中国银保监会监管数据安全管理办法(试行)

第一章 总 则

第一条 为规范银保监会监管数据安全管理工作，提高监管数据安全保护能力，防范监管数据安全风险，依据《中华人民共和国网络安全法》《中华人民共和国银行业监督管理法》《中华人民共和国保险法》《工作秘密管理暂行办法》等法律法规及有关规定，制定本办法。

第二条 本办法所称监管数据是指银保监会在履行监管职责过程中，依法定期采集,经监管信息系统记录、生成和存储的，或经银保监会各业务部门认定的数字、指标、报表、文字等各类信息。

本办法所称监管信息系统是指以满足监管需求为目的开发建设的，具有数据采集、处理、存储等功能的信息系统。

第三条 本办法所称监管数据安全是指监管数据在采集、处理、存储、使用等活动(以下简称监管数据活动)中，处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。

第四条 银保监会及受托机构开展监管数据活动，适用本办法。

本办法所称受托机构是指受银保监会委托或委派，为银保监会提供监管数据采集、处理或存储服务的企事业单位。

第五条 开展监管数据活动，必须遵守相关法律和行政法规。任何单位和个人对在监管数据活动中知悉的国家秘密、工作秘密、商业秘密和个人信息，应当依照相关规定予以保密。

第六条 银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。

第二章 工作职责

第七条 监管数据安全管理实行归口管理，建立统筹协调、分工负责的管理机制。

银保监会统计信息部门是归口管理部门，负责统筹监管数据安全管理工作。银保监会各业务部门负责本部门监管数据安全管理工作。

第八条 归口管理部门具体职责包括：

(一)制定监管数据安全工作规则和管理流程；

(二)制定监管数据安全技术防护措施；

(三)组织实施监管数据安全评估和监督检查。

第九条 各业务部门具体职责包括：

(一)规范本部门监管数据安全使用，明确具体工作要求，落实相关责任；

(二)组织开展本部门监管数据安全管理工作；

(三)协助归口管理部门实施监管数据安全监督检查。

第三章 监管数据采集、存储和加工处理

第十条 监管数据的采集应按照安全、准确、完整和依法合规的原则进行，避免重复、过度采集。

第十一条 监管数据应通过监管工作网或金融专网进行传输。因客观条件限制需要通过物理介质、互联网或其它网络传输的，应经归口管理部门评估同意。

第十二条 监管数据应存储在银保监会机房，并具有完备的备份措施。确有必要存储在受托机构机房的，应经归口管理部门评估同意。

第十三条 监管数据存储期限、存储介质管理应按照国家和银保监会有关规定执行。

第十四条 监管数据的加工处理应在监管工作权限或受托范围内进行。未经归口管理部门同意，任何单位和个人不得将代码、接口、算法模型和开发工具等接入监管信息系统。

第十五条 监管数据采集、传输、存储、加工处理、转移交换、销毁，以及用于系统开发测试等活动，应根据监管数据类型和管理要求采取分级分类安全技术防护措施。

第四章 监管数据使用

第十六条 监管数据仅限于银保监会履行监管工作职责使用。纪检监察、司法、审计等党政机关为履行工作职责需要使用监管数据时，按照有关规定办理。

第十七条 监管数据的使用行为应通过管理和技术手段确保可追溯。监管数据用于信息系统开发测试以及对外展示时，应经过脱敏处理。

第十八条 使用未公开披露的监管数据，原则上应在不可连接互联网的台式机或笔记本等银保监会工作机中进行。因客观条件限制需采取虚拟专用网络等方式使用监管数据时，应经归口管理部门评估同意。

第十九条 因工作需要下载的监管数据，仅可存储于银保监会的工作机中。承载监管数据的使用介质应妥善保管，防止数据泄露。

第二十条 在使用监管数据过程中产生的加工数据、汇总结果等信息应视同监管数据进行安全管理。

第二十一条 监管数据对外披露应由指定业务部门按照有关规定和流程实施。

第二十二条 各业务部门因工作需要向非党政机关单位、个人提供监管数据时，应充分评估数据安全风险，经本部门主要负责人同意后实施，必要时与对方签订备忘录和保密协议并报归口管理部门备案。

与境外监管机构或国际组织共享监管数据时，应由国际事务部门依照银保监会签署的监管合作谅解备忘录、合作协议等约定或其他有关工作安排进行管理。

法律法规另有规定的，从其规定。

第二十三条 各业务部门因工作需要和系统下线停用监管数据时，应及时对其采取封存或销毁措施。

第五章 监管数据委托服务管理

第二十四条 各业务部门监管数据采集涉及受托机构提供服务时，应事先与归口管理部门沟通并会签同意。受托机构的技术服务方案，应通过归口管理部门的安全评估。技术服务方案发生变更的，应事先报归口管理部门进行安全评估。

安全评估不通过的，不得开展委托服务或建立委派关系。

第二十五条 为银保监会提供监管数据服务的受托机构，应满足以下基本条件：

(一)具备从事监管数据工作所需系统的自主研发及运维能力；

(二)具备相关信息安全管理资质认证;

(三)拥有自主产权或已签订长期租赁合同的机房;

(四)网络和信息系统具备有效的安全保护和稳定运行措施,三年内未发生网络安全重大事件;

(五)具备有效的监管数据安全管理措施,能够保障银保监会各部门对监管数据的访问和控制;

(六)具有监管数据备份体系、应急组织体系和业务连续性计划。

第二十六条 银保监会通过与受托机构签订协议,确立监管数据委托服务关系。协议应明确服务项目、期限、安全管理责任和终止事由等内容。

银保监会通过委派方式确立监管数据服务关系的,应下达委派任务书。

第二十七条 因有关政策调整导致原委托或委派事项无需继续履行,或发现受托机构监管数据服务出现重大安全问题的,银保监会有权终止委托或委派关系。

委托或委派关系终止时,受托机构应及时、完整地移交监管数据,并销毁因委托或委派事项而获取的监管数据,不得保留相关数据备份等内容。

第六章 监督管理

第二十八条 各业务部门及受托机构应按照监管数据安全工作规则定期开展自查,发现监管数据安全缺陷、漏洞等风险时,应立即采取补救措施。

第二十九条 归口管理部门应定期对各业务部门及受托机构开展监管数据安全管理评估检查工作。

各业务部门及受托机构对于评估和检查中发现的问题应制定整改措施,及时整改,并向归口管理部门报送整改报告。

第三十条 各业务部门及受托机构发生以下监管数据重大安全风险事项时,应立即采取应急处置措施,及时消除安全隐患,防止危害扩大,并于48小时内向归口管理部门报告。

(一)监管数据发生泄露或非法使用;

(二)监管数据发生损毁或丢失;

(三)承载监管数据的信息系统或网络发生系统性故障造成服务中断 4 小时以上；

(四)承载监管数据的信息系统或网络遭受非法入侵、发生有害信息或计算机病毒的大规模传播等破坏；

(五)监管数据安全事件引发舆情；

(六)《网络安全重大事件判定指南》列明的其他影响监管数据安全的网络安全重大事件。

辖区发生以上监管数据重大安全风险事项时，各银保监局应立即采取补救措施，并于 48 小时内向银保监会归口管理部门报告。

第三十一条 归口管理部门应建立监管数据安全事件通报工作机制，及时通报监管数据安全事件。

第七章 附 则

第三十二条 涉密监管数据按照国家和银保监会保密管理有关规定进行管理。

第三十三条 各银保监局承担辖区监管数据安全管理责任，参照本办法制定辖区监管数据安全管理办法，明确职责和管理要求，强化监管数据安全保护。

第三十四条 本办法自印发之日起施行。