金融业网络安全管理办法

（征求意见稿）

第一章 总则

第一条（目的和依据）为了全面规范金融业网络安全管理，保障金融服务，维护金融安全，根据《中华人民共和国网络安全法》《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》《关键信息基础设施安全保护条例》《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条（适用范围）金融从业机构在中华人民共和国境内建设、运营、维护和使用网络，以及金融业网络安全的监督管理，适用本办法。其他有关主管部门有规定的，还应当依法遵守其规定。国家对存储、处理涉及国家秘密信息的网络安全管理有规定的，从其规定。

第三条（网络安全保护总体要求）金融从业机构应当依照法律、行政法规、国家和国务院金融管理部门有关规定履行网络安全保护义务，对本机构网络安全负主体责任。金融从业机构应当坚持网络安全与信息化发展并重，为网络安全工作提供必要资源保障，建立健全适用本机构的网络安全保障体系，提高网络安全保护能力，有效管控网络安全风险，防范网络违法犯罪活动。

金融从业机构应当积极为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第四条（行业自律）金融业各行业协会应当加强自律管理，依法制定网络安全行为规范和团体标准，指导会员加强网络安全保护。

第二章 网络安全保护义务

第五条（网络安全工作责任制）金融从业机构应当按照国家有关规定建立和落实网络安全责任制，确定网络安全负责人。

第六条（网络安全治理）金融从业机构应当建立网络安全管理组织架构和议事决策机制，指定网络安全牵头管理部门，保障本机构网络安全资金和人员投入，制定内部网络安全管理制度和操作规程，明确本机构、分支机构、下属法人机构等的网络安全保护职责，督促落实网络安全保护责任。

第七条（网络运行安全）金融从业机构应当依照法律、行政法规、国家和国务院金融管理部门有关规定，开展网络运行监测、网络安全风险和事件处置报告等工作，建立健全网络安全事件应急预案，采取相应的技术和管理措施，保障网络运行安全。

第八条（网络安全等级保护）金融从业机构应当按照国家网络安全等级保护制度要求，合理确定网络的安全保

护等级，履行定级备案义务，按期开展网络安全等级测评，及时整改测评发现的风险。

第九条（商用密码使用）金融从业机构应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国务院金融管理部门对使用商用密码有进一步规定的，金融从业机构应当按照规定执行。

第十条（网络数据保护）金融从业机构应当依照法律、行政法规、国家和国务院金融管理部门有关规定，加强网络数据分类分级管理，采取相应的技术和管理措施，防止网络数据遭到篡改、破坏、泄露或者非法获取、非法利用。

第十一条（网络个人信息保护）金融从业机构应当依照法律、行政法规、国家和国务院金融管理部门有关规定，规范个人信息处理活动，保障个人信息安全。

鼓励金融从业机构使用国家网络身份认证公共服务开展用户身份核验。

第十二条（技术创新应用）金融从业机构应当依照法律、行政法规、国家和国务院金融管理部门有关规定，做好信息技术应用创新的风险管理。

第十三条（违法违规信息防范）金融从业机构应当采取措施并依照法律、行政法规、国家和国务院金融管理部门有关规定，加强对网络发布信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记

录，并向有关主管部门报告。

第十四条（信息服务安全管理）向公众提供应用软件下载服务的金融从业机构，应当采取措施并依照法律、行政法规和国家有关规定，履行恶意程序和违法违规信息检测等安全管理义务。发现应用软件存在设置恶意程序，或者含有法律、行政法规禁止发布、传输的信息的，金融从业机构应当立即停止提供下载服务，保存有关记录，并向有关主管部门报告。

第十五条（金融业关键信息基础设施认定）国务院金融管理部门按照金融业关键信息基础设施认定规则组织识别金融业关键信息基础设施，确定认定结果，及时通知金融业关键信息基础设施运营者（以下简称运营者），并通报国务院公安部门，抄送国家网信部门。

运营者发生合并、分立、解散等情况，或者关键信息基础设施发生较大变化可能影响认定结果的，运营者应当按照国务院金融管理部门有关规定及时报告相关情况。

第十六条（运营者组织架构及履职保障）运营者主要负责人对金融业关键信息基础设施安全保护负总责，运营者应当明确主管网络安全的领导班子成员作为首席网络安全官，分管关键信息基础设施安全保护工作，并为每个关键信息基础设施明确一名安全管理责任人，负责组织落实该关键信息基础设施的安全保护工作。

运营者应当设置专门安全管理机构，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。

专门安全管理机构应当按照国务院金融管理部门有关规定，报送关键信息基础设施安全保护计划和网络安全工作总结。

第十七条（供应链安全）运营者应当按照国家网络安全审查规定和金融行业预判指南申报网络安全审查，并按照国务院金融管理部门有关规定报送年度网络产品和服务、云计算服务采购清单。

运营者应当按照关键信息基础设施商用密码使用管理相关规定，规范商用密码使用。

第十八条（风险评估）运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，内容至少应当包括网络安全等级测评、商用密码应用安全性评估、关键信息基础设施安全保护相关制度和国家标准的落实情况、关键信息基础设施处理的数据和个人信息的保护情况、关键信息基础设施相关网络安全风险监测处置情况和网络安全事件应急处置改进落实情况。运营者应当及时整改检测评估发现的安全问题，按照国务院金融管理部门有关规定每年报送检测评估和整改情况。

第十九条（网络安全事件应急预案）运营者应当按照国家网络安全事件应急预案和金融业关键信息基础设施网络安全事件应急预案，制定本机构关键信息基础设施应急预案，定期进行演练，规范与关键信息基础设施相关的网络安全事件和重大网络安全威胁的报告与处置程序。

第三章 监督管理协同

第二十条（监督管理协同原则）国务院金融管理部门依照法律、行政法规和党中央、国务院决策部署，按照监管职责分工，在职责范围内负责金融从业机构网络安全管理相关工作。

国务院金融管理部门应当支持配合国家网信部门、国务院公安部门、国家密码管理部门和其他有关主管部门依据职责开展涉及金融业的网络安全保护和监督管理工作。

国务院金融管理部门分支机构、派出机构按照国务院金融管理部门职责分工，开展本辖区内的网络安全监督管理工作。

第二十一条（网络安全专项任务协同落实）党中央、国务院或者有关决策议事协调机构已明确分工的，由国务院金融管理部门按照分工负责；已明确由某一国务院金融管理部门牵头负责的事项，该牵头负责部门应当依据法律法规的授权与规定，在既定职责框架内进一步细化相关国务院金融管理部门的职责分工；不属于以上两类情形的，由国务院金融管理部门沟通协商后，明确各自职责分工。

第二十二条（信息共享）国务院金融管理部门及其同级分支机构、派出机构间强化网络安全事件、风险、态势、情报等信息的共享，视情会商研判涉及金融业的整体风险态势。

第二十三条（配合监督管理）金融从业机构应当自觉接受、配合有关主管部门和国务院金融管理部门及其分支机构、派出机构对其开展的各项网络安全监督管理工作，按时提供真实完整信息、资料，不得拒绝、阻碍有关主管部门和国务院金融管理部门及其分支机构、派出机构依法实施的监督检查。

第四章 法律责任

第二十四条（传输违法违规信息的处理）金融从业机构对恶意程序和法律、行政法规禁止发布或者传输的信息，未及时停止传输、采取消除等处置措施、保存有关记录的，国务院金融管理部门及其分支机构、派出机构将相关案件信息移送同级有关主管部门，并配合其依法依规予以处理。

第二十五条（未按照规定使用商用密码的处理）金融从业机构未按照国家网络安全等级保护制度要求使用商用密码保护网络安全的，运营者违反关键信息基础设施商用密码使用管理规定的，国务院金融管理部门及其分支机构、派出机构将相关案件信息移送同级密码管理部门，并配合其依法依规予以处理。

第二十六条（不配合监督检查的处罚）金融从业机构拒绝、阻碍国务院金融管理部门及其分支机构、派出机构对其开展网络安全监督检查的，国务院金融管理部门及其

分支机构、派出机构分别依照《中华人民共和国中国人民银行法》《中华人民共和国商业银行法》《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》《中华人民共和国证券法》《中华人民共和国证券投资基金法》《中华人民共和国期货和衍生品法》《中华人民共和国网络安全法》《私募投资基金监督管理条例》《中华人民共和国外汇管理条例》有关规定予以处罚。

第二十七条（违反其他网络安全保护义务的处罚）金融从业机构未履行本办法规定的网络安全保护义务，《中华人民共和国网络安全法》《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》《关键信息基础设施安全保护条例》《网络数据安全管理条例》已作出处罚规定的，国务院金融管理部门及其分支机构、派出机构，依照上述法律、行政法规规定，按照监管职责分工予以处罚；上述法律、行政法规未作出处罚规定但其他法律、行政法规作出处罚规定的，依照规定予以处罚。

第二十八条（其他法律责任）金融从业机构未履行本办法规定的网络安全保护义务，涉嫌构成违反治安管理行为的，移送公安机关予以处理；构成犯罪的，移送司法机关依法追究刑事责任。

第二十九条（管理人员违反规定的处理）国务院金融管理部门及其分支机构、派出机构工作人员存在玩忽职守、滥用职权、徇私舞弊情形的，依法依规给予处分；构成犯罪的，移送司法机关依法追究刑事责任。

第五章 附则

第三十条（术语定义）本办法下列用语的含义:

（一）金融从业机构，是指金融机构以及经国务院金融管理部门批准设立或者认定的其他机构。

（二）国务院金融管理部门，是指中国人民银行、国家金融监督管理总局、中国证券监督管理委员会、国家外汇管理局。

（三）关键岗位，是指与关键信息基础设施安全保护直接相关，掌握较全面信息的规划建设、开发测试、安全运营和日常运维岗位。

第三十一条（地方金融组织网络安全管理）地方金融管理机构牵头负责地方金融组织履行网络安全保护义务的监督管理，可参照本办法和国务院金融管理部门网络安全相关规定，制定相应的管理制度。

第三十二条（解释权）本办法由国务院金融管理部门负责解释。

第三十三条（生效期）本办法自 2026 年××月××日起施行。