和信息安全管理机制。

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和信息安全工作的第一责任人，分管网络和信息安全工作的领导班子成员或者高级管理人员为直接责任人。

核心机构和经营机构应当建立网络和信息安全工作协调和决策机制，保障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或者设立网络和信息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、组织应急演练等工作。

第十二条 核心机构和经营机构应当保障人员和资金投入与业务活动规模、复杂程度相适应，确保网络和信息安全人员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。

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网络安全等级保护相关要求，开展网络和信息系统定级备案、等级测评和安全建设等工作。

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工作开展情况报送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，应当充分评估技术和业务风险，制定风险防控措施、应急处置和回退方案，并对相关结果进行复核验证；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。

核心机构和经营机构不得在交易时段对重要信息系统进行变更，重要信息系统存在故障、缺陷，经评估须进行紧急修复的情形除外。

第十六条 核心机构和经营机构在重要信息系统上线、变更前应当制定全面的测试方案，持续完善测试用例和测试数据，并保障测试的有效执行。

除必须使用敏感数据的情形外，核心机构和经营机构应当对测试环境涉及的敏感数据进行脱敏，对未脱敏数据须采取与生产环境同等的安全控制措施。

核心机构交易、行情、开户、结算、通信等重要信息系统上线或者进行重大升级变更时，应当组织市场相关主体进行联网测试。

第十七条 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、替代方式及应对措施。

第十八条 核心机构和经营机构应当建立健全网络和信息安全监测预警机制，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。重要信息系统业务日志应当保存五年以上，系统日志应当保存六个月以上。

第十九条 核心机构和经营机构应当构建网络和信息安全防护体系，综合采取网络隔离、用户认证、访问控制、策略管理、数据加密、网站防篡改、病毒木马防范、非法入侵检测和网络安全态势感知等安全保障措施，提升网络和信息安全防护能力，及时识别、阻断相关网络攻击，保护重要信息系统和相关基础设施，防范信息泄露与损毁。

第二十条 核心机构和经营机构应当建立本地、同城和异地数据备份设施，重要信息系统应当每天至少备份数据一次，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重要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业务影响情况，确定恢复目标，保证业务连续运行。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，在确保业务连续运行的前提下，任一数据中心可视为其他数据中心的灾难备份设施。

第二十一条 核心机构和经营机构应当每年至少开展一次重要信息系统压力测试；发现市场较大波动，重要信息系统的性能容量可能无法保障安全平稳运行的，应当及时对相关信息系统开展压力测试。

核心机构和经营机构应当依照有关行业标准，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，从系统性能、网络负载、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，并保存五年以上。

核心机构和经营机构重要信息系统的性能容量应当在历史峰值的两倍以上。核心机构交易时段相关网络近一年使用峰值应当在当前带宽的百分之五十以下，经营机构交易时段相关网络近一年使用峰值应当在当前带宽的百分之八十以下。

第二十二条 核心机构和经营机构应当建立健全供应商管理机制，明确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，及时改进风险管理措施，健全应急处置机制，确保重要信息系统运行安全可控。

核心机构和经营机构应当与供应商签订合同及保密协议，明确约定各方保障网络和信息安全的权利和义务；在使用供应商提供产品或者服务时引发网络安全事件的，相关供应商有义务配合中国证监会及其派出机构查明网络安全事件原因，认定网络安全事件责任。

第二十三条 供应商为核心机构和经营机构提供重要信息系统相关产品或者服务的，应当依法作为信息技术系统服务机构向中国证监会备案。

核心机构和经营机构应当督促相关信息技术系统服务机构依法履行备案义务。

第二十四条 任何机构和个人不得违规开展证券期货业信息系统认证、检测、风险评估等活动，不得违规发布证券期货业信息安全漏洞、计算机病毒、网络攻击、网络侵入等信息。

第二十五条 核心机构和经营机构应当建立信息发布审核机制，加强对本机构和本机构运营平台发布信息的管理，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。

第二十六条 核心机构应当对交易、行情、开户、结算、风控、通信等重要信息系统具有自主开发能力，掌握执行程序和源代码并安全可靠存放。

经营机构应当根据自身发展需要，加强自主研发能力建设，持续提升自主可控能力。

核心机构和经营机构应当按照国家及中国证监会有关要求，开展信息技术应用创新以及商用密码应用相关工作。

第二十七条 中国证监会可以委托相关机构建设证券期货业备份数据中心，开展行业数据的集中备份和管理工作，并采取有效安全防护手段，防范数据损毁泄露风险，持续提升证券期货业重大灾难应对能力。

鼓励证券期货业关键信息基础设施运营者及时向证券期货业备份数据中心备份数据。其他核心机构和经营机构可以结合经营需要，自主选择证券期货业备份数据中心，开展数据级灾难备份工作。

第二十八条 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，不侵犯他人的知识产权，并采取有效措施保护本机构自主知识产权。

第三章 投资者个人信息保护

第二十九条 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，规范投资者个人信息处理行为，履行投资者个人信息保护义务，不得损害投资者合法权益。

第三十条 核心机构和经营机构处理投资者个人信息，应当建立健全投资者个人信息保护体系，明确相关岗位及职责要求，建立健全投资者个人信息处理、安全防护、应急处置、审计监督等管理机制，加强投资者个人信息保护。

第三十一条 核心机构和经营机构应当按照法律法规的规定及合同的约定处理投资者个人信息，明确告知投资者处理个人信息的目的、方式、范围和隐私保护政策，不得超范围收集和使用投资者个人信息，不得收集提供服务非必要的投资者个人信息。合同约定事项应当基于从事证券期货业务活动的必要限度。

核心机构和经营机构不得以投资者不同意处理其个人信息或者撤回同意为由，拒绝向投资者提供服务，为投资者提供服务所必需、履行法定职责或者法定义务等情形除外。

第三十二条 核心机构和经营机构处理投资者个人信息时，应当确保个人信息在收集、存储、使用、加工、传输、提供、公开、删除等处理过程中的合规、安全，防止个人信息的泄露、篡改、丢失。

第三十三条 核心机构和经营机构应当依法依规向第三方机构提供投资者个人信息，明确告知投资者个人信息处理目的、处理方式、个人信息种类、保存期限、保护措施以及相关方的权利和义务等，并取得投资者个人单独同意，履行法定职责或者法定义务的情形除外。

第三十四条 核心机构和经营机构在本机构网络安全防护边界以外处理投资者个人信息的，应当采取数据脱敏、数据加密等措施，防范化解投资者个人信息在处理过程中的泄露风险。

核心机构和经营机构通过短信、邮件等非自主运营渠道发送投资者敏感个人信息的，应当将投资者账号信息、身份证号码等敏感个人信息进行脱敏处理。

第三十五条 核心机构和经营机构利用生物特征进行客户身份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的客户身份认证方式，强制客户同意收集其个人生物特征信息。

第四章 网络和信息安全应急处置

第三十六条 核心机构、经营机构和信息技术系统服务机构发现网络和信息安全产品或者服务存在安全缺陷、安全漏洞等风险隐患的，应当及时核实并加固整改；可能对证券期货业网络和信息安全平稳运行产生较大影响的，应当向中国证监会及其派出机构报告。

第三十七条 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、自然灾害和公共卫生事件、本机构网络和信息安全相关重大人事变动、主要信息技术系统服务机构退出等情形。

第三十八条 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，每年至少开展一次，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。

第三十九条 核心机构和经营机构应当建立应急处置机制，及时处置网络安全事件，尽快恢复信息系统正常运行，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。

信息技术系统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。

第四十条 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，及时组织内部调查，完成问题整改，认定追究事件责任，并按照有关规定报告中国证监会及其派出机构。

第四十一条 核心机构和经营机构发生网络安全事件，对投资者造成影响的，应当及时通过官方网站、客户交易终端、电话或者邮件等有效渠道通知相关方可以采取的替代方式或者应急措施，提示相关方防范和应对可能出现的风险。

第五章 关键信息基础设施安全保护

第四十二条 证券期货业关键信息基础设施运营者应当按照法律法规及中国证监会有关规定，强化安全管理措施、技术防护及其他必要手段，保障经费投入，确保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。

第四十三条 证券期货业关键信息基础设施运营者应当将关键信息基础设施安全保护情况纳入网络和信息安全工作第一责任人、直接责任人和相关人员的责任考核机制。

第四十四条 证券期货业关键信息基础设施运营者应当指定专门机构或者部门负责关键信息基础设施安全保护管理工作，为每个关键信息基础设施指定网络和信息安全管理责任人，依法认定网络安全关键岗位，配备充足的网络和信息安全人员，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。

第四十五条 证券期货业关键信息基础设施运营者新建承载关键业务的重要网络设施、信息系统等，投入使用前应当按照关键信息基础设施安全保护相关要求开展安全检测和风险评估，检测评估通过后上线运行。

证券期货业关键信息基础设施运营者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，组织开展专家评审；未通过评审的，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，相关运营者应当及时将相关情况报告中国证监会及其派出机构。

第四十六条 证券期货业关键信息基础设施运营者应当每年至少进行一次网络和信息安全检测和风险评估，对发现的安全问题及时整改，网络和信息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。

第四十七条 证券期货业关键信息基础设施运营者采购网络产品或者服务的，应当按照国家网络安全审查制度要求开展风险预判工作；采购网络产品或者服务与关键信息基础设施密切相关，投入使用后可能影响国家安全的，应当及时申报网络安全审查。

第四十八条 证券期货业关键信息基础设施运营者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，确保系统性能容量在历史峰值的三倍以上，交易时段相关网络带宽应当在近一年使用峰值的两倍以上。

第四十九条 证券期货业关键信息基础设施运营者应当在符合本办法第二十条规定的基础上，建设同城和异地灾难备份中心，实现数据同步保存。

第六章 网络和信息安全促进与发展

第五十条 鼓励核心机构、经营机构和信息技术系统服务机构在依法合规的前提下，积极开展网络和信息安全技术应用工作，运用新技术提升网络和信息安全保障水平。

第五十一条 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和信息安全的前提下，为行业统筹提供服务，提升信息技术资源利用和服务水平。

第五十二条 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。

信息技术系统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。

第五十三条 核心机构可以申请开展证券期货业网络和信息安全相关认证、检测、测试和风险评估等监管支撑工作。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情况开展评估，评估通过的，可以将其作为证券期货业网络和信息安全监管支撑单位，相关工作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。

第五十四条 核心机构和经营机构应当加强网络和信息安全人才队伍建设，建立与网络和信息安全工作特点相适应的人才培养机制，确保人才资质、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和信息安全培训计划，定期组织培训交流，提高证券期货从业人员网络和信息安全意识和专业素养。

第五十五条 核心机构和经营机构应当加强本机构网络和信息安全宣传与教育，每年至少开展一次全员网络和信息安全教育活动，提升员工网络和信息安全意识。

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

第五十六条 行业协会应当鼓励、引导网络和信息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系统服务机构规范参与行业网络和信息安全和信息化工作，提升服务的安全合规水平，促进市场有序竞争。

第七章 监督管理与法律责任

第五十七条 核心机构、经营机构和信息技术系统服务机构应当向中国证监会及其派出机构报送或者提供证券期货业网络和信息安全管理相关信息和数据，确保有关信息和数据的真实、准确、完整。

第五十八条 中国证监会负责建立健全行业网络和信息安全态势感知工作机制，并就相关安全缺陷、安全漏洞等风险隐患开展行业通报预警。核心机构、经营机构和信息技术系统服务机构应当及时排查并采取风险防范措施。

第五十九条 核心机构和经营机构应当于每年 4 月 30 日前，完成对上一年网络和信息安全工作的专项评估，编制网络和信息安全管理年报，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和信息安全治理情况、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和信息安全管理年报时，可以与中国证监会要求的信息科技管理专项报告等其他年度信息科技类报告合并报送，关键信息基础设施安全保护年度计划除外。

证券期货业关键信息基础设施运营者应当将关键信息基础设施网络和信息安全检测和风险评估情况纳入网络和信息安全管理年报。

第六十条 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漏洞扫描、风险评估等方式，协助对核心机构、经营机构和信息技术系统服务机构开展监督、检查。

第六十一条 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和信息安全保障。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系统服务机构落实相关工作要求。

证券期货业重要时期网络和信息安全保障期间，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，严格落实信息报送要求。

第六十二条 核心机构违反本办法规定的，中国证监会可以对其采取责令改正、监管谈话等监管措施；对有关高级管理人员给予警告、记过、记大过、降级、撤职、开除等行政处分，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系统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、责令公开说明、责令定期报告、责令增加内部合规检查次数等监管措施；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。

第六十三条 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《证券法》、《期货和衍生品法》、《证券投资基金法》相关规定，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。

信息技术系统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》、《期货和衍生品法》相关规定予以处罚。

第六十四条 核心机构、经营机构和信息技术系统服务机构违反本办法第九条、第十条、第十八条、第十九条、第二十条、第三十七条、第三十九条规定，未履行网络和信息安全保护义务，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照《网络安全法》相关规定予以处罚。

证券期货业关键信息基础设施运营者未履行本办法第九条、第十条、第十八条、第十九条、第二十条、第二十二条、第三十七条、第三十八条、第四十二条、第四十四条、第四十六条、第四十九条、第五十五条规定的网络安全保护义

务的，中国证监会及其派出机构可以依照《网络安全法》、《关键信息基础设施安全保护条例》相关规定予以处罚。

第六十五条 核心机构和经营机构违反本办法第十七条、第三十六条规定，擅自暂停或者终止借助网络向投资者提供服务，对其产品、服务存在安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时报告的，中国证监会及其派出机构可以依照《网络安全法》相关规定予以处罚。

第六十六条 违反本办法第二十四条规定，开展证券期货业信息系统认证、检测、风险评估等活动，或者向社会发布证券期货业信息安全漏洞、计算机病毒、网络攻击、网络侵入等信息的，中国证监会及其派出机构可以依照《网络安全法》相关规定予以处罚。

第六十七条 核心机构和经营机构违反本办法第二十五条规定，对法律、行政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》相关规定予以处罚。

第六十八条 核心机构和经营机构违反本办法第三十一条第一款、第三十二条、第三十三条规定，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》、《个人信息保护法》相关规定予以处罚。

第六十九条 核心机构、经营机构和信息技术系统服务机构拒绝、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。

第七十条 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

第七十一条 本办法中下列用语的含义：

（一）核心机构，包括证券期货交易场所、证券登记结算机构等承担证券期货市场公共职能、承担证券期货业信息技术公共基础设施运营的证券期货市场核心机构及其承担上述相关职能的下属机构。

（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）信息技术系统服务机构，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）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。

（五）重要信息系统，是指承载证券期货业关键业务活动，如出现系统服务异常、数据泄露等情形，将对证券期货市场和投资者产生重大影响的信息系统。

（六）可能对证券期货市场安全平稳运行产生较大影响，是指依据网络安全事件调查处理有关办法，可能引发较大或者以上级别网络安全事件的情形。

（七）“以上”含本数，“以下”不含本数。

第七十二条 本办法规定的核心机构、经营机构和信息技术系统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系统服务机构原则上应当向属地中国证监会派出机构报告。

第七十三条 国家对存储、处理涉及国家秘密信息的网络和信息安全管理另有规定的，从其规定。

第七十四条 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，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基金份额持有人账户合计一千人以上的私募证券投资基金管理人，应当根据相关信息系统网络和信息安全管理的特点，参照适用本办法。

核心机构和经营机构设立信息科技专业子公司，为母公司提供信息科技服务的，信息科技专业子公司应当按照本办法落实网络和信息安全相关要求。

第七十五条 本办法自2023年5月1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。