中国银河证券股份有限公司
隐私和数据安全管理声明

（本管理声明适用于中国银河证券股份有限公司总部、分支机构及各子公司）

中国银河证券股份有限公司（简称“中国银河证券”“公司”）作为国有大型综合类券商中国证券行业领先的综合金融服务提供商，深入践行数字化发展战略，始终将隐私和数据安全保护作为企业发展的核心任务，筑牢金融科技创新的安全防线，为数字化转型提供坚实保障。

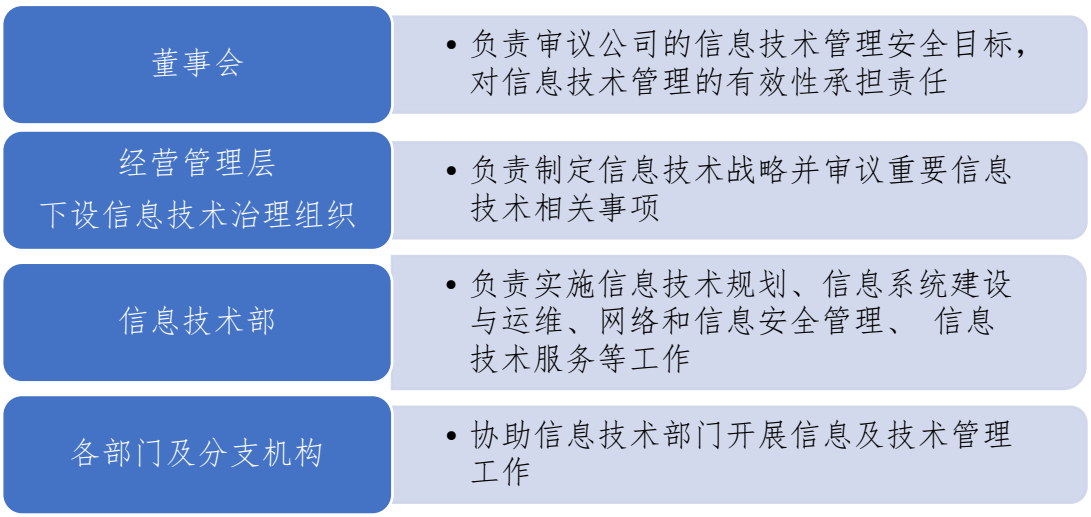
公司严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《证券期货业网络和信息安全管理办法》等法律法规及行业监管要求，完善治理架构、构建覆盖数据全生命周期的安全管理机制、规范客户隐私保护原则，筑牢数据资产安全与客户信息保护的双重防线。

一、管理制度与架构

中国银河证券依据法律法规及行业监管要求，制定《信息技术管理办法》《网络与信息安全管理办法》《个人信息保护管理办法》等制度，构建层次分明、职责明确的信息技术管理体系，并将隐私和数据安全作为信息技术管理的重点内容，明确主体责任与组织分工，确保管理体系高效运作，为

隐私和数据安全管理提供有力保障。

中国银河证券隐私和数据安全治理架构



二、数据安全管理措施

中国银河证券通过部署多层次安全防护系统、建立应急预案机制、定期开展内外部审计等措施，打造数据安全防线，有效提升数据安全风险防范能力。

（一）开展数据泄露主动应对措施。

1．搭建安全防护体系。公司构建涵盖边界防护、网络准入、身份鉴别、外联控制、入侵检测、加密传输、终端管理等技术内容的纵深、多层次的安全防护体系。

2．部署安全防护平台及工具。公司部署防火墙、应用防火墙、流量安全分析系统、安全态势平台、终端安全管理系统、主机安全系统、防病毒系统、安全蜜罐、邮件安全防护系统、数据防泄漏系统、数据分类分级、数据脱敏、透明文

档加解密等平台和工具。

3.建立预防预警监测机制。公司遵循安全优先原则通过人工巡检、自动化监控、事件报告等途径发现风险隐患，及时评估并采取防范措施，必要时向应急领导小组和监管机构预警报告。预警内容包括基本情况、影响范围、防范措施及建议，风险解除时需及时取消预警并报告。

（二）建立数据泄露被动响应机制。

1.建立应急管理工作机制。公司制定《信息系统突发事件应急预案》《应急联络手册》等制度文件，建立"统一指挥、密切协同、快速反应、科学处置"的应急管理工作机制，通过强化风险排查、完善预案体系、明确责任分工、畅通信息报送等措施，构建起全方位、多层次的突发事件应对体系，确保应急处置工作科学高效、协同有序。

2.定期开展应急演练。公司制定年度应急演练计划，及时开展各类数据安全应急演练工作，提升全员应急处置能力，最大限度地减少数据安全事件发生后的损失。

（三）通过信息安全管理体系认证。

公司已通过 ISO 27001 信息安全管理体系认证，认证范围涵盖核心信息系统开发运维、智能灾备体系建设及全域软硬件运维体系等关键领域，深度嵌入公司 90%以上的关键业务场景，实现对证券交易、客户服务、风险管控等核心业务系统的标准化管理。

（四）构建信息安全审计监督体系。

1．年度全景扫描：开展覆盖隐私保护、数据安全等核心领域的信息技术管理专项内审，同步将信息技术风险纳入年度内控评价必检项，聚焦公司个人信息保护、信息技术安全、灾备机房建设、运维以及应急管理等核心管控领域。

2．定期外部诊断：定期引入外部专家机构开展穿透式审计，评估范围涵盖相关治理架构有效性、合规与风险矩阵、信息技术安全管理及应急管理等维度。

三、客户隐私保护措施

中国银河证券规范客户个人信息收集处理，坚决履行客户信息保护责任，确保客户信息在全周期处理过程中的合规性，保障客户的合法权益不受侵害。

（一）客户信息收集与处理。

1．公司遵循“合法正当、最小必要”原则，通过隐私政策向客户明确告知数据收集范围、使用目的及保存期限，在取得客户明确授权的前提下，以对个人权益影响最小的方式开展信息收集工作。

2．公司承诺不超范围收集个人信息，不从第三方收集个人信息，并依据国家、行业主管部门及内部规章有关规定，针对不同类型的数据设定其数据保存期，在数据超出保存期限后，执行数据删除操作。

3．公司在与外部合作方开展客户个人信息委托处理时，

通过合同等与受托方约定委托处理的目的、期限、处理方式、处理范围、个人信息的种类、保护措施以及双方的权利和义务等，并对受托方的个人信息处理活动进行监督。除交易及服务的必要情况或相关法律另有规定外，公司不会向第三方公司、组织或个人提供或转移客户的个人信息。

（二）客户管理信息权限。

公司为客户提供查询、复制、更正、删除、授权同意撤回、自动化决策选项变更、账户注销等个人信息保护相关权利，保障客户对自己信息的知情权与决定权。

（三）敏感数据访问控制与脱敏。

1.公司建立敏感数据访问控制与保护机制，覆盖数据的传输、存储和使用等环节。在传输环节，采用安全通道和加密传输技术，监控协议接口和 API 接口的访问情况，识别异常并限制或过滤不安全输入参数；在存储环节，运用加密等安全技术手段，确保数据安全防护；在使用环节，严格执行“必须知道”“最小授权”“最小功能”原则，强化访问控制，最大程度降低客户隐私泄露和信息滥用风险。

2.公司构建静态数据脱敏系统，对开发测试环境中的敏感数据进行脱敏处理，并部署网络数据防泄漏产品，实时监测和防范敏感数据的外泄风险；推进动态数据脱敏系统建设，实现对交互式访问场景中个人敏感数据的实时脱敏，进一步提升客户隐私安全防护能力。

（四）产品和服务开发规范。

1．公司建立覆盖产品和服务全生命周期的安全管控机制，在开发前期开展安全需求分析与方案评审；开发过程中严格执行安全方案；上线前实施漏洞扫描、渗透测试及隐私合规检测等安全评估。

2．对部分交付源代码的产品，公司通过专业平台进行源代码安全检测，确保产品和服务的安全性达到最高标准。

四、隐私和数据安全生态共建

中国银河证券构建全链条防护体系，在强化员工合规培训与投资者隐私教育的同时，建立供应商准入评估、全周期安全管控及保密协议约束机制，形成内外部协同的隐私和数据安全生态共建格局。

（一）员工与投资者培训教育。

1．公司高度重视员工的隐私和数据安全宣导教育，并要求信息技术部门及相关部门在其职责范围内，定期面向全体工作人员（包括公司正式员工及劳务派遣工）开展个人信息保护培训，相关工作每年至少开展一次。此外，公司通过多种形式强化员工安全意识，包括制作安全意识宣导系列小视频并在内部宣传屏循环播放，以及组织信息安全与保密意识专题培训，全面提升员工的数据安全认知和合规意识。

2．公司积极开展投资者隐私保护教育宣传活动，通过网络大讲堂等形式，向投资者普及网络安全知识，提升投资者

的隐私保护意识和自我防范能力。

（二）供应商数据安全管理。

公司推动供应商及合作伙伴建设数据安全保护机制，针对供应商从项目开展前、项目过程中及项目完成后实行全方位数据安全管理。公司在选用供应商前会组织开展中介机构信息安全风险评估工作，对相关中介服务机构及其服务人员的资质和过往安全记录进行评估，并在与供应商签署的合同中包含信息安全与保密条款，同时要求其服务人员签署保密协议以确保供应商遵守公司信息安全要求。在项目实施过程中，公司加强对供应商及其服务人员的安全管控，并在项目完成后对供应商及其服务人员的项目实施情况进行评价。2024 年，公司供应商信息安全管理覆盖率 100%。