招商证券信息安全及客户隐私保护管理声明

一、管理制度与架构

公司根据《中华人民共和国证券法》《中华人民共和国个人信息保护法》《证券基金经营机构信息技术管理办法》《个人金融信息保护技术规范》等法律法规，制定并持续更新隐私保护类管理规范，包括《招商证券股份有限公司投资者个人信息保护管理办法》《招商证券股份有限公司投资者个人信息保护专项工作领导小组议事规则》；制定并持续更新信息与数据安全类管理规范，包括《招商证券股份有限公司数据安全分类分级管理办法》《招商证券股份有限公司数据安全管理办法》《招商证券股份有限公司网络安全管理办法》《招商证券股份有限公司信息系统账号和口令管理办法》等，上述制度适用于公司所有业务部门、分支机构及子公司，此外，分支机构和子公司还需同时遵照所在地法律法规及相关规定执行。

类别	制度名称
隐私保护	《招商证券股份有限公司投资者个人信息保护管理办法》
	《招商证券股份有限公司投资者个人信息保护专项工作领导小组议事规则》
信息安全	《招商证券股份有限公司数据安全分类分级管理办法》
	《招商证券股份有限公司数据安全管理办法》
	《招商证券股份有限公司网络安全管理办法》

	《招商证券股份有限公司信息系统账号和口令管理办法》

公司健全信息安全及数据治理工作架构和职责分配机制，建立自上而下、权责明确的信息安全及隐私保护管理架构。信息安全和隐私保护管理架构由决策层、管理层、执行层和监督层组成：决策层由公司信息技术治理委员会构成，由董事长和公司总裁负责牵头；管理层由公司投资者个人信息保护专项工作领导小组构成，并在公司财富管理及机构业务总部财富管理部设立秘书处作为日常工作机构；执行层由投资者个人信息保护专项工作小组、金融科技中心及公司各部门构成，保障个人信息保护工作有效开展；监督层由公司稽核部、法律合规部、风险管理部构成，履行信息安全和隐私保护的监督职能。

招商证券信息安全和隐私保护管理架构

层级	委员会/部门	职责分工
决策层	信息技术治理委员会	负责审议公司的信息安全管理方针、策略、原则，负责审议、决策与信息安全管理工作相关的重大、难协调的事项，为信息安全管理提供组织保障。
管理层	投资者个人信息保护专项工作领导小组	负责投资者个人信息保护专项工作的统筹协调、任务下达、工作指导等相关重大事项协同。
执行层	投资者个人信息	负责组织开展投资者个人信息保护各

	保护专项工作小组	项工作，包括制度、流程、系统建设的审议，培训、自查等。
	金融科技中心	负责制定和落实数据活动中的系统与个人的安全技术防控要求，保障数据全生命周期的机密性、完整性和可用性，确保公司数据资产和投资者信息安全。
	公司各部门	负责本单位所辖范围内的业务数据全生命周期的安全管理与数据安全合规监督工作，防范业务数据泄密。
监督层	稽核部、法律合规部、风险管理部	负责对信息安全、隐私保护管理情况和效果进行检查、评价，并督促整改。

二、信息安全管理机制

1、信息安全审计

在外部审查方面，公司基于公司内控自评价、网络安全等级保护与 ISO20000 认证需要，组织外部机构开展外部审计，落实信息安全审计管理要求。在信息安全等级保护工作方面，公司按年度开展网络安全等级保护测评工作，做到定期测评、定期发现、定期整改。同时，公司依照监管要求，每三年聘请专业第三方机构实施信息技术管理工作专项审计，覆盖信息技术治理、信息技术合规风险管理、安全管理、运维管理等信息技术管理各个方面。

在内部审查方面，公司结合监管要求及公司内部管理规定，每年度通过专项审计、专项评估、专项调查等多种审计形式，对公司信息技术管理工作进行监督检查，并将信息技术内部控制有效性纳入公司年度内控有效性评价，通过多种角度强化信息科技内控水平。近三年内部审计内容已按要求覆盖信息技术治理、信息技术合规与风险管理、信息技术安全管理、重要信息系统开发测试、应急管理等信息技术管理事项。

2、信息安全主动措施

在信息安全保护技术层面，招商证券通过边界安全、应用安全和主机安全的三道防线建设，以主机加固为核心，以安全基础设施及日志平台为全局防护与监测能力支撑，以有效性验证平台为驱动，结合全时全域流量采集分析技术，形成了较为完备的信息安全防护体系，有效防范各类系统破坏、业务滥用、信息盗窃等恶意攻击。

在强化数据安全主动管理方面，招商证券基于数据全生命周期进行安全管控，主要分为开发、采集、加工、传输、使用、存储和销毁7个阶段，各环节均建立有严格的治理机制。公司通过定义开发业务需求的人数场关系、规范数据采集流程及采集方式、开发测试数据脱敏、大数据平台权限管控、数据加密传输、脱敏展示及访问权限控制、分级及加密存储、可靠的数据销毁手段等措施，避免数据安全管理各环节的泄露风险。公司在数据访问层面建立了账号访问权限申请授权机制和审批流程，严格限制系统关键功能和超级账号的授权，访问授权遵循“权限最小化”原则，经授权批准后才可查看授权范围内数据。

在信息安全保护培训方面，公司面向全体员工每年开展包括网络安全、数据安全的全员安全意识培训及考试，以提升员工信息安全意识及能力。

3、信息安全被动措施

在加强信息安全事件应急处理方面，招商证券设立有信息技术应急管理领导小组，负责落实公司信息安全应急管理工作，并建立了《招商证券股份有限公司网络安全事件应急管理办法》及《招商证券股份有限公司信息技术应急预案与应急演练管理办法》，针对事件影响范围、受影响客户数量、经济损失等维度进行安全事件等级划分，明确各等级安全事件的处理时限要求及事件升级机制，形成从信息安全预防预警到应急响应的闭环处理模式，并在日常运营及业务开展过程中进行信息安全应急演练。

三、客户隐私及数据保护

1、用户个人信息及数据控制权利

在用户使用招商证券 APP 过程中，公司向用户提供包括但不限于访问、修改、删除用户的个人信息的权利，以及告知、同意、查看、撤回、注销账号等自主化个人信息和数据管理服务，确保用户对个人信息的控制权。

a. 访问、修改个人信息

用户可随时通过 APP 内“我的 - 我的业务办理”菜单访问及查看用户的个人基本信息及账户信息。若用户需要修改个人信息，或发现公司处理用户的个人信息出错，用户有权通过“我的 - 我的业务

办理”菜单作出修改，或随时联系 0755-95565 客服热线向用户的所属营业厅提出更正信息的需求。

b.删除个人信息

若用户认为公司使用、采集用户个人信息的行为违反了法律、行政法规规定或与用户的约定以及出现错误的，或者发现公司采集、储存用户的个人信息有误的，用户可以随时联系 0755-95565 客服热线删除个人信息。在用户删除个人信息后，我们将不再收集、使用或共享与用户账户相关的个人信息。

c.告知与同意

在用户使用 APP 各项功能前，如涉及到需要用户授权个人信息的场景，APP 会主动以多种方式提示用户，用户可以选择同意或者拒绝授权。只有得到用户的授权，APP 才会访问对应的信息；如用户拒绝授权，则可继续使用与该信息无关的其他功能。

d.查看与撤回

用户可以随时通过 APP 设置的权限控制功能查看各项信息的授权情况及使用情况，并可以随时通过点击菜单来撤回授权。

e.注销账号

用户可以通过账号管理页面注销账号，申请删除个人账号相关数据。公司将配合删除个人信息。如个人发现未删除到位，可通过客服热线 95565 或在线客服，向公司提出删除相关数据的请求。

2、用户信息及数据收集

在用户信息收集方面，招商证券建立了个人信息收集与使用清单，

仅收集和留存业务办理过程中所需的最少必要信息，且公司不会从第三方收集个人数据（法律另有要求的除外）。同时，在《招商证券 APP 隐私协议》中已明确告知客户收集数据范围和目的，充分揭示客户个人权利，让客户知悉相关数据使用用途等内容。

3、用户信息及数据留存

招商证券仅在《招商证券 APP 隐私协议》所述目的、期间和法律法规及监管规定的时限内保存用户个人信息。对于开户的客户，根据《中华人民共和国证券法》第一百三十七条要求：“证券公司应当妥善保存客户开户资料、委托记录、交易记录和与内部管理、业务经营有关的各项信息，任何人不得隐匿、伪造、篡改或者毁损。上述信息的保存期限不得少于二十年。”，招商证券后台数据采取与历史库分离，以备份的方式进行留存，直至法律法规要求的保存期限届满。对于招商证券 APP 的非交易用户，当其注销会员用户时，公司会在 15 天内删除与其相关的数据(法律另有要求的除外)。

4、用户数据访问及使用

根据《招商证券股份有限公司投资者个人信息保护管理办法》规定，公司处理投资者个人信息时，应当确保个人信息的合规、安全，防止个人信息的泄露、篡改、丢失。各单位应结合本单位实际情况建立完善的投资者个人信息保护管理流程，制定相关管理规则。公司在数据访问层面建立了账号访问权限申请授权机制和审批流程，严格限制系统账号授权。

根据《招商证券股份有限公司投资者个人信息保护管理办法》规

定，公司在引入外部中介机构、信息技术服务机构等第三方服务机构时，严格规范第三方服务机构的准入要求，全面考察相关机构的人员、资质、技术和信誉等，并将投资者个人信息保护能力作为重要评估指标，从事前、事中和事后重点防范投资者个人信息泄露风险。

在数据使用方面，对业务上不需要对证件号码、账号、姓名、预留手机号码或其他类识别个人身份信息完整展示的，进行去标识化及匿名化处理。公司对信息开展分类分级管理，加强对个人信息敏感程度的识别，对不同类别、级别的个人信息，实施相应的安全策略和保障措施，严格保护敏感个人信息。

四、合作方信息安全管理要求

公司根据《招商局集团采购和合作伙伴合规管理办法》、《招商证券股份有限公司供应商管理细则》，要求公司需与所有信息技术供应商签署保密协议、和驻场外包人员签署保密承诺书，承诺严格遵守保密协议的数据保密要求且不会向第三方提供个人数据。公司数据、信息类合同模板中设置合作方禁止行为条款、合作方产品安全承诺条款、合作方保密承诺条款，并签订保密协议，以约束相关供应商行为。

在相关合规性检查检验制度及流程方面，公司信息技术服务机构管理部门、合规风险管理相关部门对信息技术服务机构进行必要的审查评估，通过合同协议审核、履约验收跟踪等方式，对服务机构和服务人员的访问权限、数据使用、保密义务与责任进行约束。公司发现信息技术服务机构等相关方违规存储或者使用公司经营数据和客户信息的，责令其立即改正并销毁已获取的经营数据和客户信息，并将

其纳入不良行为清单。供应商拒绝配合整改的，公司立即停止与其合作，将其纳入诚信黑名单，并根据合同条款采取措施维护自身及客户的合法权益。要求信息技术服务机构健全内部质量控制机制，定期监测产品或服务。如信息技术服务机构出现异常情形，公司根据法律法规、监管规定、内部制度和管理需要，按照应急预案开展内部评估与审查、处置工作。