

关于印发《证券期货业信息安全保障管理暂行办法》的通知

上海、深圳证券交易所，上海期货交易所，大连、郑州商品交易所，中国证券登记结算公司，中国证券业、期货业协会：

为规范行业网络与信息系统建设和安全保障工作，中国证监会制定了《证券期货业信息安全保障管理暂行办法》，现印发给你们，请遵照执行。

请中国证券业协会、中国期货业协会将本通知转发至各会员单位。

中国证券监督管理委员会

二〇〇五年四月八日

证券期货业信息安全保障管理暂行办法

第一章 总则

第一条 为加强证券期货业信息安全保障工作的组织协调，建立、健全信息安全管理制度和运行机制，提高行业信息安全保障工作水平，切实保护投资者合法权益，根据国家有关法律、法规和相关规定，制定本办法。

第二条 本办法适用于证券期货市场的监管机构、行业自律组织及经营机构。监管机构为中国证券监督管理委员会（以下简称“中国证监会”）；行业自律组织包括证券、期货交易所及其通信公司，证券登记结算公司、中国证券业协会和中国期货业协会；经营机构包括证券、期货公司，基金管理公司及证券、期货投资咨询公司。

第二章 安全职责划分

第三条 中国证监会负责证券期货行业信息安全保障工作的监督管理及组织协调。

第四条 证券、期货交易所及其通信公司，登记结算公司，证券、期货公司，基金管理公司，证券、期货投资咨询公司等是各自信息系统安全运营管理的责任主体单位（以下简称“主体单位”）。

第五条 证券交易所负责证券交易、信息发布及市场监管信息系统的安全运营。证券通信公司受证券交易所及证券登记结算公司、经营机构的委托，负责通信系统的安全运营，保障交易、结算等业务数据的及时安全传送。期货交易所负责期货交易和结算处理、信息发布、市场监管信息系统及通信系统的安全运营。

第六条 证券登记结算公司负责证券登记、结算业务信息系统的安全运营。

第七条 中国证券业协会负责证券公司、基金管理公司、证券投资咨询公司等会员单位信息安全保障的组织、协调工作。

中国期货业协会负责期货公司、期货投资咨询公司等会员单位信息安全保障的组织、协调工作。

第八条 证券、期货公司，基金管理公司及证券、期货投资咨询公司负责总部及下属经营机构信息系统的安全运营。

第三章 安全目标与基本原则

第九条 信息安全保障工作的总体目标是确保信息和信息系统的完整性、保密性、可用性、时效性、可审查性和可控性，切实保护市场参与各方的合法权益，促进证券期货市场的持续、稳定、健康发展。

第十条 信息安全保障工作的具体目标是：

（一）保护证券期货业信息系统的物理环境、设备设施和运行环境，保证信息系统的环境安全；

（二）确保信息内容的合法性，保护信息在采集、传输、使用和存储过程中的保密性、完整性、可用性、时效性、可审查性和可控性，保证信息的安全；

（三）提高证券期货业人员的信息安全意识、安全专业素质以及安全管理与服务水平；

（四）提高信息系统的可用率和灾难恢复能力，为业务的可持续性运行提供保障。

第十一条 信息安全保障工作应遵循以下基本原则：

（一）责任制原则：安全管理应做到“谁主管，谁负责”、“谁运营，谁负责”，注重以法律手段明确与他方的责任关系，通过契约、协调等方式与他方进行责任划分，明确进行风险转移，通过责任主体制约他方。

（二）规范化原则：遵循国内、国际的信息安全标准及行业规范，对信息系统实行等级保护。

（三）全面统筹原则：信息安全保障工作应贯穿于信息化全过程，坚持统筹规划、突出重点，安全与发展并进，管理与技术并重，应急防御与长效机制相结合。

（四）实用性原则：在确保信息系统性能和安全的前提下，充分利用资源，讲究实效，避免重复和盲目投资，积极采用国家法律法规允许的、成熟的先进技术和专业安全服务，运用科学的经营管理方法，降低成本，保障安全运行。

第四章 安全保障要求

第十二条 主体单位应建立以安全组织体系为核心、安全管理体系为保障、安全技术体系为支撑的全面信息安全体系，保持三个体系稳定、均衡发展。

第十三条 主体单位应建立明确的信息安全组织体系：

（一）建立决策层、管理层和执行层三层工作关系，明确信息安全主管领导，落实信息安全管理部門，指定信息安全执行岗位；

（二）设立专职的安全管理员和安全审计员岗位，分别负责信息安全工作的实施和审计；

（三）通过多种安全培训方式加强信息安全人才队伍的建设，提高信息安全工作人员的技能水平，提高员工安全意识。

第十四条 主体单位应建立全面的信息安全管理体系：

（一）制定统一的信息安全策略和全面、可操作的信息安全管理制度，指导和规范信息系统的安全规划与建设，确保策略和制度得到恰当的理解并得到有效的遵循和执行；

（二）加强信息系统资产安全管理，保护信息系统设备、软件、数据和技术文档的安全，实行信息系统资产管理责任制，实现等级管理、密级管理，重点保护核心信息系统资产的安全；

（三）强化信息系统的物理安全保护，执行严格的机房安全管理、环境安全管理和有效的物理控制措施；

（四）建立信息系统网络、系统、应用等各层面的安全管理流程，实现对信息系统规划、建设、运行、维护各个阶段的安全管理，开发与运营独立管理，严格执行日常的实时管理和定期管理工作；

（五）实现对信息系统的安全风险管理，对信息资产、威胁和脆弱性的状况进行定期评估，及时发现安全隐患并进行预防性的保护，选择适用、有效的安全措施。

第十五条 主体单位应建立有效的信息安全技术体系：

（一）建立完善的安全预警体系，及时发现安全隐患；

（二）强化现有的安全防护体系，实现对核心业务系统的重点保护；

（三）建立有效的安全监控体系，监控核心业务系统，为进一步完善信息安全体系提供决策依据；

（四）建立全面的应急响应体系，制定规范、完整的应急处理和响应流程，定期进行应急恢复的演练和测试，完善信息安全通报机制；

（五）按照不同的安全保护等级建立相应的灾难恢复体系，定期进行灾难恢复的演练和测试，确保灾难发生后能够充分发挥备份的效能，降低造成的影响和损失。

第五章 附则

第十六条 中国证监会对证券期货业信息系统安全保障情况组织安全检查，检查方式包括自查、委托检查等方式。

第十七条 本办法由中国证监会负责解释。

第十八条 本办法自印发之日起执行。