

附件

贵州省金融城域网接入管理办法

第一章 总 则

第一条 为加强贵州省金融城域网安全运行管理，规范金融城域网的接入程序和日常运维管理，提升金融城域网服务品质，防范和化解金融城域网运行风险，保障相关金融信息系统安全稳定运行，根据《中国人民银行金融城域网入网管理办法》及相关法律法规的要求，结合贵州省实际情况，制定本管理办法。

第二条 贵州省金融城域网（以下简称金融城域网）是中国人民银行贵阳中心支行（以下简称贵阳中心支行）与贵州省各接入金融城域网机构因业务工作需要而组成的计算机通信网络。

第三条 接入金融城域网机构（以下简称接入机构）是指通过金融城域网与贵阳中心支行进行信息交互的银行业金融机构、非银行业金融机构及相关财政、税务等政府职能部门。

第二章 接入条件和流程

第四条 技术条件：

（一）拟接入机构准备在金融城域网上使用资金交易类业务系统的，其接入关键网络设备和线路应采取双机双线热备方式，在边界部署边界防火墙（双机热备）。网络安全类设备必须使用国产品牌设备。

（二）接入机构要按照自身需求和人民银行端设备端口情况合理选择网络线路类型。

（三）接入机构本端金融城域网部分应符合《GB/T22239-2008 信息安全技术信息系统安全等级保护基本要求》的第三级基本要求。

（四）需要访问资金交易类业务系统的接入机构至少需要配备 2 名以上技术人员负责管理相关联网设施设备和系统；只访问账户系统、征信系统、身份证核查系统等接入机构至少要配备 1 名技术人员负责管理相关联网设施设备和系统。上述技术人员必须经过贵阳中心支行的资格审核、技术培训和考核，经批准后才能上岗。

第五条 入网准备：新设金融机构拟接入金融城域网的，应在《关于加入中国人民银行贵阳中心支行金融管理与服务体系的请示》时一并提出申请；现有金融机构可向贵阳中心支行提出专项申请开通金融城域网。金融机构应在提出申请时完成各项入网前期准备工作。

第六条 接入申请材料应包含如下要素：

（一）申请机构名称

（二）接入金融城域网目的及拟开展业务种类

（三）联网设施、线路、设备系统准备情况（附件形式）

（四）《技术人员基本情况登记表》（照片、姓名、年龄、性别、学历、专业、从事相关专业情况，联系电话等）（附件 1）

（五）人民银行相关业务处室同意访问相关业务系统的书面意见（附件形式）

（六）《贵州省金融城域网接入机构保密承诺书》（附件 2）

(七)《接入机构网络接入方案及相关应急预案》(附件形式)

(八)《拟接入机构技术条件确认表》(附件3)

(九)其他材料。

第七条 现场核查：贵阳中心支行在开通金融城域网前要实地审核验收拟接入机构各项准备情况。

第八条 接入网络：经前期材料报送和现场核查后，符合入网要求的金融机构在现场检查10个工作日内委托线路运营商开通网络，不符合的金融机构不予接入。

第三章 接入机构联网运行日常管理

第九条 接入机构应针对本机构金融城域网设施、设备和系统使用情况制定相应的运行管理制度，并遵守《贵州省金融城域网接入机构保密承诺书》相关条款。

第十条 接入机构技术人员应每日巡检本机构金融城域网设施、设备和系统运行情况并将设备系统运行情况记录在巡检登记簿中，确保其安全稳定运行。

第十一条 接入机构每年6月、12月应向贵阳中心支行提交本机构金融城域网设施、设备和系统运行情况报告。

第十二条 接入机构应采取相应安全访问控制措施，防止本机构金融城域网相关网络、服务器、客户端设备与国际互联网及内部业务网互联互通。

第十三条 接入机构要建立本机构金融城域网应急预案，每年至少开展1次应急演练，并将演练情况报告贵阳中心支行。

第十四条 接入机构要变更本机构金融城域网线路带宽及类型时，应向贵阳中心支行提交申请和报备；如需修改网络参数，应在贵阳中心支行批准后方可实行。

第十五条 接入机构如需增加访问金融城域网人民银行端应用系统，应向贵阳中心支行提交书面申请（含人民银行相应业务主管部门是否允许访问该应用系统的批复等书面文件）。贵阳中心支行科技部门根据“先有访问需求才能联网”的原则综合考虑新增访问需求是否批准。

第十六条 接入机构需减少访问金融城域网人民银行端应用系统或退出金融城域网时，应提前 1 周书面报告贵阳中心支行。

第十七条 接入机构应在本机构金融城域网边界防火墙配置 IP 地址转换及对应访问控制包过滤规则，粒度应达到端口级。

第十八条 接入机构本端网络故障导致业务中断时，应立即报告贵阳中心支行，并按照应急预案处理事件，在排除故障后，应以书面形式报贵阳中心支行备案。接入机构本端金融城域网网络发生故障，超过 4 小时未及时发现并报告的，贵阳中心支行将对其进行通报。

第十九条 接入机构对本端设施、设备和系统进行维护、升级、搬迁可能影响金融城域网正常使用时，应根据影响范围和时间书面通知贵阳中心支行。

第二十条 接入机构负责本机构金融城域网相关工作的技术人员发生工作变动，应在 1 周内向贵阳中心支行报备接替人员材料并经过贵阳中心支行的资格审核、技术培训和考核批准后才能上岗。

第四章 责任和义务

第二十一条 拟接入机构应按照贵阳中心支行要求的组网方式接入金融城域网，遵守国家及人民银行相关保密条款，接入机构不得为其他机构或个人提供金融城域网转接服务。

第五章 附 则

第二十二条 本办法适用于贵州省内金融城域网的接入机构。

第二十三条 村镇银行、小额贷款公司、小额贷款担保公司等地方性中小金融机构参照本办法执行，接入方式另行规定。

第二十四条 本办法由贵阳中心支行负责解释。

第二十五条 本办法从公布之日起执行。

附：1. 技术人员基本情况登记表

2. 贵州省金融城域网接入机构保密承诺书

3. 拟接入机构技术条件确认表

附 1

技术人员基本情况登记表

单位:

填表日期: 年 月 日

| | | | | | | |
|----------------------|--|---------------|--|------|--|----|
| 姓名 | | 性别 | | 出生年月 | | 照片 |
| 政治面貌 | | 联系电话 | | | | |
| 学历 | | 现任职务/ 任职时间 | | | | |
| 从事 相关 专业 情况 | | | | | | |

附 2

贵州省金融城域网接入机构保密承诺书

贵州省金融城域网是贵州省辖内金融行业的重要基础设施。目前，
_____（以下简称我方）已接入该金融城域网。为了保守国家和中国人民银行秘密，维护国家和人民银行利益，维护贵州省金融安全，遵照国家对金融城域网安全和保密等方面的有关规定，我方特作如下承诺：

一、我方严格遵守中国人民银行贵阳中心支行发布的《贵州省金融城域网接入管理办法》各项规定。

二、我方对所掌握的金融城域网网络架构、运行参数、配置、IP 地址资源等一切相关技术信息进行严格保密。

三、配合中国人民银行贵阳中心支行有关部门对我方接入金融城域网各项工作进行安全保密检查，不以任何方式阻扰。

四、我方及我方人员若有违反本承诺书事件，我方负责赔偿由此造成的一切经济损失，并承担相应法律责任。

接入机构（签字，盖章）：

日期：

拟接入机构技术条件确认表

| 相关技术项目 | | 要求 | 实际情况 | 备注 |
|---------|-----------------|---|---|----|
| 金融网管理情况 | 定岗，定责 | 岗位设置清晰明确，责任到人。 | | |
| | 人员配备 | 按要求设置应用系统管理员，网络管理员，技术支持与运维人员等 | | |
| | A, B 角配备 | A, B 角配备齐全，同时有效轮岗，轮岗运维资料有据可查 | | |
| | 技术参数，相关建设维护资料管理 | 资料集中统一管理，资料有异地备份，文档可操作性强，查阅方便，不受人员变动影响。 | | |
| 金融网相关制度 | | 网络，涉及主机，机房，安全等相关制度和规范 | 相关规范和制度包含金融网相关建设，运行，管理，维护，资源分配回收，安全技术保障等工作，有相应应急预案及操作手册 | |
| 安全措施 | 网络隔离 | 与国际互联网隔离情况 | 物理隔离 | |
| | | 与办公业务网隔离情况 | 至少逻辑隔离，有严格安全访问控制 | |
| | | 与其他网络隔离情况 | 未经批准不允许与其他网络连接 | |
| | 防病毒 | 软件种类 | 具有相关国家认可的防病毒安全资质 | |
| | | 更新情况 | 版本更新周期快 | |
| | | 补丁情况 | 操作系统补丁更新策略和频率满足相关要求 | |
| | 防攻击 | 非法外联 | 防止内部使用金融网的终端连接非金融网的其他网络 | |
| | | 入侵检测 | 预警并防止非法入侵 | |
| | | 漏洞扫描 | 发现系统存在隐患 | |
| | | 加密措施 | 远程通信或本地加密措施 | |

| 相关技术项目 | | 要求 | 实际情况 | 备注 |
|--------|------------|-----------------------------------|------|----|
| 应急管理 | 故障响应时间 | 技术故障响应时间应满足业务需求，其中线路故障响应时间小于 4 小时 | | |
| | 应急预案有效性 | 相关规程合理有效，相应技术支持联系人/电话有效 | | |
| | 应急演练实效性 | 具有完整的应急演练记录，且应急操作手册根据业务发展需要同步更新 | | |
| 网络情况 | 网络拓扑 | 网络拓扑简洁清晰，随网络情况实时更新 | | |
| | 路由协议 | 路由协议选择以公有协议为主，具有相应加密或控制措施 | | |
| | 网段划分 | 相关服务器具有专用网段，不同网段有严格访问控制 | | |
| | 配置规则 | 配置简明扼要，无多余配置 | | |
| | 防火墙策略 | 满足约定通信要求，不开放无关的端口与 ip | | |
| | 口令及日志管理 | 专人管理相关网络设备口令，相关网络设备日志可查询回溯 1 个月以上 | | |
| | 通信线路 | 租用不同线路运营商线路实现广域网热备 | | |
| | 冗余情况 | 关键网络设备及安全设备有冗余设计，非关键设备至少达到冷备 | | |
| | 集成商与技术支持情况 | 集成商资质，响应时间及服务水平符合要求 | | |
| 机房环境 | 物理位置 | 周围无易燃易爆等隐患，是否为危险建筑，机房承重符合要求 | | |
| | 门禁 | 存储记录 1 个月以上，授权人员符合相关要求 | | |

| 相关技术项目 | | 要求 | 实际情况 | 备注 |
|--------|---------|---|------|----|
| | 消防 | 按国家相关机房消防标准设计，经权威部门检验通过 | | |
| | 供电及 ups | 强弱电分布符合国家标准，统一供电停止后，依靠 ups 系统可平稳运行 8 小时以上 | | |
| | 空调 | 温度湿度及新风符合机房有关标准 | | |
| | 综合布线 | 布线清晰，合理。容易扩展及维护 | | |
| | 管道 | 按有关保密要求铺设管道，保证机房其他管线互不影响 | | |
| | 人员值守 | 重要系统实现 24 小时专人值守，值守人员有相应记录 | | |

检查结论:

金融网外联机构代表
(签字，盖章)

检查工作组签字:

年 月 日