海通证券股份有限公司信息安全及客户隐私保护管理声明

海通证券股份有限公司（以下简称海通证券或公司）作为大型国有金融企业集团，始终高度重视公司信息安全及客户隐私保护工作，在数据流转的全生命周期和业务运营的各个环节，建立了严格的管理机制，力求全方位守护信息安全和客户隐私。

一、管理机制

海通证券注重信息安全及客户个人隐私保护，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》《计算机信息系统安全保护条例》等国家法律、监管机构法规及行业规范对信息安全的要求，对全体客户信息和交易数据进行规范管理，切实保障全体客户信息安全和交易安全。

（一）管理架构

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客户隐私保护管理架构。信息安全和隐私保护管理架构由决策层、管理层、执行层、监督层组成，决策层由网络和信息安全领导小组及信息技术治理委员会组成，管理公司网络与信息安全工作和个人信息保护工作。网络和信息安全领导小组下设网络和信息安全领导小组办公室，日常办公机构设在数据中心，并由董事长、总经理共同担任网络和信息安全工作领导小组组长，保障个人信息保护工作有效开展。信息技术治理委员会下设数据治理工作办公室，日常办公机构设在运营中心，履行公司个人信息保护工作的协调管理职能。

海通证券信息安全和隐私安全保护管理架构

层级	部门/委员会	职责分工
决策层	网络和信息安全领导小组	• 下设信息安全领导小组办公室，负责全面统筹规划公司网络与信息安全工作，并组织协调与推进落实； • 由董事长及总经理共同担任网络和信息安全领导小组组长。
	信息技术治理委员会	• 履行公司个人信息保护工作的决策职能； • 审议公司数据治理目标、工作计划及计划落实情况。
管理层	网络和信息安全领导小组办公室	• 日常办公机构设在数据中心。网络和信息安全领导小组办公室负责人由数据中心主要负责人承担； • 负责推动、执行公司网络安全管理及常态

		化运营。
	数据治理工作办公室	• 履行公司个人信息保护工作的协调管理职能； • 负责推动、执行、落实公司数据治理相关工作； • 数据治理办公室日常办公机构设在运营中心，数据治理工作办公室主任由运营中心主要负责人担任。
执行层	个人信息保护专项工作组	• 负责公司个人信息保护工作的执行落实，由运营中心、金融科技部、数字金融部、财富管理总部、证券金融部、私人银行部、企业金融部、软件开发中心、数据中心、合规管理部、风险管理部等部门组成； • 组织制定个人信息保护管理制度，建立个人信息保护组织架构和管理机制，制定个人信息保护解决方案并组织实施； • 组织开展个人信息保护相关培训，逐步提升专业人员能力水平和员工安全保护意识； • 对公司及子公司开展个人信息保护监督、检查、问题通报、督促整改； • 建立健全个人信息保护考核评估机制。
监督层	稽核部	• 作为个人信息保护工作的监督部门； • 定期对公司处理个人信息遵守法律、行政法规、公司管理制度的情况进行专项稽核； • 发布稽核报告，督促问题整改，保障个人信息保护工作有效开展。

（二）管理制度

公司根据《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，制定并持续更新修订隐私保护类管理规范，包括《海通证券股份有限公司个人信息和隐私安全保护管理办法》《海通证券股份有限公司客户信息管理办法》《e 海通财 APP 隐私保护政策》；以及信息与数据安全类管理规范，如《海通证券股份有限公司数据分类分级管理办法》《海通证券股份有限公司信息安全管理办法》《海通证券股份有限公司信息资产安全管理办法》《海

通证券股份有限公司生产系统存储介质安全管理实施细则》，政策适用于公司所有业务条线，子公司结合所在地法律法规和所属行业监管规定参考执行。

类别	政策名称
隐私保护	《海通证券股份有限公司个人信息和隐私安全保护管理办法》
	《海通证券股份有限公司客户信息管理办法》
	《e 海通财 APP 隐私保护政策》
信息安全	《海通证券股份有限公司信息安全管理办法》
	《海通证券股份有限公司网络系统安全管理办法》
	《海通证券股份有限公司数据分类分级管理办法》
	《海通证券股份有限公司信息资产安全管理办法》
	《海通证券股份有限公司生产系统存储介质安全管理实施细则》

二、信息安全管理

海通证券注重信息安全管理，遵循“责任明确、授权合理、流程规范、技管结合”的工作方针，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》等文件要求，制定《海通证券股份有限公司信息安全管理办法》《海通证券股份有限公司网络系统安全管理办法》《海通证券股份有限公司个人信息和隐私安全保护管理办法》等多项制度，对全体客户信息和交易数据进行规范管理，定期、不定期开展内部和外部信息安全审查，落实信息安全保护措施，切实保障全体客户信息安全和交易安全。结合监管要求及公司内部管理规定，内外部审计对数据安全及隐私保护的覆盖频率至少为每年一次。2022 年，公司未发生客户信息泄露事件。

（一）信息安全保护措施

在信息安全保护机制方面，公司建立了包括主动预防措施和被动应对措施的全方位防护体系。

1.主动预防措施

- 公司建立“四横四纵”的纵深防御体系（四条防线四个重点区域），通过安全运营平台 7*24 实时监控及处置响应。针对来自不同设备的日志、多源情报进行关联分析，设计了多个关联场景，支撑安全运营中心实时检测，实时分级分类，实时告警。针对告警信息进行富化，及时发现网络攻击、病毒木马传播、漏洞隐患等威胁，从而使一线监控人员能及时闭环处置所有安全事件。
- 公司安全运营平台通过 SOAR（Security Orchestration, Automation and Response，安全编排和自动化响应）模块，针对固化的响应流程进行自动化编排，对恶意 IP 进行有效封禁，从而干扰攻击行为。

- 公司配合 BAS（Breach and Attack Simulation，入侵与模拟攻击）平台开展常态化网络安全防护措施有效性验证，从互联网侧及内网侧同时验证网络安全防护设备的有效性、防绕过安全能力以及覆盖程度，持续迭代验证场景，不断优化验证效果。互联网侧非对客系统采用零信任技术，做到“应收尽收”。
- 在集团各部门联动方面，公司构建分子公司一体化指挥“烽火台”，实现公司内共享威胁情报，联动处置，形成总部、分公司、子公司、服务商等一整套技术自查体系和责任落实体系。

2.被动应对措施

- 公司制定《海通证券网络安全事件应急预案》，其中包括发生数据泄露、数据损毁、个人信息泄露、个人信息篡改共 4 个场景的应急预案。公司根据有关情况变化及时更新预案。
- 公司定期开展应急预案相关培训、安全测试和应急演练，通过多层次的网络安全实战对抗演习，不断验证防护措施有效性，强化网络安全队伍实战能力，随时应对各类突发事件。数据中心通过每年两次的“红蓝紫”实战对抗演习，及时复盘总结形成加固整改专项，例如暴露面收敛、密码与权限加固等。

（二）信息安全审查

1.外部审查

在外部审查方面，公司基于网络安全等级保护工作、ISO27001 认证、组织开展外部审计，落实信息安全治理的审计管理。

在等级保护工作方面，公司按年度开展网络安全等级保护测评工作，做到有计划、有落实、有整改。公司已获得 ISO27001 认证证书（有效期至 2025 年 4 月 7 日），认证范围覆盖公司 100%的数据中心，其中包括主数据中心浦东新区德安路机房、异地备份数据中心广东东莞市凤岗镇机房（深交所南方中心），公司业务系统均部署在上述两个机房内。

2023 年 5 月 9 日，海通证券 e 海通财 APP 通过中证信息技术服务有限责任公司组织的证券期货业移动互联网应用程序安全认证（安卓和 iOS 双平台）。中证信息 APP 安全认证证书（有效期至 2026 年 5 月 8 日）覆盖海通证券财富管理业务条线 e 海通财 APP 所有业务。

同时，公司不定期聘请专业第三方机构实施信息技术管理工作专项审计。2021 年末，公司聘请 KPMG 实施信息技术管理工作专项审计，对数据治理组织架构、数据分类分级、数据安全、权限管理、数据应用等数据治理工作进行检查。

2.内部审查

在内部审查方面，公司结合监管要求及公司内部管理规定，每年度开展一系列信息安全审查活动，对数据治理组织架构、数据分类分级、数据安全、权限管理、数据应用等工作进行检查。业务部门梳理分管系统客户信息保护情况并提出优化改进措施。同时，公司每季度开展 IT 运维工作检查，每年度开展网络和信息安全专项检查，对信息技术治理、数据治理、信息安全等内容进行审查。2022 年 11 月，稽核部实施信息技术治理专项稽核，对数据安全、数据使用、数据销毁、隐私保护、数据备份、数据分类等数据治理工作进行检查。

三、隐私保护管理

公司充分尊重并保护用户隐私，制定《海通证券股份有限公司个人信息和隐私安全保护管理办法》《海通证券股份有限公司客户信息管理办法》等文件，规范管理用户隐私数据及信息。其中，e 海通财 APP 是公司获取客户个人信息的主要平台，公司制定《e 海通财 APP 隐私保护政策》，该政策覆盖公司财富管理业务条线，适用于所有 e 海通财 APP 个人用户。

（一）信息收集和存储

1.收集

在用户信息收集方面，公司建立个人信息收集与使用清单、个人信息与第三方共享清单，要求各单位只收集保留业务办理过程中所需的最少信息，并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《e 海通财 APP 隐私保护政策》中，明确告知客户收集数据范围和目的，并在隐私协议中充分揭示个人权利、告知客户相关数据使用用途等内容。

2.存储

海通证券仅在《e 海通财 APP 隐私保护政策》所述目的、所必需期间和法律法规及监管规定的时限内保存用户个人信息。如根据《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。"因此，海通证券后台数据采取与历史库分离，磁带库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 e 海通财 APP 的社区注册会员用户，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)。

（二）个人信息控制权利

在用户使用 e 海通财 APP 过程中，公司向用户提供包括但不限于访问、更正或修改、撤回同意、注销账号、拒绝个性化推送、自主化管理和保护信息等服务，以确保用户对个人信息的控制权。

1.访问

当个人依法提出查阅其信息的需求时，或当个人请求将其信息转移至指定第三方且符合国家网信部门规定条件的，公司会及时提供访问、转移途径。

2.修改

用户可通过线上、线下(临柜、见证)等多种渠道进行资料变更。e 海通财 APP 用户可通过“业务办理”版块，查询其个人资料，并进行资料变更。

3.删除

e 海通财 APP 用户可通过账号注销的方式，申请删除个人社区会员的相关数据。另外，当个人撤回同意信息收集授权时，公司将配合删除个人信息。如个人发现未删除情况，可通过客服热线 95553 或在线客服，向公司提出删除相关数据的请求。

（三）访问控制与保护

1.在访问控制方面，根据《海通证券股份有限公司个人信息和隐私安全保护管理办法》，公司建立个人信息访问控制管理机制，通过防火墙访问控制，严格对不同功能区域进行隔离。同时，根据业务需要和最小权限原则，合理控制和分配个人信息访问、使用策略和操作权限，确保不同职能人员具有对应级别的信息访问权限，避免越权操作行为。

2.在保护机制方面，根据《海通证券股份有限公司个人信息和隐私安全保护管理办法》，公司信息技术部门通过数据加密、鉴权、访问控制等技术手段，确保个人信息存储安全，并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。同时，公司开展个人信息分类分级管理，对其他个人信息进行重点保护，对敏感个人信息实行严格保护。公司建立健全数据分类分级管理制度和管理系统，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。

（四）产品开发中的隐私保护措施

公司要求在开发、测试环境不应使用真实的个人信息，如果测试需要，运维部门应进行去标识化或匿名化脱敏处理后使用，如开发、测试环境使用未脱敏数据的，应当采取与生产环境同等的安全控制措施；在开源技术应用的开发阶段，引入制品库专业软件，对超 10 万的开源组件进行依赖管理，并定期进行高危漏洞、开源协议扫描，促进安全开发；移动应用方面，公司在移动终端安全、身份鉴别、网络通信安全、数

据安全、开发安全和安全审计等方面进行规范化建设，满足《证券期货业移动互联网应用程序安全规范(JR/T 0192-2020)》要求，e 海通财 APP 于 2023 年 5 月完成证券期货业 APP 安全认证；大数据应用方面，相关需求内容需进行业务合规性评估。

四、能力建设与合作伙伴管理

（一）信息安全培训

为提升员工对于信息安全保护的意识和风险识别能力，公司定期组织信息安全教育活动，如国家网络安全宣传周。同时，公司通过邮件知识推送、张贴海报、发布线上学习课程等方式，向全体员工进行信息安全与隐私保护方面的理念宣导。2022 年，公司累计开展 4 次信息安全意识及数据安全管理培训，累计 7,500 人次参与培训。此外，2022 年，公司围绕个人信息数据安全、数据治理方面，开展 10 期宣贯活动，及时宣传国家法律及行业标准。

（二）信息技术服务机构管理

公司信息技术服务机构类型主要包括：硬件制造商、硬件代理服务商、应用软件制造商、软件代理服务商、信息咨询服务商、信息安全服务商、数据内容服务商、人力外包服务商、技术支持服务商、基础软件制造商、电信运营服务商等。根据《海通证券信息技术服务机构管理细则》，要求所有信息技术供应商需与公司签订保密协议，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。

公司在进行信息系统立项、采购招标、供应商遴选和履约管理的过程中，要求上述服务机构认真制定信息保密、数据保护等政策和方案，并在项目招投标、合同履约过程中进行评估、监督和跟踪。

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；若信息技术服务机构等相关方拒绝配合整改，公司将立即停止与其合作，并采取措施维护公司及客户的合法权益。信息技术服务机构对信息安全事件负有责任的，公司视查实的情节轻重与服务机构暂停或终止合作。

根据《证券基金经营机构信息技术管理办法》第三十四条要求，“除法律法规和中国证监会另有规定外，证券基金经营机构不得以任何方式向其他机构、个人提供客户信息”。因此，公司不会以任何方式向第三方机构、个人出租、出售或提供客户信息（法律法规和中国证监会另有规定、为完成交易和提供服务的用途除外）。

同时，根据《海通证券股份有限公司数据治理管理办法》第六十八条规定，“公司应当记录经营数据和客户信息的使用情况，并持续监督信息技术服务机构等相关方落实保密协议的情况”。在针对第三方服务机构的年度备案中，要求其提供投资者信息保密承诺；对驻场人员的年度运维工作情况进行检查；持续监督保密协议履行情况。公司将信息技术服务机构对投资者信息保护情况、保密协议履行情况纳入年度考评，在 2022 年考评中暂未发现服务机构泄密的相关事件。