（2）金融级全维度数据安全防护

针对社保基金账户信息、资金流转数据、存单凭证资料、对账报表数据、业务操作日志、财政备案信息等核心涉密数据，我行实行全流程、全维度、金融级加密保护。所有业务数据在传输、存储、调取、导出、使用全过程采用国家最高安全等级AES256加密算法进行加密处理，数据密文全程流转，无明文外露风险。

建立严格的数据管控机制，明确财政社保数据为最高涉密等级数据，严禁任何形式的私自拷贝、外传、截图、转发、泄露、篡改。所有数据调取、导出、查询、使用操作均执行多级审批制度，普通经办人员仅可查询本职工作范围内的基础数据，对账、审计、核查类数据需业务主管审批，核心涉密数据需支行分管行长审批，审批通过后方可操作。所有数据操作全程留痕、日志永久留存、操作全程溯源，一旦出现数据异常可立即定位责任人、追溯操作全过程。同时，我行搭建分布式数据存储架构，核心数据多副本存储，避免数据丢失、损坏、篡改问题，全方位保障财政社保数据安全、完整、真实、有效。

（3）分级授权权限管控体系

我行严格遵循“专人专岗、岗权匹配、分级授权、权限最小化、相互制衡、全程管控”的原则，搭建科学严谨的财政社保业务权限管控体系，彻底杜绝越权操作、违规操作、权限滥用、岗位失控等风险。按照“业务经办、复核审批、科技运维、风控监督、审计核查”五大岗位体系，实行岗位权限拆分、权责分离、相互制约、互不越权。

业务经办人员仅具备业务录入、资料上传、基础查询权限，无审核、修改、划转、删除权限；复核审批人员仅具备业务审核、合规校验、流程审批权限，无直接经办操作权限；科技运维人员仅负责系统运维、设备检修，无业务操作、数据查询、账务修改权限；风控监督人员全程监控业务流程、核查操作合规性，无业务经办权限；审计人员负责事后审计溯源，不参与日常业务操作。所有岗位权限独立划分、闭环管控，形成岗位制衡机制。

同时，所有财政业务操作系统实行实名登录、动态口令、设备绑定、离岗锁屏制度，操作人员必须使用专属工号、动态密码登录专属终端，终端设备与工号唯一绑定，禁止跨设备、跨账号操作；操作人员离岗立即自动锁屏，杜绝他人代为操作、无人值守操作风险。所有权限开通、变更、注销均需层层审批、备案登记，权限变动全程留痕，确保权限管控严谨规范、全程可控。

（4）常态化网络安全运维与风险排查

我行建立常态化、制度化、专业化的网络安全运维体系，组建专项网络安全运维团队，定期开展网络安全漏洞扫描、渗透测试、风险排查、攻防演练、策略优化工作，全方位封堵网络安全漏洞、化解安全风险。每日实时监控财政专网运行状态、网络流量、设备运行参数，及时发现异常流量、非法访问、设备故障等问题；每周开展网络安全漏洞扫描，针对系统漏洞、设备缺陷、策略短板及时修复优化；每月开展专项网络安全风险排查，全面排查网络架构、数据防护、权限