证联网信息安全管理规范

证联网管理办公室

2018.05

第一章 总则

第一条 为保障证联网安全稳定运行，加强证联网信息安全管理工作，根据《中华人民共和国网络安全法》《证券期货业信息安全保障管理办法》《证券期货业信息系统运维管理规范》《证券期货业信息系统安全等级保护基本要求》《证券期货业信息系统审计指南》等相关法律法规、规章制度，制定本规范。

第二条 本规范适用于证联网信息安全管理与保障等相关工作。

第三条 证联网信息安全管理工作实行“谁运行、谁负责，谁使用、谁负责”和“安全优先、保障发展”的原则。

第四条 证券期货业信息化工作领导小组办公室（以下简称证信办）负责证联网信息安全管理工作的指导、监督和检查。证联网管理办公室（以下简称网管办）是证信办领导下的证联网议事机构，负责制定证联网信息安全工作的总体方针、安全策略和管理制度。

第五条 证联网运管中心（以下简称运管中心）负责证联网信息安全的整体监测、协调等工作。证联网各承建单位（以下简称承建单位）负责各自节点的信息安全监测和保障工作，并承担本节点的安全运行责任。

第六条 证联网接入机构（以下简称接入机构）负责本机构网络的安全管理，并负责本机构业务系统的安全保障。

第二章 基本要求

第七条 网管办、运管中心、承建单位和接入机构在证联网规划、建设、运维过程中应充分考虑国家和监管部门的信息安全相关要求，

同步配套健全安全管理制度和设施。

第八条 运管中心、承建单位和接入机构应加强沟通协作，共同保障证联网安全。

第九条 运管中心、各承建单位应当按照证券期货业信息安全等级保护第三级的要求，保障证联网生产网的网络安全。接入机构应按照所属行业信息安全等级保护第三级的要求，做好直连证联网生产网设备的安全防护。

第十条 承建单位和接入机构应当确保接入证联网的设备符合国家和金融行业的安全标准、技术规范和质量要求。

第十一条 本规范中的相关要求纳入《证券期货行业信息系统审计指南》，运管中心、各承建单位以及接入机构应严格按照相关要求进行自我检查和评价，做好证联网信息安全管理工作。

第三章 网管办职责

第十二条 网管办负责制定证联网信息安全工作的总体方针、安全策略和管理制度，并根据证联网的发展情况及时评估调整。

第十三条 网管办负责对接入机构的证联网接入方案和业务上线方案进行安全评估。

第十四条 网管办负责证联网内部安全审计、安全检查等工作。

第四章 承建单位及运管中心职责

第十五条 承建单位应设置证联网信息安全管理员，建立主备岗，并对其进行安全背景审查。信息安全管理员负责本节点信息安全工作。

第十六条 运管中心和承建单位应按照《证联网信息安全事件应急预案》要求，做好应急准备工作，并按要求报告和处置信息安全事件，运管中心应定期组织各承建单位进行应急演练。

第十七条 运管中心和承建单位定期开展证联网配置检查。一旦发现接入机构违反证联网有关规定，将视情况要求限期整改或暂停证联网服务。

第十八条 承建单位应建立节点网络安全监测系统，实现对本节点的网络攻击、网络侵入和计算机病毒等危害网络安全行为的监测。运管中心应建立全网集中安全监测系统，汇总各节点网络安全事件，实现全网安全监测。

第十九条 承建单位应建立节点网管系统，实现本节点网络设备和线路的实时监控。运管中心应建立全网集中网管系统，实现全网运行状态监控。网络日志应留存不少于六个月。

第二十条 运管中心和承建单位发现接入机构在证联网传播法律、法规禁止传输的信息，或者对证联网进行网络攻击、网络侵入、传播计算机病毒等危害网络安全的行为，应立即通知接入机构停止违规行为，并报告证信办。机构拒不执行的，运管中心和承建单位有权暂停其接入证联网。

第二十一条 运管中心应当建立网络信息安全投诉举报热线和邮箱，及时受理投诉和举报，并协调相关机构处理。

第二十二条 承建单位应当与证联网设备和服务提供商签订安全保密协议，明确安全保密责任义务。

第二十三条 运管中心应每月编制全网运行状况和网络安全报告，报送证信办并通告承建单位。

第五章 接入机构职责

第二十四条 接入机构应根据国家、行业信息安全和应急管理相关规定以及本规范的要求，制定网络和信息安全应急预案，并定期演练。

第二十五条 接入机构应当配合运管中心和承建单位进行配置检查、应急演练和应急处置等工作。

第二十六条 接入机构应当按照证联网要求的网络接入方式接入，并按要求为接入路由器、服务器、终端等设备分配 IP 地址并进行网络配置。

第二十七条 接入机构负责自身网络和业务系统的安全保障，应当采取足够的安全防护措施，有效防范其他接入机构的安全隐患波及自身安全。发现其他接入机构存在安全隐患时，应及时告知相关机构，并向运管中心报告。

第二十八条 接入机构负有保护证联网安全的共同义务，应在网络边界处部署设备或采取相应的技术措施，按照权限最小化原则进行双向访问控制，检查并阻止非授权的、非法的流量进入证联网，防止非授权用户、病毒、恶意程序和黑客通过接入机构的网络、系统或终端攻击证联网。

第二十九条 接入机构应做好网络隔离和安全防护措施，实现机构内网、证联网与互联网的有效隔离，禁止接入证联网的服务器、终

端等设备访问互联网。

第三十条 接入机构自身业务系统不得设置恶意程序，发现自身设备、系统存在安全缺陷、漏洞等风险时，应当立即采取补救措施。如可能对证联网造成安全隐患，应及时向运管中心报告。

第三十一条 接入机构负责自身接入证联网终端的安全管理，接入证联网的终端设备必须按照国家及行业发布的相关法律、法规、规定做好安全加固及防护工作。此外，接入机构还应该采取必要的技术措施，对接入证联网的终端进行主机监控、移动介质管理、非授权外连管理等。

第三十二条 接入机构应当充分了解并评估证联网的安全保密条件是否满足自身业务的需求，如果业务有更高的安全保密要求，接入机构应当自行采用数据加密等安全措施，保障数据安全。

第三十三条 接入机构应当充分了解评估证联网的传输能力、备份能力和容错能力能否满足自身业务的连续性要求，如果业务需要更高的保障条件，接入机构应当自行采取额外的线路备份、系统备份和业务备份等措施，切实保证自身业务的连续性。

第三十四条 接入机构不得在证联网上传播威胁国家安全，危害公民隐私等法律、法规禁止传输的信息。

第六章 附则

第三十五条 本规范由证信办负责发布和解释。

第三十六条 本规范自发布之日起施行。