第一创业证券股份有限公司

数据安全与隐私保护管理声明

第一创业证券股份有限公司（以下简称“第一创业”或“公司”）始终将信息安全视为业务发展的核心，严格遵守《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》《证券期货业网络和信息安全管理办法》等法律法规要求，致力于确保公司数据管理系统的安全，保护客户隐私数据，并积极推动创新以应对不断演变的信息安全挑战。

公司制定《第一创业证券股份有限公司数据安全与隐私保护管理声明》（以下简称“本声明”），涵盖数据安全与隐私保护管理体系、数据安全保障举措、客户隐私保护原则三个方面，以进一步加强公司信息安全治理，并承诺持续改进信息安全措施，以确保客户、合作伙伴和员工的信息始终得到最佳保护。

本声明适用于公司各部门、各分支机构、各全资及控股子公司。

本声明所述的数据为公司经营和管理活动中产生、采集、加工、使用或管理的业务数据、系统数据和管理数据。业务数据主要包括交易数据、清算数据、客户资料数据、经纪数据、投资研究数据、客户服务数据、邮件数据、日志数据等；系统数据主要包括数据字典、权限设置、硬件配置及其它系统配置参数；管理数据是指经营管理相关系统的数据，主要包括办公数据、人力资源数据、财务数据、内控管理数据等。

一、数据安全与隐私保护管理体系

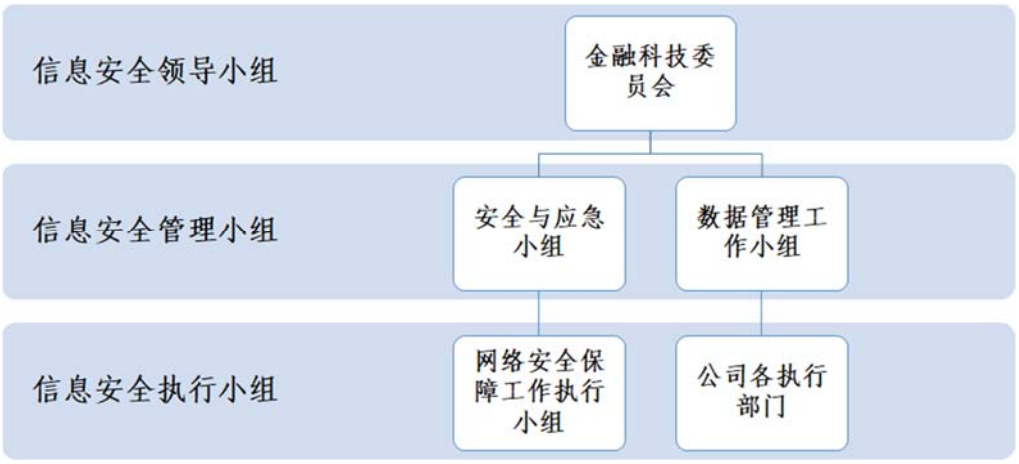
公司严格遵守法律法规要求，制定《第一创业证券股份有限公司信息安全管理总则》《第一创业证券股份有限公司数据安全管理办法》《第一创业证券股份有限公司数据生命周期管理办法》等制度，搭建了以计划（Plan）、实施和运行（Do）、监控和评审（Check）、维护和改进（Act）的 PDCA 模型为基础的信息安全管理体系，建立了“信息安全领导小组-信息安全管理小组-信息安全执行小组”三级信息安全管理架构，确保公司信息安全管理能力与业务活动发展需求相

匹配。公司的信息系统已通过 ISO27001 国际信息安全管理体系标准认证和审核，且信息系统相关业务认证覆盖率达 100%。

公司金融科技委员会为信息安全工作领导小组，统筹规划、决策公司的信息安全工作和数据治理工作。其中，公司金融科技委员会主任委员由公司总裁担任，为公司信息安全工作的第一责任人，公司首席信息官为信息安全工作的直接责任人。

公司金融科技委员会下设“安全与应急小组”、“数据管理工作小组”，为公司信息安全管理小组，对金融科技委员会负责。安全与应急小组负责公司信息安全工作的实施管理、检查等工作，下设“网络安全保障工作执行小组”，负责公司网络安全防护工作的组织、协调与落实；数据管理工作小组是公司数据治理体系的管理主体，负责协调公司各相关部门具体推进数据管理的执行工作。

图：公司信息安全管理架构



二、数据安全保障举措

公司坚定执行高标准的数据安全保障举措，以确保数据的完整性、可用性和保密性，防止数据被未经授权的实体访问或损坏。

（一）建立数据安全事件应急响应机制：公司制定了应急处置管理办法和应急联系手册，明确安全事件处置汇报途径及应急响应方式。一旦发生数据安全事件，公司安全与应急小组将迅速组织相关部门和人员对事件进行分析和处置，确

保在第一时间内有效控制事件，同时向受影响的用户进行通知并为其提供必要的支持和帮助。

（二）开展信息系统专项风险审查：公司定期开展信息系统应急演练和风险监测评估，并及时收集演练和评估报告进行汇总和总结，根据发现的风险点修订优化应急预案、处理流程、系统部署。公司每年组织外部专业审计机构开展专项技术审计，内容包含网络监控、网站监控、网站防篡改、系统漏洞扫描、渗透测试等。

（三）组织员工信息安全意识培训：公司制定年度信息安全宣导计划，定期开展安全意识宣导工作。根据计划对公司全体工作人员（包括与公司建立劳动关系的正式员工、与公司签署委托协议的经纪人、劳务派遣至公司的其他人员）开展安全意识培训、安全技能培训以及相关考试，并将信息安全培训参加情况纳入各部门组织绩效评价因素。

（四）构建供应链环节数据安全保障体系：公司在《第一创业证券股份有限公司信息技术供应商管理指引》中明确规定了对客户数据的保护，确保供应商遵守公司数据安全和隐私保护标准，并由采购部门、信息技术中心对其数据处理和管理流程进行审查。

三、客户隐私保护原则

公司合法透明处理客户的隐私数据，尊重并维护客户的隐私权益，防止个人信息被滥用或未经授权的共享。

（一）规范客户数据生命周期管理：公司严格限制数据收集范围，仅收集与服务相关的客户数据，不使用非法或来源不明的数据。公司每季度检查备份数据的有效性和可用性，备份数据留存时间不低于监管部门要求。公司坚决不允许或协助其他机构或个人截取、留存客户信息（法律法规和中国证监会另有规定的除外），同时公司不以任何方式向其他机构或个人提供客户信息，以确保客户信息的安全和隐私。

（二）保障客户个人信息处理权限：公司信息系统在收集客户信息之前，要

求签署包含《中华人民共和国个人信息保护法》相关要求的隐私协议，明确告知获取客户信息的性质和收集信息的使用途径，保障客户的知情权。公司坚定保障客户对其个人数据享有的访问、修改和删除的权利，以便客户随时可以自主管理和控制其个人信息的使用和保护。

（三）限制客户数据内部访问权限：公司建立客户数据使用的授权审批机制，遵循“最小授权”与“最小扩散”原则，仅向职责所需的部门授权访问客户个人信息。客户数据在向外部提供或内部传输的过程中，按照公司相关数据管理规定，必须对分级为“绝密级别”的数据进行脱敏处理，最大程度降低敏感数据泄露的风险。