

团体标准汇编

T/SAC 001-2024 ~ T/TSAC 002—2025

中国证券业协会

2025年12月

目 录

证券公司投诉处理标准.....	1
证券公司客户回访标准.....	22
证券业商用密码应用上线指南.....	52
证券业区块链电子数据存证应用规范.....	59
证券公司数字化能力成熟度指引.....	93
证券公司投资者个人信息保护技术规范.....	115
证券行业应用 RPA 技术的通用功能和接口规范.....	170

证券公司投诉处理标准

T/SAC 001—2024

（经协会第七届常务理事会第八次会议审议通过，2024年5月15日发布实施）

（中证协发〔2024〕92号）

前 言

本文件按照 GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国证券业协会投资者服务与保护专业委员会提出。

本文件起草单位：华福证券有限责任公司。

本文件起草人：邓长祺、陈代全、林佳、骆锦田、叶芳、郑明、林健芳、林业、张丹妮、林艳。

本文件为首次发布。

1 范围

本文件提供了证券公司投诉处理的工作要求、管理体系和组织实施标准，以及在具体实施过程中可能遇到的场景的建议处理方法，适用于证券公司投诉处理工作的管理与实施。本文件涉及的法规条款，如后续有修改的，以最新颁布的法规条款为准。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款，其最新版本（包括所有的修改单）适用于本文件。

GB/T 17242-1998 中华人民共和国国家标准：投诉处理指南

3 背景

近年来，多项关于建立健全证券公司投诉处理机制与指导投诉处理工作开展的制度有效实施，取得良好效果。为落实建设以投资者为本的资本市场，在制度机制设计上更加体现投资者优先，加大举措增强投资者的获得感和安全感，本文件结合相关规定及证券行业发展特点，将证券公司投诉处理工作进一步标准化，建立投诉处理团体标准，标准内容突出以投资者为本的理念，指导证券公司投诉处理工作有效执行。本文件供会员单位或社会组织自愿采用。

4 术语和定义

下列术语和定义适用于本文件。

4.1 投诉 complaint

投诉指投资者在购买证券公司产品或者接受相关服务时，与证券公司及其从业人员发生民事纠纷，要求解决纠纷的行为。

4.2 投诉人 complainant

投诉人指提出投诉（4.1）的投资者。投诉主体为自然人的，原则上宜由投资者本人提出。投诉主体为机构的，由法定代表人或其代理人提出。

投诉人委托他人代为投诉的，证券公司可以要求受托人提供投诉人姓名、投诉人有效身份证件信息、投诉人联系方式等材料。同时证券公司还可以要求受托人提供姓名、有效身份证件信息、联系方式、授权委托书等材料，如需公证，可根据证券公司制度自行确定。

4.3 投诉受理人（接收人） complaint acceptor

投诉受理人（接收人）指证券公司或其辖属单位接诉第一人，为负责初步判断投诉（4.1）的有效性，如实、完整地记录投诉人（4.2）详细资料、投诉内容及申诉要求，并交予本单位投诉处理人（4.4）的人员。

4.4 投诉处理人 complaint handler

投诉处理人指证券公司负责调查、处理投诉（4.1）的人员，投诉处理人包含投诉处理工作全流程的多名人员。

4.5 投诉处理专岗 complaint handling specialist

投诉处理专岗指证券公司在总部设立或指定的负责投诉处理工作的职能部门中负责查收各类投诉（4.1），及时转办、跟踪、指导、督促、汇总投诉并作统计分析、上报，并定期在证券公司内部展开投诉工作分析及培训，做好投诉事项相关各类材料归档等职责的专职人员。

5 投诉的分类

证券公司宜在制度及投诉处理系统中提前设置投诉分类，以便及时分派投诉处理任务。证券公司可根据本公司实际情况和需要，在投诉处理系统中采用以下分类方式。

5.1 根据证券业务类型划分

a) 经纪业务投诉：

1) 账户及权限类投诉：投资者对账户相关业务办理要求或办理方式不理解，以及账户因无法开通各类权限（涵盖反洗钱、异常交易等账户受限）或对权限开通的要求不满而产生的投诉。包括但不限于：开户问题；转、销户问题；账户权限开通及注销受限、签署协议等问题；三方存管签约、撤销或变更问题；资金存取或划转问题；非交易过户问题；账户信息变更问题；账户资料管理问题；休眠账户激活或注销问题等。

2) 证券交易委托类投诉：投资者在交易过程中对业务规则、成交规则不了解、不理解而产生的投诉，及对持仓股票成本价、浮动盈亏不理解而产生的投诉。包括但不限于：股票交易问题（含申购）；可转债、债券交易问题（含申购）；港股通交易问题；转融通交易问题；股转平台业务交易问题；成本价及浮动盈亏问题等。

3) 产品类投诉：投资者对各基金、理财产品（含现金理财产品）、投资顾问产品的参与、退出规则流程等不理解或不满意而产生的投诉。产品包括但不限于：固定收益产品（收益凭证、货币基金等）；理财产品（现金理财产品）；公募基金产品；私募基金产品；投资顾问产品等。

4) 交易系统及软件投诉：投资者对行情或委托交易系统的功能、更新速度、菜单设置、故障等不满意而产生的投诉。交易系统、软件及交易方式包括但不限于：行情系统或 PC 交易系统问题；手机 APP；电话委托；现场委托等。

5) 服务及费用类投诉：投资者对从业人员服务观感较差的投诉；投资者对产品或账户佣金费率标准以及定制服务产品的佣金费率标准或交易手续费存有异议的投诉；经营机构销售产品履行适当性义务有关投诉。包括但不限于：服务态度问题；服务响应速度问题；服务专业性问题；短信、电话骚扰问题；佣金调整及各类手续费、税费问题；销售产品履行适当性管理问题等。

6) 信用业务类投诉：投资者参与融资融券、质押回购、股票期权等信用业务而产生的投诉。包括但不限于：融资融券业务投诉；股票质押业务投诉；约定购回业务投诉；期权业务投诉等。

b) 其他业务投诉：

1) 证券资产管理业务投诉。

2) 自营业务投诉。

3) 期货中间介绍业务投诉。

4) 承销与保荐业务投诉。

5) 托管业务投诉

6) 其他业务投诉。

c) 疑似证券市场违法违规行为投诉：疑似员工违规展业、代客理财、不合规开户等情况引起的投诉。

d) 疑似非法证券活动投诉：疑似冒充开户、理财、诈骗等情况引起的投诉。

e) 其他投诉。

5.2 根据同一事项投诉人数量划分

a) 个体投诉：同一事项投诉仅涉及单个或少数（10 人以下）投诉人，涉及面较小的投诉。

b) 群体投诉：同一事项投诉涉及大量投诉人，或涉及面较大，处置不当可能影响证券公司正常营业或给被投诉主体带来负面影响的投诉。群体投诉一般指有 10 人（含 10 人）以上因同一原因引起的投诉。

10 人（含 10 人）以上投诉人采取面谈方式提出群体投诉的，宜建议其推选代表，代表人数不超过 5 名。

5.3 根据投诉的重要性以及紧急程度划分

a) 重大投诉：证券公司及其工作人员可能涉及投资者资金安全、内幕交易、操纵市场、利益冲突等违法违规行为从而导致恶劣影响的；存在群体投诉、缠访闹访的；涉及重大技术系统故障等突发事件可能引起严重后果的；可能导致重大诉讼风险或对公司形象、信誉和利益造成重大影响的；其他可能引发证券公司被采取行政处罚、监管措施等重大合规风险隐患的；证券公司判断为重大投诉的其他情形。

b) 一般投诉：投诉人仅要求改进流程、提高服务质量等一般性问题或金额较小的经济纠纷，不会造成重大负面影响的投诉，以及非重大投诉范围的其他投诉。

5.4 根据投诉人投诉的合理性划分

a) 合理诉求：投诉人对证券公司及其工作人员进行投诉，对象准确、诉求合理的，证券公司宜积极安抚投诉人情绪，积极进行工作整改，完成投诉处理事项。

b) 无理投诉：投诉人对证券公司及其工作人员进行投诉，但其诉求缺乏法律法规和相关合同支持，且诉求明显超出合理范围或无正当理由，并存在发泄不良情绪情形，但暂无明显依据可以在受理时不予受理的投诉。下列判定理由供参考。

1) 投诉内容缺乏法律法规和相关合同支持，并明显超出合理范围；

2) 反映问题明显与事实不符，且后续未提供相关证据、事实凭据的，或提供虚假、伪造证据及事实凭据的，并存在宣泄个人情绪的情形；

3) 投诉内容经核实仅为与证券公司工作人员非工作原因纠纷，并不涉及投资者在购买证券公司产品或者接受相关服务时发生的；

4) 其他经审慎判定后为无理投诉的投诉情形。

无理投诉仍应遵循投诉处理流程，证券公司宜关注无理投诉分类和处理流程，无理投诉情形在答复投诉人、监管部门时宜更关注判定过程、分析理由及证据留痕。

6 投诉方式和渠道

证券公司宜建立投诉处理系统，对接所有投诉方式、投诉渠道统一管理。

6.1 投诉方式

- a) 现场投诉：指投诉人在营业场所与证券公司工作人员当面进行的投诉；
- b) 电话投诉：指投诉人通过监管机构或证券公司的服务电话进行的投诉；
- c) 信函投诉：指投诉人通过邮件、信件或发函的形式进行的投诉；
- d) 网络投诉：指投诉人通过网络形式进行的投诉；
- e) 其他投诉方式：指除现场、电话、信函、网络方式以外的其他方式。

6.2 投诉渠道

- a) 监管机构转办投诉：通过 12386 服务平台、投资者保护机构、自律组织、证券交易所、相关监管机构等转办的投诉；
- b) 证券公司自行受理的投诉：通过证券公司投资者服务热线电话、在线客服、电子邮箱、营业场所现场、营业部咨询电话、信箱等证券公司自行受理的投诉。

证券公司可以设立或者指定投诉接待区域，此区域宜与业务受理部门或办公区等可能接触到证券公司商业秘密等内部信息的内部区域分离，可配备相应的设备记录并保存投诉接待处理过程。

7 处理原则

因投诉工作复杂，特殊情况下需要处理人员灵活应对，证券公司宜在制度、业务培训、公司文化中明确处理原则，以便及时妥善完成投诉处理工作。证券公司可根据本公司实际情况和需要，采用以下原则促进投诉处理工作。

7.1 首办负责制

- a) 证券公司宜明确首个接诉单位对该投诉事项负责受理、督办，积极将相关矛盾化解在第一现场和第一环节，并如实记录投诉人诉求并根据证券公司内部流程转办。

b) 证券公司宜明确首位接诉工作人员（4.3）对该投诉事项负责受理，做到用语规范、热情周到，稳定投诉人不满情绪，不推诿投诉事项。

7.2 限时办结原则

证券公司宜规定处理投诉工作相关部门、人员在接诉、转办、处理、沟通、回复等环节保证积极响应、及时应对、限时办结。

7.3 便民性原则

证券公司宜在公司网站、营业场所、客户端的显著位置公示投诉电话、传真和电子信箱等联系方式 [来源：证券经纪业务管理办法，第三十二条]，保证投诉电话在营业时间内有人员值守及接听，提升接通率和服务质量，建议投诉电话具有录音功能。

证券公司宜在营业网点、官方网站等多种渠道展示投诉处理流程，方便投资者了解公司工作流程、提出意见建议，接受投资者监督。

7.4 客观性原则

证券公司投诉处理坚持客观、真实的原则，如实反映投诉事件。客观对待问题分歧，深入分析发生原因，并如实反映投诉人诉求和沟通处理结果。

7.5 重要优先性原则

证券公司明确投诉处理工作的重要性，并宜在投诉处理工作中划分具体投诉事项的重要性程度，采用不同的处理方式，对重要、敏感、特殊投诉事项或复杂情况第一时间处理、报告。

7.6 有效性原则

证券公司工作人员与投诉人沟通宜遵循及时、有效的原则。证券公司宜制定投诉处理工作手册供工作人员使用。工作手册宜具备可操作性和提供有助于解决争议分歧的处理方案及措施，证券公司宜定期更新方案措施，确保工作手册有效执行。

7.7 回避性原则

为保证投诉处理过程公平、公正，证券公司宜明确投诉事项中涉及的被投诉人为证券公司投诉受理人（4.3）或投诉处理人（4.4、4.5及其他可能相关的人员）的，由具有管理职能的上级部门或区域集中机构重新指定与被投诉事项无直接利益关系的人员为投诉处理人；区域集中机构，一般是指证券公司的分公司或具有管理职能的中心营业部等。

7.8 保密性原则

a) 证券公司宜规定投诉事项相关人员（4.3、4.4、4.5 及其他可能相关的人员）对投诉工作过程中所接触或获知的涉及投诉、投诉人等所有信息或资料以及投诉处理措施、处理结果等予以保密，不得擅自泄露；

b) 证券公司宜规定投诉事项相关人员（4.3、4.4、4.5 及其他可能相关的人员）自觉维护投诉人个人信息安全，依法保护国家秘密、商业秘密和个人隐私。

7.9 协同性原则

证券公司宜制定对涉及内部多部门或跨机构的投诉事项的转办机制，引导内外部投诉处理工作协同互助。

8 处理体系

8.1 投诉组织架构与职责分工

证券公司宜建立有效的投诉组织架构以保障投诉处理工作顺利开展，证券公司可根据实际投诉管理情况设立投诉组织架构与职责分工，但建议保证以下职能得到实现。

8.1.1 投诉工作领导小组与职责分工

证券公司可成立投诉工作领导小组，如证券公司已设立投资者权益保护委员会，可由投资者权益保护委员会承担具体职责或兼任：

a) 负责统筹指导和协调证券公司投诉工作落实，负责对重大、敏感、特殊投诉事项进行审议、出具处理决定、建议，并督导执行；负责督促总部相关业务条线、部门对涉及公司层面的投诉处理问题进行管理改进。

b) 至少包含一名高级管理人员，高级管理人员报证券业协会备案。[来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第二十八条]其余人员可由合规、法务及各业务相关部门负责人等人员组成。

8.1.2 投诉工作小组与职责分工

证券公司可以成立投诉工作小组，负责结合各部门职责对各部门、区域集中机构投诉处理工作进行具体指导，负责就重要、敏感、特殊投诉事项进行讨论并出具处理建议，负责督促各部门、区域集中机构存在的问题进行管理改进，负责对各部门、区域集中机构投诉处理工作情况进行检查督导和考核评价，证券公司宜根据自身业务实际扩充完善。

证券公司各部门、区域集中机构可以成立投诉工作小组，可由各部门、区域集中机构的主要负责人、合规风控负责人、部门负责人等人员组成，或指定人员作为分支机构投诉处理专员。各部门、区域集中机构负责人为投诉工作第一责任人，对投诉管理履行首要责任。

证券公司可根据实际投诉管理情况建立各层级投诉工作小组或其他常设小组、专项小组、专员等，但建议保证投诉工作小组职能得到实现。

8.1.3 投诉管理部门职责

证券公司宜在总部设立或指定负责投诉处理工作的职能部门，作为证券公司投诉管理的主要部门，负责证券公司投诉工作的全流程督导，并报证券业协会备案。[来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第二十八条]主要职责包括：

a) 负责牵头制定和完善投诉管理的相关制度、流程，负责建立投诉管理相关工作机制并确保有效运行，证券公司宜根据自身业务实际扩充完善。

b) 负责具体投诉事项的受理、转办、跟踪、督促以及反馈报送。

c) 负责牵头组织对各部门、下辖分支机构投诉处理情况、管理机制运行情况等进行检查监督。

d) 负责建立和完善证券公司投诉管理工作评价指标体系、评价机制、标准，并牵头或协调组织对区域集中机构进行考核评价，证券公司宜根据自身业务实际扩充完善。

e) 负责就投诉工作与监管机构、调解组织等外部机构进行沟通。

f) 负责召集证券公司投诉处理工作领导小组会议和投诉处理工作小组会议，并就会议相关决议落实进行跟踪督办。

证券公司可根据实际投诉管理情况调整投诉管理牵头部门职责，但建议保证相关职责得到落实。

8.1.4 相关部门投诉管理职责

证券公司宜规定相关部门应就投诉事项处理提供支持协助：

a) 证券公司相关部门负责对涉及条线业务推广、产品设计、业务管理、系统支持等方面的投诉事项处理提供业务指导、提示建议、跟踪协助，负责对投诉事项反映出的业务问题和管理不足进行分析梳理并加强管理改进。

b) 证券公司合规部门或相关职能部门负责必要的指导，并对违反投诉管理相关制度、流程及内控要求的情形以及存在投诉处理不尽职或沟通不到位等问题的单位、工作人员进行追究。

c) 证券公司法律事务相关部门负责对投诉事项的处理提供法律咨询或参与处理。

d) 证券公司其他相关管理部门负责对涉及本部门职责的投诉事项处理提供必要的支持与协助。

8.1.5 分公司或具有管理职能的区域管理总部管理职责

证券公司存在分公司或具有管理职能的区域管理总部的，宜规定投诉处理管理职责包括但不限于：

a) 负责根据证券公司要求建立区域集中机构投诉处理工作程序并具体细化工作流程与内控要求，负责督促建立证券公司区域集中机构投诉处置预案、管理联动机制并确保有效运行，证券公司宜根据自身业务实际扩充完善。

b) 负责督导区域集中机构对投诉事项进行有效处理，负责跟踪投诉事项处理进度并掌握处理情况，确保及时办结投诉事项，必要时应就重要、敏感、特殊投诉事项或其他复杂情况与证券公司总部相关业务部门进行沟通并及时反馈处理进展情况。

c) 负责对区域集中机构提交的投诉事项处理方案、意见和答复口径等进行审核、确认。

d) 负责对投诉事项反映出的业务问题和管理不足等情况进行分析梳理并加强管理改进。

e) 负责根据证券公司要求细化区域集中机构投诉管理工作评价标准并对区域集中机构直转投诉处理情况进行考核评价，证券公司宜根据自身业务实际扩充完善。

8.1.6 营业部投诉管理职责

证券公司宜规定营业部职责包括但不限于：

a) 负责对投诉事项进行具体调查、沟通、解决和反馈，并及时向分公司或上级具有管理职能的区域管理总部报告处理进度和处理措施。

b) 负责及时拟定投诉事项具体处理方案、处理意见和答复口径，根据投诉情况的轻重缓急提交分公司或上级具有管理职能的区域管理总部报备或报批。

c) 负责对投诉事项反映出的内部管理缺失、投资者服务不到位等问题进行整改并加强管理改进。

证券公司可根据实际投诉管理情况调整分公司或具有管理职能的区域管理总部、营业部或其他部门的投诉管理职责，但建议保证相关职责得到实现。

8.1.7 投诉处理专岗人员职责

证券公司应当配备至少 1 名投诉处理专岗人员，并报证券业协会备案。 [来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第二十八条]

a) 投诉处理专岗人员应于每个工作日及时查收各类投诉并及时转办至相关部门或区域集中机构，并及时与投诉处理相关人员确认收悉情况。

b) 投诉处理专岗人员在投诉事件处理过程中宜随时保持与投诉处理人的联系，并对相关部门或区域集中机构开展投诉处理工作进行指导，及时告知或了解投诉事件进展情况。投诉处理专岗人员对投诉调查处理进展做到及时跟踪、适时督促，并视情况就调查处理进展情况及时向负责投诉处理工作的部门负责人报告。

c) 投诉处理专岗人员定期汇总证券公司所接投诉以及分支机构上报投诉，实施具体分类并作统计分析，根据监管要求按期上报，并定期在证券公司内部开展投诉工作分析及培训，形成对相关部门或区域集中机构投诉处理工作的督导。

d) 投诉处理专岗人员宜及时对投诉事项跟踪督办过程留痕材料、投诉事项相关各类文档以及系统审批流程等各类材料进行归集、整理，相关示例见附录 A，证券公司宜根据自身业务实际扩充完善。

8.2 制度保障

证券公司宜建立健全投诉处理相关制度，强化工作责任落实，保护投诉人合法权益，在制度中明确投诉处理的职责分工、处理流程、时限要求、答复反馈、追踪整改、责任追究、培训安排和资料存档等。证券公司宜根据制度执行中发现的问题，完善内控机制、管理改进措施、配套相关的制度。

8.2.1 保障职责分工

证券公司宜在制度中明确各部门投诉处理职责分工（8.1）。

8.2.2 明确处理流程

证券公司宜在制度中明确各部门、各区域集中机构相关投诉处理流程（9.3.2），包括但不限于投诉的受理标准、调查要求、报告流程、材料留存等，证券公司宜根据自身业务实际扩充完善。

8.2.3 明确时限要求

证券公司宜在制度中明确各类投诉的接收及反馈时限要求（9.3.2），宜在投诉处理系统中设置 3 个交易日、20 个交易日提醒功能。

8.2.4 追踪整改机制

投诉管理部门宜适时牵头或协调组织对各部门、区域集中机构投诉管理机制运行情况、投诉事项、调查处理过程、留痕情况等进行检查，证券公司宜根据自身业务实际扩充完善。同时证券公司宜及时对反映出的问题及时采取有效措施予以纠正、整改。

8.2.5 投资者反馈机制

证券公司宜积极听取投资者对产品和服务的意见，接受投资者的监督，根据投资者投诉总结相关问题，及时发现业务风险，根据投资者的合理意见改进工作，建立完善内控制度。证券公司可以使用电话调查、网络调查、满意度调查问卷等方式收集投资者意见，证券公司宜根据自身业务实际扩充完善。

8.2.6 第三方投诉管理机制

证券公司宜加强涉及第三方专业机构合作业务投诉的管理，投资者因证券公司与第三方专业机构合作营销而购买证券产品或者提供服务从而产生民事纠纷的，证券公司宜协调相关第三方专业机构配合处理投诉，对投诉事项进行核实，及时提供相关情况，促进投诉顺利解决。

- a) 证券公司建立对合作第三方专业机构的准入退出评估机制。
- b) 证券公司与第三方专业机构的合作在许可的业务范围内进行，严格按照相关监管要求进行审核。
- c) 宜关注以下方面：
 - 1) 证券公司宜在投诉处理制度中明确对第三方专业机构投诉事项的处理机制；
 - 2) 在与第三方专业机构的合同中建议明确涉及第三方专业机构投诉事项的处理流程；
 - 3) 协商设置第三方专业机构至少一人作为对接人，负责协调沟通涉及第三方专业机构合作业务投诉的处理。

8.2.7 应急处置机制

证券公司宜建立投诉突发事件的应急处置机制，证券公司宜根据自身业务实际扩充完善。应急处置机制中应包含清晰可行的应对措施，做好重大及群体性投诉事件的预防、应急处理工作。

8.3 人员配备要求及管理

证券公司宜选择具有一定工作经验的人员从事投诉处理工作，建议符合以下要求：

- a) 熟悉相关法律法规，具有一定的证券业务知识能力及证券从业经验；
- b) 了解投诉处理制度、流程，具有一定的执行力；

c) 具有一定的沟通技巧和服务技巧，能积极安抚投诉人情绪、有效引导投诉人表明诉求或能积极向投诉人反馈投诉处理进度及结果；

d) 具有一定的调查和分析能力，能够快速组织对投诉事项的调查反馈。

作为证券公司投诉处理专岗人员，建议额外符合以下要求：

a) 具有较强的管理统筹能力；

b) 了解投诉受理及处理的全流程环节，具有一定的协调沟通能力，具有对接监管机构的经验；

c) 具有一定的调查和分析能力，对投诉数据进行分析及提出改进工作机制。

证券公司及其辖属部门可根据实际工作情况指定投诉事项相关人员（4.3、4.4、4.5 及其他可能相关的人员），不强制要求对投诉受理人、投诉处理人、投诉处理专岗人员进行岗位隔离，但建议严格遵守回避性原则（7.7）且建议由非营销序列人员担任投诉处理人。

证券公司宜定期收集投诉处理人员的意见和建议，可以建立投诉处理相关人员的评价机制，对在投诉处理工作中持续做出成绩和有突出贡献的人员予以表扬；对于违反相关制度规定的，视情节严重程度对责任人员分别予以追究，宜确保制定责任追究机制。[来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第三十二条]

8.4 保密机制

证券公司宜完善内部信息管理机制，遵守个人信息保护管理相关规定，根据投诉处理需要“最小”范围收集投资者个人信息，防止在投诉处理过程中泄露投资者资料、商业秘密、国家秘密等信息或者被不当利用，并对相关信息、投诉处理措施、处理结果等予以保密。在向监管机构等有关机构履行涉及投资者信息的数据报送义务时，应明确责任部门，按照监管机构的有关要求落实数据安全措施。

8.5 培训机制

证券公司宜安排人员收集行业及证券公司内部典型或优秀投诉处理案例资料，定期开展投诉处理工作的培训或宣导，每年开展不少于一场全体培训或宣导。建议通过对投诉案例资料等进行针对性分析、评价，总结相关经验，及时发现存在的问题，制定改进措施，加强工作人员警示培训，并注意留痕供监管检查。证券公司宜根据自身业务实际扩充完善。

8.6 评价机制

证券公司宜建立和完善投诉管理工作评价指标体系、评价机制及具体标准，并由投诉管理部门牵头或协调组织对各部门、区域集中机构进行年度评价，证券公司宜根据自身业务实际扩充完善。各部门、分支机构投诉管理工作成效作为反映合规管理水平的重要指标，建议其评价结果统一纳入分支机构年度运营内控评价、合规风控考核范畴。

9 处理程序

投诉处理程序流程示例见附录 B，证券公司宜根据自身业务实际扩充完善。

9.1 投诉受理

9.1.1 受理范围

证券公司对于存在下列情形之一的投诉，可不予受理，但应严格做好留痕工作：

- a) 投资者非该经营机构客户的；
- b) 受托人未取得投资者委托授权的；
- c) 投资者就同一事实和理由重复向经营机构进行投诉，经营机构已受理或已经做出处理意见的，但投诉人补充证明材料的除外；
- d) 投诉相关争议已进入调解、仲裁、诉讼等程序，或已通过上述程序处理的；
- e) 违反社会公序良俗以及恶意攻击、骚扰或无实质诉求内容的；
- f) 其他不予受理的情形。[以上来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第十三条]

以上范围如遇其他监管机构或其他法律法规另有要求的，应从其规定。为加强投资者权益保护，宜严格限制不予受理的情形，除严格不予受理的情形外，宜全部受理。

9.1.2 受理要求

a) 证券公司宜在接收投诉人投诉 3 个交易日内，作出是否受理的决定。[来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第十二条]

b) 对于投诉事项清晰、投诉诉求明确，提供投诉人、被投诉人基本情况，符合本文件投诉定义且不属于 9.1.1 中规定情形的投诉，建议予以受理。

c) 投诉受理人(4.3)宜如实、完整地记录投诉人详细资料、投诉内容及申诉要求。其中,如初步判断涉及重大投诉或群体投诉的,建议投诉受理人高度重视,立即启用证券公司相关重大事件报告机制及突发事件应急机制。

d) 证券公司最终决定受理的,宜按内部程序进行报告处理。证券公司做出不予受理决定的,宜采取电子邮件、短信、信函或电话等方式向投诉人进行通知,并说明不予受理的理由。

9.1.3 受理原则

a) 尽职尽责受理原则,为保护投资者权益,建议除明确可以不予受理的情形外,宜全面受理监管转接工单、自行受理工单,确保投诉处理责任落实。

b) 无理投诉全面记录原则,无理投诉经过内部审批,可以答复投资者,做完结事项处理,并如实向监管部门沟通反映、填写转接工单,为保障证券公司权益,该项工作过程建议全面记录、留痕,证券公司宜根据自身业务实际扩充完善。

9.1.4 受理程序

a) 证券公司接收投诉人投诉(T日)当天,投诉受理人(4.3)初步判断投诉有效性并决定是否受理投诉(9.1.2、9.1.3),期间可以请示投诉管理部门和投诉工作小组等(8.1.2、8.1.3、8.1.4)的建议,投诉受理人(4.3)宜及时跟进受理工作:

1) 证券公司在接收投诉人投诉3个交易日(T+3日)内,作出投诉受理决定的,投诉受理人宜核实投诉人投诉对象、投诉内容及涉诉部门等,将投诉相关记录、材料转办至证券公司内投诉处理人并及时跟踪处理进度。

2) 属于可以不予受理情形,证券公司作出不予受理决定的,应当采取电子邮件、短信、信函或电话等方式向投诉人进行通知,并说明不予受理的理由。[来源:证券基金期货经营机构投资者投诉处理工作指引(试行),第十四条]

3) 初步判断涉及无理投诉的,建议先行受理,避免投诉人负面、抵触情绪,耐心倾听投诉人诉求,耐心解释不激化矛盾。无理投诉因其复杂性、主观性,从保护投资者利益角度出发,建议证券公司及时组织投诉处理工作小组、投诉涉及部门或区域集中机构等单位对认定为无理投诉的内容进行调查说明,并出具相应的证明材料及分析报告,及时通过内部流程审批至证券公司相关职能部门,并留痕处理,避免简单定性、草率处理,相关示例见附录C,证券公司宜根据自身业务实际扩充完善。

9.2 投诉处理

9.2.1 处理要求

a) 证券公司确保营业时间内投诉渠道畅通。

b) 投诉的处理，宜实行限时管理：

1) 对能够当场解决的问题，或投诉人要求当场办理的业务确属当场能进行办理的，应立即解决；

2) 对在规定时间内能够解决的问题，应尽早解决、不得拖延。

c) 投诉处理人宜在规定完结时限内将处理意见反馈投诉人，尽量促使与投诉人达成和解。

d) 因特殊原因不能及时提出处理意见的，宜在规定完结时限内将投诉处理进展情况向投诉人作初步反馈，并在有处理意见后第一时间反馈投诉人。

e) 在规定完结反馈时限内无法联系投诉人的，可采取微信、短信、电子邮件、电话、现场走访及挂号信等多种渠道积极联系投诉人。

9.2.2 处理程序

a) 证券公司决定受理投诉（9.1.4）后，投诉受理人（4.3）派发投诉任务，投诉处理人（4.4）于接到投诉处理任务当日及时组织对投诉事项的投诉事实、投诉原因、相关展业过程及其合规性等内容进行调查核实：

1) 分析确认投诉人诉求、问题争议点、导致投诉的原因及责任工作人员，同时客观评估可能造成的不良影响后果，视情况向上级管理部门或证券公司投诉管理部门（8.1.3）进行报告。

2) 如遇特殊敏感事项或人群，投诉处理相关人员宜慎重对待、妥善处理，严防群体性、涉稳事件发生。对重大投诉、群体投诉或敏感、特殊投诉事项或其他复杂情况，投诉涉及部门或区域集中机构等单位应及时就投诉事项内容性质、投诉人背景、矛盾争议及投诉原因分析、调查处理工作进展、投诉人沟通情况、处理措施意见等形成书面报告，第一时间根据证券公司制度报证券公司相关工作小组（8.1.1、8.1.2）；必要时，及时向证券业协会及当地监管部门报告。

b) 投诉事件指向的部门或区域集中机构等单位宜配合投诉处理人就投诉事项调查处理结果如实、规范填写于相应投诉登记表中。投诉登记表应包括但不限于以下内容：

1) 投诉事实及经过，包括投诉事实与投诉人诉求、投诉事项经过、调查处理过程、与投诉人沟通情况、最终处理结果等；

2) 投诉原因及内控分析，包括问题争议点、被投诉原因、相关展业过程及其合规性、内部责任分析、影响后果分析等；

3) 内部责任追究情况（如有）；

4) 存在的不足及管理改进措施（如有）；

5) 相关工作建议（如有）。

c) 投诉事项应于证券公司接收投诉之日起 20 个交易日（T+20 日）内（如遇当地监管机构要求另行规定的可相应调整）办结。

d) 如因特殊原因确实无法在上述规定时间内办结的，投诉处理人、投诉处理部门或区域集中机构等单位宜提前向投诉管理部门并申请延期（可多次延期，但每次延期不可超过 20 个交易日且同一投诉延期总天数不可超过 20 个交易日），同时说明延迟的原因和预计提交时间。证券公司可根据实际投诉管理情况，确定审批层级。

延期申请报批通过后，建议采取电子邮件、短信、信函或电话等方式向投诉人进行告知，并说明延期的原因和预计反馈处理意见的时间。

e) 证券公司做出投诉处理决定后，投诉处理人（4.4）及时将投诉内容的核实情况、作出决定的有关依据和理由向投诉人进行说明，并保留相关证明资料。投诉人无法联系的，可采取的告知方式包括但不限于电子邮件、短信、信函、电话或现场走访等多种渠道。对于监管机构通过系统平台转办的投诉，证券公司应将处理结果填写于相应监管转办系统内。

9.2.3 处理情况报送

证券公司宜安排专人做好日常投诉材料的收集整理。

证券公司宜安排专人于每月初/每季度初收集汇总上月/上季度投诉情况，编制报送材料并根据监管要求于对应报送渠道及时报送，证券公司宜根据监管要求及时调整表格。

9.3 意见反馈

投诉处理人应将处理意见及时向投诉人与被投诉人（如有）反馈：

a) 对投诉处理结果满意的，处理办结；

b) 对投诉处理结果不满意的，无法达成和解的，证券公司宜提示投诉人可以向投资者保护机构以及其他有调解职能的组织提起调解申请；调解未果的，告知投诉人可根据合同约定提起仲裁或向法院提起诉讼。

9.4 资料归档

a) 建议证券公司建立投诉处理台账，证券公司宜根据自身业务实际扩充完善。台账中宜如实登记投诉人投诉事由、调查处理过程、处理结果、投诉受理和处理人、处理责任部门等要素，其中投诉人投诉事由宜逐项记录投资者投诉的基本情况，包括但不限于投诉时间、投诉人基本情况、投诉对象、投诉请求、主要事实和理由。[来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第十一条、第十四条]

b) 证券公司宜妥善保存投诉相关信件、电子邮件、电话语音、录音及投诉登记记录、处理意见等材料，保存时间原则上不低于十年，有特殊监管规定的根据其他法律法规遵照执行。[来源：证券基金期货经营机构投资者投诉处理工作指引（试行），第三十条]

c) 证券公司宜建立全流程的投诉处理系统，包括投诉转办、处理、审批、数据统计等流程性管理功能，以及材料的留痕功能。

10 投诉处理监督

a) 投诉处理的监督主要包括投诉事件本身合规性、投诉处理过程规范性、投诉事项涉及内部合规有效性等方面，持续提升证券公司投诉处理的质效，强化内控和自查机制。

b) 证券公司宜建立投诉处理责任追究机制，对投诉处理不力的部门或人员根据情况追究相关责任，证券公司宜将投诉处理情况列入工作人员评价体系。

11 投诉处理工作总结与提升

证券公司宜定期梳理投诉事项，结合统计分析、投诉事项整改等途径，及时总结易诉人群、易诉问题，积极构建事前防诉机制，以减少投诉发生，证券公司宜根据自身业务实际扩充完善。

12 附则

12.1 本文件所称“交易日”、所称“内”包括本数。

12.2 本文件规定事项，如遇其他监管机构或其他法律法规另有要求的，应从其规定。

附录 A (规范性) 归档材料清单

A.1 分支机构自行受理的投诉，在受理、处理流程中的相关书面材料、录音、视频等（如有）

A.2 监管机构转办的投诉，在受理、处理流程中的相关书面材料、录音、视频等（如有）

A.3 投诉事项跟踪督办过程留痕材料、投诉事项相关各类文档以及系统审批流程等各类材料（如有）

A.4 投诉处理台账

A.5 投诉统计表（如有）

A.6 审计、监管机构检查等应检材料（如有）

A.7 公司投诉培训相关材料（如有）

A.8 投诉处理典型案例（如有）

注：以上要素宜在投诉系统内实现。

附录 B
(规范性)
投诉处理流程图

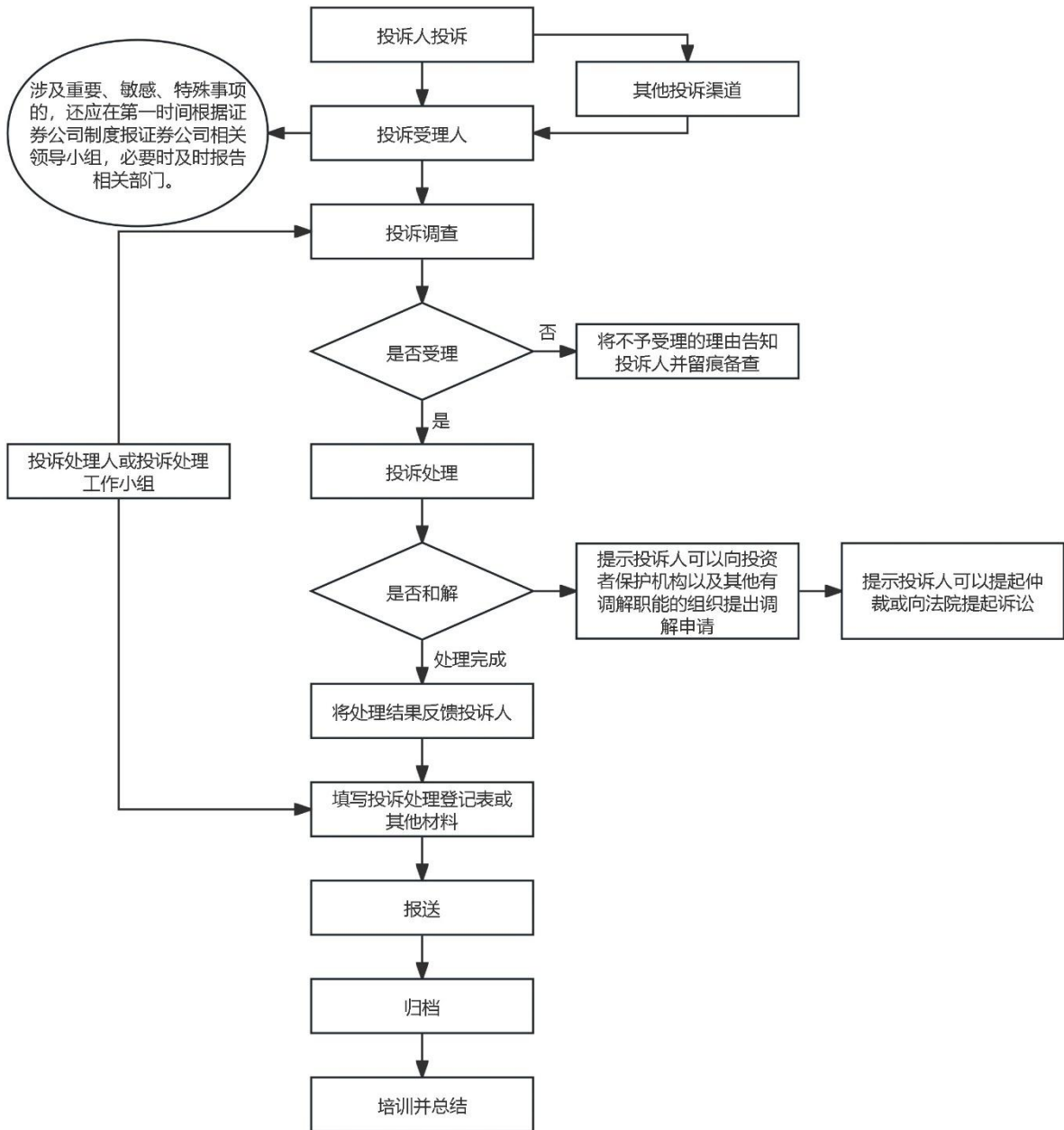


图 B.1 投诉处理流程图

附录 C
(规范性)
无理投诉流程图

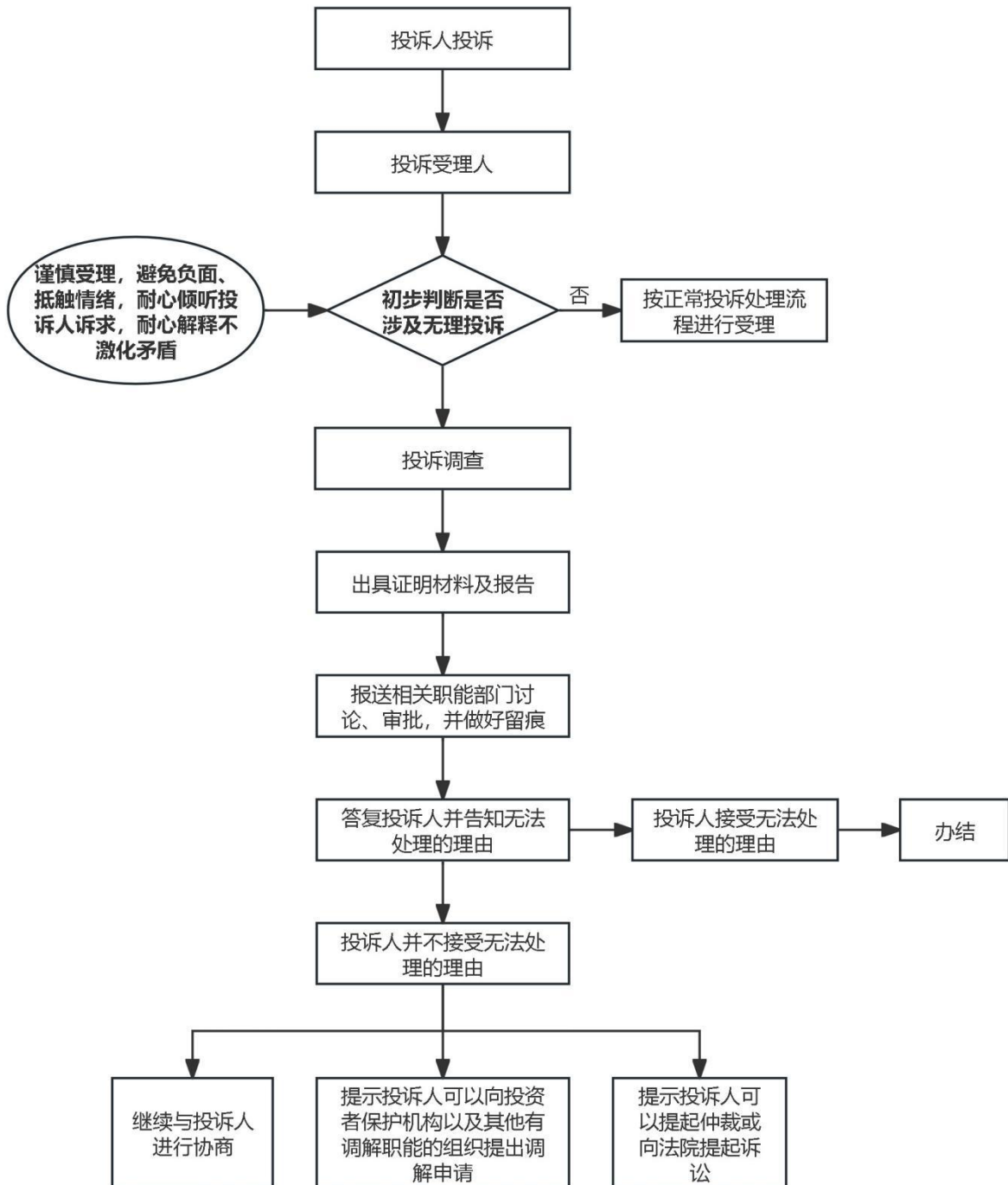


图 C.1 无理投诉处理流程图

证券公司客户回访标准

T/SAC 002—2024

（经协会第七届常务理事会第八次会议审议通过，2024年5月15日发布实施）

（中证协发〔2024〕92号）

前 言

本文件按照 GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国证券业协会投资者服务与保护专业委员会提出。

本文件起草单位：华安证券股份有限公司。

本文件起草人：刘晓东、余海春、张文、姜利泉、钱家悦、戴钰、刘俊、刘芷清、王焱、钱文君。

本文件为首次发布。

1 范围

本文件提供了证券公司客户合规性回访的工作要求、管理体系和组织实施标准,以及在具体实施过程中可能遇到的场景的建议处理方法,适用于证券公司客户回访工作的管理与实施。

2 规范性引用文件

下列文件中的内容(包含注明“来源”内容)通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

DA/T 79-2019 证券业务档案管理规范

3 背景

近年来,多项关于建立健全证券公司客户回访机制与指导客户回访工作开展的制度有效实施,取得良好效果。为落实建设以投资者为本的资本市场,在制度机制设计上更加体现投资者优先,加大举措增强投资者的获得感和安全感,本文件结合相关规定及证券行业发展特点,将证券公司客户回访工作进一步标准化,建立客户回访团体标准,标准内容突出以投资者为本的理念,指导证券公司客户回访工作有效执行。本文件供会员单位或社会组织自愿采用。

4 术语和定义

下列术语和定义适用于本文件。

4.1 客户 client

客户是指在证券公司开户或就获取产品和服务与证券公司签订协议的自然人、法人、非法人组织等。

4.2 客户回访 client review

证券公司向客户了解销售产品或提供服务的过程是否符合相关要求的行为。

5 客户回访的分类

5.1 根据业务场景划分

5.1.1 新开户回访

经纪业务中对新开资金账户和证券账户的客户,证券公司宜及时进行回访,回访确认后新开账户方可使用。[来源:证券经纪业务管理办法,第三十一条]其中宜特别关注非现场开户客户。

5.1.2 新增交易权限回访

经纪业务中对新增相关交易权限的客户，在开通相应交易权限后三十日内完成回访。[来源：证券经纪业务管理办法，第三十一条]

5.1.3 异常情形回访

经纪业务中对账户使用、资金划转、证券交易等存在异常情形的客户进行回访。[来源：证券经纪业务管理办法，第三十一条]

a) 账户使用异常情形参考：单个客户账户在多个设备或站点登录交易、多个客户账户在同一个设备或站点登录交易以及其他可能不符合账户实名制要求的情形。

b) 资金划转异常情形参考：客户账户出现大额资金划转，大额资金划转的金额标准宜参照反洗钱主管部门制定的大额交易报告相关标准。

c) 证券交易异常情形参考：客户账户发生虚假申报、拉抬打压股价、维持涨（跌）幅限制价格、自买自卖或者互为对手方交易、严重异常波动股票申报速率异常以及违反法律、行政法规、部门规章、规范性文件或者各证券交易所业务规则的其他异常交易行为。

5.1.4 其他客户回访

经纪业务中除新开户、新增交易权限、账户异常交易等已即时完成回访的情形外，其他客户每年回访比例不得低于上年末客户总数（不含休眠账户及中止交易账户客户，下同）的5%。[来源：证券经纪业务管理实施细则，第十二条] 此处宜关注其他存量客户的回访。

经纪业务中所有回访类型总计，每年回访比例不得低于上年末客户总数的10%。[来源：证券经纪业务管理实施细则，第十二条]

5.1.5 适当性回访

证券公司宜对购买产品或接受服务的客户，每年抽取不低于上一年度末购买产品或接受服务的投资者总数（含购买或者接受产品或服务的风等级高于其风险承受能力的投资者，不含休眠账户及中止交易账户投资者）的10%进行回访。[来源：证券经营机构投资者适当性管理实施指引（试行），第二十三条] 宜关注该比例是对于需要做适当性管理的客户数量。

宜特别关注增加适当性回访频次的情形：证券公司向普通投资者销售高风险产品或者提供相关服务。[来源：证券期货投资者适当性管理办法，第二十条]

5.1.6 相关业务回访

a) 代销金融产品。证券公司宜在客户回访制度中专门明确代销金融产品的回访要求，以及时发现并妥善处理不当销售金融产品及其他违法违规问题。[来源：证券公司代销金融产品管理规定，第十八

条]

b) 场外期权。证券公司应当至少每年对投资者的资质复核一次,并通过定期回访、监测评估等方式确保投资者持续符合适当性管理要求。[来源:证券公司场外期权业务管理办法,第三十二条]建议与适当性回访相结合并作为工作重点。

c) 基金销售。基金销售人员应当积极为投资者提供售后服务,回访投资者,解答投资者的疑问。[来源:证券投资基金销售人员职业守则,第二十五条]

d) 相关募集工作。证券公司宜在回访制度中关注相关募集工作,对购买基金产品或者服务的普通投资者定期抽取一定比例进行回访,对持有 R5 等级基金产品或者服务的普通投资者增加回访比例和频次。[来源:基金募集机构投资者适当性管理实施指引(试行),第十二条]

募集机构应当在投资冷静期满后,指令本机构从事基金销售推介业务以外的人员以录音电话、电邮、信函等适当方式进行投资回访。回访过程不得出现诱导性陈述。募集机构在投资冷静期内进行的回访确认无效。[来源:私募投资基金募集行为管理办法,第三十条]

5.1.7 执业情况回访

a) 证券公司每年宜对证券经纪人招揽和服务的客户进行回访,了解证券经纪人的执业情况,并作出完整记录。负责客户回访的人员不得从事客户招揽和客户服务活动。[来源:证券经纪人管理暂行规定,第十六条]

b) 证券公司从事证券投资顾问业务,应当建立客户回访机制,明确客户回访的程序、内容和要求,并指定专门人员独立实施。[来源:证券投资顾问业务暂行规定,第二十一条]

c) 证券公司宜按监管要求或自身实际需要开展相关回访工作,例如对拟离职人员、被投诉人员名下客户进行回访,了解该人员的服务情况、是否存在违规行为;在投诉事项处理完结前,对提出投诉的客户进行回访,了解是否存在投诉纠纷未了事项、客户对投诉处理及证券公司服务是否满意。[来源:相关通知]

回访类型包括但不限于上述类型,宜对专门列明的回访类型严格对照落实,相关业务、服务回访和适当性管理回访如有重叠可合并进行,为严格落实投资者保护工作,宜选取覆盖较多客户的比例对照落实。

5.2 根据回访方式划分

5.2.1 人工电话回访

人工电话回访是指回访人员通过电话外呼,按照规定的回访要点向客户提问,并记录客户的回答结果的回访方式,通话录音及回访结果等随系统以电子化形式保存。人工电话回访适用于高风险业务或产品相关的回访场景,以便及时判断客户是否知悉相关风险、是否存在工作人员违规行为或投诉事项,可

以在异常情形回访、高风险的产品及服务回访、拟离职人员名下客户回访、被投诉人员名下客户回访、投诉事项处理完结回访等场景使用。

5.2.2 智能语音回访

智能语音回访是指证券公司通过智能外呼系统电话联系客户,按系统预设的回访要点向客户播报规定的回访内容,并对客户的回答进行识别与判断,自动生成记录结果的回访方式,通话录音及回访结果等随系统以电子化形式保存。智能语音回访适用于新开户、中低风险业务或产品相关的回访场景,推荐新开户回访、中低风险的产品及服务回访、客户满意度回访等场景使用。

5.2.3 问卷回访

问卷回访是指证券公司通过业务终端、交易终端、官方网站、邮箱、短信和即时通讯等渠道向特定客户发布既定内容的电子问卷或通过信函方式发放纸质问卷,由客户进行填写反馈,证券公司进行收集、留痕。宜关注非强制问卷回访存在滞后性,适用于低风险业务或产品相关的回访场景,推荐低风险的产品及服务回访、经纪人执业情况回访、客户满意度回访等场景使用。设置为必要环节、不可自行关闭的强制性问卷回访可适用于大部分回访场景,宜关注在业务系统中设置自动触发环节。

5.2.4 即时通讯回访

即时通讯回访是指回访人员通过短信、微信、5G消息等方式,与客户实时地传递文字、文件、语音以及视频等,并对回访结果进行收集、留痕。即时通讯回访适用于低风险业务或产品相关的回访场景,推荐低风险的产品及服务回访、客户满意度回访,以及多种方式无法联系到客户等场景使用。

5.2.5 面见回访

面见回访是指回访人员直接面见客户,通过现场访谈和填写回访纪要的方式进行信息交互,并对访谈过程以视频或音频的方式记录,证券公司进行收集、留痕。面见回访适用于高风险业务或产品相关的回访场景,以便详细了解客户情况,及时判断客户是否知悉相关风险、是否存在工作人员违规行为或投诉事项,推荐在异常情形回访、高风险的产品及服务回访、拟离职人员名下客户回访、被投诉人员名下客户回访、投诉事项处理完结回访、证券公司需要详细了解客户情况、客户提出面见需求等场景使用。

6 客户回访的基本要求

客户回访旨在及时了解和掌握客户需求,持续改进产品和服务,保障客户合法权益,促进证券公司业务规范发展。证券公司相关部门及人员在客户回访各环节宜严格落实监管规定、切实保护客户权益及个人信息、坚决回避利益冲突。

6.1 落实监管规定

证券公司开展客户回访工作,不仅是完善自身客户服务体系的需要,同时也是落实反洗钱、客户账

户实名制、投资者保护和适当性管理等监管规定的需要，证券公司在业务开展过程中宜严格按照证券行业相关监管规定和要求，组织开展客户回访工作。

6.2 保护客户权益

在开展客户回访工作过程中，证券公司宜充分尊重客户意愿、考虑客户体验，选择合适的回访方式、选定适宜的回访时间、保持合理的回访频次、采用清晰易懂的话术，确保回访工作有效开展。

证券公司及相关工作人员对在客户回访过程中所接触或获知的客户信息或资料予以保密，自觉维护客户个人信息安全，依法保护国家秘密、商业秘密和个人隐私不受侵犯。

6.3 防止利益冲突

为保护客户权益、防范业务风险，证券公司确保回访人员在执行回访任务时不存在利益冲突，回访人员不得对与本人有营销服务或有直接利益相关的客户进行回访，负责客户回访的人员不得从事客户招揽和客户服务活动。涉及回访人员被客户投诉的情况，宜由客户回访管理人员重新指定与被投诉事项无直接利益关系的回访人员对该客户进行回访。

7 客户回访的管理体系

7.1 组织架构

客户回访宜同时关注业务流程及内部控制两个方面，证券公司宜明确客户回访是业务流程的重要环节，需要纳入业务统一管理，避免出现回访执行与业务管理要求不一致的情形；同时，证券公司建立科学合理的客户回访组织架构，各相关部门宜各司其职、勤勉尽责，从职责分工、制度建设、岗位设置和技术支持等方面保障客户回访工作顺利开展，确保沟通协作和信息互通，提升客户回访工作质量和客户服务水平。证券公司可根据本公司实际情况和需要，采用以下管理模式来开展客户回访工作。

7.1.1 总部集中管理模式

a) 证券公司可以根据业务需要，总部设置回访工作管理部门负责公司客户回访的统筹管理。采用总部集中模式的证券公司宜在总部指定部门负责公司客户回访的统筹管理，指定部门或机构负责回访执行工作，管理及执行部门可为同一部门。回访执行机构包括受委托的第三方专业机构。

b) 部分证券公司的客户回访管理工作由多个业务部门自行管理，并由专门部门按照业务部门要求执行回访工作，建议该种形式宜指定总部部门统筹管理。

7.1.2 总分结合管理模式

a) 证券公司可以根据业务需要，总部设置回访工作管理部门负责公司客户回访的统筹管理，由区域集中机构或分支机构协助管理并负责回访执行工作。一般可分为：总部+区域集中机构、总部+分支

机构、总部+区域集中机构+分支机构，以及第三方专业机构与前三种相结合的形式。区域集中机构，一般是指证券公司的分公司或具有管理职能的中心营业部等。

b) 总分结合管理模式适宜“工作人员-客户”稳定对接的工作模式，建议该种形式宜提高总部部门统筹权限，通过制定数据报送途径等方式加强监督。

7.1.3 补充工作组模式

a) 证券公司可以根据业务需要，由客户服务中心管理、执行回访工作，为最普遍模式。证券公司宜关注客户服务中心职责一般为执行业务部门的需求，回访、汇总、反馈回访结果，缺少督导职责。

b) 宜在客户服务中心设置回访工作组，由客户服务中心、业务部门相关人员组成。工作组作为实际统筹机构，并确定责任人，各业务部门宜指定回访工作负责人，当客户回访中涉及具体业务场景时，作为该回访工作的共同责任人。

7.2 职责分工

7.2.1 统筹管理部门或机构职责

作为证券公司客户回访工作的统筹管理部门，主要职责包括但不限于：

a) 组织建立本公司客户回访制度，协调各业务部门建立和完善客户回访部门制度及流程，制度中宜明确规定业务部门、分支机构的职责和对第三方专业机构的管理（7.3）。

b) 组织建立和完善本公司客户回访电子系统、智能系统。

c) 监督执行部门按要求完成客户回访。

d) 组织协调本公司相关部门对回访结果进行应用。

e) 明确具体业务的回访标准、制定回访话术要点、确定需回访的客户类别或范围，对回访人员进行培训，并对回访工作落实情况进行监督。

f) 总部统筹管理部门负责人、客户所对应的分支机构的负责人、业务部门回访负责人均宜设置为本公司客户回访管理工作责任人，对客户回访管理履行相应责任。

7.2.2 执行部门或机构职责

作为证券公司客户回访工作的执行部门，主要职责包括但不限于：

a) 按制度和流程要求执行本公司客户回访工作。

b) 组织协调本公司相关部门对回访结果进行应用。

c) 及时反馈客户回访工作中遇到的特殊情况、异常情形，畅通报告路径。

d) 对客户回访工作资料进行归集、整理，并妥善保管。

e) 落实客户回访相关培训。

执行部门一般为客户服务中心或第三方专业机构，工作制度及履职重点宜关注时效、执行、客户信息保护方面。

7.2.3 业务部门职责

- a) 提出回访需求，宜重点关注时限要求及必要回访内容。
- b) 明确具体业务的回访标准、制定回访话术要点、确定需回访的客户类别或范围。
- c) 对回访人员进行培训，并对回访工作落实情况进行监督。

7.3 制度保障

证券公司应建立由相对独立人员对重点客户进行定期回访的制度。[来源：证券公司内部控制指引，第四十五条]证券公司的客户回访制度宜明确各类客户回访工作的分工、要求和时限等，并对公司客户回访工作的执行情况进行评价。证券公司可根据本公司实际情况和需要，在制度中明确以下重点内容。

7.3.1 明确职责分工

证券公司宜在制度中明确回访工作职责分工，可以设置客户回访管理部门负责回访工作的整体流程及标准框架等；回访前、回访后工作宜根据业务归属由相应部门负责；相关部门和机构宜在职责范围内积极配合回访工作的组织和落实。

7.3.2 明确工作流程

证券公司宜在客户回访制度中明确客户回访工作流程，包括但不限于客户回访工作的准备、实施、结果应用等。

7.3.3 明确时限要求

证券公司宜在客户回访制度中明确各类客户回访工作的时限要求，其中重点关注：

- a) 新开户回访：应在账户可使用之前完成客户回访工作。
- b) 异常情形回访：应在发现异常情形后的两个交易日内开展客户回访工作。
- c) 适当性回访：宜在每个自然年度结束前完成客户回访工作，新增交易权限应在三十个自然日内完成客户回访工作。
- d) 经纪人执业情况回访：宜在每个自然年度结束前完成客户回访工作。
- e) 其他类型回访：宜根据具体业务需要适时开展客户回访工作。

相关示例见附录 A，证券公司宜根据自身业务实际扩充完善。

7.3.4 明确人员任职要求

证券公司宜明确客户回访相关岗位人员的具体任职要求，并按照客户回访工作开展的实际需要任用相关岗位人员，不强制要求进行岗位专一、隔离，但宜严格遵守回避利益冲突的要求。

客户回访相关岗位人员的任职要求宜根据工作内容进行差异化设定，具体任职要求包括但不限于：

a) 熟悉客户回访相关法律法规、部门规章及自律规则等，具有较强的管理能力和理解能力，了解客户回访工作全流程，掌握一定的沟通技巧。

b) 具备证券专业知识以及客户服务专业能力、数据和信息分析能力、培训讲师专业能力、系统运维能力。

c) 宜重点关注劳务派遣人员的资质，建议证券公司可以通过自行设置客户回访人员任职能力测试等方式，确保其符合岗位任职要求。

7.3.5 明确保护个人信息

证券公司宜完善内部信息管理机制，遵守个人信息保护管理相关规定。根据客户回访工作需要最小范围收集客户个人信息，防止在客户回访执行过程中泄露客户资料、商业秘密等信息，或者被不当利用，并对客户信息予以保密。在向外部单位履行涉及客户信息的数据报送义务时，宜明确责任部门，按照监管机构的有关要求落实数据安全措施。

a) 收集的客户个人信息宜与实现业务功能有直接关联。直接关联是指没有该信息的参与，业务功能无法实现。

b) 自动采集客户个人信息的频率宜是实现业务功能所必需的最低频率。

c) 直接或间接获取客户个人信息的数量宜是实现业务功能所必需的最少数量。

d) 开展客户回访前，客户服务条款宜载明根据相关要求，向客户告知个人信息处理规则，包括处理目的、处理方式和处理的个人信息种类、保存期限等内容。

7.3.6 明确培训机制

证券公司宜定期或不定期对客户回访岗位人员进行培训，包括但不限于岗位技能培训、服务技能培训、合规培训等。证券公司客户回访制度宜明确培训的频次，建议不低于每年一次。

7.3.7 明确评价机制

证券公司宜建立和完善客户回访工作评价指标体系、评价机制及具体标准，并由客户回访管理部门按年度组织对执行客户回访工作的部门或机构进行评价，相关评价指标示例参见附录B，证券公司宜根据自身业务实际扩充完善。客户回访工作由本公司机构承担执行的，客户回访工作评价结果宜统一纳入本公司年度机构运营内控评价、合规评价范畴；客户回访工作由第三方专业机构负责实施的，客户回访工作评价结果宜纳入合作第三方专业机构的准入退出评估范畴。

7.4 岗位设置

证券公司可根据本公司实际情况和需要，在遵循回避利益冲突的前提下，根据自身实际设置下列岗位，实施各岗位轮岗或兼岗。

7.4.1 客户回访管理岗

负责客户回访任务的组织分配、实施管理和检查监督，确保客户回访工作有效完成，完善客户回访工作制度和流程。

客户回访管理岗主要职责如下：

- a) 通过回访任务系统，统一组织分配各类型回访任务至客户回访执行岗。
- b) 通知回访执行人员在规定任务期限内执行客户回访任务。
- c) 实时监测回访执行人员任务完成进度，并做好相应提醒。
- d) 做好回访质检人员质检结果的复核工作，并公布评价结果。

7.4.2 客户回访质检岗

负责对客户回访工作全流程进行质检分析，及时发现存在的问题，并提出相应整改措施。质检岗可由证券公司其他部门人员兼任。

客户回访质检岗主要职责如下：

- a) 确定各回访类型相关要求。
- b) 定期质检回访内容，对发现的问题及时提出整改措施。
- c) 汇总回访执行效果，做好执行人员回访质量评价。
- d) 不定期召开回访质量分析会，协助培训人员开展人员培训工作。

7.4.3 客户回访培训岗

负责制定客户回访培训计划，编制培训资料，并实施培训工作。培训岗可由证券公司其他部门人员兼任。

客户回访培训岗主要职责如下：

- a) 根据业务开展需要，确定培训时间、频次及内容。
- b) 通知相关人员参与培训，记录、统计人员参训情况。
- c) 采用合适的方式实施培训。
- d) 定期总结分析培训效果，提升培训质量。

7.4.4 客户回访执行岗

负责客户回访任务的具体执行、客户回访资料的登记与归档、客户回访信息的收集、分发与反馈，相关客户回访资料归档登记表示例见附录 C，证券公司宜根据自身业务实际扩充完善。

客户回访执行岗主要职责如下：

- a) 熟悉回访话术及回访相关要求。
- b) 根据要求及时执行回访任务，遇到异常情况及时反馈相关人员。

- c) 结束回访任务时，做好回访登记，记录客户相关建议和诉求。
- d) 定期或不定期做好回访工作总结，包括但不限于执行任务数量、遇到的问题等，按要求参加培训，持续提升客户回访工作质量。

7.4.5 客户回访运维岗

负责客户回访系统的运行维护，制定系统应急处理方案，针对客户回访系统的使用需求及使用过程异常情况，会同系统开发厂商完成优化工作。运维岗可由证券公司其他部门人员兼任。

客户回访运维岗主要职责如下：

- a) 回访系统的搭建、运行维护，定期收集汇总系统相关意见和建议，提升系统使用体验。
- b) 智能外呼回访知识内容维护、人机交互设计、调优训练、性能测试等工作。
- c) 通过服务数据标注、问题优化、客户满意度分析等，推动智能回访服务能力提升。
- d) 配合相关人员对客户回访结果数据进行统计分析。

7.5 技术支持

7.5.1 客户回访系统建设

证券公司宜建立客户回访电子管理系统，具体功能包括但不限于回访人员及权限管理、回访任务及流程管理、回访话术及问卷管理、回访档案资料管理、系统日志管理，在客户管理中增加回访模块。

7.5.2 客户回访系统维护

证券公司宜安排专门技术人员负责客户回访系统的运行维护，确保系统的安全、高效、稳定、可持续运行。建立适度的冗余备份机制，制定系统应急处理方案，保障客户回访工作的正常开展，确保客户回访电子数据的安全完整。

7.6 外包管理

委托第三方专业机构实施客户回访的证券公司，宜参照 7.2、7.3 及 7.4 要求，加强机构准入和客户回访人员管理，确保客户信息安全，相应的法律责任由证券公司承担。[来源：证券经纪业务管理实施细则，第十二条]

- a) 证券公司宜建立对合作第三方专业机构的准入退出评估机制，且符合以下要求：
 - 1) 具有完整的法人治理结构和内部组织架构；
 - 2) 具有相应的业务资质和经营许可，符合法律法规备案要求；
 - 3) 具有良好的信誉和财务状况；
 - 4) 不存在影响合作的内部或外部阻碍，包括但不限于受到有关部门立案调查、存在重大违法行为或可能影响合作的仲裁或诉讼。

b) 证券公司宜加强涉及第三方专业机构合作客户回访业务投诉的管理，客户因证券公司与第三方专业机构合作提供产品或服务而产生民事纠纷的，证券公司宜要求相关第三方专业机构配合处理投诉纠纷，对投诉纠纷事项进行核实，及时提供相关情况，促进投诉纠纷顺利解决。

8 客户回访的组织实施



图 1

8.1 回访工作准备

8.1.1 制定回访方案

回访工作相关部门（7.2.1、7.2.2、7.2.3）制定回访方案，包括客户回访目的和要求、实施计划和步骤、回访的类型和方式、回访客户的范围。客户回访方案示例见附录 D，证券公司宜根据自身业务实际扩充完善。

8.1.2 确定回访内容

回访工作相关部门（7.2.1、7.2.2、7.2.3）根据客户回访事项和适当性要求确定客户回访内容。相关示例见附录 A、附录 E，证券公司宜根据自身业务实际扩充完善。

8.2 回访工作实施

8.2.1 生成回访任务

按照客户回访工作的具体要求确定回访目标客户，由系统生成、系统分配客户回访任务，如有必要也可以通过系统手工录入的方式生成回访任务。

a) 确定实施客户回访人员名单，明确回访责任（7.4.1、7.4.4）。

b) 做好回访宣传投资者教育工作，在办理业务时向客户做好回访提醒。

8.2.2 执行回访任务

客户回访执行岗（7.4.4）宜在规定时间内，使用规范话术，收集客户回访数据，完成客户回访任务，

回访未触达客户的情形及对应建议处理方式参见附录 F，证券公司宜根据自身业务实际扩充完善。

8.2.3 规范回访登记

证券公司宜规范登记客户回访情况，登记要素包括客户身份信息、回访类型、回访方式、回访完成情况等。

8.2.4 回访资料管理

客户回访资料宜由专人负责保管。客户回访记录无论通话录音、电子介质或书面方式载体，所有回访资料保存期限不得少于 20 年。客户回访资料归档登记表示例参见附录 C，证券公司宜根据自身业务实际扩充完善。

8.3 回访结果应用

8.3.1 回访结果统计分析

回访工作统筹管理部门（7.2.1）宜定期或不定期对客户回访结果数据（回访客户数、回访完成率、各问题答案的回答客户数及占比等）进行统计分析，充分使用回访结果，助力公司业务发展，客户回访分析示例参见附录 G，证券公司宜根据自身业务实际扩充完善。

8.3.2 回访结果应用方式

客户回访结果的应用方式包括但不限于：

a) 将产品与服务类回访的结果数据反馈给相关部门，可用于结合证券公司实际业务发展情况改进产品和服务质量。

b) 掌握证券公司及工作人员的合规经营展业情况，对发现的违规情形及时进行核实、处理，对可能存在风险的事项及时进行干预、解除，提高公司合规风控水平。

c) 通过对客户提出的意见、建议的统计与分析，了解证券公司为客户提供的交易终端使用便捷性、系统运行稳定性、客户使用满意度以及客户对新功能的需求等情况，可用于证券公司完善相关系统建设。

d) 通过对回访结果数据的综合分析，对证券公司运营情况进行整体把握，优化相关制度流程，为证券公司各项经营决策提供参考依据和数据支持。

8.3.3 回访结果异议处理

客户所属分支机构或证券公司相关部门对客户回访结果存在异议的，包括但不限于产品和服务质量、违规情形、系统建设等方面，可向客户回访管理部门进行反馈，由客户回访管理部门会同相关业务部门进行核实，并给出核实结果及处理建议。

客户回访执行人员对回访结果存在异议的，可向客户回访管理人员进行反馈，由客户回访管理人员进行核实，并给出核实结果及处理建议。

证券公司宜在制度中专门设置该环节。

8.4 涉嫌违规事项处置

证券公司在回访过程中发现涉嫌违规事项，可建立事件上报处置流程。

- a) 回访执行部门在回访过程中发现涉嫌违规事项，可向回访管理部门上报。
- b) 回访管理部门分析评估涉嫌违规事项后，可向风险管理部门或相关业务管理部门报告。

9 附则

9.1 本文件所称“交易日”、所称“内”包括本数。

9.2 本文件规定事项，如遇当地监管机构要求或其他法律法规另有要求的，应从其规定。

附录 A

(规范性)

常见客户回访类型及操作要求

表 A.1 常见客户回访类型及操作要求

序号	回访类型	回访对象	回访比率	回访时间要求	回访方式	回访关注要点	参考文件
1	新开户回访	新开资金账户和证券账户的客户	100%	账户可使用前	所有回访方式中的任一种。	包括但不限于： 1、确认客户身份；客户委托他人代理开户的，应向客户确认代理人身份及代理权限； 2、确认客户已阅读各类风险揭示文件并理解相关条款； 3、确认客户开户为其真实意愿； 4、提醒客户自行设置和妥善保管密码。	《证券经纪业务管理办法》 《证券经纪业务管理实施细则》 《证券账户非现场开户实施细则》
		非现场新开户客户	100%	账户可使用前	所有回访方式中的任一种。单向视频开户必须人工电话。	包括但不限于： 1、客户身份识别； 2、客户开户意愿； 3、关注投资者是否对不同市场交易规则的差异有清晰的了解、在开户过程中是否认真阅读并亲自签署了风险揭示书。	《证券账户非现场开户实施细则》
2	新增交易权限	新增设定准入条件的交易权限的客户	100%	交易权限开通后三十个自然日内	所有回访方式中的任一种。	1、客户账户权限变动确认； 2、证券公司从业人员是否违规操作客户账户； 3、适当性等关注点。	《证券经纪业务管理办法》 《证券经纪业务管理实施细则》 《证券期货投资者适当性管理办法》

常见客户回访类型及操作要求（续）

3	异常情形回访	账户使用、资金划转、证券交易等存在异常情形的客户	100%	两个交易日内	所有回访方式中的任一种，建议人工参与回访。	包括但不限于： 1、对异常情形的询问，应当注意识别客户身份及是否为本人操作，关注可能的风险； 2、是否向投资者充分揭示风险。	《证券经纪业务管理办法》 《证券经纪业务管理实施细则》
4	适当性回访	购买产品或接受服务的客户（包括但不限于购买金融产品、签约投顾服务等客户）	上一年度未购买产品或者接受服务的客户总数（含购买或者接受产品或服务风险等级高于其风险承受能力的客户，不含休眠账户及中止交易账户）的10%	每个自然年度结束前	所有回访方式中的任一种。	包括但不限于： 1、客户身份识别； 2、客户是否按规定签署《投资者基本信息表》《投资者风险承受能力评估问卷》； 3、客户是否知晓产品或服务风险及相关业务规则等； 4、客户是否知晓自己的风险承受能力等级、购买的产品或者接受服务的风险等级以及适当性匹配意见； 5、客户是否知晓承担的费用以及可能产生的投资损失； 6、证券公司人员是否违规操作客户账户； 7、客户是否存在全权委托； 8、是否存在《证券期货投资者适当性管理办法》第二十二条情况。	《证券经纪业务管理办法》 《证券经纪业务管理实施细则》 《证券经营机构投资者适当性管理实施指引》 《证券公司代销金融产品销售管理规定》 《证券公司场外期权业务管理办法》 《基金募集机构投资者适当性管理实施指引（试行）》及其他业务办法等
		购买代销金融产品、场外期权业务等专门提示的服务或产品的客户	1、确保在适当性回访比例中包括专门业务的回访； 2、宜对购买高风险产品的普通投资者明显增加其回访次数。	每个自然年度结束前	所有回访方式中的任一种。		

常见客户回访类型及操作要求（续）

5	执业情况回访	经纪人、证券投资顾问名下客户	经纪人、投资顾问名下客户，可与适当性回访比例结合。	每个自然年度结束前	所有回访方式中的任何一种，宜关注不得由从事招揽客户、服务的人员进行回访。	包括但不限于： 1、经纪人、投资顾问的执业情况； 2、经纪人、投资顾问是否违规操作客户账户、违规推荐产品或接受客户全权委托等。	《证券经纪人管理暂行规定》 《证券经纪业务管理办法》 《证券经纪业务管理实施细则》 《证券投资顾问业务暂行规定》
6	其他应关注的回访类型	购买了私募基金的客户	100%，可以结合合同和机构投资者因素	在投资冷静期满后（此处回访是业务流程重要环节）	以录音电话、电邮、信函等适当方式。	包括但不限于： 1、客户是否知悉投资冷静期的起算时间、期间以及享有的权利； 2、客户是否知悉风险揭示、未来可能承担投资损失； 3、《私募投资基金募集行为管理办法》第三十条和《基金募集机构投资者适当性管理实施指引（试行）》第十三条规定的内容。	《私募投资基金募集行为管理办法》
		拟离职人员名下客户	拟离职人员名下客户，可与适当性回访比例结合。	人员离职前	所有回访方式中的任何一种。	包括但不限于： 证券公司人员是否存在操作客户账户、违规推荐产品、承诺收益或接受客户全权委托等违规行为。	相关通知

		被投诉人员名下客户	被投诉人员名下客户，可与适当性回访比例结合。	投诉事项处理完结后			
--	--	-----------	------------------------	-----------	--	--	--

常见客户回访类型及操作要求（续）

补充：

- 1、宜关注资金账户包括普通资金账户、信用资金账户、衍生品资金账户等；
- 2、回访金融产品户等情形时，宜关注受访者是否为对应产品的实际管理人；
- 3、对除新开户、新增交易权限及账户使用、资金划转、证券交易等存在异常情形之外的其他经纪业务客户，每年回访比例不得低于上年末客户总数（不含休眠账户及中止交易账户客户）的5%；
- 4、证券公司开展经纪业务回访工作的，每年回访比例不得低于上年末客户总数的10%；
- 5、回访如有重叠可合并进行，为保障落实投资者权益保护，建议选取覆盖回访人数较多的方案进行操作；
- 6、回访方式宜从其相关制度要求；无特别要求的，可选择所有回访方式中的任一种，也可按需使用多种方式组合回访；为保障投资者权益，异常情形、高风险业务宜使用人工回访。

附录 B

(资料性)

客户回访工作评价指标

表 B.1 客户回访工作评价指标

评价周期		评价时间		评价组织部门					
评价说明									
客户回访评价指标		工作的制度与合规情况 (权重30%)			工作执行情况 (权重50%)		结果与资料管理情况 (权重20%)		
参评单位	主要评价内容	制度与流程 (10%)	岗位要求 (10%)	信息保密 (10%)	任务完成率 (20%)	执行登记 (10%)	异常情形处理 (20%)	编写回访报告 (10%)	管理回访资料 (10%)
	得分								
单位A (回访执行部门或机构)	评价简述 (若有)								
	得分								
单位B (回访执行部门或机构)	评价简述 (若有)								
	得分								
.....						(宜关注应急能力)		

附录 C

(规范性)

客户回访资料归档登记表

表 C.1 客户回访资料归档登记表

序号	归档日期	客户账号	客户姓名	回访任务名称	归档人姓名	备注
1	年/月/日					
2	年/月/日					
3	年/月/日					
...						

备注：以上要素宜在回访系统内实现。

附录 D
(规范性)

客户回访方案

表 D.1 客户回访方案

回访需求部门：

方案制定时间： 年/月/日

回访目的	
回访实施计划	1、确定回访类型、回访对象、回访比率、回访时间要求； 2、确定回访实施步骤，如回访方式、回访任务分配渠道等。 (参照附录A 常见客户回访类型及操作要求)
回访时间	年/月/日
回访类型	<input type="checkbox"/> 新开户回访 <input type="checkbox"/> 适当性回访 <input type="checkbox"/> 异常情形回访 <input type="checkbox"/> 其他_____
回访方式	<input type="checkbox"/> 人工电话 <input type="checkbox"/> 智能语音 <input type="checkbox"/> 问卷 <input type="checkbox"/> 即时通讯 <input type="checkbox"/> 面见
回访客户范围	
回访实施部门	
回访人员	
回访风险提示	<input type="checkbox"/> 是 <input type="checkbox"/> 否

备注：以上要素宜在回访系统内实现。

附录 E

(资料性)

客户回访话术要点示例

E.1 客户回访开头语

示例 1:

您好! 我是 XXX 证券 XXX 部工作人员, 工号是 XXX。请问您是 XXX 先生(女士)吗?

(客户回答: 是本人) 今天打电话是想就** (回访业务类型) 对您做一个简单的回访, 耽误您两分钟, 请问您现在方便吗?

a) (客户回答: 方便) 谢谢!

b) (客户回答: 不方便) 很抱歉, 打扰了! 请问您大概什么时间有空?

1) (客户提供方便时间) 谢谢! 到时候我们再联系您。(记录客户方便时间, 在客户方便时再联系重新进行回访)

2) (客户暂时不确定或暂时无法提供) 我们改日再联系您。祝您愉快! 再见!

3) (客户明确拒绝再联系) 很抱歉, 打扰了! 祝您愉快! 再见!

示例 2:

您好! 我是**证券**部工作人员, 我的工号是**。请问您是***先生(女士)吗?

(客户回答: 非本人) 很抱歉, 打扰了! 请问您知道***先生(女士)的联系方式吗?

a) (客户回答: 知道) 方便提供一下他(她)的联系方式吗?

1) (客户愿意提供) 谢谢! (记录客户联系方式, 稍后联系客户重新开始回访)

2) (客户不愿提供) 打扰了! 祝您愉快! 再见!

b) (客户回答: 不知道) 很抱歉, 打扰了! 祝您愉快! 再见!

E.2 回访场景话术

E.2.1 新开户回访话术

a) 请问开户是您本人真实意愿吗?

b) 请问您是否已阅读并充分理解开户协议相关条款?

c) 温馨提示: 请您务必妥善保管好自己的账户和密码, 切勿交由他人使用或操作。

E.2.2 异常情形回访话术

a) 请问账户是您本人操作吗?

b) 我司发现您的(账户使用、资金划转、证券交易等)存在异常情形,在此郑重提醒:请您务必妥善保管好自己的账户和密码,切勿交由他人使用或操作,也不得借用他人账户使用。(账户使用、资金划转、证券交易等)必须严格遵守相关法律法规。对于违规行为,我司有权对(账户使用、资金划转、证券交易等)进行限制,并上报监管机构。

E.2.3 适当性回访话术

a) 请问账户是您本人操作吗?

b) 请问是您本人自愿申请并亲自办理(开通交易权限/购买金融产品/签约投顾服务等)的吗?

c) 请问您是否自愿并按规定签署了相关协议及问卷?

d) 请问您是否已知晓所购买产品或接受服务的业务规则;请问您是否已阅读并充分理解产品或服务相关风险揭示书等文件内容;请问您是否已知晓自己的风险承受能力等级、购买的产品或者接受服务的风险等级以及适当性匹配意见;是否知晓承担的费用以及可能产生的投资损失?

e) 按规定,我公司工作人员在产品销售或提供服务的过程中,不允许发生违规代客操作或接受全权委托等损害您合法权益的行为。请问我司工作人员是否存在上述违规行为?

f) 温馨提示:您账户的XXX信息(常用联系方式、家庭住址、身份证有效期等基本信息,但应注意个人信息保护)近期若有变更,可及时在我司交易软件等办理更新。(证券公司回访人员涉及第三方外包人员、劳务派遣人员、营业部人员等,考虑到客户信息安全,宜慎重由回访人员进行知悉并核对)。

g) 根据客户情况适当增加《证券经营机构投资者适当性管理实施指引(试行)》第二十三条、《私募投资基金募集行为管理办法》第三十条和《基金募集机构投资者适当性管理实施指引(试行)》第十三条内容。

E.2.4 经纪人执业情况回访

a) 请问您对XXX的服务满意吗?

b) 按规定,我公司工作人员在产品销售或提供服务的过程中,不允许发生违规代客操作或接受全权委托等损害您合法权益的行为。请问我司工作人员是否存在上述违规行为?

E.2.5 拟离职人员名下客户回访

a) 您的客户经理/服务人员XXX岗位调整,请问您对XXX的服务满意吗?

b) 按规定,我公司工作人员在产品销售或提供服务的过程中,不允许发生违规代客操作或接受全权委托等损害您合法权益的行为。请问我司工作人员是否存在上述违规行为?

c) 我们已经为您安排了新的客户经理/服务人员XXX，他的联系方式是XXX，如有问题可直接与其联系。

E.2.6 被投诉人员名下客户回访

a) 请问您对 XXX 的服务满意吗?

b) 按规定，我公司工作人员在产品销售或提供服务的过程中，不允许发生违规代客操作或接受全权委托等损害您合法权益的行为。请问我司工作人员是否存在上述违规行为?

E.2.7 投诉处理完结回访

a) 根据我们工作人员反馈，对于X年X月X日您投诉的关于XXX事项，已经与您进行了沟通并达成了和解，请问是否还存在未了事项?

b) 请问您对我公司的服务满意吗?

E.3 客户回访结束语

非常感谢您的支持! 今后若有问题或建议，欢迎拨打咨询电话***，我们将竭诚为您服务。祝您投资愉快! 再见!

附录 F

(规范性)

客户回访未触达情形及处理

表 F.1 客户回访未触达情形及处理

序号	回访方式	场景	系统临时登记状态	处理方式	系统最终登记状态
1	人工电话回访或智能语音回访	拒绝回访	未完成: 拒绝回访	1、建议系统触发短信告知客户回访事项; 2、系统保存通话记录; 3、将系统登记状态修改为“已完成: 拒绝回访”, 不再拨打, 完成回访。	已完成: 拒绝回访
2		电话占线	未完成: 电话占线	1、建议每次间隔 10 分钟以上再次拨打; 2、连续拨打不少于 2-3 次, 且最后一次拨打与第一次拨打时间间隔超过 2 小时; 3、如接通后, 正常完成回访, 则将系统登记状态修改为“已完成: 已回访”, 不再拨打, 完成回访; 如接通后, 客户挂断或拒绝回访, 则按本表对应场景处理; 4、如均提示占线, 则系统触发短信告知客户回访事项并保存每次拨打记录后, 可以将系统登记状态修改为“已完成: 电话占线”, 不再拨打, 完成回访。 5、	已完成: 已回访 或 已完成: 电话占线
3		客户挂断	未完成: 客户挂断	1、建议每次间隔 1 小时以上再次拨打; 2、连续拨打 2-3 次, 且最后一次拨打与第一次拨打时间间隔超过 4 小时; 3、如接通后, 正常完成回访, 则将系统登记状态修改为“已完成: 已回访”, 不再拨打, 完成回访; 如接通后, 客户挂断或拒绝回访, 则按本表对应场景处理; 4、如均被客户挂断, 则系统触发短信告知客户回访事项并保存每次拨打记录后, 可以将系统登记状态修改为“已完成: 客户挂断”, 不再拨打, 完成回访。	已完成: 已回访 或 已完成: 客户挂断
4		无人应答	未完成: 无人应答	1、建议每次间隔 1 小时以上再次拨打; 2、连续拨打不少于 2-3 次, 且最后一次拨打与第一次拨打时间间隔超过 4 小时; 3、如接通后, 正常完成回访, 则将系统登记状态修改为“已完成: 已回访”, 不再拨打, 完成回访; 如接通后, 客户挂断或拒绝回访, 则按本表对应场景处理; 4、如均无人应答, 则系统触发短信告知客户回访事项并保存每次拨打记录后, 可以将系统登记状态修改为“已完成: 无人应答”, 不再拨打, 完成回访。	已完成: 已回访 或 已完成: 无人应答

客户回访未触达情形及处理（续）

序号	回访方式	场景	系统临时登记状态	处理方式	系统最终登记状态
5	人工电话回访或智能语音回访	无法接通	未完成: 无法接通	1、建议每次间隔 1 小时以上再次拨打； 2、连续拨打不少于 2-3 次，且最后一次拨打与第一次拨打时间间隔超过 24 小时； 3、如接通后，正常完成回访，则将系统登记状态修改为“已完成: 已回访”，不再拨打，完成回访；如接通后，客户挂断或拒绝回访，则按本表对应场景处理； 4、如均无法接通，则系统触发短信告知客户回访事项并保存每次拨打记录后，可以将系统登记状态修改为“已完成:无法接通”，不再拨打，完成回访。	已完成: 已回访 或 已完成: 无法接通
6		关机	未完成: 关机	1、建议每次间隔 1 小时以上再次拨打； 2、连续拨打不少于 2-3 次，且最后一次拨打与第一次拨打时间间隔超过 24 小时； 3、如接通后，正常完成回访，则将系统登记状态修改为“已完成: 已回访”，不再拨打，完成回访；如接通后，客户挂断或拒绝回访，则按本表对应场景处理； 4、如均提示关机，则系统触发短信告知客户回访事项并保存每次拨打记录后，可以将系统登记状态修改为“已完成:关机”，不再拨打，完成回访。	已完成: 已回访 或 已完成: 关机
7		停机	未完成: 停机	1、建议每次间隔 24 小时以上再次拨打； 2、连续拨打不少于 2-3 次； 3、如接通后，正常完成回访，则将系统登记状态修改为“已完成: 已回访”，不再拨打，完成回访；如接通后，客户挂断或拒绝回访，则按本表对应场景处理； 4、如均提示停机，则通过客户本人留存的即时通讯工具、电子邮箱、其他电话等联系方式中的任意一种告知客户回访事项，并提醒账户本人是否需要更新联系方式。系统留存相关记录后，可以将系统登记状态修改为“已完成: 停机”，不再拨打，完成回访。	已完成: 已回访 或 已完成: 停机
8		空号	未完成: 空号	1、建议通过客户本人留存的即时通讯工具、电子邮箱、其他电话等联系方式中的任意一种告知客户回访事项； 2、提醒账户本人尽快更新联系方式； 3、系统留存相关记录后，可以将系统登记状态修改为“已完成:空号”，不再拨打，完成回访。	已完成: 空号

客户回访未触达情形及处理（续）

序号	回访方式	场景	系统临时登记状态	处理方式	系统最终登记状态
9	人工电话回访或智能语音回访	错号	未完成：错号	1、建议通过客户本人留存的即时通讯工具、电子邮箱、其他电话等联系方式中的任意一种告知客户回访事项； 2、提醒客户尽快更新联系方式； 3、系统留存相关记录后，可以将系统登记状态修改为“已完成：错号”，不再拨打，完成回访。	已完成：错号
10	面见回访或问卷回访	拒绝回访	未完成：拒绝回访	1、建议转为人工电话回访或智能语音回访方式进行； 2、如通过人工电话回访或智能语音回访，能正常完成回访，则将系统登记状态修改为“已完成：已回访”，完成回访；如回访过程中出现未触达情形，则按本表对应场景处理。	已完成：已回访或已完成：拒绝回访
<p>执行回访任务登记完成代表已执行相关操作，不表示整体回访工作完成，回访未触达情况应持续关注：</p> <p>1、如回访为必要业务流程，宜即时暂停相关业务或启动应急预案；</p> <p>2、如为适当性回访，宜在年度内继续使用短信、邮件、APP 弹窗等方式进行问卷回访，宜采取问答及选项方式；</p> <p>3、在同批次电话回访中，电话未接通、接通后无法确认身份且客户未拒绝的情况下，对于涉及高风险（R5）产品或服务的客户回访拨打次数不宜低于 3 次，对于其他类型回访拨打次数不宜低于 2 次。</p>					

附录 G

(资料性)

客户回访分析示例

一、客户回访情况总述

(一) 本次客户回访的背景、目的、执行时间等

(二) 客户回访执行情况和结果概述

.....

二、客户回访结果总结分析

(一) 客户回访相关数据统计(回访客户数、回访完成率、各问题答案的回答客户数及占比等)

(二) 客户回访中出现的异常情况、接到的客户投诉、发现的不合规情形等处理情况

(三) 客户提出的意见与建议

(四) 对各项回访数据的含义、成因、影响进行分析

(五) 客户回访效果是否达到预期,未达预期的原因分析

.....

三、客户回访结果应用

(一) 对于客户提出的意见、建议的采纳与应用计划

(二) 针对回访中发现的问题,下一步的改进措施与安排

(三) 客户回访工作的持续优化方案

.....

附录 H

(资料性)

客户回访工作年度总结报告示例

20XX 年按照年初工作计划，有序推进客户回访工作，增加智能科技在客户回访工作中的应用，同时落实适当性回访相关工作要求，认真总结分析客户回访情况，并收集、整理、汇总和及时反馈客户回访工作相关建议。现将年度客户回访工作进展及下一年度回访工作计划汇报如下。

一、20XX 年度客户回访工作概述

(一) 20XX 年度客户回访整体情况

20XX 年客户回访共完成 XXX，全年智能外呼回访数 XXX，电子回访问卷 XXX，人工回访数 XXX，智能回访占比回访任务数的 XXX。

(二) 20XX 年度客户回访详细数据

主要客户回访类型完成数据详见下表：

适当性回访						新开户回访			
人工回访数	智能外呼 回访数	电子问卷 回访数	任务总数	回访完成 总数	回访完成率	参考前列			

(三) 客户回访工作近三年主要数据

项目	时间	20XX 年	20XX 年	20XX 年
人工回访任外呼总数				
外呼接通数				
接通率				
智能机器人外呼数				
外呼接通数				
接通率				

电子回访问卷任务完成数			
.....			

二、20XX 年度客户回访重点工作内容

- (一) 加强人工回访合规检查
- (二) 增加智能回访应用场景

.....

三、分支机构关于客户回访工作的建议

.....

四、下一年度客户回访工作计划

- (一) 进一步加强客户回访质检与管理工作
- (二) 增加智能科技在回访工作中的应用
- (三) 持续做好智能外呼系统优化工作

.....

五、建议客户回访工作总结中关注的问题

(一) 客户回访对于落实适当性工作的效用，如通过回访发现的展业不合规现象、工作人员管理问题的分析；

(二) 客户回访对于证券公司改进产品和系统的效用，如通过回访获得客户对于公司产品或交易软件的优化建议、客户需求偏好的分析；

(三) 客户回访对于证券公司提升客户服务体验的效用，如通过回访收集客户对证券公司服务的建议和需求、服务升级产生的具体效果的分析；

(四) 客户回访对于证券公司把握整体运营情况的效用，如通过回访了解公司制度流程的合理性、为各项经营决策提供参考依据的分析，工作人员培训方向的建议。

证券业商用密码应用上线指南

T/SAC 003—2024

（经协会第七届常务理事会第二十一次会议审议通过，2024年6月21日发布实施）

（中证协发〔2024〕118号）

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件起草单位：中国银河证券股份有限公司、广发证券股份有限公司、兴业证券股份有限公司。

本文件主要起草人：罗黎明、华阳、魏自恩、梅养真、魏振宇、鹿群、杜瑞罡、谈加虎、王金刚、樊丹、王栩。

1 范围

本文件给出了证券业机构开展密码应用上线的要求。本文件适用于证券业核心机构、经营机构等相关信息系统进行商用密码应用改造后的上线工作。

2 规范性引用文件

下列文件对于本指南的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本指南。凡是不注日期的引用文件，其最新版本适用于本指南。

《中华人民共和国密码法》

GB/T 39786—2021 《信息安全技术 信息系统密码应用基本要求》

GB/T 22239—2019 《信息安全技术网络安全等级保护基本要求》

GB/T 37092—2018 《信息安全技术 密码模块安全要求》

JR/T 0060—2021 《证券期货业网络安全等级保护基本要求》

JR/T 0191—2020 《证券期货业软件测试指南 软件安全测试》

JR/T 0099—2012 《证券期货业信息系统运维管理规范》

GM/T 0115—2021 《信息系统密码应用测评要求》

GM/T 0116—2021 《信息系统密码应用测评过程指南》

GM/T 0039—2015 《密码模块安全检测要求》

GM/T 0028—2014 《密码模块安全要求》

GM/T 0024—2014 《SSL VPN 技术规范》

GM/T 0015—2012 《基于SM2密码算法的数字证书格式规范》

GM/T 0009—2012 《SM2密码算法使用规范》

GM/T 0004—2012 《SM3密码杂凑算法》

GM/T 0003—2012 《SM2椭圆曲线公钥密码算法》

GM/T 0002—2012 《SM4分组密码算法》

3 术语和定义

下述术语和定义适用于本文件。

3.1

密钥 key

控制密码算法运算的关键信息或参数。

3.2

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等密钥生存周期的管理。

4 基本要求

4.1 基本原则

确保系统正常运行的原则。证券业信息系统商用密码应用改造工作涉及面广、衔接性强、实时性要求高，实施操作必须要以确保系统和业务的正常运行为前提。

坚持“谨慎试点、新老并行、业务不中断”的原则，并制定相关业务应用推广和应急回退等方案。

4.2 组织保障

为保障商用密码应用上线正常运行，应成立专门的商用密码应用领导小组（以下简称“领导小组”）和商用密码应用工作小组（以下简称“工作小组”），明确相应职责和任务分工，建立定期汇报交流的工作机制。

领导小组在系统上线全过程中应履行全局协调、整体指挥的职责。对系统上线涉及到所有业务做到统一调度，发现问题统一排查、解决。领导小组负责人由首席信息官或分管信息技术的公司高级管理人员承担。

工作小组负责商用密码应用项目的技术方案论证、设计、系统建设、运维管理和技术保障，以及对相关制度、业务流程的合规性审定等工作。同时要对业务人员开展客户咨询、应急情况客户响应等培训。工作小组至少包含信息技术人员、相关业务人员、客服人员、法律合规人员、风险管理人員等。工作小组组织相关人员持续开展商用密码相关知识及标准规范学习培训，落实系统上线后的运维和管理保障工作。

4.3 经费保障

为保障项目顺利实施及上线后运维、扩容等预备必要的经费，应为商用密码应用改造预留充足的预算。

4.4 管理制度要求

按照GB/T 39786相关要求，制定密码应用、密码安全管理制度及安全操作规范。包括但不限于：

- 采用密码技术提供物理和环境、网络和通信、设备和计算以及应用和数据的安全；
- 人员管理制度，至少包含密码安全人员管理制度和密码安全人员岗位划分制度等；
- 密钥管理制度，至少包含密钥管理和口令管理等；
- 建设运行制度，至少包含密码应用方案和密码安全性策略等；
- 应急处置制度，至少包括应急处理和报告制度。

4.5 产品资质要求

应使用国家密码主管部门认证核准的密码技术和产品，采用的密码服务符合国家密码主管部门的要求。

5 运行保障

为保障商用密码应用上线后安全、高效和稳定运行，上线前对其存在的风险点进行分析、分类，并对风险点做好应对策略，便于在发生安全事件时可以根据应对策略快速响应。

5.1 密码应用安全性评估

网络安全等级保护二级以下信息系统商用密码应用在正式上线前，可聘请商用密码主管部门认可的安全性评估机构开展密码应用安全性评估，并达到符合及以上要求。

网络安全等级保护二级信息系统商用密码应用在正式上线前，宜聘请商用密码主管部门认可的安全性评估机构开展密码应用安全性评估，并达到符合及以上要求。

网络安全等级保护三级及以上信息系统商用密码应用在正式上线前,应聘请商用密码主管部门认可的安全性评估机构开展密码应用安全性评估, 并达到符合及以上要求。

5.2 上线后监控和质量保证措施

商用密码应用上线工作完成后, 应将涉及的服务器、软件、网络设备以及专用设备纳入监控和报警体系, 并且将应用性能、应用日志、系统容量、关键业务场景指标等纳入监控和报警体系, 定期进行分析, 确保相关指标在预期范围内。

6 系统上线

商用密码应用上线时, 应制定完整的上线方案, 内容包括但不限于测试方案、上线策略、部署方案、上线实施和回退方案, 保障商用密码应用上线后安全、高效和稳定运行。

6.1 系统测试

商用密码应用改造上线或重要升级前进行严格的测试, 测试内容包括但不限于功能测试、压力测试、安全测试和场景对比测试。

6.1.1 功能测试

工作小组制定详细的商用密码应用测试方案, 对各系统模块以及系统整体进行测试。测试模块包括但不限于商用密码相关的协同签名模块、应用安全网关、数字证书、密码模块。测试场景包括但不限于证书申请、更新、注销, 以及应用安全网关流程、协同签名流程、业务全链路场景。

6.1.2 压力测试

根据系统技术特点和承载业务类型, 设定测试场景, 制定测试方案, 从系统处理能力、业务响应时间等方面设置测试指标, 有序组织测试工作。信息系统的性能容量、响应时间和系统资源利用率等应控制在合理范围内并满足业务开展需要。测试完成后形成压力测试报告存档备查。

需重点关注以下两类指标:

- 系统性能指标: 包括吞吐量、并发数和响应时间等, 指标将从单位时间、特定长度时间、数据从源端到目标端流转时间和数据请求发起到服务完成时间等不同角度反映被测系统处理数据的效率和能力;
- 资源性能指标: 包括服务器主要硬件资源(CPU、内存、磁盘等)的利用率和操作系统软件资源(进程数、网络连接数量、文件句柄占用数量等)的使用情况。

6.1.3 安全测试

在上线前针对商用密码应用编制详细的安全测试计划和测试用例, 执行相关测试并确保测试结果符合要求。

测试内容包括但不限于:

- 安全功能检查: 通过人工检查、审核的方式对软件开发过程中涉及的安全策略、进度、技术决策(如开发模型等)进行安全功能检查;
- 代码安全测试: 通过对软件源代码进行安全扫描和审计, 排除代码中的漏洞及恶意代码(如外购类软件系统, 可由开发商提供代码安全测试报告);
- 漏洞扫描: 通过扫描等手段对指定系统进行检测, 发现可利用漏洞的一种安全检测行为;
- 渗透测试: 以攻击者视角进行的黑盒测试, 从而获得对应用系统的安全评价;

- 模糊测试：以向目标系统提供非预期输入的方式，提高应用程序的健壮性及抵御意外输入时的安全性。

测试范围包含但不限于多种安全类型：身份认证安全、口令安全、访问权限安全、会话管理安全、通信安全、业务逻辑安全、输入数据安全、存储数据安全、提示信息安全、个人信息保护安全、日志数据安全、算法安全、安全审计、配置安全、拒绝服务、源代码数据安全、架构安全、运行环境安全、卸载安全、组件安全、权限安全、第三方库安全（若涉及）等。

6.1.4 场景对比测试

对比改造前后的使用体验、延迟变化，分析和评估对用户应用操作和实际体验的影响。

6.2 上线策略

可采用逐步替换或逐步切换流量的方式，做好系统开关控制方案的设计、评审和验证，实现通过系统参数控制功能或流量切换。提供紧急情况下通过系统参数进行的回退机制，并及时收集用户反馈。

6.3 上线方案

系统上线前审慎地根据系统部署方案，制定详尽的系统上线方案，经由工作小组评审通过，并由领导小组审批。

上线方案包括上线相关参与方、具体参与人员、合理的上线时间、应用备份工作、数据备份工作、前序工作检查步骤、上线详细操作步骤、检验步骤等。

6.4 上线实施

系统上线时组织好具体参与人员，按照上线方案的操作细节步骤实施操作，并且做好相关的验证工作。上线成功后，工作小组向领导小组进行报告，并启动上线后的监控工作和质量保证措施。

系统改造上线前，制定上线回退方案，保障商用密码应用上线过程中出现异常时，可回退到改造前系统状态。回退管理主要内容包括但不限于：

- 回退方案：回退方案包括回退工作的具体操作步骤、后续检验步骤等。在上线前进行相应的系统回退演练，确保方案切实可行。
- 回退触发：针对上线过程中可能会遇到的各种异常情况，制定相应的指标，在触发异常并且已达到相关指标时，工作小组启动回退的决策流程，并报告领导小组。经由领导小组决策后是否继续上线工作还是启动回退方案。
- 回退执行：如果领导小组决策启动回退方案，工作小组执行系统的回退工作，终止本次商用密码应用上线工作，系统回退到上线前的系统状态。

7 应急管理

7.1 应急准备

- 建立健全软硬件应急知识库，发生故障时及时向工作小组上报，工作小组协调技术人员进行事件评估与处置；
- 准备充足的重要设备备品配件（包括但不限于密钥管理系统、SSL 接入网关等），并进行定期评估，检测和维护；
- 对客服人员统一培训，所有客服人员熟练掌握应对投资者咨询、投诉等非现场服务处理流程；
- 制定应急演练场景，定期进行应急演练，重点演练出现过的异常情况。

7.2 应急处理

- 查找知识库信息，确认此软硬件事件是否有记录，若有记录则依据知识库现场恢复后验证有效性并上报事件信息；
- 若知识库无记录此软硬件事件，需联系厂商人员提供远程技术支持，并联系厂商技术人员分析事故影响，厂商提供事件恢复方案，厂商需依据方案的时效性给出相应的替换方案，技术人员验证方案的有效性，上报事件问题和现场恢复状况，将恢复方案记录知识库；
- 厂商无法远程恢复，需立刻上报工作小组并联系厂商负责人派遣专业人员到现场提供技术支持，联系厂商给出现状描述，并提供确保系统服务稳定的解决方案，事件恢复后厂商需提交报告说明情况，验证方案的有效性，将事件描述和恢复记录知识库；
- 任何软硬件事件恢复现场后需持续监控修复后的软硬件运行状况，并按有关规定报告事件情况，对可能构成特别重大、重大网络安全事件的保持持续报告，直至系统恢复正常运行，报告要素应完备、及时、准确，不得迟报、漏报、谎报或瞒报；
- 由客服中心统一处理投资者咨询和投诉。

7.3 调查处理

调查处理过程中，应对工作底稿进行有效保护，扩展分析相关问题及研究制定可行对应的解决方案，可适时组织外部专家进行会审，尽量避免相关问题再次发生。同时，工作小组根据事件响应和处理情况编制报告并上报领导小组。

7.4 典型应急场景

本指南收录应急场景典型案例参见附录A。

附 录 A
(资 料 性)
应急场景典型示例

A.1 SSL接入网关故障

故障描述：SSL接入网关设备无法正常提供服务，可能造成的影响有：客户端无法与SSL接入网关建立连接，客户端的业务请求无法通过SSL接入网关转发至后台系统，导致业务功能无法完成。

处理建议：接入网关采用多点部署模式，部分接入网关设备无法正常提供服务，客户端会自动切换到其他接入网关；若所有接入网关故障，可采用相关旁路机制绕过SSL接入网关，让客户端系统请求正常发送至后台应用服务器，保证交易的连续性。

A.2 数字证书认证系统故障

故障描述：CA无法正常提供服务，可能造成的影响有：客户端无法申请签名证书和加密证书。

处理建议：CA服务供应商提供备份线路，当主线路无法提供服务时，自动切换到备份线路，继续提供服务。在CA无法正常提供的情况下，启用商用密码SSL单向认证或旁路机制。

A.3 密钥管理系统（KMS）故障

故障描述：密钥管理系统（KMS）无法正常提供服务，可能造成的影响有：服务端产生的协同签名密钥分量无法存储到密钥管理系统，导致SSL接入网关不能提供协同签名密钥生成服务；未申请密钥的客户端将无法使用协同签名服务，无法完成商用密码SSL双向认证连接。已申请密钥的客户端由于无法从KMS中获取用户服务端密钥分量参数，无法实现协同签名运算，导致商用密码SSL双向认证失败。

处理建议：密钥管理系统支持主备部署模式，在主节点异常的情况下，支持服务切换到备份节点，继续提供服务。在主备密钥管理系统均无法提供的情况下，启用商用密码SSL单向认证或旁路机制。

证券业区块链电子数据存证应用规范

T/SAC 004—2024

（经协会第七届常务理事会第八次会议审议通过，2024年7月29日发布实施）

（中证协发〔2024〕163号）

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国证券业协会归口。

本文件起草单位：国泰君安证券股份有限公司、海通证券股份有限公司、东吴证券股份有限公司、兴业证券股份有限公司。

本文件主要起草人：杨晨旭、詹婷婷、任荣、唐淑艳、石良生、吴鑫涛、应原、杨琦路、张子华、付益明。

引 言

随着金融科技快速发展，区块链技术在金融行业的应用场景逐渐增多，其中区块链存证技术越来越成熟并被行业机构应用在合同签署、版权保护等领域。然而目前证券行业缺乏统一的规范性指导文件，相关标准内容存在一定的局限性且缺乏对行业的指导意义，存证业务面临着数据格式不一致、技术要求不统一、存证流程不完整等问题。鉴于此，进行行业标准化研究，夯实区块链技术标准化发展基础，提升区块链技术标准化研究水平，推进证券行业区块链技术应用标准体系建立至关重要。通过制定证券行业团体标准对存证流程加以规范，对业务场景统一标准，以建设规范的区块链存证应用环境，从而推动区块链存证业务在行业的广泛应用，为加速推进行业数字化高质量转型、有效引领行业金融科技高速发展、有力保障金融科技在行业内的行稳致远贡献力量。

1 范围

本文件规定了基于区块链技术的电子数据存证应用的术语和定义、存证应用区块链技术要求、区块链存证平台、区块链存证过程、区块链存证模型。

本文件适用于证券业基于区块链技术的电子数据存证应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20520—2006 信息技术安全 公钥基础设施 时间戳规范
GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 25069—2022 信息安全技术 术语
GB/T 35273—2020 信息安全技术 个人信息安全规范
GB/T 43572—2023 区块链和分布式记账技术 术语
GB/T 43580—2023 区块链和分布式记账技术存证通用服务指南
GM/T 0024—2014 SSL VPN技术规范
GM/T 0111—2021 区块链密码应用技术要求
JR/T 0184—2020 金融分布式账本技术安全规范
SF/Z JD0400001—2014 电子数据司法鉴定通用实施规范

3 术语和定义

GB/T 20520—2006、GB/T 25069—2022、GB/T 43572—2023、GB/T 43580—2023、JR/T 0184—2020、SF/Z JD0400001—2014 界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

使用密码链接将共识确认的区块按顺序追加形成的分布式账本。

[来源：GB/T 43572—2023，3.6]

3.2

联盟链 consortium blockchain

由一组利益相关的参与者管理和使用，仅有授权节点可接入，接入节点可按规则参与共识和读写数据的区块链部署模型。

3.3

电子数据 digital evidence

以电子手段生成、发送、接收或存储的信息。

[来源：GB/T 43580—2023，3.2]

3.4

存证 preserve evidence

通过技术手段对电子数据进行保存和验证的行为，保证其完整性和真实性并可追溯。

[来源：GB/T 43580—2023，3.3]

3.5

区块链存证 blockchain preservation

基于区块链技术实现多节点共识的电子数据存证。

[来源：GB/T 43580—2023, 3.4]

3.6

电子数据存证平台 digital evidence preservation platform

可实现电子数据存证相关功能的平台或系统。

3.7

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。

[来源：GB/T 25069—2022, 3.576]

3.8

散列值 hash value

为了标识电子数据的唯一性或完整性而通过特定的散列算法把任意长度的输入数据变换成的固定长度的输出值。散列值又称哈希值或校验码，常用散列算法包括 SM3、MD5 和 SHA256 等。

[来源：SF/Z JD0400001—2014, 3.8]

3.9

共识机制 consensus mechanism

使节点见达成共识的规则和程序。

[来源：GB/T 43572—2023, 3.12]

3.10

默克尔树 merkle tree

区块链的重要数据结构，其本质由节点组成的二叉树，其中每个叶节点代表一段数据，每个非叶（内部）节点代表其子节点的加密哈希，其作用是快速归纳和校验区块数据的存在性和完整性。

3.11

分布式账本技术 distributed ledger technology

实现分布式账本的技术的集合，是密码算法、共识机制、点对点通讯协议、分布式存储等多种核心技术体系高度融合形成的一种分布式基础架构与计算范式。

[来源：JR/T 0184—2020, 3.19]

3.12

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

[来源：GB/T 43572—2023, 3.72]

3.13

加密 encipherment encryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 25069—2022, 3.278]

3.14

可信时间 trusted time

准确的、值得信赖的当前时间值，这个时间值的来源应是高度权威的。

[来源：GB/T 20520—2006, 3.2]

3.15

时间戳 time stamp

对时间和其他待签名数据进行签名得到的，用于表明数据时间属性的数据。

[来源：GB/T 25069—2022，3.541]

3.16**去标识化 de-identification**

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

[来源：GB/T 35273—2020，3.15]

3.17**匿名化 anonymization**

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

[来源：GB/T 35273—2020，3.14]

3.18**数据完整性 data integrity**

数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变。

[来源：GB/T 25069—2022，3.574]

3.19**保密性 confidentiality**

信息对未授权的个人、实体或过程不可用或不泄露的性质。

[来源：GB/T 25069—2022，3.41]

3.20**机密性 confidentiality**

采用密码技术保证信息不泄露的性质。

[来源：GB/T 25069—2022，3.259]

3.21**单点数据 single-point data**

静态、相对恒定的数据序列。

3.22**链式数据 chain data**

一组存在逻辑、勾稽关系的数据序列。

3.23**流式数据 streaming data**

一组顺序、大量、快速、连续到达的数据序列。一般情况下，流数据可被视为一个随时间延续而无限增长的动态数据集合。

3.24**业务数据 business data**

存证业务系统运行产生的数据。

3.25**存证数据 preservation data**

写入区块链的数据，它可以是一个字符串、一个文件的散列值等形式，用于表示文本、文件等电子数据，确保这些数据在区块链上得到安全存储和验证，以作为有效的法律或商业证据。

4 存证应用区块链技术要求

4.1 账本技术

4.1.1 账本结构

- a) 账本结构由区块头和区块体组成。
- b) 账本结构中区块头应包括上一个区块 ID、版本号、时间戳、难度、默克尔树根等信息。
- c) 账本结构中区块体应包括所有交易信息以及所有交易信息的默克尔树信息。
- d) 账本结构应具备数据防篡改性以及校验数据完整性的功能。

4.1.2 账本数据管理

- a) 账本数据应能正确查询到当前状态信息。
- b) 账本数据应能正确查询到历史更新记录及交易详情。
- c) 账本数据应对数据来源和变更的操作者身份进行追溯。
- d) 账本数据应能正确查询到状态变更记录所在区块文件的唯一标识和时间戳。
- e) 账本数据应保证节点从异常状态恢复后，仍能够正确完成历史数据溯源。

4.1.3 数据同步

- a) 账本数据同步应保证需同步数据的节点与源节点的数据一致。
- b) 账本数据同步应保证新增节点在同步所需历史数据之后与其他节点数据一致。
- c) 账本数据同步应保证单节点同步增量数据后与其他节点的数据一致，且支持动态切换源数据节点。
- d) 账本数据同步应确保在多节点网络中，节点同步历史数据的一致性和时效性，避免同步错乱。
- e) 账本数据同步应确保账本状态数据可重建，可根据交易序列重建账本状态数据。
- f) 账本数据同步应具备断电、重启、网络波动等异常情况下的断点续传能力。
- g) 账本数据同步应确保节点可通过数据同步纠正本节点的数据异常问题，保证整个网络数据的一致性。

4.1.4 数据归档

- a) 账本应提供数据归档功能，包括但不限于磁盘文件数据、数据库存储数据，存储介质应具备高可靠性。
- b) 归档数据与节点本地存储的数据应完整，不缺失账本数据。
- c) 不同节点归档的数据应存放在不同的存储设备中，防止出现集中数据丢失。
- d) 数据归档应支持用户设置归档数据范围，包括但不限于根据时间、区块序号等范围限定。
- e) 节点在数据归档过程中，应能够继续提供系统服务，可暂时停止历史状态查询功能。
- f) 节点数据归档完成后，应支持对归档数据进行历史状态查询。
- g) 节点从断电、重启、网络波动等异常场景恢复后，应可继续完成数据归档操作。
- h) 数据归档应支持归档数据恢复还原。

4.1.5 数据扩容

- a) 账本应提供存储的扩容技术和方案。
- b) 扩容前，应做好数据归档操作，确保异常情况下的数据可恢复性。
- c) 扩容过程中，应确保用户对账本的操作不会导致节点账本数据文件异常，扩容方案应具备平滑伸缩能力，保障在线系统不必中断运行。
- d) 扩容完成后，节点应能够正常运行、性能稳定，应保证扩容前后数据一致。

4.1.6 数据跨链功能

- a) 账本应建立跨链交易机制，可采用公证人机制、侧链/中继、哈希锁定、分布式私钥控制等实现方式。
- b) 跨链交易过程应保证状态数据修改可正确更新到账本中。
- c) 跨链交易应满足事务完整性、一致性。

- d) 跨链功能应支持基于当前链的账本状态单独验证跨链交易。
- e) 节点从断电、重启、网络波动等异常场景恢复后，应可继续完成被中断的跨链交易。

4.2 共识协议

4.2.1 共识算法

- a) 系统基于声明的所有不同的共识算法，均能实现所有节点达成共识，系统正常运行。
- b) 联盟链可选用的共识机制包括基于投票的共识机制、基于公信力节点的共识机制等。
- c) 共识算法应限定每一次共识出块的最长时间，保证既定的共识出块频率，确保共识机制的可用性。
- d) 共识机制应支持在节点在线、节点离线、网络规模调整等情况下，可切换共识机制能达成全网新的共识。

4.2.2 共识协议一致性

- a) 共识协议应保证每个节点更新账本状态写操作的一致性。
- b) 共识协议应保证每个节点账本的最终状态一致性。
- c) 共识协议应保证节点从断电、重启、网络波动等异常场景恢复后，所有节点交易执行的结果应保持一致。
- d) 共识协议应保证同样的交易在同一或不同节点多次运行，共识结果一致。

4.2.3 共识协议可靠性

- a) 共识协议的安全性要求应符合 GM/T 0111—2021 中第 7.7 款规定。
- b) 共识协议应具备可靠的身份鉴别机制，对可参与共识的节点进行严格准入。
- c) 共识协议应具备一定的抗攻击和识别恶意节点的能力。
- d) 共识协议应保证篡改节点数与故障节点数之和小于最大阈值时可正常达成全网共识。
- e) 共识协议应保证节点从异常场景恢复后数据正常恢复、数据不丢失及正常参与共识流程。

4.2.4 共识协议可拓展性

- a) 共识协议支持动态或静态增加节点。
- b) 共识协议支持动态或静态删除节点。

4.3 智能合约

4.3.1 智能合约正确性

智能合约应保证对其的执行调用能获得与参数输入相对应的正确结果。

4.3.2 智能合约一致性

- a) 智能合约应保证在参数、环境等外部要素一致情况下，在各节点上的执行结果相同。
- b) 智能合约执行时，各节点数据应互不干扰。

4.3.3 智能合约可靠性

- a) 智能合约的安全性要求应符合 GM/T 0111—2021 中第 7.8 款规定。
- b) 智能合约应保证执行的原子性，调用智能合约执行异常操作能够正常回滚，调用智能合约执行有效操作，各节点执行结果准确一致。
- c) 智能合约应保证可向下兼容，在系统环境升级迭代后仍可正常运行。
- d) 智能合约应支持冻结、解冻、销毁、升级和版本管理，以保证智能合约的全生命周期可控。

4.3.4 智能合约隔离性

- a) 智能合约应支持业务数据存储按需隔离，不同智能合约的业务数据传输应互不干扰。
- b) 智能合约应确保没有业务依赖的不同智能合约可并行执行互不干扰。

- c) 智能合约的使用应进行严格授权管理，确保管理员或创建者对合约的控制权，参与成员仅可在授权范围内使用和执行智能合约逻辑。

4.3.5 智能合约安全性

智能合约应保证可安全执行，避免因安全漏洞、外部攻击导致的资金损失、数据泄露和合约功能瘫痪等异常情况。

4.4 密码算法

4.4.1 算法基本条件

- a) 算法的采用应符合 GM/T 0111—2021 中第 7.1 款规定。
- b) 算法应符合预期输出并满足正确性和一致性，并能支撑系统正常服务。

4.4.2 算法特性

算法应保障敏感信息的保密性、完整性，应保障实体的真实性。

4.4.3 密钥管理

密钥的使用应符合 GM/T 0111—2021 中第 7.4 款规定。

5 区块链存证平台

5.1 区块链存证平台系统框架

区块链存证平台系统框架包含存证业务系统、区块链存证系统、存证证明机构系统，见图 1：

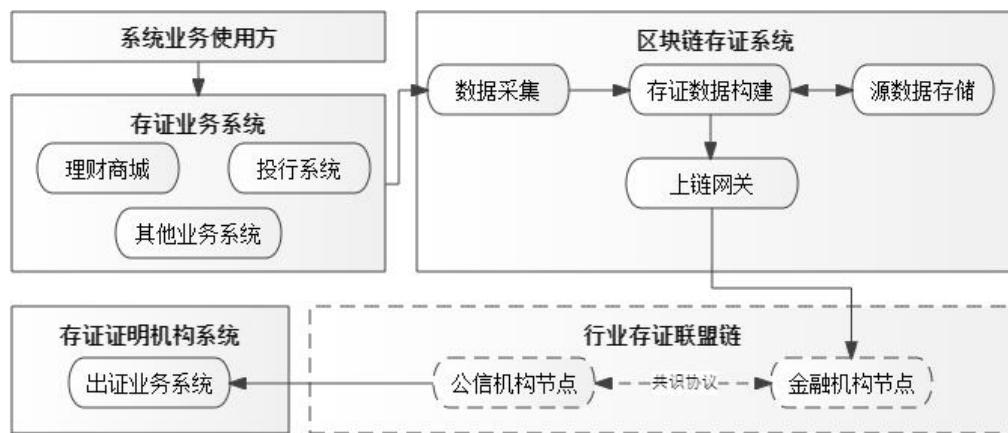


图 1 区块链存证平台系统框架

5.2 存证业务系统

存证业务系统是具有实际存证业务需求的应用系统，包括但不限于财富管理业务系统、投行业务系统、研究所业务系统等，应具有一定的开放能力，可以对接到区块链存证系统进行数据传输上链。

存证业务系统业务逻辑应完备，业务流程应设计完整。

存证业务系统应给客户揭示相关业务数据散列值将提供区块链存证系统和存证证明机构用于存证用途进行使用。

存证业务系统应具备完善的鉴权机制，同时具备清晰、易用、周全的权限控制能力。

存证业务系统应具备身份鉴别机制，以保障存证操作行为与用户的强关联性。

存证业务系统应完整记录用户的操作日志，日志格式应规范完整、日志存储应进行备份。

存证业务系统应具备保障存证数据完整性、机密性的技术机制。可使用哈希校验、电子签名、加密等技术防止存证数据被篡改，确保存证数据在存储、传输过程中的安全性。

存证业务系统应具备一定的容错性，在存证异常产生时，能及时重试以提高存证成功率。

存证业务系统应具备高可用性，通过同城双活、异地容灾等机制保障业务连续性，建立防御防攻击系统，防御大流量 DDoS 等攻击。应具备完善的应急预案，定期进行应急预案演练。

存证业务系统的密钥管理、证书管理方面的安全要求应符合 GM/T 0111—2021 中第 7.4、7.5 款规定。

5.3 区块链存证系统

区块链存证系统由数据采集模块、数据构建模块、数据存储模块以及对接区块链的上链网关组成，实现过程可根据实际需要构建相应的功能模块，支持扩展。其中，数据采集模块负责从各存证业务系统采集需存证的业务数据；数据构建模块负责基于各业务定义的存证模型构建存证数据；数据存储模块负责存储、归档存证数据；上链网关负责对接外部存证联盟链，对内提供上链存证服务。

区块链存证系统应保证系统安全，应达到 GB/T 22239—2019 的第三级基本要求。

区块链存证系统应保证运行环境安全，应 7*24 稳定运行，应具备完善的监控体系，应具有完整的安全防护措施及应急预案。

区块链存证系统应保证存储安全，应具备冗余备份、存储扩展、异地容灾的能力，确保用户隐私数据安全。

区块链存证系统应保证通信网络安全，应具备防御网络攻击、防病毒的能力，系统应定期检查排除风险。

区块链存证系统应保证数据安全，相关密码、密钥等技术的应用应符合 GM/T 0111—2021 相关规定。

区块链存证系统应可支持国产化、自主可控等国家信创要求。

区块链存证系统应具备跨链对接能力，如适配不同区块链的数据模型转换能力、匹配不同区块链的共识机制兼容能力、开放规范的通用 API 能力等。

区块链存证系统应具备一定的并发性能，以保障正常的业务需求。避免使用过度耗时的算法、性能较差的服务器建设区块链存证系统。

5.4 存证证明机构系统

存证证明机构系统由是中立、具有公信力的机构构建，如法院、公证机构、仲裁机构、审计机构、司法鉴定中心等，可对存证的电子数据出具公证鉴定报告，公证鉴定报告可按不同出证场景、不同出证对象制定相应模板，由各存证证明机构统一维护并遵循。

存证证明机构节点的存证证明源数据与其他节点应保持实时同步，可采用网络专线等方式保障通信。

存证证明机构节点与其他节点的通信通道应做加密处理，节点对外提供的 API 服务应做加密处理，采用的 SSL 协议及加密算法应符合 GM/T 0024—2014 SSL、GM/T 0111—2021 相关规定。

6 区块链存证过程

6.1 区块链存证平台应用框架

区块链存证平台应用框架包含应用原则、相关参与方和关键过程，见图2：

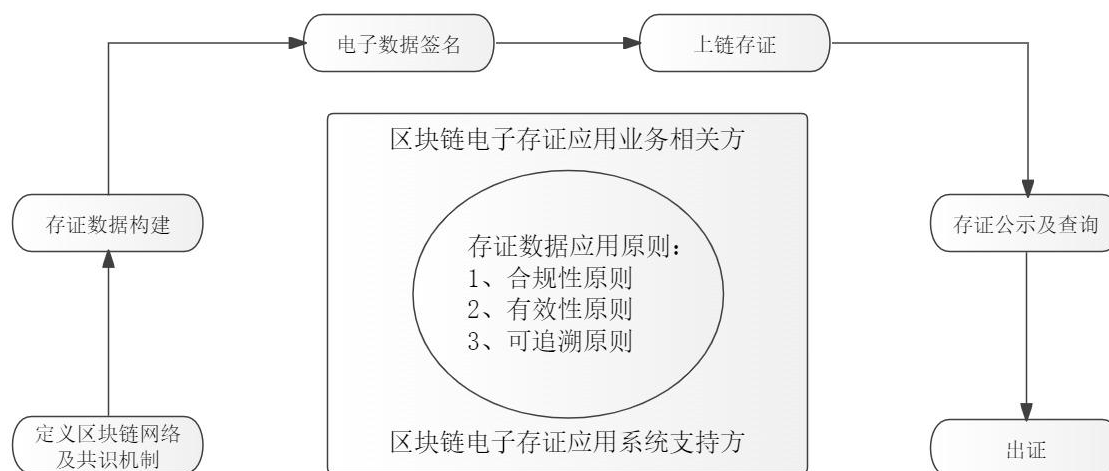


图2 区块链存证平台应用框架

6.2 应用原则

区块链存证过程应用原则包括合规性原则、有效性原则、可追溯原则。

合规性原则：应保证存证行为合规、存证信息保密合规、存证信息披露合规、取证流程合规。

有效性原则：应保证业务系统数据有效、电子存证数据存取有效、可信时间标识有效、第三方鉴定机构有效、存证核验有效。

可追溯原则：应保证存证数据不可篡改可溯源、存证行为过程可溯源、出证链路可溯源。

6.3 参与方

区块链存证过程参与方分为区块链电子存证应用业务相关方和区块链电子存证应用系统支持方。

区块链电子存证应用业务相关方提供存证场景、存证数据。

区块链电子存证应用系统支持方提供存证服务、存证合法性校验服务、存证查询核验服务、出证服务。

6.4 关键过程

6.4.1 定义区块链网络及共识机制

在建立区块链存证平台时，可按照存证场景及需求目标定义或选择区块链网络的共识机制。适用于联盟链的共识机制包括基于投票的共识机制、基于公信力节点的共识机制等。具体如下：

- a) 基于投票的共识机制：基于区块链节点资源量化等特定算法来确定链上可记账节点的共识机制；
- b) 基于公信力节点的共识机制：由区块链上单个或多个具备公信力的节点进行鉴证，通过该节点执行强制校验的共识机制。

6.4.2 存证数据构建

存证数据构建过程如下：

- a) 存证平台根据业务场景按需预先定义存证模板，根据存证模板规定各业务场景下的存证数据字段，也可定义适用不同业务场景的通用业务模板；
- b) 应对存证模板建立合理的版本管理规范，建立不同版本与存证数据、业务数据的关联关系，模板应具备普适性、时效性和扩展性；
- c) 存证业务系统根据存证模板提取构建存证数据，存证数据应在保证存证有效性的前提下进行结构化及去标识化处理；
- d) 存证数据应满足国家法律法规要求，隐私数据应进行匿名化处理；
- e) 存证数据应具备完整性、真实性、有效性；
- f) 存证数据大小应有最大单元限制，超限时应在保证数据安全、不失真的前提下进行合理的分片；
- g) 针对流式数据，按预设的标准对数据流进行切片，切片的大小决定了流式数据存证的颗粒度。切片的标准包含但不限于固定的时间、固定的大小等。并应针对切片建立索引。详细过程参考可参见附录 C。

6.4.3 电子数据签名

区块链存证平台对存证内容进行电子数据签名时：

- a) 应使用合法授权的身份数字证书进行签名，证书私钥本地保存，公钥及证书信息公开；
- b) 证书私钥应具有有效期，过期无效；
- c) 应使用存证主体区块链节点私钥对数据进行数字签名后发送共识；
- d) 已签名数据可在区块链网络内各节点进行合法性验证。

6.4.4 上链存证

上链存证过程如下：

- a) 存证业务系统将存证数据提交上链节点进行上链存证，可根据实际需要灵活使用实时上链、异步上链、定时批量上链等上链机制，可使用分布式事务、补偿事务等方式避免数据单边问题；
- b) 应确保存证过程中的数据提取、构建、存储、传输所依赖的软硬件环境安全、可靠；
- c) 数据上链可根据不同场景要求采用不同的存证信息生成算法，可包括原文存证、Hash 存证、默克尔树存证（可参考附录 C）等；
- d) 区块链共识可采用白名单机制，只允许白名单内的节点进行存证数据传输共识，传输信道可靠；
- e) 存证电子数据存储于区块链节点数据库中，每个共识节点均保留有区块链账本的完整备份，数据应定期共识同步避免异常或状态单边；
- f) 针对流式数据，将数据的切片内容、位置以及索引信息同时上链存证。详细过程可以参考附录 C。

6.4.5 存证公示及查询

区块链存证数据应支持所有区块链网络参与者查询本机构节点的存证公示信息：

- a) 业务层存证结果查询：存证平台区块链浏览器可采用网站形式构建，参与者可登录区块链浏览器查询链上的存证数据散列值以及相对应的区块信息等；
- b) 系统层存证结果查询：存证平台应提供存证查询 API 接口，区块链网络内各节点可采用接口调用的方式查询获取电子存证数据结果；
- c) 节点层存证结果查询：每个区块链节点均提供服务查询本节点的存证数据散列值，区块链浏览器以及存证业务系统对接均可指定某一特定区块链节点进行存证数据散列值以及存证上链结果的查询；
- d) 针对流式数据，查询时应利用分片索引优化查询效率，并保证流式数据的完整性以及连续性。详细过程可以参考附录 C。

6.4.6 出证

区块链存证平台应提供出证功能，相应的公证鉴定报告由链上存证证明机构出具。

区块链网络参与方可通过存证平台区块链浏览器网站、API 调用等方式进行出证申请获取存证数

据，存证数据直接来源于区块链共识账本。

出证过程应确保数据提取、构建、存储、传输所依赖的软硬件环境安全、可靠。

出证数据提取过程应可重现，提取过程的记录是连续的：同一电子存证数据支持无限次出证提取，区块链的不可篡改特性保证每次提取的内容相同。每次出证提取行为，各区块链节点的行为数据区块链存证平台均会记录留痕。

出证数据应包括：链上存证信息、存证信息加密算法、存证各参与方身份信息、存证可信时间戳、存证节点网络信息、出证结论、其他必要信息。

7 区块链存证模型

7.1 存证数据模型定义

存证数据模型定义应具备根据不同业务类型定义不同存证数据模板的能力并支持灵活扩展。

存证数据模型定义可建立通用的标准化模型，提供一组标准的业务数据模型的定义，模型应具有通用公共信息字段，可根据实际业务需求，参考使用本文附录中的存证数据模型示例。

存证数据模型定义应提供符合跨链技术标准的数据模型，包含对业务元素的存储模型规范，包括单点数据模型、链式数据模型、流式数据模型。

单点数据模型：单点数据是指静态、相对恒定的数据集，基于单点数据构建存证标准化数据模型的场景包括但不限于静态文本、静态图片、投行底稿文件等。本文定义的单点数据存证标准化模型参考附录 A。

链式数据模型：链式数据是指一组存在逻辑、勾稽关系的数据集，基于链式数据构建存证标准化数据模型的场景包括但不限于理财产品购买、投顾服务签约等。本文定义的链式数据存证标准化模型参考附录 B。

流式数据模型：流式数据是指一组顺序、大量、快速、连续到达的数据集，基于流式数据构建存证标准化数据模型的场景包括但不限于交易日志、委托记录等。本文定义的流式数据存证标准化模型参考附录 C。

7.2 业务数据提取

业务数据提取过程对于标准化模型的通用公共信息字段宜应填尽填。

业务数据提取手段应安全可靠，可采用加密、备份冗余、数字签名、时间戳、消息摘要等技术手段对业务数据第一时间进行固化，保证业务数据的保密性、完整性和真实性，确保业务数据提取后不被篡改和破坏。

业务数据提取应保证数据的可管理性、可查询性、可追溯性和可还原性，应制定详细的存储规范明确数据的存储位置、存储格式、存储期限等关键要素，可采用分布式存储、云存储等多种存储方式确保数据的可靠和安全。

7.3 存证数据传输

存证数据传输应保证存证数据的安全性，可通过加密的方式保证存证数据的机密性，可通过数字证书私钥签名保证存证数据的完整性。

存证数据传输应保证传输信道的安全性，可通过使用符合 GM/T 0111—2021 相关规定的加密算法加密通信信道，来保证存证数据的安全传输。

7.4 存证数据隐私保护

存证数据隐私保护应符合 GB/T 35273—2020 相关规定。

存证数据构建前，应对存证原始数据中的个人敏感信息进行去标识化处理。

存证数据和业务系统中的客户信息等数据应分开存储、隔离保存。

存证数据的访问及提取应具备完善的鉴权机制，同时具备清晰、易用、周全的权限控制能力。

存证数据上链以及传输过程均应采用加密的方式进行交互，可通过使用符合 GM/T 0111—2021 相关规定的算法进行数据摘要信息提取、数据加解密、数字签名以及加密通信信道，保证数据安全传输。

附录 A
(资料性)
单点数据存证模型应用示例

对于区块链存证在证券行业内的应用场景，各机构可根据实际业务、技术需求灵活选择数据模型。单点数据存证模型示例以投行底稿文件业务的存证模型定义进行说明。

投行底稿文件存证模型包含存证主体信息、底稿数据信息两个部分。属性分类信息如表 A.1 所示：

表 A.1 投行底稿文件存证模型表

一级分类	二级分类
存证主体信息	主体基本信息
	主体区块链节点信息
底稿数据信息	项目信息
	底稿信息

a) 存证主体信息

存证主体用于记录行业区块链存证平台各参与方，主要包括行业联盟链上各类有存证需求的机构。存证主体信息划分为一到二级属性分类，属性分类应符合表 A.2 的内容。二级子类包括存证主体的基本信息、区块链节点信息，基于该主体的实际业务填写必要或非必要的所有源数据，如：企业名称、机构类型、行政区域、机构性质等。

表 A.2 存证主体信息表

一级分类	二级分类
存证主体信息	主体基本信息
	主体区块链节点信息

表 A.2 中具体信息的说明如下：

主体基本信息见表 A.3：

表 A.3 主体基本信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
主体名称	subject_company_name		CHARACTER	256	Y	
主体英文名称	subject_company_english_name		CHARACTER	256		
主体行政区域	subject_main_administrative_region		NUMBER		Y	枚举-境内外类别
主体信息维护时间	subject_create_time	业务操作时间	TIME		Y	
机构性质	subject_organization_nature		NUMBER			枚举-机构性质
所有制性质	subject_ownership_nature		NUMBER			枚举-所有制性质
证件类型及证件号码	subject_document_information		对象数组			枚举-机构代码类型
注册日期	subject_registry_date		DATE			
主营业务	subject_company_business		CHARACTER	2048		
公司简介	subject_company_profile		TEXT			

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
注册资本	subject_registered_capital		DECIMAL			
注册资本币种	subject_registered_capital_currency		CHARACTER	16		枚举-币种类型
实收资本	subject_paid_in_capital		DECIMAL			
实收资本币种	subject_paid_in_capital_currency		CHARACTER	16		枚举-币种类型
注册地址	subject_registered_address		CHARACTER	512		
办公地址	subject_office_address		CHARACTER	512		
联系地址	subject_contact_address		CHARACTER	128		
联系电话	subject_contact_number		CHARACTER	512		
企业传真	subject_fax		CHARACTER	64		
邮政编码	subject_postal_code		CHARACTER	32		
互联网地址	subject_internet_address	企业官网地址	CHARACTER	256		
电子邮箱	subject_mail_box		CHARACTER	64		
主管单位	subject_regulator		CHARACTER	128		

主体区块链节点信息见表 A.4:

表 A.4 区块链节点信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
节点所属主体 ID	node_subject_id		CHARACTER			
节点名称	node_name		CHARACTER			
节点英文名称	node_english_name		CHARACTER			
节点类型	node_type		NUMBER			枚举-节点类型
节点接入时间	node_access_time		TIME			
节点接入方式	node_access_method		CHARACTER			
节点接入网络	node_access_network		CHARACTER			
节点机器数量	node_machine_numbers		CHARACTER			

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
节点机器类型	node_machine_type		NUMBER			枚举-机器类型
节点 IP	node_ip		CHARACTER			
节点物理位置	node_position		CHARACTER			
节点系统版本	node_system_version		CHARACTER			
节点备注信息	node_remark		CHARACTER			

b) 底稿数据信息

底稿数据信息用于记录各参与主体在行业联盟链上进行区块链存证的底稿数据信息。底稿数据信息划分为一到二级属性分类,属性分类应符合表 A.5 的内容。其中项目信息用于记录存证的投行项目信息,如项目编号、项目名称、项目类型、项目状态、项目发行人信息、项目当前阶段、项目负责人、项目行业、项目主办部门等。底稿信息用于记录存证的底稿文件信息,如底稿文件名称、文件大小、文件上传时间、底稿文件散列值等。

表 A.5 底稿数据信息表

一级分类	二级分类
底稿数据信息	项目信息
	底稿信息

表 A.5 中具体信息的说明如下:

二级分类项目信息见表 A.6:

表 A.6 项目信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
项目编号	project_code		CHARACTER		Y	
项目名称	project_name		CHARACTER		Y	
项目类型	project_type		CHARACTER			
项目状态	project_status		CHARACTER			
项目发行人信息	project_issuer_information		CHARACTER			
项目当前阶段	project_current_state		CHARACTER			
项目负责人	project_pr		CHARACTER			
项目行业	project_industry		CHARACTER			
项目主办部门	project_host_department		CHARACTER			
项目描述	project_description		CHARACTER			

二级分类底稿信息见表 A.7:

表 A.7 底稿信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
底稿所属项目目标号	working_papers_project_code		CHARACTER		Y	
底稿所属项目名称	working_papers_project_name		CHARACTER		Y	
底稿文件名	working_papers_name		CHARACTER		Y	
底稿文件描述	working_papers_description		CHARACTER			
底稿文件大小	working_papers_size		CHARACTER			
底稿文件上传时间	working_papers_upload_time		TIME			
底稿文件散列值	working_papers_hash		CHARACTER		Y	

c) 上链数据示例

```
{
  "transaction_info_array": [{
    "transaction_info": {
      "transaction_detail_info": {
        "biz_data": {
          "bizName": "投行底稿文件存证",
          "businessData": [{
            "StageHash":
"60c8847b8a2e3f8e71420d1c7756d943132e174f80674683fb70bc86c4362baa",
            "StageName": "存证主体-主体基本信息"
          }, {
            "StageHash":
"52c8847a842e369efe656b00d128505501f9418ea9641cc5c0308c8c4361d1fb",
            "StageName": "存证主体-主体区块链节点信息"
          }, {
            "StageHash":
"46e1eb2d8785badc69fe850386f02e174f80674683fb70bc9f8f1cd1d1fb6658",
            "StageName": "项目信息"
          }, {
            "StageHash":
"af8205ffbbcc5c0308c8af8c1fc3a90b0674e9efda69efe656b00d128505501f",
            "StageName": "底稿信息"
          }
        ]
      },
      "necessaryData": {
        "CreateTime": "2022-08-12 12:01:22",
        "PackageHash":
"588750387566580de8ba6e6a19bccdf5cb4bfad7dadfef6bc1aef4ac1346866",

```

```
    "UploadTime": "2022-08-12 13:02:42"  
  }  
}  
}  
}  
}]  
}
```

附录 B
(资料性)
链式数据存证模型应用示例

对于区块链存证在证券行业内的应用场景，各机构可根据实际业务、技术需求灵活选择数据模型。链式数据存证模型示例以公募基金委托下单业务的存证模型定义进行说明。

公募基金委托下单业务存证模型包含存证主体、存证数据两个部分，其中存证数据包含实际业务过程中的账号、产品以及事务环节信息。属性分类信息如表 B.1 所示：

表 B.1 公募基金委托下单业务存证模型表

一级分类	二级分类	三级分类	
存证主体信息	主体基本信息	--	
	主体区块链节点信息	--	
存证数据信息	客户账号信息	--	
	产品信息	--	
	事务环节信息	登录信息	
		浏览记录信息	
		适当性匹配信息	
		协议签署信息	
委托下单信息			

a) 存证主体信息

存证主体用于记录行业区块链存证平台各参与方，主要包括行业联盟链上各类有存证需求的机构。存证主体信息划分为一到二级属性分类，属性分类应符合表 B.2 的内容。二级子类包括存证主体的基本信息、区块链节点信息，基于该主体的实际业务填写必要或非必要的所有源数据，如：企业名称、机构类型、行政区域、机构性质等。

表 B.2 存证主体信息表

一级分类	二级分类
存证主体信息	主体基本信息
	主体区块链节点信息

表 B.2 中具体信息的说明如下：

主体基本信息见表 B.3：

表 B.3 主体基本信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
主体名称	subject_company_name		CHARACTER	256	Y	
主体英文名称	subject_company_english_name		CHARACTER	256		
主体行政区域	subject_main_administrative_region		NUMBER		Y	枚举-境内外类别
主体信息维护时间	subject_create_time	业务操作时间	TIME		Y	
机构性质	subject_organization_nature		NUMBER			枚举-机构性质
所有制性质	subject_ownership_nature		NUMBER			枚举-所有制

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
						性质
证件类型及证件号码	subject_document_information	只可选1或者同时提供2/3/4,枚举值只用于标记type类型。数据格式为: [{ "type": 1, "code": "123" }, { "type": 1, "code": "123" }]	对象数组			枚举-机构代码类型
注册日期	subject_registry_date		DATE			
主营业务	subject_company_business		CHARACTER	2048		
公司简介	subject_company_profile		TEXT			
注册资本	subject_registered_capital		DECIMAL			
注册资本币种	subject_registered_capital_currency		CHARACTER	16		枚举-币种类型
实收资本	subject_paid_in_capital		DECIMAL			
实收资本币种	subject_paid_in_capital_currency		CHARACTER	16		枚举-币种类型
注册地址	subject_registered_address		CHARACTER	512		
办公地址	subject_office_address		CHARACTER	512		
联系地址	subject_contact_address		CHARACTER	128		
联系电话	subject_contact_number		CHARACTER	512		

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
企业传真	subject_fax		CHARACTER	64		
邮政编码	subject_postal_code		CHARACTER	32		
互联网地址	subject_internet_address	企业官网地址	CHARACTER	256		
电子邮箱	subject_mail_box		CHARACTER	64		
主管单位	subject_regulator		CHARACTER	128		

主体区块链节点信息见表 B.4:

表 B.4 区块链节点信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
节点所属主体 ID	node_subject_id		CHARACTER			
节点名称	node_name		CHARACTER			
节点英文名称	node_english_name		CHARACTER			
节点类型	node_type		NUMBER			枚举-节点类型
节点接入时间	node_access_time		TIME			
节点接入方式	node_access_method		CHARACTER			
节点接入网络	node_access_network		CHARACTER			
节点机器数量	node_machine_numbers		CHARACTER			
节点机器类型	node_machine_type		NUMBER			枚举-机器类型
节点 IP	node_ip		CHARACTER			
节点物理位置	node_position		CHARACTER			
节点系统版本	node_system_version		CHARACTER			
节点备注信息	node_remark		CHARACTER			

b) 存证数据信息

存证数据用于记录各参与主体在行业联盟链上进行区块链存证的数据信息。存证数据信息划分为一到三级属性分类，属性分类应符合表 B.5 的内容。例如二级子类包括客户账号信息、产品信息、事务环节信息。存证数据信息对公募基金委托下单进行全生命周期管理，通过事务环节唯一编码将客户下单公募基金的全流程数据串联形成链式证据，进行区块链存证。

表 B.5 存证数据信息表

一级分类	二级分类	三级分类
------	------	------

存证数据信息	客户账号信息	--
	产品信息	--
	事务环节信息	登录信息
		浏览记录信息
		适当性匹配信息
		协议签署信息
委托下单信息		

表 B.5 中具体信息的说明如下：

二级分类客户账号信息见表 B.6：

表 B.6 客户账号信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
账号所属主体	account_subject		CHARACTER		Y	
客户账号	account_code		CHARACTER		Y	
账号类型	account_type		NUMBER		Y	枚举-账号类型
账号用途	account_purpose		CHARACTER		Y	
账号状态	account_status		NUMBER		Y	枚举-账号状态
账号信息维护时间	account_create_time		TIME		Y	
账号创建日期	account_establish_date		DATE			
账号开户日期	account_opening_date		DATE			
账号开户文件	account_opening_doc		FILE_OBJECT			
账号销户日期	account_closing_date		DATE			
账号销户文件	account_closing_doc		FILE_OBJECT			
账号冻结日期	account_frozen_date		DATE			
账号冻结文件	account_frozen_doc		FILE_OBJECT			
账号解冻日期	account_thaw_date		DATE			
账号解冻文件	account_thaw_doc		FILE_OBJECT			
账号关联关系	account_association		NUMBER			枚举-关联关系
账号关联对象引用	account_associated_account_ref		CHARACTER			

二级分类产品信息见表 B.7：

表 B.7 产品信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
产品代码	product_code		CHARACTER		Y	
产品全称	product_name		CHARACTER		Y	

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
产品简称	product_name_abbreviation		CHARACTER			
产品类型	product_type		NUMBER		Y	枚举-公募基金产品类型
产品风险等级-适当性	product_risk_level_suitability		NUMBER		Y	枚举-风险等级
产品投资品种-适当性	product_invest_kind_suitability		NUMBER		Y	枚举-投资品种
产品投资期限-适当性	product_invest_term_suitability		NUMBER		Y	枚举-投资期限
产品可承受亏损-适当性	product_affordable_of_loss_suitability		NUMBER		Y	枚举-可承受亏损
产品最新净值	product_new_nav		CHARACTER			
产品累计净值	product_net_value		CHARACTER			
产品净值日期	product_nav_date		CHARACTER			
产品成立以来收益率	product_rate		CHARACTER			
产品规模	product_scale		CHARACTER			
信息披露方式	product_info_disclosure_way	公募基金均为公开披露	CHARACTER			
产品规模币种	product_scale_currency		CHARACTER			
产品规模总额	product_scale		CHARACTER			
联系人	product_issuer_contact_person		CHARACTER			
联系信息	product_issuer_contact_info		CHARACTER			
备注	product_remark		CHARACTER			
产品信息维护时间	product_create_time		TIME			
投资产品类型	product_investment_products_type		CHARACTER			
投资比例范围	product_investment_proportion_range		CHARACTER			
投资产品详情	product_investment_product_details		CHARACTER			
投资产品详情说明文件清单	product_detailed_description_document		CHARACTER			
发行成功日期	product_release_date		DATE			

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
基金成立日期	product_foundation_date		DATE			
基金状态	product_fund_status		NUMBER		Y	枚举-基金状态
募集开始日期	product_raise_start_date		DATE			
募集结束日期	product_raise_end_date		DATE			

三级分类登陆信息见表 B.8:

表 B.8 事务环节登录信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
事务环节唯一编码	transaction_link_unique_code	一次存证环节的唯一编码	CHARACTER		Y	
登录账号	login_account		CHARACTER		Y	
登录时间	login_time		TIME		Y	
登录系统	login_application	客户登录的应用系统	CHARACTER		Y	
登录 IP	login_ip		CHARACTER			
登录终端信息	login_terminal	PC: MAC/移动端: 设备标识码	CHARACTER			
登出时间	logout_time		TIME			

三级分类浏览记录信息见表 B.9:

表 B.9 事务环节浏览记录信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y/N)	枚举值说明
事务环节唯一编码	transaction_link_unique_code	一次存证环节的唯一编码	CHARACTER		Y	
一级页面名称	primary_page_name	例如: 产品详情页	CHARACTER		Y	
一级页面内容	primary_page_content		CHARACTER		Y	
一级页面点击操作	primary_page_click		CHARACTER			
一级页面浏览开始时间	primary_page_begin_time		TIME			
一级页面浏览结束时间	primary_page_end_time		TIME			
二级页面名称	secondary_page_name		CHARACTER			

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y/N)	枚举值说明
二级页面包含内容	secondary_page_content		CHARACTER			
二级页面点击操作	secondary_page_click		CHARACTER			
二级页面浏览开始时间	secondary_page_begin_time		TIME			
二级页面浏览结束时间	secondary_page_end_time		TIME			

三级分类适当性匹配信息见表 B.10:

表 B.10 事务环节适当性匹配信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
事务环节唯一编码	transaction_link_unique_code	一次存证环节的唯一编码	CHARACTER		Y	
客户账号	account_code		CHARACTER		Y	
适当性匹配结果	suitability_match_result		NUMBER		Y	枚举-是否
风险等级匹配结果	risk_match_result		NUMBER		Y	枚举-是否
投资品种匹配结果	invest_kind_match_result		NUMBER		Y	枚举-是否
投资期限匹配结果	term_match_result		NUMBER		Y	枚举-是否
可承受亏损匹配结果	affordable_of_loss_match_result		NUMBER		Y	枚举-是否
产品风险等级-适当性	product_risk_level_suitability		NUMBER		Y	枚举-风险等级
产品投资品种-适当性	product_invest_kind_suitability		NUMBER		Y	枚举-投资品种
产品投资期限-适当性	product_invest_term_suitability		NUMBER		Y	枚举-投资期限
产品可承受亏损-适当性	product_affordable_of_loss_suitability		NUMBER		Y	枚举-可承受亏损
客户风险等级-适当性	cust_risk_level_suitability		NUMBER		Y	枚举-风险等级
客户投资品种-适当性	cust_invest_kind_suitability		NUMBER		Y	枚举-投资品种
客户投资期限-适当性	cust_invest_term_suitability		NUMBER		Y	枚举-投资期限
客户可承受亏损-适当性	cust_affordable_of_loss_suitability		NUMBER		Y	枚举-可承受亏损
适当协议名称	suitability_agreement_name		CHARACTER			

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
			R			
适当性协议编号	suitability_agreement_number		CHARACTER			
适当性协议散列值	suitability_agreement_hash	协议摘要信息	CHARACTER			
适当性协议签名串	suitability_agreement_signature	客户签署协议形成的密文串	CHARACTER			

三级分类协议签署信息见表 B.11:

表 B.11 事务环节协议签署信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
事务环节唯一编码	transaction_link_unique_code	一次存证环节的唯一编码	CHARACTER		Y	
客户账号	account_code		CHARACTER		Y	
协议名称	agreement_name		CHARACTER		Y	
协议编号	agreement_number		CHARACTER		Y	
协议散列值	agreement_hash		CHARACTER			
客户证书 sn	cust_certificate_sn		CHARACTER			
客户证书 dn	cust_certificate_dn		CHARACTER			
协议签名串	agreement_signature		CHARACTER			
签署时间	sign_time		TIME		Y	

三级分类委托下单信息见表 B.12:

表 B.12 事务环节委托下单信息表

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
事务环节唯一编码	transaction_link_unique_code	一次存证环节的唯一编码	CHARACTER		Y	
客户账号	account_code		CHARACTER		Y	
产品代码	product_code		CHARACTER		Y	
产品全称	product_name		CHARACTER			

中文名称	英文名称	详细说明	数据类型	数据长度	是否必填 (Y)	枚举值说明
			R			
产品类型	product_type		NUMBER			枚举-公募基金产品类型
委托编号	entrust_number		CHARACTER		Y	
委托时间	entrust_time		TIME		Y	
委托金额	entrust_amount		CHARACTER			
委托终端	entrust_terminal	客户委托下单的平台终端	CHARACTER			

枚举项信息见表 B.13:

表 B.13 枚举项信息表

枚举项	枚举值	说明
枚举-境内外类别	0	空值
	1	境内
	2	境外
	255	其他
枚举-机构性质	0	空值
	1	企业
	2	国家行政机关
	3	事业单位
	4	合作组织
	5	社会团体
	6	农民专业合作社
	7	个体工商
255	其他	
枚举-所有制性质	0	空值
	1	中央国有控股
	2	地方国有控股
	3	外资
	4	民营
	255	其他
枚举-机构代码类型	0	空值
	1	社会统一信用代码
	2	组织机构代码证
	3	营业执照
	4	税务登记证
	255	其他
枚举-币种类型	156	人民币
	840	美元
	036	澳元
	978	欧元
	276	德国马克
	344	港币
枚举-节点类型	1	全节点

枚举项	枚举值	说明
	2	轻节点
枚举-机器类型	1	物理机
	2	虚拟机
枚举-账号类型	1	证券账号
	2	资金账号
	3	游客账号
枚举-账号状态	1	正常
	2	注销
	3	冻结
	4	未实名认证
枚举-关联关系	0	空值
	1	资金账号与证券账号关联
枚举-公募基金产品类型	1	股票型
	2	债券型
	3	混合型
	4	货币型
	255	其他
枚举-是否	1	是
	2	否
枚举-风险等级	1	低风险
	2	中低风险
	3	中风险
	4	中高风险
	5	高风险
枚举-投资品种	1	债券、货币市场基金、债券基金等固定收益类投资品种
	2	股票、混合型基金、偏股型基金、股票型基金等权益类投资品种
	3	期货、期权等金融衍生品
	4	其他产品或服务
	255	其他
枚举-投资期限	1	没有经验
	2	少于2年
	3	2-5年
	4	5-10年
	5	10年以上
	255	其他
枚举-可承受亏损	1	10%以内
	2	10%-30%
	3	30%-50%
	4	超过50%
	255	其他
枚举-基金状态	1	可申购赎回
	2	发行
	3	停止申购赎回
	4	停止申购
	5	停止赎回
	6	基金终止

枚举项	枚举值	说明
	7	基金封闭
	255	其他

c) 上链数据示例

```

{
  "transaction_info_array": [{
    "transaction_info": {
      "transaction_detail_info": {
        "biz_data": {
          "bizName": "公募基金委托下单业务存证",
          "businessData": [{
            "StageHash":
"24fc216d15df3a4fe7c913f1f1feb4653d0438115b6fc59e91ca99f56637a70c",
            "StageName": "存证主体-主体基本信息"
          }, {
            "StageHash":
"48c8847a842e3f8e71420d1c7756d94313d96518ea96415aad9b986c4362baea",
            "StageName": "存证主体-主体区块链节点信息"
          }, {
            "StageHash":
"ecd8afeb7116e88d873d356e84fc788c54c7532ffd5fe3be0f25b05a7f7c9735",
            "StageName": "存证数据-客户账号信息"
          }, {
            "StageHash":
"bcf97a74cca8ad29169b5781e32b0f5a7e82876d323728785fc5b130b285b2d2",
            "StageName": "存证数据-产品信息"
          }, {
            "StageHash":
"7d1d8ceb46aa648d65f312652d74440e6cc0dad6fc5eba24e3997259794a0d9f",
            "StageName": "存证数据-事务环节-登录信息"
          }, {
            "StageHash":
"32c6a4f18634abcb72646c34d0732a824ea64e00fa33fa2215772ef5fa306cc6",
            "StageName": "存证数据-事务环节-浏览记录信息"
          }, {
            "StageHash":
"43908904e1b9cd01f9dc4bab65adb4b190c02353151af54ec6fa970f67f40f7a",
            "StageName": "存证数据-事务环节-适当性匹配信息"
          }, {
            "StageHash":
"633d65ceb72f40123e9f05ad8a4126123d2475620e3680793f835df755e623c9",
            "StageName": "存证数据-事务环节-协议签署信息"
          }, {

```

```
        "StageHash":
"cf6dcb876c2d49ec23e06b16880192524795119ef0f350b6a8259c53bea9b3ed",
        "StageName": "存证数据-事务环节-委托下单信息"
    },
    "necessaryData": {
        "CreateTime": "2022-08-11 16:01:51",
        "PackageHash":
"964eb249e0b660ed24fa08f195093b4642775b3921b49951ceffb464af0d3304",
        "UploadTime": "2022-08-22 10:45:09"
    }
}
}
}
}
}
```

附录 C
(资料性)
流式数据存证模型应用示例

C.1 存证过程消息流图

存证过程消息流图给出了存证过程中的主要消息流向和交互过程的示例，如图 C.1 所示（红色箭头表示）：

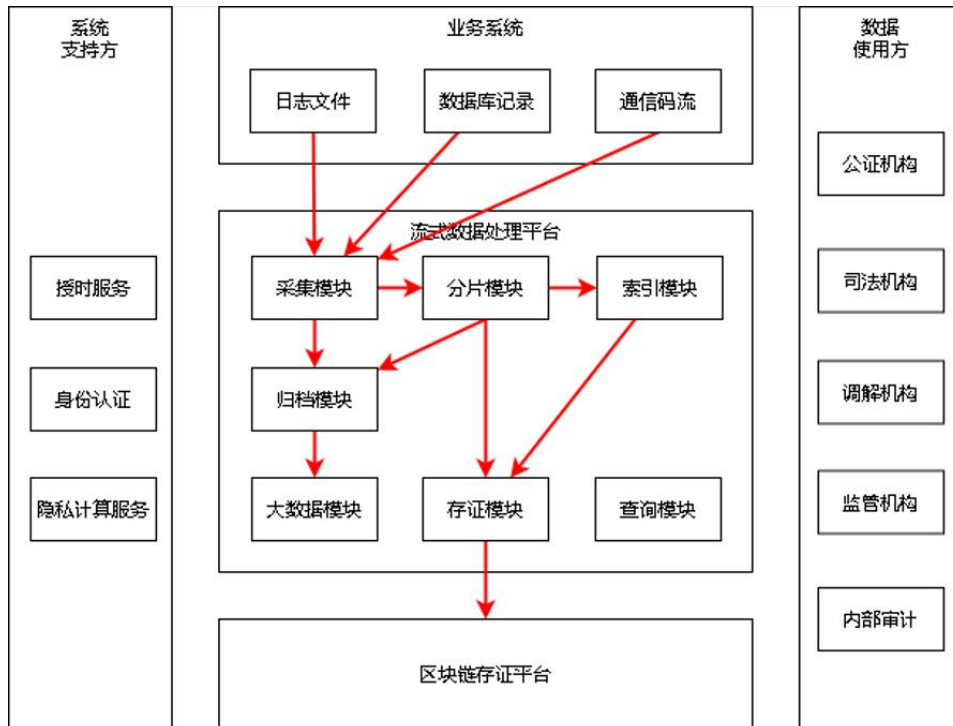


图 C.1 存证过程的消息流图

存证过程主要包括以下几个方面：

- a) 流式数据处理平台实时从业务系统上采集流式数据；
- b) 流式数据处理平台实时将数据存档至大数据模块；
- c) 利用分片模块进行实时分片，并将分片归档，同时将分片存证至区块链存证平台；
- d) 计算分片索引，并将索引归档，同时将索引存证至区块链存证平台。

C.2 取证过程消息流图

取证过程消息流图给出了取证过程中的主要消息流向和交互过程的示例，如图 C.2 所示（红色箭头表示，箭头上的数字表示顺序）：

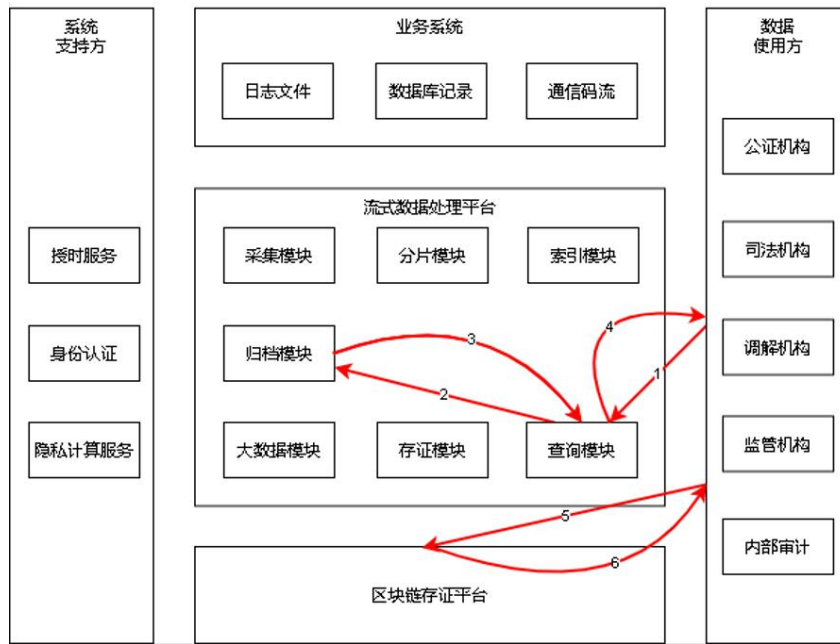


图 C.2 取证过程的消息流图

主要包括以下几个方面：

- a) 数据使用方请求流式数据处理平台查询相关流式数据；
- b) 查询模块请求归档模块返回相关信息；
- c) 归档模块返回相关索引、分片信息；
- d) 查询模块组织查询结果，并返回；
- e) 数据使用方请求区块链存证平台返回存证信息。

C.3 切片算法与数据结构示例

流式数据由于自身的特性实际处理时应对其进行分片处理，如图 C.3 所示：

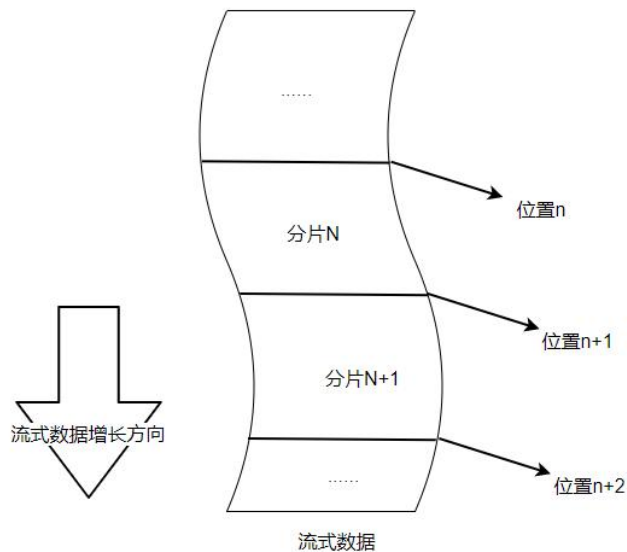


图 C.3 流式数据分片示意图

随着流式数据的不断采集，我们利用分片策略持续生成分片，可选的分片策略有：

- a) 以固定的频率进行分片；
- b) 以固定的大小进行分片；
- c) 以数据流业务上的属性进行分片（包括指定的日志行数、网络交互的数据包等）；
- d) 分片应该足够小，这样能够保证上链的实时性，分片应包含以下字段：
 - 流式数据标识：唯一标识流式数据；
 - 分片的标识：唯一标识分片；
 - 分片生成的时间；
 - 分片的起始位置；
 - 分片的截止位置。

C.4 索引算法与数据结构示例

为了能够加速查询、确保流式数据完整性，流式数据分片后应建立索引。利用索引可以在不了解原文的情况下确认分片是否有相关信息，并且利用索引信息可以保障数据完整无缺失。建立索引的关键过程如下：

- a) 根据业务系统特点得到关键字集合 $\{k|k \text{ 属于业务上可供查询的关键字}\}$ ，记作 K ；
- b) 针对集合 K 中的所有关键字 k ，计算出分片中关键字出现的次数，从而得到集合 $\{(k, n)|k \in K, n \text{ 为分片中 } k \text{ 出现的次数}\}$ ，标识成集合 KN ，集合 KN 即为此分片的索引；
- c) 索引信息应包含以下字段：
 - 流式数据标识：唯一标识数据流；
 - 分片的标识：唯一标识分片；
 - 关键字及出现次数列表。

C.5 存证信息生成算法

分片以及索引文件中可能存在用户隐私数据，根据实际业务场景以及隐私保护要求，可以选择不同的存证信息算法，从而达到隐私保护的目标。这里我们列举两种常见的算法：

- a) Hash 存证：存证时计算原文的 Hash 值并上链，取证的过程中利用 Hash 校验完整原文，可以得到原文是否被篡改结论。Hash 存证信息算法简单，但是实际取证的过程中需要有完整的原文信息，这里有隐私泄露的风险；
- b) 默克尔树存证：存证时计算默克尔树，并将根节点上链，取证时只需要原文中少部分信息，连同默克尔树部分节点即可得到信息是否被篡改结论，默克尔树算法相对复杂，但是更有利于隐私保护。

下面详细介绍默克尔树在分片、索引信息存证中的应用示例，默克尔树生成的具体的过程如下：

- a) 假定分片中的内容可以从业务上分为不同的条目（日志文件的单行，数据库的单条记录等），索引信息中的 (k, n) 也可以看成一个条目，这些条目记作 $item$ ，分片或者索引信息可以看成条目的列表，记作 $[item]$ ；
- b) 将 $[item]$ 中的元素进行 Hash 运算得到序列 $[H]$ 其中每个元素 $H_i = \text{Hash}(item_i)$ ，利用 $[H]$ 中的元素生成默克尔树的根节点；
- c) 根节点两两组合并计算组合后的 Hash 函数得到第二层节点；
- d) 重复 b) 步，直到生成一个根节点 H_{root} ；
- e) H_{root} 的值即为索引文件的存证值，上传到区块链中进行存证。

索引文件默克尔树结构如图 C.4 所示：

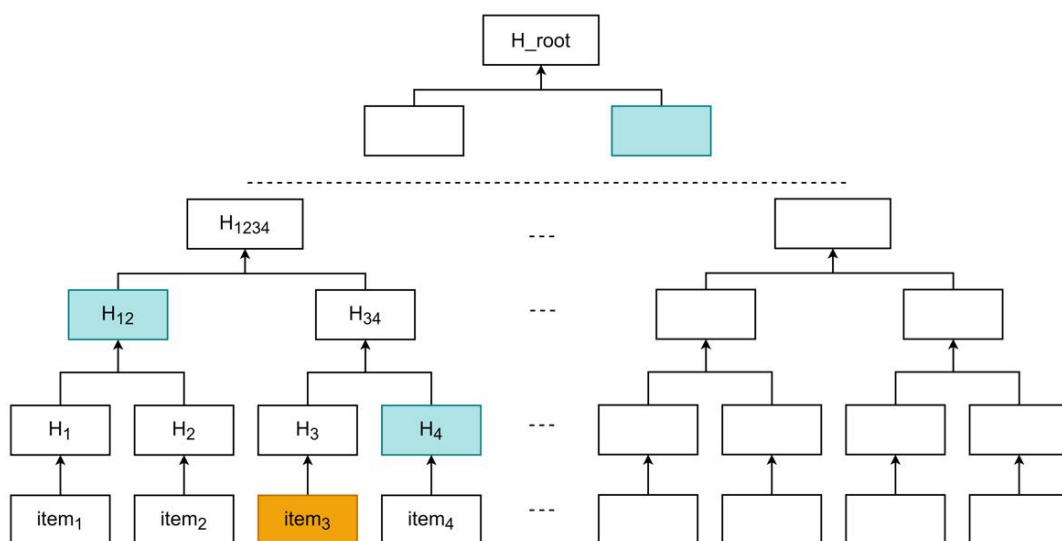


图 C.4 索引文件默克尔树示意图

取证时，利用默克尔树验证数据的真实完整性过程如下：

- 需要原始数据中待验证的条目 item（如图 C.4 中 $item_3$ ）记作 $item_c$ ；
 - 以及相关的默克尔树节点（如图 C.4 中 H_4 、 H_{12} 等）这些节点可以同 $item_c$ 计算出默克尔树根节点；
 - 计算出默克尔树根节点 H_{root} ，该根节点值即为索引信息的存证值；
 - 通过区块链存证平台可以验证 H_{root} 的有效性从而证实 $item_c$ 的真实可靠。
- 存证信息生成算法的选择可以参考表 C.1：

表 C.1 存证信息生成算法选择参考

场景	分片存证信息算法	索引存证信息算法
业务不涉及隐私	Hash 存证	Hash 存证
分片涉及隐私,索引不涉及隐私	默克尔树存证	Hash 存证
分片、索引均涉及隐私	默克尔树存证	默克尔树存证

证券公司数字化能力成熟度指引

T/SAC 005—2024

（经协会第七届常务理事会第二十六次会议审议通过，2024年10月11日发布实施）

（中证协发〔2024〕230号）

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国证券业协会提出并归口。

本文件起草单位：中国银河证券股份有限公司、中信建投证券股份有限公司、中国证券监督管理委员会北京监管局、中国标准化研究院、国泰君安证券股份有限公司、华泰证券股份有限公司、国信证券股份有限公司、长江证券股份有限公司、华创证券有限责任公司。

本文件主要起草人：罗黎明、华阳、唐沛来、罗清平、霍宇红、邓廷勋、刘永旗、马冰珂、肖钢、孟晋津、徐志彬、李剑戈、宋璐璐、蔡跃、张畅、李至炫、陈镛、邵健、王春艳、侯韩芳、贺欢、王俊杰、王逸、周睿、王和全。

1 范围

本文件提出了证券公司数字化能力成熟度模型的构成，明确了成熟度要求以及成熟度等级判定方法。

本文件适用于指导证券公司开展数字化转型、衡量自身数字化建设水平等工作，也适用于监管部门、第三方机构开展证券公司数字化能力评价活动。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0059—2010 证券期货经营机构信息系统备份能力标准

JR/T 0060—2021 证券期货业网络安全等级保护基本要求

JR/T 0271—2023 金融数字化能力成熟度指引

3 术语和定义

JR/T 0271—2023界定的以及下列术语和定义适用于本文件。

3.1

数字化能力 digital capability

在依法合规前提下运用技术和数据要素，对各种业务流程、产品服务和管理进行数字化重塑与创新，以提高运营效率、优化客户体验、增强风险管理水平，并创造新的价值提供方式和商业模式的能力。

3.2

数字化转型 digital transformation

在信息化建设的基础上，利用数字化能力（3.1），对企业战略体系、商业模式、业务流程、生产运营、组织架构等进行全方位、系统化地变革和重塑。

3.3

数字化能力成熟度 digital capability maturity

对数字化能力（3.1）发展阶段和水平的度量。

3.4

数字化人才 digital professionals

推动数字化转型（3.2）或者构建数字化能力（3.1）的人员。

注：包括企业内部数字化工作各级领导者、数字化技术专业人员以及应用数字化技术优化创新经营管理和业务模式的人员等。

3.5

数字化办公 digital work

利用信息技术将办公业务流程、信息资源等进行数字化处理，实现办公全流程数字化管理。

3.6

数字化营销 digital marketing

利用信息技术，基于多维数据对客户进行画像，并通过分析其潜在需求和消费特点等方式精确找到目标客户，为其提供定制化、个性化的服务。

4 成熟度模型

证券公司数字化能力成熟度模型由成熟度等级、能力域和成熟度要求构成，其中，能力域由能力子域构成，能力子域由能力项构成，如图1所示。

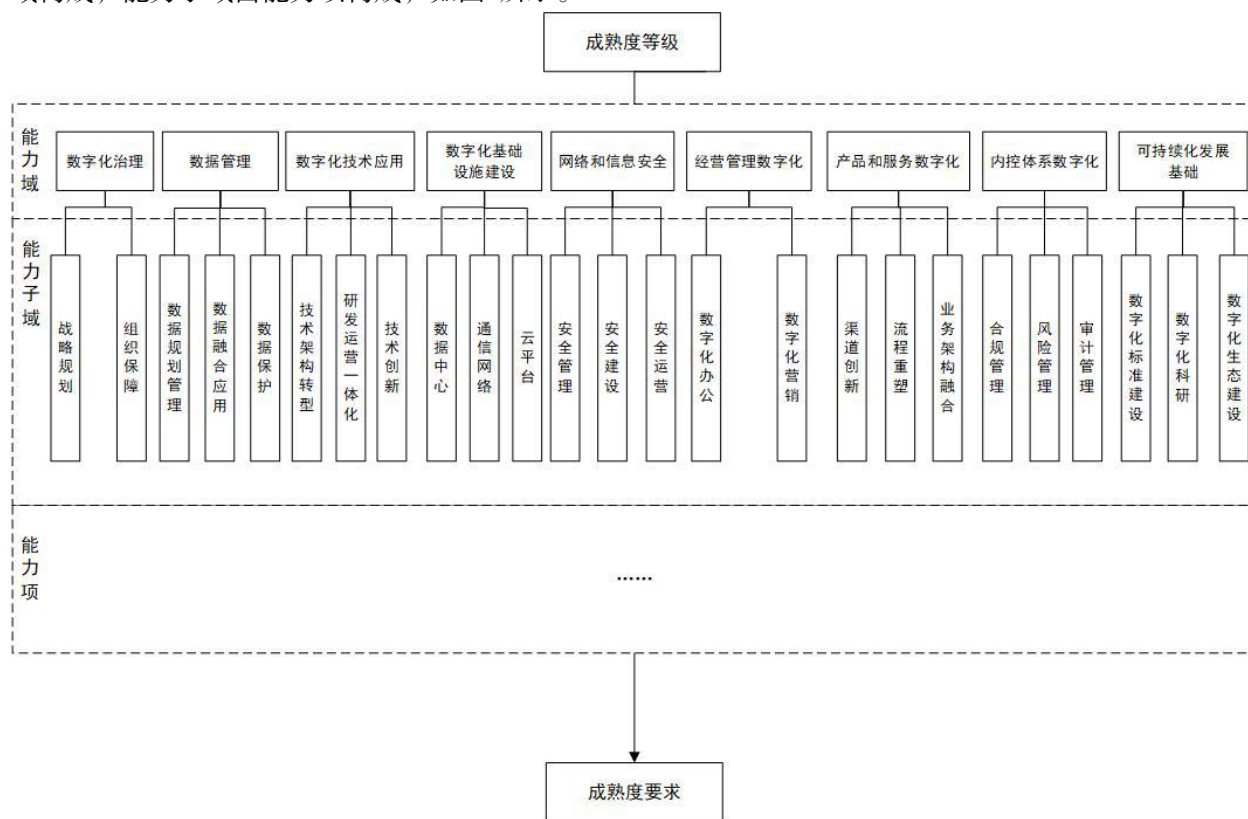


图 1 证券公司数字化能力成熟度模型构成

5 成熟度等级

成熟度等级规定了证券公司数字化能力建设不同阶段应达到的水平。成熟度等级分为五级，自低至高，依次为一级（萌芽级）、二级（基础级）、三级（发展级）、四级（优化级）和五级（引领级），较高的成熟度等级包含了低成熟度等级的要求。

一级（萌芽级）：企业领导层面具有一定的数字化转型意识，对组织、技术、数据、设施等基础条件开始初步规划，但尚不具备数字化转型所需的基础能力，经营和管理基于内外部需求开展数字化转型探索，但仍以传统模式为主。

二级（基础级）：初步形成企业级数字化战略规划和统筹协调机制，着手对组织、技术、数据、设施等基础条件进行建设与升级，完成局部业务的数据收集、整合与应用，开始运用数据辅助经营和管理决策。

三级（发展级）：建立明确的数字化转型战略规划并有序组织实施，组织、技术、数据、设施等基础条件基本满足数字化转型需要，主要业务范围内具备集成协同的数字化能力，企业经营和管理实现基于数据的效率和质量提升。

四级（优化级）：企业形成完善的数字化治理模式，组织、技术、数据、设施等基础条件根据数字化转型需要及时优化调整，数据要素可以高效获取、开发和利用，管理、运营、产品和服务模式由数据驱动得到持续创新，部分业务实现智能化管理和运营。

五级（引领级）：企业具备成熟先进的数字化治理能力，管理和经营模式为智能驱动型，已实现数据、技术、流程和组织的智能协同、动态优化和互动创新，数字化能力在行业处于领先水平，能够基于共建、共享、共赢的生态圈赋能行业数字化发展。

6 能力体系

能力域给出了证券公司开展数字化转型发展的关键要素，包括数字化治理、数据管理、数字化技术应用、数字化基础设施建设、网络和信息安全、经营管理数字化、产品和服务数字化、内控体系数字化以及可持续化发展基础9个方面，能力子域包括战略规划、组织保障等25个方面，能力项包括战略规划制定、规划落地实施等40个方面，见表1。证券公司或评价机构可根据具体的业务活动或者评价目标对能力子域和能力项进行裁剪。

表 1 能力域构成

能力域	能力子域	能力项
数字化治理	战略规划	战略规划制定
		规划落地实施
	组织保障	机构组建
		文化建设
		IT投入
		IT投入占营业收入比例
		人才培养
数据管理	数据规划管理	数据发展规划
		数据治理体系建设
	数据融合应用	数据架构
		数据规范
		数据质量
		数据应用
		数据共享
	数据保护	数据安全
		个人信息保护
数字化技术应用	技术架构转型	技术架构转型
	研发运营一体化	研发运营一体化能力
	技术创新	前沿技术应用
		自主创新
		产学研用合作
数字化基础设施建设	数据中心	资源能力建设
		备份能力建设
	通信网络	承载能力建设
云平台	云化部署	
网络和信息安全	安全管理	安全管理
	安全建设	安全建设
	安全运营	安全运营
经营管理数字化	数字化办公	数字化办公能力建设
	数字化营销	数字化营销能力建设

产品和服务数字化	渠道创新	渠道创新
	流程重塑	流程重塑
	业务架构融合	业务架构融合
内控体系数字化	合规管理	合规体系数字化
	风险管理	新技术风险管理
		风险体系数字化
审计管理	审计体系数字化	
可持续化发展基础	数字化标准建设	标准制定
	数字化科研	科研项目开展
	数字化生态建设	生态营造

7 成熟度要求

7.1 概述

成熟度要求规定了能力项各档应满足的具体要求，从1档到5档的要求依次提高，高档覆盖低档的具体要求。

7.2 数字化治理

7.2.1 战略规划

战略规划能力子域包括战略规划制定、规划落地实施2个能力项。各能力项的成熟度分档要求，见表2。

表2 战略规划的成熟度要求

能力项	1档	2档	3档	4档	5档
战略规划制定	企业领导层面具备数字化转型意识，初步明确了企业数字化转型的重点和方向，着手推动制定企业数字化发展战略规划	企业数字化发展战略规划初步制定完成并由企业数字化工作牵头部门组织发布，但规划尚未全方位覆盖企业生产、经营、管理等各个方面	①企业数字化发展战略规划基本覆盖企业生产、经营、管理等各个方面并由企业信息技术治理委员会或指定专门委员会审议发布； ②企业在制度、组织、流程等方面对企业数字化发展战略提出了配套的落实机制和措施	①企业数字化发展战略规划覆盖企业生产、经营、管理等各个方面并上升由企业董事会或最高决策机构审议发布； ②企业建立了数字化发展规划动态调整机制，能够根据规划执行情况及行业发展情况适时优化调整规划目标和重点建设任务	企业具备对行业内产业链上下游形成全视角影响力的数字化规划策略的能力
规划落地实施		企业着手推进数字化转型规划的落地实施	企业及时将数字化发展规划任务目标进一步细化，转化为具体行动计划，明确每项行动相应的责任部门、完成时间节点等要求	企业建立数字化转型任务实施评估体系，定期开展考核评价	企业建立了成熟的覆盖数字化转型任务实施运行、考核评价和规划设计改进完善闭环管理工作机制

7.2.2 组织保障

组织保障能力子域包括机构组建、文化建设、IT投入、IT投入占营业收入比例、人才培育5个能力项。各能力项的成熟度分档要求，见表3。

表3 组织保障的成熟度要求

能力项	1档	2档	3档	4档	5档
机构组建	①领导层面：尚未设立数字化工作领导组织和专门的数字化高层管理职位； ②执行层面：尚未设立专门的机构推进企业数字化转型工作	①领导层面：由CIO等高层领导兼职管理数字化工作，数字化工作领导决策职能赋予现有领导组织； ②执行层面：由IT部门或其他某个管理部门统筹，其他部门设立数字化工作小组或岗位协同推进企业数字化转型工作	①领导层面：建立了专门的数字化工作领导组织，如数字化转型工作领导小组等； ②执行层面：成立了专门的数字化工作组（如数字化办公室等）统筹，其他部门设立数字化工作小组或岗位协同推进企业数字化转型工作	①领导层面：数字化工作上为由企业主要负责人负责，如董事长； ②执行层面：成立了专门的数字化工作组织（如数字化办公室等）统筹，打破传统的部门式、竖井式的组织架构，向敏捷化组织形态转变，推进企业数字化转型工作	企业能够根据数字化发展趋势及自身数字化转型诉求，及时动态调整、优化企业组织形态，确保与企业数字化转型发展目标相适应

表3 组织保障的成熟度要求（续）

能力项	1档	2档	3档	4档	5档
文化建设	开展数字化转型宣传工作，但员工对于数字化认知较为模糊	对业务、管理、技术等各部门组织开展数字化培训、研究、竞赛等多样化活动，营造数字化氛围，有效提高员工数字化认知水平	对业务、管理、技术等各部门定期开展多样化数字化文化建设活动，制定有关鼓励或考核措施推动业务、管理等部门积极应用数字化工具、技术	将数字文化作为企业文化的重要组成部分，员工能够主动利用数字化工具、技术创新工作模式，共享数字化知识、技能和经验	企业全员建立数字化思维，形成良好的数字文化理念，并在行业中具备一定影响力
IT投入	IT投入总量在行业内排前80名（含）	IT投入总量在行业内排前50名（含）	IT投入总量在行业内排前30名（含）	IT投入总量在行业内排前20名（含）	IT投入总量在行业内排前10名（含）
IT投入占营业收入比例	IT投入总量在行业内排前50名（含）且IT投入占营业收入比例在行业内排前50名（含）	IT投入总量在行业内排前50名（含）且IT投入占营业收入比例在行业内排前40名（含）	IT投入总量在行业内排前50名（含）且IT投入占营业收入比例在行业内排前30名（含）	IT投入总量在行业内排前50名（含）且IT投入占营业收入比例在行业内排前20名（含）	IT投入总量在行业内排前50名（含）且IT投入占营业收入比例在行业内排前10名（含）
人才培养	尚未形成具体的数字化人才培养策略，沿用传统的信息技术人才管理机制	明确数字化人才培养目标，建立了初步的数字化人才培养、激励等工作机制	数字化人才引进、培养、激励等制度措施进一步完善，如建立数字化人才选拔招聘、分层分类培养、职级晋升、薪酬激励等管理体系	数字化人才引进、培养、激励等制度措施全面完善，建成数字化人才引进、培养、认证、激励、晋升等闭环管理体系	不仅关注企业内部数字化人才的培养和管理，还与外部环境（如高校、研究机构、行业协会、合作伙伴）进行互动，共同构建数字化人才生态
注：IT投入、营业收入指最近一个财政年度的费用。					

7.3 数据管理

7.3.1 数据规划管理

数据规划管理能力子域包括数据发展规划、数据治理体系建设2个能力项。各能力项的成熟度分档要求，见表4。

表4 数据规划管理的成熟度要求

能力项	1档	2档	3档	4档	5档
数据发展规划	有部门级的数据规划或目标计划	开始对企业数据工作进行整体谋划，明确企业数据工作的目标、范围、主要任务等	建立企业级数据发展规划，并纳入企业整体数字化战略规划	进一步明确企业数据发展规划分阶段实施目标，能够长期投入、持续推进	建立规划落地的长效反馈机制，数据战略动态优化，可有效提升企业竞争力，并成为行业标杆

数据治理体系建设	在项目层面开展数据需求管理,但尚未制定统一的管理流程	根据管理策略要求制定了部分数据管理规范和流程,对重要关键领域制定了相关管理措施	在组织层面明确了数据管理部门,建立了企业级数据管理的规章制度体系和考核评价机制	在企业级数据管理制度度的基础上,建立了较为详细的管理规范与执行标准,指导企业各领域数据管理工作的有效落实	具备完善的数据治理体系,能够落地应用并显著提升数据使用过程中的准确性、有效性和易用性,对在证券行业推广具有指导意义
----------	----------------------------	---	---	--	---

7.3.2 数据融合应用

数据融合应用能力子域包括数据架构、数据规范、数据质量、数据应用、数据共享5个能力项。各能力项的成熟度分档要求,见表5。

表5 数据融合应用的成熟度要求

能力项	1档	2档	3档	4档	5档
数据架构	应用系统维护了各应用的数据字典,具备元数据变更流程;主要通过离线方式进行数据交换,各部门间存在数据孤岛,数据相对独立	应用系统维护了各应用的数据模型,在部分应用中实施了主数据的管理,具备元数据变更与数据交换规范;建立了部门级的结构化、非结构化数据集成平台,开展了部门级的数据集成	建立了企业级的数据模型,梳理了数据源和数据分布关系,在企业内部实现了主数据的有效管理;建设了企业统一的数据集成管理平台与采集工具,实现数据统一采集与集中管理	①形成了成熟的企业级数据模型,建立企业级数据资源目录,实现数据资源统一管理;能够通过数据分布关系梳理持续优化数据的存储和集成关系;建设了实时数据采集与计算平台,在企业内部支持实时数据使用; ②根据数据资源目录建立形成企业级数据资产目录	①建立了支持数据架构各领域工作的系统工具,实现数据分布关系自动监测、数据模型一致性自动校验,保障数据存储和集成关系的持续优化,全面满足企业离线和实时的各项数据使用需求; ②将数据资产作为生产要素,形成新型数据业务
数据规范	执行国家和证券行业已有的数据元、参考数据和主数据等基础标准规范	建立完善了企业内部的数据元、参考数据和主数据标准规范,保障各重要信息系统参考数据和主数据标准的一致性	进一步执行和建立完善了明细数据和指标数据规范	建立形成了覆盖数据元、主数据、参考数据、指标数据等完善的企业数据标准体系,数据标准涵盖投研、销售、运营、监管报送等主要业务领域;能定期分析标准规范执行情况,不断优化完善	建立了数据标准体系落实和业务价值度量的评价体系,基于业务价值度量指标反映数据标准管理价值
数据质量	在项目或系统层面根据业务需要建立了数据质量管理规范	建立了企业级数据质量管理方案,明确了数据质量管理目标与质量需求,基于数据质量需求建立数据质量规则库	①建立了覆盖数据全生命周期的数据质量管理体系,设立数据质量管理岗位; ②利用技术工具实现对数据质量的管理和监控	①建立数据质量分级标准,数据质量分析知识库、案例库,数据质量管理体系在组织建设、制度流程等方面持续完善; ②形成数据质量评价指标体系,衡量并改进数据质量管理体系和技术工具	建立了数据质量问题的效益评估模型,通过量化分析指标反映数据质量问题对企业效益的影响
数据应用	项目层面开展了常规报表分析、数据接口分析、数据查询服务,相关的分析报表、数据服	各部门根据自身数据需求独立开展各自数据分析应用与数据服务建设,采用点对点的方式处理数据分析	建立了企业级统一的数据分析管理平台,数据分析结果能在各个部门之间复用,分析口径定义明	建立了数据分析模型库,支持业务人员进行数据分析处理,能够运用数据仓库、数据挖掘、机器学习、数据可视化	建立了数据分析结果和数据服务的评价方法,持续提升数据价值驱动能力;能够利用数据支持业务创新、产品创新,实现

	<p>务分散在各部门、各系统实现</p>	<p>中跨部门的数据需求和数据服务产品建设，数据分析结果和数据服务应用于部门内部</p>	<p>确，分析数据统一管理、按需调用；编制并发布了统一的数据服务目录，相关的数据分析结果能够在风险管理、业务经营与内部控制中得以应用，实现数据驱动</p>	<p>等技术方法开展数据分析；建立较全面的数据产品体系，充分发挥了数据价值</p>	<p>服务实体经济领域的综合应用和多向赋能或取得卓越成果</p>
--	----------------------	--	---	---	----------------------------------

表5 数据融合应用的成熟度要求（续）

能力项	1档	2档	3档	4档	5档
数据共享	在企业内部按照数据需求进行了点对点的数据共享	实现主要业务系统数据归集，对数据资源开展共享分级分类工作	建立了企业级数据共享机制，搭建了企业级数据共享平台，建立了数据共享目录和分级共享体系	对内数据共享能力和数据规模不断完善，覆盖主要业务场景，对外通过系统交互等方式进行数据对外共享	企业级数据共享机制和数据共享平台成为证券行业典型实践，并输出数据共享能力和经验

7.3.3 数据保护

数据保护能力子域包括数据安全、个人信息保护2个能力项。各能力项的成熟度分档要求，见表6。

表6 数据保护的成熟度要求

能力项	1档	2档	3档	4档	5档
数据安全	在项目中进行了数据访问授权和数据安全监控，对出现的数据安全问题进行分析和处理	①依据数据安全标准在部门内部对数据进行安全等级的划分； ②部门内部进行了数据利益相关者需求的识别，并进行数据访问授权以及数据安全保护； ③部门内部进行了数据访问、使用等方面的监控； ④部门内部对潜在数据安全风险进行了分析，制定了预防措施	①对数据进行全面的安全等级划分，每级数据的安全需求能清晰定义，能明确安全需求的责任部门； ②能系统梳理数据使用的场景和场景内围绕采集、传输、存储、加工、共享、删除、销毁等各环节的数据处理活动，通过引入新的技术和方法，持续提升梳理的准确度和效率； ③在企业范围内制定统一的安全策略标准，能结合具体使用场景，对各级数据进行安全授权，采用身份认证、访问控制、数据脱敏、加密、过滤等技术保证数据的隐私性，满足最小化授权要求； ④重点规范核心数据、重要数据的有效识别、重点保护和安全管理，能够刻画和动态监测数据全链路流转和访问现状，持续识别数据安全风险，及时响应处理，并定期汇总、分析数据安全问题，形成数据安全知识库	①定义了数据安全管理的考核指标和考核办法，并定期进行相关的考核； ②定期总结数据安全管理工作，在企业层面发布数据安全管理工作报告； ③能够持续量化评估数据安全策略的管控效果和安全偏差，建立数据安全生命周期的安全管理长效机制和防护措施	采用大数据和人工智能等技术对数据全链路流转进行刻画和动态监测，主动预防数据安全风险

表6 数据保护的成熟度要求（续）

能力项	1档	2档	3档	4档	5档
个人信息保护	<p>①对个人信息保护有基本的认知和了解,但尚未形成系统的管理体系和流程;</p> <p>②个人信息被简单地存储在未加密的数据库中,且访问控制机制较为松散</p>	<p>已经建立了基本的个人信息保护管理制度和流程,并开始采用一些基本的技术手段来提升个人信息的安全性。例如,实施了数据加密和访问控制机制,并对个人信息的收集、使用、存储和销毁等环节进行了规范</p>	<p>①建立了完善的个人信息保护体系;</p> <p>②建立了完善的个人信息安全应急响应机制,以应对可能发生的个人信息安全事件</p>	<p>利用先进的技术手段进行精细化管理,采用了大数据和人工智能等技术对个人信息安全风险进行持续预警和动态监控,及时发现和处理潜在风险</p>	<p>①在个人信息保护方面达到了行业领先水平,不仅具备强大的个人信息保护能力和完善的管理体系,还能够根据客户需求和业务变化灵活调整个人信息保护策略;</p> <p>②积极与业界和监管机构合作,交流个人信息保护的经验和做法,在行业内形成具有广泛影响力的最佳实践和标准</p>

7.4 数字化技术应用

7.4.1 技术架构转型

技术架构转型能力子域包含技术架构转型1个能力项。该能力项的成熟度分档要求,见表7。

表7 技术架构转型的成熟度要求

能力项	1档	2档	3档	4档	5档
技术架构转型	<p>①通过集成接口实现信息在不同系统间流转,接口开发由业务需求被动触发,尚未形成统一的接口标准和规范,定制化开发缺乏需求管理;</p> <p>②重要信息系统IT架构全部采用集中式架构</p>	<p>①信息系统IT架构兼具集中式与分布式,已建立统一的接口标准和规范,具备接口开发需求管理机制;</p> <p>②重要信息系统采用分布式架构占比小于30%</p>	<p>①已探索运用服务化、组件化设计的系统云原生技术架构,建成统一的、可扩展的、高可用的服务配置化架构原型,开始搭建证券场景通用的功能组件并面向传统架构系统提供服务;</p> <p>②10%以上的新建系统具备云原生特性;</p> <p>③重要信息系统采用分布式架构占比小于50%</p>	<p>①40%信息系统采用云原生技术架构,具备统一的开发框架、运行支撑、运维模式、安全能力,已实现服务配置化技术架构,对外提供平台化的应用程序接口和服务标准;</p> <p>②35%以上的新建系统具备云原生特性;</p> <p>③重要信息系统采用分布式架构占比小于80%</p>	<p>①60%以上信息系统采用服务化、组件化设计的云原生技术架构,具备统一的开发框架、运行支撑、运维模式、安全能力,已实现统一的、可扩展的、高可用的服务配置化技术架构,对外提供平台化的应用程序接口和服务标准,可基于应用系统在运行、运维过程中产生的一系列指标数据以及管控机制,提供面向业务的智能运营能力;</p> <p>②80%以上的新建系统具备云原生特性;</p> <p>③重要信息系统采用分布式架构占比不小于80%</p>
注:以上均包含本数。					

7.4.2 研发运营一体化

研发运营一体化能力子域包含研发运营一体化能力1个能力项。该能力项的成熟度分档要求,见表8。

表 8 研发运营一体化的成熟度要求

能力项	1档	2档	3档	4档	5档
研发运营一体化能力	研发运营过程依赖团队成员手工管理,源代码、制品、变更等配置信息分散,缺乏规范、自动化工具;无持续集成、持续部署服务;无自动化测试	研发运营过程在小范围内实现了自动化,源代码、制品、变更等配置统一管理;可按不同维度聚合管理业务容量,并进行基本的容量监控与告警;小范围实现持续集成、持续部署;测试自动化程度低;建立了环境管理机制;初步建立了度量驱动改进策略	在组织内大范围推行研发运营一体化实践,系统化配置管理和变更管理;根据不同运维对象的容量特征自定义容量计算方法;有专门团队持续集成标准化和自动化;测试高度左移;基于工具自动化的开发和测试环境;具有完善的度量指标系统和可视化报告	在组织内全面落地研发运营一体化,在深度规范化的前提下,建立了完善的配置管理和变更管理体系;持续集成实现自助化和服务化;部署和发布流程灵活编排,实现按需发布;具备常态化压测容量基线;建立了组织级统一的测试管理平台和测试左移实践;能够快速创建各类环境;建立了统一的数据度量平台和持续改进机制	在组织内全面形成持续优化和持续改进的文化,团队实现自我驱动的改变,资源配置更弹性,变更全程可追溯和全自动回滚;结合基础资源容量数据和业务容量数据,对容量进行预测;持续优化和改进构建平台、集成服务、自动化测试平台,提升组织交付能力;测试管理智能化;能弹性分配各类环境;实现智能化度量和改进,并基于大数据分析和人工智能等手段自动识别和推荐动态调整指标优先级

7.4.3 技术创新

技术创新能力子域包含前沿技术应用、自主创新、产学研用合作3个能力项。各能力项的成熟度分档要求,见表9。

表 9 技术创新的成熟度要求

能力项	1档	2档	3档	4档	5档
前沿技术应用	在前沿技术应用方面开始尝试应用人工智能等技术解决方案;已经实施了一些基本的前沿技术应用项目,但应用范围和深度有限	在前沿技术应用方面能够较为灵活运用人工智能等技术解决方案,能够开展复杂的前沿技术应用项目,探索前沿技术在业务中的应用潜力	在前沿技术应用方面能够推动人工智能等技术在业务中的深度融合和创新应用	在前沿技术应用方面具备综合应用能力,能够整合各方资源,构建系统化、整体化的前沿技术应用解决方案,能够展示前沿技术的综合应用实力,为业务发展提供全方位的技术支持和创新驱动	在前沿技术应用方面具备行业领先水平的应用能力,能够在行业范围内展示领先的人工智能等技术应用实力,能够引领金融科技发展,推动前沿技术在业务中的全面应用和创新
自主创新	①企业在系统自主可控方面具有基础创新能力,能够应对基本的网络和信息安全挑战; ②自研能力比率较低	①企业在系统自主可控方面具备一定的技术创新能力,能够开展较复杂的技术研究和创新; ②自研能力比率一般	①企业在系统自主可控方面具备前沿技术创新能力,能保障系统的自主性和可控性; ②自研能力比率较高	①企业在系统自主可控方面具备综合创新能力,能够整合各方资源,构建系统化、整体化的解决方案; ②自研能力比率高,	①企业在系统自主可控方面具备行业领先水平的创新能力,能够对行业发展产生深远影响,确保系统的自主性和可控性; ②自研能力比率达到行业

	<p>低,但已开始建立自主研发团队和流程,以提高系统自主可控的能力; ③企业能够掌握核心技术的基本要点,但需要进一步加强理解,对关键技术的深入理解,以确保系统的可控性</p>	<p>般,能够独立开发具有一定创新性的技术解决方案,以提升系统的自主性和可控性; ③企业已经开始在核心技术领域取得一定突破,能够应对日益复杂的安全挑战,确保系统的稳定性和安全性</p>	<p>高,能够独立开发前沿性的技术解决方案; ③企业在核心技术方面取得显著进展,能够应对未来技术挑战,确保系统的安全可控性</p>	<p>能够与合作伙伴共同推动技术的创新和应用,以提高系统的自主性和可控性; ③企业在核心技术掌握上达到了较高水平,能够为系统的安全性和可控性提供全面保障,确保系统在多方面的自主性</p>	<p>领先水平,能够在行业范围内独立开展具有行业影响力的技术研究和创新,以确保系统的领先地位; ③企业在核心技术掌握方面达到行业领先水平,能够引领行业发展方向,为公司和行业带来持续创新和展动力,确保系统在各方面的自主性</p>
--	---	--	---	---	---

表9 技术创新的成熟度要求（续）

能力项	1档	2档	3档	4档	5档
产学研用合作	尚未建立产学研用合作机制	已在个别领域探索开展产学研用合作	已建立产学研用合作机制与相关制度，已与高校、科研院所、头部企业等机构开展产学研用合作并有实践案例	已广泛参与核心技术金融应用前瞻性和战略性的研究与攻关，并有实践案例	已深度参与核心技术金融应用前瞻性和战略性的研究与攻关，并承担部分关键核心技术研究或在行业率先开展试点工作等

7.5 数字化基础设施建设

7.5.1 数据中心

数据中心能力子域包含资源能力建设、备份能力建设2个能力项。各能力项的成熟度分档要求，见表10。

表 10 数据中心的成熟度要求

能力项	1档	2档	3档	4档	5档
资源能力建设	基础资源能满足业务系统运行	基础资源能基本满足业务系统运行，并具备一定的扩展能力	已建设多地数据中心，各中心资源均满足相应功能定位需求且整体具备扩展能力	能充分利用各地差异化资源优化中心功能布局，整体上形成敏捷高效的数据中心资源架构	整体形成安全可靠、绿色节能、敏捷高效的数据中心布局
备份能力建设	①重要信息系统数据备份能力符合JR/T 0059—2010第二级要求； ②重要信息系统故障应对能力符合JR/T 0059—2010第二级要求	①重要信息系统数据备份能力符合JR/T 0059—2010第三级要求； ②重要信息系统故障应对能力符合JR/T 0059—2010第三级要求	①重要信息系统数据备份能力符合JR/T 0059—2010第四级要求； ②重要信息系统故障应对能力符合JR/T 0059—2010第四级要求	①重要信息系统数据备份能力符合JR/T 0059—2010第五级要求； ②重要信息系统故障应对能力符合JR/T 0059—2010第五级要求； ③重要信息系统灾难应对能力符合JR/T 0059—2010第五级要求	①重要信息系统数据备份能力符合JR/T 0059—2010第六级要求； ②重要信息系统故障应对能力符合JR/T 0059—2010第六级要求； ③重要信息系统灾难应对能力符合JR/T 0059—2010第六级要求； 重大灾难应对能力符合JR/T 0059—2010第六级要求

7.5.2 通信网络

通信网络能力子域包含承载能力建设1个能力项。该能力项的成熟度分档要求，见表11。

表 11 通信网络的成熟度要求

能力项	1档	2档	3档	4档	5档
承载能力建设	能够应用各种技术手段，实现网络资源池化，构建数据中心网络弹性承载能力，流量承载能力达到实际应用流量的110%	能够应用各种技术手段，实现网络资源池化、流量调度智能化，构建数据中心网络、广域网等区域弹性承载能力，流量承载能力达到实际应用流量的120%	能够应用各种技术手段，实现网络资源池化、流量调度智能化能力，构建数据中心网络、广域网、互联网等区域弹性承载能力，流量承载能力达到实际应用流量的150%	构建端到端弹性承载网络，范围可覆盖大部分业务，具备自动化伸缩能力，流量承载能力达到实际应用流量的200%	构建端到端弹性承载网络，范围可覆盖全国业务，具备自动化伸缩能力，流量承载能力达到实际应用流量的300%

7.5.3 云平台

云平台能力子域包含云化部署1个能力项。该能力项的成熟度分档要求，见表12。

表 12 云平台的成熟度要求

能力项	1档	2档	3档	4档	5档
云化部署	①云平台具备虚拟化资源池、自动化部署、高可靠、云管理平台等服务能力,在少量人工配合下,可以做到资源基本弹性伸缩; ②信息系统设施云化率在30%以下	①云平台支持容灾、数据备份、多云架构、云安全等能力,可以做到资源自动化弹性伸缩,无需人工干预; ②信息系统设施云化率在30%以上	①云平台支持容器化运行、基础中间件服务化、数据库服务化、中间件集成、日志和监控服务、一云多芯、云网协同等能力,可以做到资源在线弹性伸缩,伸缩过程对业务无影响; ②信息系统设施云化率在50%以上	①云平台支持开发运维一体化敏捷开发与运营能力、一体化运维运营能力,可以做到资源自动化弹性伸缩,伸缩模式丰富,支持不同的模式、策略定义基础资源的伸缩,伸缩过程对业务无影响; ②信息系统设施云化率在70%以上	①云平台支持多地多活能力; ②信息系统设施云化率在90%以上; ③围绕云化转型战略,设置云化组织、云化流程,以及跨领域产品实体化团队,制定相应考核措施
注: ①信息系统不包含核心交易系统。 ②以上均包含本数。					

7.6 网络和信息安全

7.6.1 安全管理

安全管理能力子域包含安全管理1个能力项。该能力项的成熟度分档要求，见表13。

表 13 安全管理的成熟度要求

能力项	1档	2档	3档	4档	5档
安全管理	在安全管理制度、安全管理机构、安全管理人员等方面至少符合JR/T 0060-2021规定的第二级标准要求的80%	在安全管理制度、安全管理机构、安全管理人员等方面至少符合JR/T 0060-2021规定的第二级标准要求的90%	在安全管理制度、安全管理机构、安全管理人员等方面至少符合JR/T 0060-2021规定的第三级标准要求的80%	在安全管理制度、安全管理机构、安全管理人员等方面至少符合JR/T 0060-2021规定的第三级标准要求的90%	在安全管理制度、安全管理机构、安全管理人员等方面完全符合JR/T 0060-2021规定的第三级标准要求

7.6.2 安全建设

安全建设能力子域包含安全建设1个能力项。该能力项的成熟度分档要求，见表14。

表 14 安全建设的成熟度要求

能力项	1档	2档	3档	4档	5档

安全建设	在定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面至少符合JR/T 0060-2021规定的第二级标准要求的80%	在定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面至少符合JR/T 0060-2021规定的第二级标准要求的90%	在定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面至少符合JR/T 0060-2021规定的第三级标准要求的80%	在定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面至少符合JR/T 0060-2021规定的第三级标准要求的90%	在定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面完全符合JR/T 0060-2021规定的第三级标准要求
------	--	--	--	--	--

7.6.3 安全运营

安全运营能力子域包含安全运营1个能力项。该能力项的成熟度分档要求，见表15。

表 15 安全运营的成熟度要求

能力项	1档	2档	3档	4档	5档
安全运营	在环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面至少符合JR/T 0060-2021规定的第二级标准要求的80%	在环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面能够至少符合JR/T 0060-2021规定的第二级标准要求的90%	在环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面至少符合JR/T 0060-2021规定的第三级标准要求的80%	在环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面至少符合JR/T 0060-2021规定的第三级标准要求的90%	在环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面完全符合JR/T0060-2021规定的第三级标准要求

7.7 经营管理数字化

7.7.1 数字化办公

数字化办公能力子域包含数字化办公能力建设1个能力项。该能力项的成熟度分档要求，见表16。

表 16 数字化办公的成熟度要求

能力项	1档	2档	3档	4档	5档
-----	----	----	----	----	----

数字化办公能力建设	<p>①建设文件管理、邮件管理、会议管理、人事管理、财务管理、采购管理等各种基于流程的办公系统；</p> <p>②经营管理模式基本为经验驱动型，各项活动由管理人员根据经验作出决策</p>	<p>①搭建综合性的办公自动化系统，实现门户、新闻管理、流程管理和审批、公文管理等主要办公场景的线上化；</p> <p>②经营管理模式转变为数据和经验相结合，部分领域初步具备利用数据辅助管理决策的能力</p>	<p>①基于统一的数字化办公平台入口，通过流程和数据打通，整合各办公管理系统，支持员工与客户、前台与后台、公司上下资源的信息连接；并提供移动办公平台，支持员工全天候、随时随地移动办公；</p> <p>②经营管理模式以数据驱动为主，主营业务范围内初步实现依托数据推动内部流程和外部服务优化</p>	<p>①结合企业主要岗位的工作特征和办公诉求，打造个性化的数字职场，提供差异化功能体验、内容推送，以精细化管理赋能业务。利用协作平台、云服务应用等，支持跨设备和地点的访问和协作，提升办公体验和协作效率；</p> <p>②经营管理模式为数据驱动型，形成管理驾驶舱等全局性的可视化管理工具，形成经营分析及绩效考核权威依据，为企业高层管理者提供业务洞察和决策支持</p>	<p>①利用大数据分析、AI和大模型等技术，基于多元化办公场景为员工提供智能助手，与智能化办公硬件设备融合，支持智能人机交互，为员工提供更加便捷、高效、协同的办公体验；</p> <p>②管理和经营模式为智能驱动型，升级管理驾驶舱，满足全面、深度、实时的经营管理需求，覆盖集团各部门，支持指标事前预警和业绩变动归因溯源，打通业财数据，指标实时展示赋能更高效、智能的经营管理决策</p>
-----------	---	--	---	--	---

7.7.2 数字化营销

数字化营销能力子域包含数字化营销能力建设1个能力项。该能力项的成熟度分档要求，见表17。

表 17 数字化营销的成熟度要求

能力项	1档	2档	3档	4档	5档
数字化营销能力建设	<p>形成数字化获客、活客、留客营销方案，并初步开展实践探索</p>	<p>①具备一定的线上获客能力；</p> <p>②具备一定的客户行为分析与活动运营能力，并通过营销活动提升客户活跃度；</p> <p>③具备一定的客户关系管理能力，尚未形成客群经营能力</p>	<p>①初步建成数字化营销平台，驱动营销获客向线上发展；</p> <p>②初步建立客户标签体系，能够较为精准地向客户推送金融信息与产品，具备多样化的活客手段；</p> <p>③建立客户关系管理体系，识别、经营重点客群</p>	<p>①持续完善数字化营销平台，实现多场景融合、多元化触达，初步具备规模化获客能力；</p> <p>②建立完善的客户标签体系，精准洞察客户需求，合理精准推送金融信息与产品；</p> <p>③建立客户分层分类管理体系和全方位客户画像，并开展精准服务，以客户为中心实现信息共享</p>	<p>①建成智能化营销平台，具备规模化、低成本的获客能力，赋能公司经营获客决策；</p> <p>②基于客户体验全流程开展精准营销和智能匹配，提供智能化、人性化营销服务；</p> <p>③建立客户全生命周期管理体系，具备精细化、智能化客户关系管理能力，客户粘性较强</p>

7.8 产品和服务数字化

7.8.1 渠道创新

渠道创新能力子域包含渠道创新1个能力项。该能力项的成熟度分档要求，见表18。

表 18 渠道创新的成熟度要求

能力项	1档	2档	3档	4档	5档
渠道创新	具备PC端和移动端等线上服务渠道，覆盖50%的产品和服务	能够采用5G消息、API等丰富线上服务渠道，线上服务渠道覆盖70%的产品和服务	已建立线上渠道综合金融服务平台，探索云网点和云工作室等创新渠道，能够通过线上唤起线下服务，线上服务渠道覆盖90%的产品和服务	具备金融开放、服务输出和融合能力，能够实现对第三方渠道有效对接，探索推进渠道云化转型，已具备云网点和云工作室等新型渠道，线上服务渠道全面覆盖产品和服务	渠道类应用系统基本实现云化升级，实现服务渠道多媒体化，各渠道服务交互体验良好，新产品和服务可以及时实现线上化办理
注：监管政策要求必须线下办理的产品和服务除外。					

7.8.2 流程重塑

流程重塑能力子域包含流程重塑1个能力项。该能力项的成熟度分档要求，见表19。

表 19 流程重塑的成熟度要求

能力项	1档	2档	3档	4档	5档
流程重塑	开始进行线上化建设，主要业务服务和内部协作流程基本实现线上化，线上化覆盖率达到30%	基本完成主要业务流程的线上化并开始应用自动化技术，业务流程线上化覆盖率达60%，业务流程中使用RPA等自动化技术，自动化覆盖率达到30%	实现大部分业务流程线上化，覆盖率达80%，能够规模使用RPA等自动化技术，自动化覆盖率达到50%	主要业务流程实现全面线上化，并进行流程优化以提升协作效率，能够使用人工智能技术构建业务智能化，70%以上关键业务环节实现自动化、智能化运用	能够成熟应用自动化和智能化等技术，实现业务流程各环节无缝对接、信息实时交互、资源高效协同，推动业务模式创新，自动化/智能化能够覆盖90%的业务处理领域
注：以上均包含本数。					

7.8.3 业务架构融合

业务架构融合能力子域包含业务架构融合1个能力项。该能力项的成熟度分档要求，见表20。

表 20 业务架构融合的成熟度要求

能力项	1档	2档	3档	4档	5档
业务架构融合	应用系统建设呈现烟囱式特点，以单独项目建设为主，信息和资源暂未实现有效共享和协同，尚未对业务模型统一规划	个别业务功能具备模块化、组件化能力，具有可配置的业务模版和业务流程，形成个别业务领域快速迭代创新的系统能力	基于部分业务场景、业务功能已搭建可复用的通用服务组件，可根据业务需求灵活配置业务模版和业务流程	建成企业级业务模型，搭建具备面向业务场景的可复用服务组件的业务架构，实现应用功能敏捷开发、业务模版和业务流程灵活配置，基本实现业务架构驱动企业级IT架构设计	采用企业级业务架构规划设计，企业级业务模型已涵盖主要业务领域，组件模版可灵活定制组装，业务与技术高度融合，业务产品服务快速迭代创新

7.9 内控体系数字化

7.9.1 合规管理

合规管理能力子域包含合规体系数字化1个能力项。该能力项的成熟度分档要求，见表21。

表 21 合规管理的成熟度要求

能力项	1档	2档	3档	4档	5档
合规体系数字化	初步建立合规信息收集机制,能够对主要监管规则、合规要求进行系统化、结构化、标准化的解析和处理	建立较为完备的合规信息收集机制,能够对各类合规相关数据进行系统化、结构化、标准化的解析和处理	能够对各类合规相关数据提取量化数据、禁止性条款、工作流程等需求指标,建立监管规则数据库	建立合规数据分析模型,可以对业务等数据进行全方位分析	能够基于规则数据库建立监管规则知识图谱,能够运用大数据、人工智能等技术,对客户交易行为监控、反洗钱管理等业务,提供更加快速、准确的合规管理

7.9.2 风险管理

风险管理能力子域包含新技术风险管理、风险体系数字化2个能力项。各能力项的成熟度分档要求,见表22。

表 22 风险管理的成熟度要求

能力项	1档	2档	3档	4档	5档
新技术风险管理	已初步形成新技术风险的识别和管理机制	能够通过开展新技术风险的测试和评估,有效识别风险并制定相应的防范和应急措施	能够基于相关标准规范运用技术手段对新技术风险进行监测评估和应急管理	能够对新技术风险进行事前、事中、事后的全生命周期管理,具备防范化解风险的能力	能够对新技术底层机理和风险形成原理开展研究,并通过综合运用数字化手段,化解依靠单一信息系统、单一风控技术无法有效应对的风险
风险体系数字化	开始汇聚内外部客户、业务、舆情,初步建立风险数据集市	初步建立风险管理相关系统,开始运用大数据、人工智能等数字技术,探索建立风控模型和算法模型	建设形成风险管理体系、风险预警系统,开始整合单风险系统,构建全面风控管理数字化平台	风控数字化平台整合完成所有风险系统,并具备风险态势感知、综合分析、实施预警等能力	风控数字化平台可以实现对客户、业务等各类风险的全面动态监测、智能研判预警,风险预警的覆盖率和有效率得到大幅提升

7.9.3 审计管理

审计管理能力子域包含审计体系数字化1个能力项。该能力项的成熟度分档要求,见表23。

表 23 审计管理的成熟度要求

能力项	1档	2档	3档	4档	5档
审计体系数字化	建设审计作业及管理系统,满足线下作业转向线上作业的需求,能够使审计项目实现全过程线上管理	开始搭建审计数据集市,开展审计模型建设,对审计工作提供一定的数据支撑	集合系统与数据,构建数字化审计工具或平台,与企业的财务、业务、运营等平台对接,引入外部政府公共数据、行业数据等形成审计数据集市	数字化审计工具或平台建设完成,具备监控、预警、自动化审计等功能,可以利用数字化审计工具或平台开展审计工作	利用数字化审计工具或平台实现业务全覆盖审计,实现持续性、敏捷性审计

7.10 可持续化发展基础

7.10.1 数字化标准建设

数字化标准建设能力子域包含标准制定1个能力项。该能力项的成熟度分档要求，见表24。

表 24 数字化标准建设的成熟度要求

能力项	1档	2档	3档	4档	5档
标准制定	近3年围绕金融科技领域建立了相应内部企业标准	近3年参与了2项以上金融科技领域相关国家标准/行业标准/团体标准制修订工作	近3年主导了2项以上金融科技领域相关国家标准/行业标准/团体标准制修订工作	近3年主导了4项以上金融科技领域相关国家标准/行业标准/团体标准制修订工作	近3年主导了1项以上金融科技领域相关国际标 准制修订工作
注：①“参与”表示该企业不是标准第一起草单位，“主导”表示该企业是标准第一起草单位。 ②以上均包含本数。					

7.10.2 数字化科研

数字化科研能力子域包含科研项目开展1个能力项。该能力项的成熟度分档要求，见表25。

表 25 数字化科研的成熟度要求

能力项	1档	2档	3档	4档	5档
科研项目开展	正在参与地区或行业有关组织开展的金融科技研究项目或金融科技创新试点项目	近3年参与了地区或行业有关组织开展的金融科技研究项目或金融科技创新试点项目，并全部通过验收	近3年牵头了不少于3项地区或行业有关组织开展的金融科技研究项目或金融科技创新试点项目，并全部通过验收	①近3年牵头了不少于6项地区或行业有关组织开展的金融科技研究项目或金融科技创新试点项目，全部通过验收； ②近3年至少参与了1项国家级金融科技项目或课题	①近3年牵头了不少于10项地区或行业有关组织开展的金融科技研究项目或金融科技创新试点项目，全部通过验收； ②近3年至少参与了2项国家级金融科技项目或课题，或牵头了国家级金融科技项目或课题
注：“牵头”表示该企业是项目第一完成单位，“参与”表示该企业非项目第一完成单位。					

7.10.3 数字化生态建设

数字化生态建设能力子域包含生态营造1个能力项。该能力项的成熟度分档要求，见表26。

表 26 数字化生态建设的成熟度要求

能力项	1档	2档	3档	4档	5档
生态营造	关注行业数字化生态建设，参加行业数字化建设研讨交流类活动	参与各类数字化联盟等组织建设，正在与供应链、产业链上下游探索开放合作的数字化生态建设发展机会	参与建设行业数字化开放共享平台，可以在数据、资源或业务等方面开展数字化生态建设相关合作	推动建设行业数字化开放共享平台，实现与供应链、产业链上下游的数据贯通、资源共享和业务协同	能够与合作伙伴共同建设完善的数字化生态体系

8 成熟度等级判定方法

8.1 评分方法

可通过统计、测评、访谈、调研等形式，掌握数字化转型取得的成果，将数字化能力现状与成熟度分档要求进行对照，客观地进行数字化能力成熟度定级。

8.2 评估权重

各能力域权重之和为1，权重可根据实际需要灵活调整，也可通过专家打分法等方式确定。

8.3 计算方法

能力项、能力子域、能力域以及总体得分计算方法如下：

——各能力项成熟度1档至5档对应1分至5分。证券公司应完全达到某能力项某档成熟度的全部要求，方可取得对应分数，如未完全满足1档要求，得0分。如同时满足不同档的部分能力，则不可得分；

——能力子域内各能力项的平均得分即为该能力子域得分；

——能力域内各能力子域的平均得分即为该能力域得分；

——各能力域的得分加权计算后，得出证券公司总体的数字化能力成熟度水平，具体按公式（1）计算：

$$M = \sum(\delta \times N) \dots\dots\dots (1)$$

式中：

N——能力域得分；

δ ——能力域权重；

M——总体得分。

8.4 成熟度等级判定方法

证券公司数字化能力总体得分所对应的成熟度等级见表27。

表 27 分数与等级的对应关系

成熟度等级	对应评分区间
五级（引领级）	4.5（含）-5分（含）
四级（优化级）	3.5（含）-4.5分
三级（发展级）	2.5（含）-3.5分
二级（基础级）	1.5（含）-2.5分
一级（萌芽级）	0-1.5分

参 考 文 献

- [1] GB/T 23011—2022 信息化和工业化融合 数字化转型 价值效益参考模型
 - [2] GB/T 33136—2016 信息技术服务 数据中心服务能力成熟度模型
 - [3] GB/T 35273—2020 信息安全技术个人信息安全规范
 - [4] GB/T 36073—2018 数据管理能力成熟度
 - [5] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
 - [6] GB/T 39116—2020 智能制造能力成熟度模型
 - [7] GB/T 39117—2020 智能制造能力成熟度评估方法
 - [8] GB/T 43439—2023 信息技术服务 数字化转型 成熟度模型与评估
 - [9] JR/T 0201—2020 金融科技发展指标
 - [10] JR/T 0218—2021 金融业数据能力建设指引
 - [11] T/AITRE 10001—2020 数字化转型 参考架构
 - [12] T/AITRE 10004—2023 数字化转型 成熟度模型
-

证券公司投资者个人信息保护技术规范

T/TSAC 001—2025

（经协会第七届理事会第三十九次会议审议通过，2025年9月25日发布实施）

（中证协发〔2025〕198号）

前 言

本文件按照GB/T1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中泰证券股份有限公司提出。

本文件由中国证券业协会归口。

本文件起草单位：中泰证券股份有限公司、财信证券股份有限公司、中国信息通信研究院、万联证券股份有限公司、国泰海通证券股份有限公司、腾讯科技（北京）有限公司、东北证券股份有限公司、国联民生证券股份有限公司、招商证券股份有限公司。

本文件主要起草人：张勇、张佳佳、李赛男、杨玲玲、王恩潭、孙文渊、陈杨、宁文卓、刘洋、熊嘉、黄志程、王健、秦维华、李奕、董延敏、马国文、张秀敏、马原、钟雪玲、杨曦、邓韬、杜楚逸、齐欢、梁叶、夏曼、郭恋、陶茜、马书原、李姣、韩冰。

引 言

证券公司因业务需要收集、使用投资者个人信息，给证券公司和客户业务办理带来便利的同时，也可能出现投资者个人信息的非法收集、篡改、滥用、泄露、丢失等问题，投资者个人信息安全面临一定风险。投资者个人信息一旦泄露，不仅会直接侵害投资者的合法权益、影响证券公司的正常运营，甚至可能会带来行业系统性金融风险。为加强证券公司投资者个人信息保护管理，指导证券公司规范处理投资者个人信息，最大程度保障投资者合法权益，维护金融市场稳定，编制本文件。

1 范围

本文件规定了证券公司投资者个人信息的保护要求，包含基本原则、投资者个人信息分类分级、投资者个人信息保护体系、投资者个人信息全生命周期保护要求、特定场景中的投资者个人信息保护、个人信息保护政策模板等。

本文件适用于证券公司以及其开展证券、期货、基金等业务的子公司在提供相关产品和服务的过程中开展投资者个人信息保护工作参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 35273—2020 信息安全技术 个人信息安全规范
GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
GB/T 25069—2022 信息安全技术 术语
GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求
GB/T 42574—2023 信息安全技术 个人信息处理中告知和同意的实施指南
GB/T 42775—2023 证券期货业数据安全风险防控 数据分类分级指引
GB/T 43697—2024 数据安全技术 数据分类分级规则
JR/T 0158—2018 证券期货业数据分类分级指引
JR/T 0171—2020 个人金融信息保护技术规范
JR/T 0250—2022 证券期货业数据安全管理与保护指引

3 术语和定义

GB/T 35273—2020 和 JR/T 0171—2020 界定的以及下列术语和定义适用于本文件。

3.1

投资者 investor

开展证券交易的自然人、法人、非法人组织，以及依法设立的金融产品。

3.2

个人信息 personal information

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.3

投资者个人信息 investors' personal information

投资者（3.1）所涉及的自然人的个人信息，不包括匿名化处理后的信息。

3.4

敏感个人信息 sensitive personal information

一旦泄露或者非法使用,容易导致自然人的尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。

注:具体参见附录A“敏感”标识为“是”的数据类别。

3.5

公开/公开披露 public disclosure

向社会或不特定群体发布信息的行为。

[来源: GB/T 35273—2020,3.11]

3.6

明示同意 explicit consent

投资者(3.1)通过书面声明或主动作出肯定性动作,对其个人信息进行特定处理作出明确授权的行为。

肯定性动作包括投资者主动作出声明(电子或纸质形式)、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

[来源: JR/T 0171—2020,3.22,有修改]

3.7

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

3.8

去标识化 de-identification

个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的过程。

注:去标识化建立在个体基础之上,保留了个体颗粒度,采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

3.9

鉴别 authentication

验证某一种实体所声称身份的过程。

[来源: GB/T 25069—2022,3.296]

3.10

单独同意 separate consent

个人针对其个人信息进行特定处理而专门作出具体、明确授权的行为,不包括一次性针对多种目的或方式的个人信息处理活动作出的同意。

注:单独同意的告知内容与取得同意的方式需与其他处理活动予以区分。

[来源：GB/T 42574—2023,3.7]

3.11

自动化决策 automated decision making

通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

3.12

用户画像 user profile

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

注：直接使用特定自然人的个人信息，形成该自然人的特征模型，称为直接用户画像。使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型，称为间接用户画像。

[来源：GB/T 35273—2020,3.8]

3.13

可识别 identifiable

仅凭某个信息本身无法识别出特定的自然人，但是只要将该等信息进行结合就可以识别出特定的自然人。即采用可能使用的手段、考虑所有客观因素，通过要素结合分析能识别到特定身份的可能。

3.14

汇聚融合 convergence

集成多个数据源以产生比任何单独数据源更有价值的过程，包括个人信息处理者内部不同业务线的数据“打通”实现共享、融合，以及集团内不同关联企业之间的数据融合。

3.15

提供 provide

个人信息处理者通过共享、转移等方式将个人信息传输或披露给其他个人信息处理者的行为。

注：委托第三方处理个人信息的，不属于向其他个人信息处理者提供个人信息的行为。

[来源：GB/T 42574—2023,3.8]

3.16

转让 transfer of control

将投资者个人信息控制权由一个控制者向另一个控制者转移的过程。

[来源：GB/T 42574—2023,3.12,有修改]

3.17

删除 delete

本指引所称“删除”是指在实现日常业务功能所涉及的系统或档案中除去个人信息的行为，使其保持不可被检索、访问的状态。删除所要实现的目的为保持个人信息不可通过任何形式被检索、访问，不包括删除前端数据但存于后端做访问限制的形式。

3.18

使用 use

个人信息的使用有广义和狭义之分，狭义的个人信息的使用不包括个人信息的存储、加工、传输、提供以及公开，仅指个人信息处理者对个人信息进行的分析和利用。

4 缩略语

IP：互联网协议（Internet Protocol）

SDK：软件开发工具包（Software Development Kit）

5 基本原则

证券公司在落实投资者个人信息保护有关要求时，应遵守有关法律法规和中国证监会的规定。

证券公司应以“权责一致、目的明确、告知同意、最小必要、分级保护、公开透明、确保安全、主体参与、确保质量”为原则，制定并实施覆盖投资者个人信息全生命周期的安全保护策略，具体包括：

- a) 权责一致：采取技术和其他必要的措施保障投资者个人信息的安全，对其个人信息处理活动对投资者合法权益造成的损害承担责任；
- b) 目的明确：具有正当、明确、清晰、具体的投资者个人信息处理目的；
- c) 告知同意：向投资者明示投资者个人信息处理目的、方式、范围等规则，取得其授权同意或具备处理投资者个人信息的其他合法性基础；
- d) 最小必要：只处理满足投资者授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时按照相关法律法规相关规定处理投资者个人信息。建议证券公司遵循具体业务规则，根据具体业务需要，严格执行最小必要原则处理投资者个人信息；
- e) 分级保护：结合证券公司自身数据管理需要，依据投资者个人信息的数据类型、敏感程度等差异，划分不同的数据安全层级，采取针对性的安全保护措施。应当按照投资者个人信息的不同安全级别进行分级别安全防护，安全层级越高的数据应当采用更严格的防护措施；
- f) 公开透明：以明确、易懂和合理的方式公开处理投资者个人信息的范围、目的、规则等，并接受外部监督；
- g) 确保安全：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性；
- h) 主体参与：向投资者提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法；
- i) 确保质量：保证所处理的个人信息的质量，避免因为个人信息的不准确、不完整对个人权益造成不利影响。

6 投资者个人信息分类分级

6.1 概述

证券公司应遵循 JR/T 0158—2018 的要求，根据证券公司各自情况对投资者个人信息进行分类分级，可参考附录 A。

6.2 证券公司投资者个人信息内容及分类

证券公司应遵循系统性、规范性、稳定性、明确性、扩展性原则对投资者个人信息进行分类。

证券公司投资者个人信息包括投资者个人基本信息、身份信息、鉴别信息、账户信息、交易信息、财产信息、信用信息、合约信息、行为信息、衍生信息、设备信息、位置信息和其他反映特定投资者个人信息主体某些情况的信息，具体如下：

- a) 投资者个人基本信息指参与证券期货市场业务活动的自然人、法人、非法人组织、依法设立的金融产品涉及的自然人个人基本信息，包含姓名、性别、民族、出生日期、年龄、联系地址、移动电话、电子邮件、国籍等信息；
- b) 投资者个人身份信息是指参与证券期货市场业务活动的自然人、法人、非法人组织、依法设立的金融产品涉及的自然人身份信息，包含个人身份证件信息、个人特定身份信息，个人身份证件信息包括投资者个人证件类型、证件号码、证件地址、证件有效期、签发机关等；个人特定身份信息指残障人士身份信息、犯罪人员身份信息、特定工作信息（如军人、警察）等；
- c) 投资者个人鉴别信息指投资者的账户认证信息和个人生物识别信息，账户认证信息包含账户密码、数字证书、动态口令、口令保护答案、短信验证码等信息，个人生物识别信息包括指纹认证信息、人脸认证信息等；
- d) 投资者个人账户信息包括开户/账户信息、投资者编码信息。开户/账户信息指投资者与业务活动相关的识别信息，包含账户名称、投资者标识、账户类别、证券账户编码、账户用途、账户状态代码等信息，投资者编码指投资者在证券公司的内部统一编码；
- e) 投资者个人交易信息指投资者在参与证券期货市场交易活动中产生的各类信息，包括但不限于成交信息、委托信息、银证转账、交易业务参数信息、交易日志信息以及有关规定要求的反映交易真实情况的合同、业务凭证、单据、业务函件和其他资料；
- f) 投资者个人财产信息指证券公司在提供金融产品和服务过程中，收集或生成的投资者个人财产信息，包括但不限于持仓信息、银行账务信息、资金状况信息、资金账户金额、个人收入状况等；
- g) 投资者个人信用信息指投资者的信用相关信息，包含账户编码、信用等级、信用额度、融资融券偿还情况以及投资者在交易活动中形成的，能够反映其信用状况的其他信息；
- h) 投资者个人合约信息指参与交易活动所产生的契约信息。包含账户编码、流水号、合同号、市场代码、证券代码、证券数量、发生金额、归还日期等；
- i) 投资者个人行为信息指在开展业务或参与交易等活动中记录下来的投资者行为过程数据，包含投资者在 App、网站中的行为信息，操作日志等；
- j) 投资者衍生信息指对投资者交易及行为数据进行处理、分析所形成的反映特定投资者某些情况的信息，包含投资者分类、投资能力、投资意愿、行为习惯、兴趣偏好等；
- k) 投资者个人设备信息指投资者个人在证券公司提供产品或服务过程中使用的设备信息，包括但不限于硬件序列号、设备 MAC 地址、唯一设备识别码（如 IMEI/Android

ID/IDFA/Open UDID/GUID/SIM 卡 IMSI 信息等)、机型、系统版本、存储位置、应用软件列表等在内的描述个人常用设备基本情况的信息;

- l) 投资者个人位置信息指投资者个人粗略位置信息、精准定位信息、经纬度等。

6.3 证券公司投资者个人信息的分级

证券公司应依据依从性、可执行性、时效性、自主性、合理性、客观性原则对投资者个人信息进行分级。

证券公司应根据个人信息的安全性(保密性、完整性、可用性等)遭受破坏后的影响和危害大小,将投资者个人信息从高到低分为4级、3级、2级、1级四个级别:

- a) 4级主要指用于大型或特大型行业机构中的重要业务,一般针对特定人员公开,且仅为必要知悉的对象访问或使用的投资者个人信息。主要包括投资者鉴别信息。该类信息一旦遭到未经授权的查看、变更或者破坏,会对投资者个人信息安全与财产安全造成特别严重危害;
- b) 3级主要指用于重要业务,针对特定人员公开,且仅为必要知悉的对象访问或使用的投资者个人信息。主要包括投资者个人身份信息与财产信息,以及用于相关产品与服务的关键信息。该类信息一旦遭到未经授权的查看、变更或者破坏,会对投资者的信息安全与财产安全造成严重危害;
- c) 2级主要指用于一般业务,针对受限对象公开且不宜广泛公开的投资者个人信息。该类信息一旦遭到未经授权的查看、变更或者破坏,会对投资者的信息安全与财产安全造成一般危害;
- d) 1级主要指可被公开或可被公众获知、使用的投资者个人信息。该类信息一旦遭到未经授权的查看、变更或者破坏,不会对投资者的信息安全与财产安全造成实质危害。

投资者敏感个人信息一般定义为3级及以上。上述两种或两种以上的低敏感程度信息经过组合、关联和分析后可能产生高敏感程度的信息,宜参照高敏感程度信息进行安全防护。同一信息在不同的服务场景中可能处于不同的级别,可依据服务场景以及该信息在其中的作用对信息的类别进行识别和定级,并实施针对性的保护措施。

7 证券公司投资者个人信息保护体系

证券公司处理投资者个人信息,应当建立健全投资者个人信息保护体系,明确相关岗位及职责要求,建立健全投资者个人信息处理、安全防护、应急处置、审计监督等管理机制,加强投资者个人信息保护。

7.1 建立健全内控制度体系

证券公司应建立投资者个人信息保护制度体系,明确工作职责,规范工作流程。制度体系的管理范畴需要涵盖本机构、外包服务机构与外部合作机构,确保相关制度发布、传达给本机构员工,并确保可落地执行。相关制度包括但不限于投资者个人信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案。具体要求如下:

- a) 制定覆盖投资者个人信息保护全过程的管理制度,提出本机构投资者个人信息保护工作方针、目标和原则;
- b) 开展投资者个人信息分类分级管理,针对不同类别、级别的投资者个人信息,实施相应的安全策略和保障措施;

- c) 建立日常管理及操作流程,对投资者个人信息的收集、存储、使用、加工、传输、提供、公开、删除等环节提出具体保护要求,制定投资者个人信息时效性管理规程,确保符合所在国家或地区法律法规有关规定;
- d) 建立投资者个人信息脱敏管理规范 and 制度,明确不同类别、级别的投资者个人信息脱敏规则、脱敏方法和脱敏数据的使用限制;
- e) 制定并公开投资者个人信息处理规则,明确告知投资者个人信息处理目的、处理方式、处理投资者个人信息种类、保存期限等内容;
- f) 制定外包服务机构与外部合作机构管理制度,内容包括但不限于:
 - 1) 应自行对外包服务机构与外部合作机构的个人信息保护能力进行审查,或要求对方提供第三方评估认证机构证明其个人信息保护能力符合相关标准的评估证书,以评估其个人信息的保护能力是否达到国家个人信息保护主管监管部门、证券期货行业主管部门以及金融监督管理部门的要求;
 - 2) 对外包服务机构与外部合作机构明确其在投资者个人信息安全保护能力、定期审查、留存信息、保密责任等方面的要求,根据要求落实控制措施,并将资料留档备查;
 - 3) 对可能访问投资者个人信息的外包服务机构、外部合作机构及其人员,证券公司应要求外包服务机构与外部合作机构向有关人员传达投资者个人信息保护要求,与其签署保密协议;
 - 4) 为防范因外包人员因素导致的信息泄露风险,原则上对于外包人员接触投资者敏感个人信息的情况,要求其在现场办公,并明确规定不得复制敏感信息或将敏感信息带离现场;对于非现场办公的情形,应加强对外包人员的操作监督,定期对外包人员查询、复制、导出、下载敏感个人信息等操作行为进行审计;
 - 5) 应定期对外包服务机构、外部合作机构的投资者个人信息保护措施落实情况进行确认,确认的方式包括但不限于外部信息安全评估、现场检查等。
- g) 建立投资者个人信息安全检查及监督机制,包括投资者个人信息安全日常检查机制和 workflows 等,必要时可将个人信息相关合规及安全事件纳入公司内部的奖惩管理办法和要求中;
- h) 将投资者个人信息泄露等相关事件处理纳入机构网络安全事件应急处置工作机制,明确应急处置流程和预案,定期评估应急处置流程和预案的有效性,及时保障、有效应对投资者个人信息网络安全事件,降低网络安全事件造成的损失和不利影响;
- i) 建立健全内部检查问责机制,根据检查结果,及时组织调查,完成问题整改,追究问题责任;
- j) 建立投资者个人信息投诉与申诉处理程序,明确投诉与申诉受理部门、处理程序,对投资者要求更正或删除证券公司收集其个人信息的情况,及时受理、核实,并依据法律或证券期货行业主管部门的要求予以处理;
- k) 建立投资者个人信息保护意见反馈机制,意见反馈渠道可参照投诉与申诉处理程序;
- l) 根据公司实际情况,在管理制度或投资者个人信息处理规则中细化投资者个人信息共享、存储、使用和销毁的期限,具备投资者个人信息存储时效性的控制能力;
- m) 对投资者个人信息保护相关管理制度进行定期的评审与修订,确保可以应对最新的安全威胁与风险。

7.2 组织架构及岗位设置

组织架构及岗位设置具体要求如下:

- a) 建立健全投资者个人信息保护组织架构,明确机构各层级内设部门与相关岗位投资者个人信息总体要求与保护职责,形成相互监督相互制约的管理机制;
- b) 应指定投资者个人信息保护负责人,负责对个人信息处理活动以及采取的保护措施进行监督。除法律法规和中国证监会另有规定外,可由合规总监、首席风险官等兼任投资者个人信息保护负责人;
- c) 明确机构内部投资者个人信息保护的牵头组织机构,并组织或监督内部相关责任机构根据职责分工履行以下工作职责:
 - 1) 制定、修订投资者个人信息保护管理制度;
 - 2) 开展投资者个人信息分类分级管理,针对不同级别和敏感程度的投资者个人信息,制定相应的安全策略和保障措施;
 - 3) 建立投资者个人信息脱敏管理规范或制度,明确投资者个人信息脱敏规则、脱敏方法等;
 - 4) 组织 App 客户端等金融产品或服务上线或重大变更前安全检测,避免未知的不当行为,包括与国家法律法规、证券行业监管要求不符,或存在潜在威胁等,并对发现的风险及时进行整改加固;
 - 5) 建立投资者个人信息安全检查及监督机制,定期评估个人信息管理方面存在的不足,并及时调整检查机制和工作流程;
 - 6) 监督本机构内部,以及本机构与外部合作方投资者个人信息保护安全管理;
 - 7) 开展投资者个人信息保护影响评估,处置发现的安全风险,提出投资者个人信息保护的对策;
 - 8) 将投资者个人信息安全事件纳入数据安全事件应急处置工作机制,制定有关应急预案;
 - 9) 投资者个人信息安全事件相关的分析、处置及内外部报告等工作,提出投资者个人信息保护的对策建议;
 - 10) 开展投资者个人信息保护培训与意识教育活动,并保留相关记录;
 - 11) 与监管、管理部门保持沟通,通报或报告个人信息保护和事件处置等情况。
- d) 明确在提供金融产品和服务的相关过程中知悉投资者个人信息的岗位,并针对相关岗位明确其投资者个人信息安全管理责任与保密责任。

7.3 人员管理

对涉及投资者个人信息相关人员的安全管理,具体要求如下:

- a) 录用员工前,应进行必要的背景调查,如除了常规的背调外,可进一步核查是否发生过个人信息违法违规事件,并与所有可访问投资者个人信息的员工签署保密协议,或者在劳动合同中设置保密条款;
- b) 在发生人员调离岗位或终止劳动合同时,立即调整并完成相关人员的投资者个人信息访问、使用等权限的配置,并明确有关人员后续的投资者个人信息保护管理权限和保密责任;若有关人员调整后的岗位不涉及投资者个人信息的访问与处理的,明确其继续履行有关信息的保密义务要求;
- c) 在个人信息保护政策、个人信息保护相关法律法规、行业规范发生重大变化时,对投资者个人信息处理岗位上的相关人员开展投资者个人信息安全专业化培训和考核,确保相关人员熟练掌握个人信息保护政策和相关规程。

7.4 安全防护技术要求和措施

证券公司应根据国家与证券期货行业主管部门的要求,加强投资者个人信息安全技术能

力建设，落实必要的管理和技术措施，防止投资者个人信息的泄露、损毁、丢失及篡改。可采取包括但不限于以下安全技术要求和措施：

- a) 信息管理流程：完善投资者信息收集、存储、使用、加工、传输、提供、公开、删除等全生命周期管理流程；
- b) 数据分类分级管理：开展投资者个人信息分类分级管理，针对不同级别和敏感程度的投资者个人信息，实施相应的安全策略和保障措施；
- c) 信息技术系统建设：可采取网络隔离、用户鉴别、数据加密、数据备份、数据销毁、病毒防范、非法入侵检测等安全技术措施，确保信息技术系统的安全性。并采取异常流量监测、用户行为分析等技术措施对投资者个人信息进行风险识别和监测；
- d) 数据传输控制措施：可采取传输途径和存储介质的安全管理，系统权限分级授权，数据加密等安全控制措施；
- e) 数据存储控制措施：可采取数据库加密、数据库防火墙、数据库运维管理、数据审计、数据库脱敏等安全控制措施；
- f) 数据展示控制措施：可通过增加桌面水印的方式，控制操作人员通过截屏/拍照的方式获取投资者敏感个人信息。

7.5 访问控制

为避免发生投资者个人信息泄露和未经授权的访问，控制投资者个人信息使用过程中的各项风险，证券公司应加强投资者个人信息的访问控制管理，具体要求如下：

- a) 对于可访问和处理投资者个人信息的系统，根据“最小必要”原则，设置访问控制策略，严格控制和分配访问、使用投资者个人信息，且仅具备完成职责所需的最少数据操作权限，权限申请经审批后方可进行分配；禁止账户共用；
- b) 传输、处理、存储投资者个人信息的系统默认用户权限应为“拒绝所有访问”；
- c) 对投资者个人信息使用的权限管理应设置权限指派、回收、超期删除等安全功能；
- d) 对存储或处理投资者个人信息的系统或设备进行远程访问时，应当采取数据脱敏、数据加密等措施，防范化解投资者个人信息在处理过程中的泄露风险，应对能通过互联网远程方式（如 VPN）访问的涉及投资者个人信息的系统增加限制，如限制通过报备或绑定 MAC 地址的电脑访问，减少因账号密码泄露造成的个人信息安全风险；
- e) 对生产网络、开发测试网络、办公网络以及相关非生产网络进行访问控制；
- f) 对投资者个人信息访问与投资者个人信息的增删改查等操作进行记录，并保证操作日志的完整性、可用性、可追溯性；系统运维管理类日志不应记录投资者个人信息；
- g) 对存储投资者个人信息的数据库及操作日志实施严格的用户授权与访问控制；
- h) 对个人信息的重要操作设置内部审批流程，如进行批量修改、拷贝、下载等重要操作；
- i) 对安全管理人员、数据操作人员、审计人员的角色进行分离设置；
- j) 确因工作需要，需授权特定人员超权限处理个人信息的，经个人信息保护责任人或个人信息保护工作机构进行审批，并记录在册；
- k) 对投资者敏感个人信息的访问、修改等操作行为，应在对角色权限控制的基础上，按照业务流程的需求触发操作授权。例如，当收到投资者投诉时，投诉处理人员才可访问该投资者的个人信息。

7.6 投资者个人信息保护影响评估

- a) 定义：针对投资者个人信息处理活动，检验其合法合规程度，判断其对投资者合法

权益造成损害的各种风险,以及评估用于保护投资者个人信息各项措施有效性的过程;

- b) 责任部门:证券公司应指定个人信息保护影响评估的责任部门、特别工作小组或第三方机构,对评估工作流程的制定、实施、改进以及评估结果负责。该责任部门、特别工作小组或第三方机构应具有独立性,不受被评估方的影响。可进一步采取流程嵌入或纳入奖惩机制等方式,保障影响评估有效开展、评估覆盖范围的完整性等;
- c) 适用条件:投资者个人信息保护影响评估的应用场景包括但不限于:
 - 1) 国家法律法规规定的应当事前进行个人信息保护影响评估的情形:处理敏感个人信息的、利用个人信息进行自动化决策的、委托处理个人信息向其他机构提供个人信息的、公开个人信息的、向境外提供个人信息的、以及其他对个人权益有重大影响的个人信息处理活动;
 - 2) 法律法规、政策、标准等出现重大变化时重新评估;
 - 3) 业务模式、互联网安全环境、外部环境等发生重大变化的重新评估;
 - 4) 发生重大投资者个人信息安全事件后重新评估;
 - 5) 发生收购、兼并、重组等情形开展评估;
 - 6) 新产品或新服务(不限于技术平台)需求设计阶段评估;
 - 7) 新产品或新服务(不限于技术平台)上线初次评估;
 - 8) 产品或服务在运营过程中发生与投资者个人信息保护相关的重大变更时,需重新开展投资者个人信息保护影响评估;
 - 9) 产品或服务的年度整体评估等。
- d) 评估内容:投资者个人信息的处理目的、处理方式等是否合法、正当、必要;对投资者个人权益的影响及安全风险;所采取的保护措施是否合法、有效并与风险程度相适应;
- e) 评估方式:评估实施过程中采用的基本评估方法,包括但不限于访谈、检查和测试;
- f) 评估程序:开展评估前,需对待评估的对象进行全面调研,形成清晰的数据清单及数据映射图表,并梳理出待评估的具体的个人信息处理活动。开展评估时,通过分析个人信息处理活动对投资者的权益可能造成的影响及其程度,以及分析安全措施是否有效,是否会导致安全事件发生及其可能性,综合两方面结果得出个人信息处理活动的风险及风险等级,并提出相应的改进,形成评估报告;
- g) 评估报告:评估报告的内容通常包括审批页面、评估报告适用范围、实施评估及撰写报告的人员信息、参考的法律、法规和标准、投资者个人信息影响评估对象、评估内容、涉及的相关方等,以及投资者个人权益影响分析结果,安全保护措施分析结果、安全事件发生的可能性分析结果、风险判定的准则、合规性分析结果、风险分析过程及综合评估结果、风险处置等;
- h) 投资者个人信息保护影响评估报告和处理情况记录应当至少保存三年。

7.7 监控

监控具体要求如下:

- a) 识别并记录相关人员(如管理员用户、业务用户)对投资者个人信息的访问;
- b) 对投资者个人信息数据交换网络流量进行安全监控和分析,并存储匹配安全规则的数据,以备事件溯源;
- c) 采取技术手段对投资者个人信息全生命周期进行安全风险识别和管控;
- d) 通过技术手段建立投资者个人信息泄露监控预警机制,及时发现信息泄露事件。

7.8 投资者个人信息安全事件处置

安全事件处置具体要求如下：

- a) 制定投资者个人信息安全事件应急预案，明确安全事件处置流程和岗位职责；
- b) 定期组织内部相关人员进行投资者个人信息保护应急预案相关培训和应急演练；
- c) 发现因系统漏洞或人为原因造成投资者个人信息遗失、损毁、泄露或被篡改等安全类事件后，及时采取必要措施进行处置，控制事态发展，消除安全隐患，并及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的投资者；难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息；证券公司及时采取措施后能够有效避免信息泄露、篡改、丢失造成危害的，可以不通知个人；
- d) 发现其他机构、个人违规存储或使用投资者个人信息的，应当排查数据泄露途径、评估影响范围，采取合理可行的整改措施，及时处置风险隐患，并按照中国证监会规定履行报告和调查处理职责。
- e) 发现信息技术服务机构等相关方违规存储或者使用投资者个人信息的，应当责令其立即改正并销毁已获取的信息；信息技术服务机构等相关方拒绝配合整改的，应当立即停止与其合作，并采取措施维护自身及投资者的合法权益。
- f) 记录事件内容，分析和鉴定事件产生的原因，评估事件可能造成的影响，制定补救措施，并向国家个人信息保护主管部门以及证券期货行业主管部门进行报告；
- g) 建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应；
- h) 采取有效措施开展舆情动态监测，持续跟踪舆情变化，对涉及公司投资者个人信息保护的舆情案件及时研判并报告，并适时进行应急处置；
- i) 根据相关法律法规的变化情况以及事件处置情况，及时更新应急预案。

7.9 安全教育与培训

安全教育与培训的要求包括但不限于：

- a) 文化宣导：应加强投资者个人信息保护宣传与教育，应每年至少一次或个人信息保护政策、个人信息保护相关法律法规、行业规范发生重大变化时开展全员投资者个人信息安全教育活动，提升员工个人信息保护意识；
- b) 应在金融产品或服务提供过程中，通过开展投资者讲堂、报告会、座谈会以及利用投资者回访、网站、App 等方式开展投资者教育和宣传：
 - 1) 明确告知投资者国家法律法规等所提供的相关权利与义务；
 - 2) 提升投资者对业务中所涉及的个人信息处理工作的基本认识；
 - 3) 增强投资者对个人信息保护的总体意识，妥善保护个人身份资料、账户信息等。
- c) 应定期(至少每年一次)或在个人信息保护政策发生重大变化时，对个人信息处理岗位上的相关人员开展个人信息安全专业化培训和考核，确保相关人员熟练掌握个人信息保护政策和相关规程：
 - 1) 投资者个人信息安全保护工作相关监管动态和处罚；
 - 2) 最新的法律法规变化；
 - 3) 引导员工正确有效遵守证券公司关于投资者信息保护的工作原则和要求；
 - 4) 提升员工对于做好投资者个人信息保护工作是树立证券公司良好声誉的重要部分的意识。
- d) 证券公司应结合行业文化建设，健全投资者个人信息保护的合规文化，通过文化建设凝聚投资者、员工以及第三方服务作机构的合力和共识，形成自觉保护投资者个

人信息的一致认识并在工作中自觉执行。

7.10 第三方服务机构管理

除法律法规和中国证监会另有规定外,证券公司不得允许或者配合其他机构、个人截取、留存客户信息,不得以任何方式向其他机构、个人提供未经匿名化处理的投资者个人信息。

证券公司应当记录投资者个人信息的使用情况,并持续监督第三方服务机构(包括外包服务机构与外部合作机构)等相关方落实保密协议的情况。

证券公司将收集的投资者个人信息传输、共享、委托给第三方服务机构(包括外包服务机构与外部合作机构)处理时,应遵循如下要求:

- a) 准入要求:应建立第三方服务机构的准入条件,并通过合同等方式约定证券公司与第三方服务机构的权利和义务;
- b) 投资者信息保护能力评估:应对第三方服务机构进行评估或要求其提供评估报告,确保第三方服务机构具备足够的信息安全能力,且提供了足够的安全保护措施;
- c) 事中监控:应对外部嵌入或接入的自动化工具(如代码、脚本、接口、算法模型、软件开发工具包等)开展技术检测,确保其投资者个人信息收集、使用行为符合约定要求;并根据合同约定对其处理投资者个人信息的行为进行监督和审计,发现超出约定行为且对客户个人信息安全产生影响的,应视后果的严重程度应及时切断接入或通知第三方服务机构在规定的时间内进行整改;
- d) 事后处置:在委托关系解除或外包服务终止时,第三方服务机构应按要求销毁其处理的投资者个人信息,并依据双方协商的期限承担后续的投资者个人信息保护责任;
- e) 第三方服务机构转委托时,应当事先取得证券公司同意。

7.11 审计监督

证券公司应根据国家法律法规相关规定,定期对其投资者个人信息处理活动遵守法律、行政法规等情况开展合规审计,具体要求如下:

- a) 明确内部开展个人信息保护合规审计的责任部门、审计工作流程、审计频率等内容,形成合规审计报告,并根据审计结果进行整改跟踪,促进个人信息内部合规管理制度、流程的完善;
- b) 委托外部专业机构开展合规审计,应当与外部专业机构签订保密协议,要求外部专业机构人员对在审计过程中所知悉的信息进行保密。

8 投资者个人信息全生命周期保护基本要求

8.1 基本要求

证券公司应当遵循合法、正当、必要和诚信原则,在收集、存储、使用、加工、传输、提供、公开、删除等个人信息全生命周期过程处理投资者个人信息,规范投资者个人信息处理行为,履行投资者个人信息保护义务,不得损害投资者合法权益。并建立健全投资者个人信息处理、安全防护、应急处理、审计监督等管理机制,加强投资者个人信息保护,防止个人信息泄露、篡改、丢失。

本章节中有关保护措施未明确具体级别的,一般是指2级及以上的投资者个人信息。

证券公司在处理投资者个人信息前,应向投资者充分履行告知义务,取得投资者的同意。符合以下情形之一的,证券公司无需取得投资者个人同意:

- a) 为订立、履行投资者作为一方当事人的合同所必需,或为维护所提供的产品和服务

- 的安全、稳定运行所必需，处理必要的投资者个人信息；
- b) 履行法定职责或者法定义务所必需的个人信息处理活动，包括但不限于：履行反洗钱、反恐怖融资、反诈等监管要求；履行投资者适当性管理义务；根据法律法规规定配合执法或司法机关要求；与履行国家法律法规和行业主管部门、行业自律组织有关规定的义务相关的；与国家安全、国防安全直接相关，或与犯罪侦查、起诉、审判和判决执行或国家机关及有权机构协查等直接相关的；
 - c) 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；
 - d) 为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；
 - e) 依照国家法律法规规定在合理的范围内处理投资者个人自行公开或者其他已经合法公开的个人信息，包括但不限于：新闻媒体公开报道的信息；司法、行政机关依据法定职责向社会公众公布的信息；个人自行公开且已知悉或应当知悉可被不特定用户访问的个人信息；
 - f) 出于维护投资者或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；
 - g) 法律、行政法规规定的其他情形。

8.2 收集

8.2.1 投资者个人信息收集的基本要求

8.2.1.1 投资者个人信息收集的情形

证券公司收集投资者个人信息的情形包括但不限于：

- a) 提供服务或产品时通过投资者个人填写、勾选、上传等方式收集个人信息；
- b) 按照《证券公司客户交易终端信息管理技术规范》确定的交易终端设备的类型，采集投资者交易终端信息，包括但不限于互联网通讯协议地址（IP 地址）、媒介访问控制地址（MAC 地址）以及其他能识别客户交易终端的特征代码；
- c) 通过证券公司 App、摄像头等软件程序或硬件设备自动采集投资者个人信息；
- d) 证券公司及其工作人员与投资者交互并记录其个人的行为；
- e) 从第三方间接获取投资者个人信息；
- f) 从非完全公开渠道获取投资者个人信息；
- g) 使用大数据、人工智能等技术分析、关联或生成投资者个人信息。

8.2.1.2 收集的基本原则

证券公司收集投资者个人信息需要遵循合法、正当、必要和诚信原则，并满足以下要求：

- a) 不得通过误导、欺诈、胁迫等方式非法采集投资者个人信息；
- b) 不得隐瞒产品或服务所具有的收集投资者个人信息的功能；
- c) 不得违法或过度收集投资者个人信息，或者擅自变更处理目的、范围和方式；
- d) 合同约定收集范围、种类应当基于从事证券业务活动的必要限度。

8.2.1.3 合法性之告知

证券公司应当按照法律法规的规定及合同约定收集投资者个人信息，明确告知投资者处理个人信息的目的、方式、范围和投资者个人信息保护政策，在实施告知时注意：

- a) 遵守公开透明、有效传达、适时充分、真实明确、清晰易懂的原则，不采用隐藏、故意遮挡等方式诱导投资者略过告知内容，不使用笼统、宽泛的表述；

- b) 需结合产品或服务的业务功能特点,选择适当的方式(如一般告知、增强告知、即时提示等)或多种告知方式的组合,友好展示,兼顾差异;

注:一般告知通常采用制定、展示个人信息保护政策的形式进行告知;增强告知系将个人信息处理规则中的关键内容或与特定业务功能处理目的相关的关键规则单独提炼并告知;即时提示系为进一步强化投资者对收集个人信息目的的理解或辅助投资者对个人信息处理规则的理解,证券公司结合产品或服务特点选择如使用弹窗、浮窗或浮层、文字说明、状态栏提示、提示条、提示音、短消息等方式及时、有效传达告知内容。

- c) 可以公开且便于查询的方式展示投资者个人信息保护政策(或被称为“隐私协议”“隐私政策”“隐私权政策”等),尽可能全面、清晰的阐述个人信息处理规则;

注:个人信息保护政策的具体内容可参见附录C。

- d) 在交互式界面中,将投资者个人信息保护政策完整内容置于产品或服务的基本业务功能开启之前,以弹窗提示、提醒勾选、突出链接等明显方式,引导投资者查阅个人信息保护政策/个人信息处理规则,避免隐私政策等收集使用规则难以访问,如进入App主界面后需多于4次点击等操作才能访问到。无法实现交互式界面展示的,可以发送通知、邮件、提供文档、张贴告示、播放音视频等方式向投资者主动提供或展示;
- e) 因产品或服务处理个人信息活动发生变更后更新个人信息保护政策的,可在个人再次使用产品或服务时,使用增强告知或即时提示的方式告知个人信息保护政策中更新的内容。

8.2.1.4 合法性之同意

证券公司收集投资者个人信息依法应当取得个人同意的,应当确保投资者在充分知情的前提下自愿、明确作出同意:

- a) 不使用默认勾选方式取得同意;
- b) 不采用捆绑方式强迫投资者一次性同意多种业务功能可能收集的个人信息或多个处理活动;
- c) 应使用可广泛适用且兼顾特定群体的同意方案,对于线上办理业务的情形,证券公司可通过由投资者在客户端或H5页面勾选同意或弹框确认的形式,事先取得其同意;对于线下办理业务的情形,证券公司可提示投资者现场签署相关协议条款后开展业务办理;
- d) 应设置撤回同意的实现机制,并告知投资者行使撤回同意权的具体路径;
- e) 不得以投资者不同意处理其个人信息或者撤回同意为由,拒绝向投资者提供服务,为投资者提供服务所必需、履行法定职责或者法定义务的除外。

8.2.1.5 特定对象或场景收集注意点

未成年投资者信息收集:提供产品或服务的业务功能主要面向不满十四周岁未成年人的,证券公司需制定专门的未成年人个人信息保护政策并予以发布。产品或服务涉及收集不满十四周岁的未成年人个人信息的,可通过增强告知方式提示需要向未成年人的监护人告知收集个人信息的情形,以及收集未成年人个人信息的目的、必要性、监护人可代为行使的权利及实现机制等规则。

证券经营场所采集:证券经营场所内安装图像采集仅应用于维护公共安全和履行法定要求目的,并在营业场所设置显著的提示标识告知。

证券App采集信息:

- a) 除法律法规另有规定,证券App收集个人生物识别信息、精准地理位置等敏感个

人信息前，应向用户告知处理敏感个人信息的目的、方式、范围等个人信息处理规则以及处理敏感个人信息的必要性和对个人权益的影响（其中证券 App 收集个人生物识别信息前需单独向用户告知），通过弹窗等方式告知并取得用户的单独同意，同时采取严格保护措施；

- b) 用户开启业务功能后方可收集其个人信息；
- c) 用户选择关闭或退出特定业务功能后，应停止该业务功能的个人信息收集活动；
- d) 不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求用户同意收集个人信息。

注：证券App、经营场所处理投资者个人信息见附录B。

8.2.1.6 间接获取个人信息

间接获取投资者个人信息时，证券公司应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认；了解个人信息提供方已获得的授权内容，包括使用目的、个人信息主体是否授权同意提供、公开披露等情况；因业务需要证券公司确需超出原授权范围处理个人信息的，应在处理个人信息前取得投资者的明示同意；在停止提供金融产品或服务时，及时停止继续收集个人信息的活动。

8.2.2 投资者个人信息收集环节的保护措施

8.2.2.1 个人信息采集安全策略

投资者个人信息的收集环节具体保护措施和安全策略如下：

- a) 3级、4级的信息不应委托或授权无金融资质的机构收集；
- b) 确保信息来源的可追溯性；
- c) 投资者个人信息的采集进行严格的输入合法性验证、准确性验证；
- d) 在证券业务信息系统中，应采取具有信息输入安全防护、即时数据加密功能的安全控件对投资者个人信息的输入进行安全保护，并采取有效措施防止合作机构获取、留存投资者个人信息；
- e) 证券公司利用生物特征进行客户身份认证的，应当对其必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的客户身份认证方式，强制客户同意收集其个人生物特征信息；
- f) 对于4级的信息，通过证券公司提供的客户端应用软件方式收集时，应使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取；
- g) 涉及嵌入的第三方代码、插件（如SDK等）收集个人信息的，应说明第三方身份，以及收集个人信息的种类、目的、方式等；
- h) 投资者通过App确认同意的记录应在后台进行留存。

8.2.2.2 个人信息质量保证

证券公司收集投资者个人信息需实施质量控制，对投资者个人信息的来源、真实性、时效性、可靠性等进行评估，确保其质量；定期对个人信息进行核查，确保个人信息的准确性和完整性；证券公司应提供投资者个人信息的更正和补充机制，对于投资者提出的更正、补充请求，证券公司应当对其个人信息予以核实，并及时更正、补充。

证券公司受理投资者账户业务时通过中国证券登记结算有限责任公司等提供的身份信息核查接口验证投资者姓名、证件号等信息的真实性和有效性。

8.2.2.3 金融科技运用评估

证券公司运用大数据技术、人工智能、区块链技术为投资者提供产品或服务前，应当对信息采集身份关联、信息流转知情权保障等进行全面测试和评估，构建具有安全性、保密性和专用性的数据处理环境。

8.3 存储

8.3.1 存储地点

- a) 投资者个人信息原则上应存储在境内。如因开展业务需要，确需出境的，应提前开展数据出境自评估和申报，详见 8.6.2；
- b) 投资者个人信息应存储在证券公司可控区域内，不得通过公有云等非可控方式存储，法律法规与监管机构认可的方式除外；
- c) 应尽量避免在公共信息中暴露证券公司投资者个人信息存储的物理地点。

8.3.2 存储期限

8.3.2.1 最小化存储要求

- a) 投资者个人信息存储期限应为实现投资者个人信息主体授权使用的目的所必需的最短时间；
- b) 超出上述投资者个人信息存储期限后，应对投资者个人信息进行删除或匿名化处理，详见 8.9；
- c) 通过投资者个人信息衍生的相关信息应同样遵循最小化存储要求。

8.3.2.2 必要化存储要求

法律法规、监管规定对投资者个人信息存储期限有最低时限要求的，证券公司应遵照相关规定执行。投资者个人信息包括但不限于：

- a) 投资者开户个人资料与录像；
- b) 投资者委托、交易、转账记录；
- c) 投资者交易终端信息；
- d) 投资者应用程序使用记录。

8.3.3 存储管理

8.3.3.1 安全管理

- a) 应对投资者个人信息存储方式、存储介质、承载的信息系统等内容进行登记管理；
- b) 应尽量提高投资者个人信息存储复用性，减少投资者个人信息多余存储；
- c) 应以最小化原则建立投资者个人信息存储的权限控制机制，严格控制投资者敏感个人信息授权。

8.3.3.2 安全防护措施

- a) 应针对投资者个人信息分级与存储方式采取合适的安全防护措施确保存储安全；
- b) 投资者个人信息应结合信息系统维度、是否结构化等因素进行分开存储；
- c) 存储投资者敏感个人信息时，可采用加密或安全级别等同的其他防护措施；
- d) 投资者个人鉴别信息任何时刻不得以明文存储；
- e) 应采取技术措施确保投资者个人信息存储的完整性；
- f) 应针对投资者个人信息建立备份机制，防止信息丢失。

8.3.3.3 其他注意事项

- a) 不得在移动互联网应用程序客户端明文存储投资者敏感个人信息；
- b) 不得在信息系统日志中记录未加密或未脱敏的投资者敏感个人信息；
- c) 应针对存储投资者敏感个人信息的移动介质采取两种及以上安全防护手段。

8.4 使用

8.4.1 投资者个人信息使用的情形

证券公司使用投资者个人信息的情形包括但不限于：

- a) 证券公司在提供金融产品交易和服务过程中根据交易行为管理、反洗钱管理、尽职调查等要求对投资者个人信息进行监测、分析和展示；
- b) 基于证券公司内部经营管理需要对投资者个人信息进行统计、分析等；
- c) 其他依据法律规定或合同约定使用投资者个人信息的情形。

8.4.2 投资者个人信息使用限制

证券公司遵循合法、正当、必要和诚信原则，按照法律法规的规定、经投资者确认的个人信息保护政策以及相关协议约定处理投资者个人信息，不得超出正常业务范围使用投资者信息，不得泄露未公开信息。如需将投资者个人信息用于个人信息保护政策未载明或合同约定之外的其他用途的，应再次征求投资者个人信息主体的同意；属于投资者敏感个人信息的，应取得单独同意。

8.4.2.1 合理使用情形

证券公司使用投资者个人信息时，应遵循目的限制原则，不得违背与法律规定的可合理使用的目的，也不得超出与收集个人信息时所告知的目的具有直接或合理关联的范围。证券公司及其工作人员的合理使用的情形有：

- a) 根据投资者个人信息主体要求签订和履行合同所必需的；
- b) 根据客户交易行为管理相关法律法规的要求开展投资者异常交易行为监测与分析等工作所必需；
- c) 开展客户尽职调查、可疑交易监测与分析等反洗钱管理工作所需要；
- d) 用于维护所提供的产品或服务的安全稳定运行所必需的，且产品或服务无法安全、稳定运行将可能导致个人权益产生重大影响的，如为发现、处置产品或服务的故障等；
- e) 根据法律法规和证券监管规定，为了日常风险管理与监测所需要；
- f) 为维护金融产品交易或改善、优化服务，或用于信息系统开发运维测试所必需，该种情形下可对投资者个人信息进行去标识化处理后再开展分析和处理；
- g) 将所收集的投资者个人信息用于投资者教育分析、学术研究，属于与收集目的具有合理关联的范围，应在展示结果中对所包括的个人信息进行去标识化处理；
- h) 法律法规规定的其他情形。

证券公司不得使用非法获取或来源不明的数据，通过短信、邮件等非自主运营渠道发送投资者敏感个人信息的，应当将投资者账号信息、身份证号码等投资者敏感个人信息进行脱敏处理。

8.4.2.2 特殊使用情形注意事项

证券公司利用算法、画像技术、人工智能等技术分析、加工生成的能识别或关联为投资

者个人的衍生信息为投资者个人信息，在使用时需注意：

- a) 证券公司应重点关注用户画像所使用的内容，不得包含违法违规情形、侵犯侵害公民、法人和其他组织的合法权益等，应尽量消除明确身份指向性，避免精准定位到特定个人；
- b) 运用于个性化推荐、广告推送、精准营销的，不得强制用户使用定向推送功能，需保障投资者知情权和拒绝权；
- c) 证券公司应保证自动化决策的透明度和结果公平、公正，以及为个人提供解释说明权、选择权和拒绝权等；
- d) 信息汇聚融合的，证券公司应当遵循目的限制原则，并根据汇聚融合后个人信息所用于的目的，开展个人信息保护影响评估，采取有效的个人信息保护措施；
- e) 在算法推荐的场景中应避免以下问题：
 - 1) 未在个人信息保护政策中对用户画像、个性化展示的应用场景及对用户可能造成的影响进行说明；
 - 2) 未取得用户的明示同意；
 - 3) 未提供非定向推送信息的选项；
 - 4) 未向用户提供拒绝接收定向推送的选项；
 - 5) 未明示信息发送者的真实身份和联系方式；
 - 6) 以其他不合理的方式影响用户正常使用服务；
 - 7) 使用非法的用户标签，对用户进行歧视性或偏见性的设置和管理；
 - 8) 证券公司利用投资者个人信息进行自动化决策时对投资者在交易价格等交易条件上实行不合理的差别待遇。

8.4.3 投资者个人信息使用控制

- a) 证券公司应明确投资者个人信息的查询和使用程序，明确数据调用审批程序，建立健全分级审批、双人控制等查询使用制度，防止工作人员行为不当造成投资者个人信息泄露或滥用；
- b) 对投资者个人信息进行后台操作应以“一事一议”为原则进行授权、采取双人复核或全程监控方式同时进行操作留痕，并建立检查或审计机制；
- c) 其他具体控制措施参见 7.5 访问控制。

8.4.4 投资者个人信息展示控制措施

- a) 证券公司提供业务办理与查询等功能的应用软件，及其后台管理与业务支撑系统，在投资者个人信息展示环节具体保护措施如下：依据业务需要，对通过计算机屏幕、客户端应用软件、受理终端设备、自助终端设备、字面等界面展示的投资者个人信息，应采取屏蔽或截词等措施，降低投资者个人信息在展示环节的泄露风险；
- b) 在未登录的状态时，不应展示投资者相关的 2 级及以上的信息；
- c) 在登录的状态时，不应明文展示 4 级投资者个人信息；对于可直接或组合后确定投资者主体的信息，应进行屏蔽展示或者由投资者选择是否屏蔽展示，如需完全展示，应进行身份鉴别，并做好有关记录，防范此类信息泄露的风险；
- d) 在登录状态时，涉及其他投资者的 3 级及以上类别个人信息时，除以下情况外，不直接以明文展示：
 - 1) 其他方主动发起的活动包含的信息，应展示必要的信息以供活动接收方对活动内容进行确认；
 - 2) 与其他方已建立信任关系（间接授权），活动发起方应确认发起活动的必要信

息的正确性。

8.4.5 投资者个人信息使用中的技术措施

投资者个人信息使用环节具体保护措施和安全策略：

- a) 客户交易等重要信息系统应确保运行始终处于证券公司自身控制范围内,不将重要信息系统的运维、日常安全管理交由信息技术服务机构独立实施；
- b) 应严格将未经加密、脱敏的投资者个人信息控制在证券公司的网络防护边界内,通过各类技术手段对相关信息进行保护,建立应对网络攻击的反应机制,加强系统防火墙的建设。如应用系统界面中个人信息的必要脱敏展示、技术人员对投资者个人信息有关数据库的脱敏访问、BI 数据分析及数据报告按需自动对投资者敏感个人信息脱敏等；
- c) 在防护边界外使用投资者个人信息时,例如外部服务机构协助证券公司进行系统运维、因业务所需与外部合作机构进行有关数据传输等,均需要对投资者个人信息进行加密或脱敏处理,有效降低投资者个人信息的泄露风险；
- d) 针对自定义的数据集和用户组,配置并执行访问控制策略,同时支持根据投资者个人信息的分类分级来配置访问控制策略。如引入虚拟账号口令方式代替数据源真实账号口令,降低数据源口令的泄露风险；实施细粒度到人的即时管控,以及监管高危特权；对于高风险数据库操作语句可以根据指令配置访问控制策略,阻断高风险指令的执行；
- e) 可采用技术手段对个人信息使用记录进行留痕处理。

8.4.6 投资者个人信息使用中的委托处理

在符合法律法规和中国证监会规定的前提下,证券公司将收集的投资者个人信息委托给第三方机构处理时,可采取以下具体保护措施：

- a) 对委托行为开展个人信息保护影响评估,并依据评估结果采取有效措施保护投资者权益；
- b) 委托行为保持在已取得的投资者授权同意的范围,同时准确记录和保存委托处理个人信息的情况；
- c) 受托人需要严格按照证券公司的要求处理投资者个人信息,如因特殊原因受托人未能按照要求处理个人信息,及时告知证券公司,并采取补救措施以保护个人信息的安全,必要时终止其对个人信息的处理；
- d) 与受托人以订立合同等方式约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。未经书面授权,受托人不应将其处理的个人信息再次委托给其他机构进行处理；
- e) 对委托处理的信息采用去标识化等方式进行脱敏处理,降低投资者个人信息被泄露、误用、滥用的风险；
- f) 对外部嵌入或接入的自动化工具开展技术检测,确保其投资者个人信息收集、使用行为符合约定要求；并依据合同约定对其收集投资者个人信息的行为进行监督和审计,发现超出约定行为时,立刻切断接入；
- g) 委托关系解除时,受托人需要按照证券公司的要求销毁其处理的投资者个人信息,并依据双方协商的期限承担后续的个人信息的保密责任。

8.5 加工

8.5.1 投资者个人信息加工的情形

证券公司加工投资者个人信息包括但不限于以下情形：

- a) 基于投资者多维度的数据处理加工后形成标签组成的,用于精准地描述一个或者是一类客户特征的用户画像；
- b) 将不同产品或服务所收集的投资者个人信息进行汇聚融合；
- c) 基于用户画像的自动化决策；
- d) 基于用户画像的客户交易行为管理；
- e) 投资者个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的去标识化；
- f) 投资者个人信息经过处理无法识别特定自然人且不能复原的匿名化；
- g) 经纪业务中运用系统自动化匹配投资者分类与产品或服务分级,并出具适当性匹配意见；
- h) 反洗钱方面,基于投资者个人信息划分客户风险等级、进行可疑交易预警等,为反洗钱涉密信息,存储于反洗钱系统中,用于金融机构反洗钱履职和洗钱风险管理。

证券公司加工投资者个人信息包括但不限于以下业务类型：经纪、财富管理、资管等业务中（两融、深沪港通、新三板、北交所等业务开通；客户金融产品购买、金融产品投后跟踪；客户投顾产品购买；客户营销展业；客户服务（资讯分享、产品推广、日常运营、好友促活等）；资管产品推荐），在开展相关业务前，判断是否需开展个人信息保护影响评估，具体参见7.6投资者个人信息保护影响评估。

8.5.2 基本原则和要求

应当确保投资者个人信息在加工处理过程中的合规、安全,防止个人信息的泄露、篡改、丢失。

8.5.3 加工处理的防护措施

- a) 应采取必要的技术手段和管理措施,确保在投资者个人信息清洗和转换过程中对信息进行保护,对3级、4级信息,应采取更加严格的保护措施；
- b) 应对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出投资者个人信息主体的风险进行识别和评估,并对数据集采取相应的保护措施；
- c) 应建立投资者个人信息防泄露控制规范和机制,防止投资者个人信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息；
- d) 应具备信息化技术手段或机制,对投资者个人信息滥用行为进行有效的识别、监控和预警；
- e) 应具备完整的投资者个人信息加工处理操作记录和管理能力,记录内容包括但不限于日期、时间、主体、事件描述、事件结果等；
- f) 汇聚融合的数据不应超出收集时所声明的使用范围。因业务需要确需超范围使用的,应再次取得投资者个人信息主体明示同意,具体参见8.2.1.3合法性之告知和8.2.1.4合法性之同意；
- g) 应根据汇聚融合后的投资者个人信息类别及使用目的,判断是否开展投资者个人信息保护影响评估。

8.6 传输

8.6.1 境内传输一般要求

- a) 证券公司投资者个人信息内部传输应根据法律法规相关要求实施安全技术措施,保证投资者个人信息传输安全性与完整性,包括但不限于：

- 1) 运用合适的加密技术和手段,保障投资者个人信息在传输过程中的安全性;
注:采用密码技术时应遵循密码管理相关国家标准。
 - 2) 采取安全传输通道或安全传输协议进行数据传输。
 - 3) 传输投资者个人信息前,通信双方通过有效技术手段进行身份鉴别和认证;
 - 4) 投资者个人信息传输的接收方对接收的信息进行完整性校验;
 - 5) 对投资者个人信息传输安全策略进行审核、监控和优化;
 - 6) 采取有效措施保证数据传输可靠性和网络传输服务可用性。
- b) 证券公司使用物理介质(主指移动介质)传输投资者个人信息,应对物理介质采取密码设置等安全措施;
 - c) 证券公司通过文件传输投资者个人信息,应采取文件加密等必要的安全手段防止信息泄露;
 - d) 证券公司通过物理介质(主指移动介质)传输投资者个人信息,应设置介质使用期限,到期后及时回收介质并清理投资者个人信息;
 - e) 向国家机关、证券行业主管和监管单位传输数据,应按照国家及行业相关管理要求进行传输。

8.6.2 跨境传输特别要求

- a) 在中华人民共和国境内运营中收集和产生的投资者个人信息向境外传输的,应遵循国家法律法规和中国证监会的规定;
- b) 在境内提供证券服务过程中收集和产生的投资者个人信息,应在境内处理。确需向境外机构(含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构)传输投资者个人信息的,应遵守法律法规和中国证监会的相关规定,并按照以下要求执行:
 - 1) 取得投资者个人单独同意,法律法规另有规定的除外;
 - 2) 依据国家、行业有关部门制定的办法与标准开展投资者个人信息保护影响评估,确保境外机构数据安全保护能力达到相应要求;
 - 3) 充分统计评估向境外机构提供投资者个人信息与投资者敏感个人信息的数据量,对照国家相关法律法规要求履行必要的前置审批程序;
 - 4) 应针对投资者个人信息跨境传输开展定期审查。当出现前置审批有效期临期或向境外提供投资者个人信息的目的、范围、种类、敏感程度、方式、保存地点发生变化或境外接收方处理个人信息的用途、方式发生变化或境外接收方当地法律法规发生变化等情形时,应遵循国家相关法律法规要求及时重新完成前置审批程序。
- c) 应对境外传输的投资者个人信息进行监控,当发生或可能发生个人信息安全事件时,应当采取补救措施并及时向行业监管部门、省级以上网信部门等相关部门报告;
- d) 投资者个人信息处理者及接收方注册于(适用于组织)/位于(适用于个人)粤港澳大湾区内地部分,即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市,或者香港特别行政区的,互相之间发生个人信息传输,可遵循《粤港澳大湾区(内地、香港)个人信息跨境流动标准合同实施指引》的规定。如所处地区对跨境传输有特别规定的,遵照相关规定执行,如《中国(上海)自由贸易试验区临港新片区数据跨境流动一般数据清单操作指南(试行)》。

注:免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证等情况应遵循《促进和规范数据跨境流动规定》。

注:如国家相关法律法规有新增或变化,应遵循国家最新相关法律法规的规定与要求。

8.7 提供

除法律法规和中国证监会另有规定外，证券公司不得以任何方式向其他机构、个人提供投资者个人信息，不得允许或者配合其他机构、个人截取、留存未经匿名化处理的投资者个人信息。

8.7.1 向第三方提供投资者个人信息的情形

证券公司向第三方提供投资者个人信息包括以下情形：

- a) 证券监管机构、公安机关、司法机关等有权机关为调查金融领域违法违规、刑事犯罪行为，需要证券公司提供相关投资者的交易数据等个人信息；
- b) 开展司法协助业务，根据司法要求配合监管机构提供证券公司客户账户与交易信息；
- c) 产品成立或存续期内执行产品报送、报备等要求，如资产管理计划成立、备案及存续运作需向证券监管机构、行业自律组织报送产品投资者信息；
- d) 证券公司履行相关法定义务向有关部门报告与报备；
- e) 配合证券监管机构、证券交易所、行业自律组织的检查与调查，按要求提供所涉投资者的个人信息；
- f) 因合并、分立、解散、被宣告破产等原因转移投资者个人信息；
- g) 依据法律法规和中国证监会规定的其他情形。

8.7.2 向第三方提供投资者个人信息的安全防护要求

在向第三方提供投资者个人信息的过程中，具体保护措施如下：

- a) 部署信息防泄漏监控工具，监控及报告投资者个人信息的违规传递行为；
- b) 部署流量监控技术措施，对共享、转让的信息进行监控和审计；
- c) 对投资者个人信息的导出进行操作授权时，应采用口令、密码技术、生物识别技术等两种或两种以上组合的鉴别技术，且其中一种鉴别技术使用密码技术实现，并对导出操作进行细颗粒度的访问控制与全过程审计；
- d) 定期检查或评估信息导出通道的安全性和可靠性；
- e) 执行严格的审核程序，并准确记录和保存投资者个人信息向第三方提供情况。记录内容包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用目的等，并确保提供过程可被追溯；
- f) 采取有效技术防护措施，防范信息转移过程中被其他个人、组织和机构截获和利用；
- g) 因合并、分立、解散、收购、兼并、重组、破产等情况，对投资者提供金融产品或服务的证券公司主体变更而发生投资者个人信息共享、转让时，证券公司应通过逐一告知（或公告）等方式通知投资者。接收方对其接收运营的金融产品或服务继续履行投资者个人信息保护责任。接收方如变更其在收购、兼并重组过程中获取的个人信息使用目的，接收方应重新取得投资者明示同意或授权。

以上要求仅适用于法律法规和中国证监会规定的向第三方提供投资者个人信息的情况。

8.7.3 投资者个人信息向境外提供的实施要点

- a) 除法律法规另有规定，向境外提供个人信息的，需向个人告知境外接收方的身份、联系方式、处理目的、处理方式，个人信息的种类、保存时间、保存区域（至少具体到国家或地区）以及个人向境外接收方行使相关权利的方式等内容，并取得个人的单独同意；

注：个人在自行了解境外接收方所公布的个人信息处理规则后，主动以邮件、短信息、点击启动服务、

在线提交信息或直接确认等方式向境外接收方发送涉及其个人信息内容的，可视为个人行为或作出了单独同意。

- b) 如产品或服务中涉及个人信息出境的业务功能可与其他业务功能相分离的,证券公司应将涉及个人信息出境的业务功能与其他业务功能区分,以便个人针对个人信息出境作出单独同意;
- c) 提供的个人信息仅限于实现处理目的所需最小范围;
- d) 个人拒绝涉及个人信息出境的业务功能后,不能影响其他业务功能的正常使用;
- e) 收集个人信息时已事前单独就个人信息出境取得个人同意,满足出境其他条件的前提下,后续在出境时可不再次取得个人单独同意。

注:涉及跨境传输的规范参见8.6.2跨境传输特别要求。

8.8 公开

8.8.1 投资者个人信息公开的基本要求

8.8.1.1 投资者个人信息公开的情形

证券公司公开投资者个人信息包括但不限于以下情形:

- a) 证券公司在开展证券承销与保荐等投资银行业务的过程中,根据法律法规、监管规定、自律规则等规定或要求,披露投资者的持股情况等个人信息;
- b) 证券公司自身在融资过程中,通过发行文件、申报材料等披露与投资者相关的重大交易、诉讼(仲裁)等信息;
- c) 投资者通过证券公司组建的群组发言、对证券公司官方社交媒体账号(如官方微博、微信公众号等)发布的信息进行评论回复、参加证券公司组织的抽奖、投票、比赛、评选、宣传、推介等活动也可能导致个人信息被公开;
- d) 其他基于法律、法定程序、有权机关强制性规定或要求等,公开投资者个人信息;
- e) 其他基于履行法定义务、法定职责或维护国家安全、公共利益,公开投资者个人信息。

8.8.1.2 公开的原则和要求

证券公司原则上不得公开所收集的投资者个人信息,经法律授权或具备合理事由确需公开时,应符合以下要求:

- a) 事先开展个人信息保护影响评估,并依据评估结果采取有效的保护个人信息主体合法权益和信息安全的保障措施,防止信息被篡改、滥用等风险;
- b) 除法律另有规定外,事先应向投资者告知信息公开的目的、类型,并取得投资者的明示、单独同意;
- c) 公开投资者的敏感个人信息前,还应事先告知投资者涉及的敏感个人信息的内容;
- d) 相关法律法规、监管规定、自律规则或与投资者签订的合同对信息公开有明确规定或约定的,应严格按照规定或约定的范围、时间、渠道、方式、程序等规则实施信息公开具体行为;
- e) 不得公开投资者的个人生物识别信息以及种族、民族、政治观点、宗教信仰等敏感个人信息的分析结果;
- f) 建立、维护、更新投资者个人信息公开记录,准确记录和保存投资者个人信息公开的情况,包括公开的日期、信息类型及具体内容、公开目的、公开渠道、公开方式、处理信息公开的人员等情况;
- g) 根据法律法规或合同约定,承担因不当公开行为损害投资者合法权益的相应责任。

8.8.2 投资者个人信息公开环节的保护措施

证券公司在公开投资者个人信息时，应采取以下措施保护投资者个人信息安全：

- a) 明确投资者个人信息公开的管理部门及人员，并对相关人员开展具体工作有关的管理与培训；
- b) 明确涉及投资者信息公开相关工作的操作规程，建立复核机制，避免因信息公开错误等不当行为给投资者造成不利后果或影响；
- c) 有效开展投资者个人信息公开前的保护影响评估；
- d) 建立投资者个人信息公开安全事件应急处置和报告、安全事件告知、补救及损害救济机制；
- e) 开展投资者个人信息保护相关的教育活动，帮助投资者了解信息公开与保护的规则、机制；
- f) 将投资者信息公开相关的活动纳入个人信息安全与保护的审计范围，对相关制度流程、保护政策和安全措施的有效性进行审计，及时发现并处理投资者个人信息公开违规行为；
- g) 通过客服热线等方式受理投资者对证券公司信息公开规则或公开活动存在的疑问或异议，及时对投资者进行解释说明或采取补救措施。

8.9 删除

8.9.1 基本要求

证券公司在处理投资者个人信息过程中应保障投资者个人信息删除权，证券公司可制定内部数据安全及档案管理相关制度，根据各业务的需要，综合考虑各项因素后（如是否已销户、是否存在纠纷、诉讼时效等）确定各业务涉及的个人信息保存期限及保存的具体方式等，并向投资者明确告知权利、权利例外、删除时限、删除渠道以及替代删除手段，并在业务环节中建立投资者个人删除的落地措施。

8.9.2 投资者个人信息删除环节的保护措施

- a) 在公司制度和操作细则中明确删除投资者个人信息的“双向主动”属性：投资者有权利主动要求证券公司删除“最小必要”原则之外的个人信息，证券公司也可按照法律法规要求主动删除“最小必要”原则之外的投资者个人信息；
- b) 因业务、产品终止或撤回同意，投资者提出删除其个人信息的要求，证券公司应依据法律法规、证券期货行业主管部门有关规定及与投资者的约定予以响应；
- c) 与证券公司提供产品或服务非直接相关投资者个人信息，如仅为改善服务、提升系统功能体验而收集的投资者个人信息，在满足法定情形、确认没有法定或主管部门规定的保存期限或超出保存期限且没有继续保存的必要性的个人信息应予以删除；
- d) 证券公司提供产品或服务时依法或者依照合同约定收集的投资者个人信息，在投资者主动提出删除要求时，应首先判断是否符合已满足法定及主管部门规定的最低保存期限。如仍在法定或主管部门规定的保存期限内或存在其他应履行的法定职责或义务需要继续保存客户个人信息的情形，证券公司可拒绝删除并告知投资者理由；如已超过法定或主管部门规定的保存期限，可对投资者进行个人信息删除后果的告知，并由投资者签署书面申请后再进行具体的删除操作；
- e) 证券公司可在信息保存满足法律法规和监管要求的基础上，结合投资者个人信息分级和监管存储期限要求，在公司制度和操作细则中针对不同分类分级的投资者个人信息，提出相应的删除时间要求。

8.9.3 证券公司删除投资者个人信息的情形

- a) 符合以下情形,根据法律法规要求,或投资者要求证券公司删除个人信息的,应及时删除个人信息:
 - 1) 违反法律法规规定,收集、使用投资者个人信息的;
 - 2) 违反与投资者的约定,收集、使用投资者个人信息的;
 - 3) 处理目的已实现、无法实现或者为实现处理目的不再必要;
 - 4) 证券公司停止提供产品或者服务,且满足有关行业监管规定时;
 - 5) 其他法律法规要求删除投资者个人信息的情形。
- b) 证券公司违反法律法规规定或违反与投资者的约定向第三方共享、转让投资者个人信息,且投资者要求删除的,证券公司应立即停止共享、转让的行为,并通知第三方及时删除;
- c) 证券公司违反法律法规规定或违反与投资者的约定,公开披露投资者个人信息,且投资者要求删除的,证券公司应立即停止公开披露的行为,并发布通知要求相关接收方删除相应的信息。

8.9.4 委托处理、共同处理、共享处理的情况下的删除

证券公司除自身保障客户删除权的行使外,还应注意委托处理、共同处理、共享处理的第三方相应删除义务的履行情况,保障投资者对于第三方信息删除的权利:

- a) 证券公司如作为投资者个人信息委托处理的委托方,应当在委托合同中明确在不生效、无效、被撤销或者终止的情况下,受托方有义务及时返还个人信息或予以删除,证券公司应通过技术手段及违约责任等方式切实约束受托方,确保受托方履行上述返还或删除义务,保障投资者信息删除权的实现;
- b) 涉及到共同处理的情况下,证券公司除应慎重选择共同处理方及在相关的协议中约定各方的责任及追偿等条款外,还应在客户要求删除相关个人信息时,提示客户存在共同处理的情形,如客户要求共同处理方删除,应将客户相关要求转达给共同处理方;
- c) 证券公司向其他个人信息处理者提供其处理的投资者个人信息的,为了避免接收方在未单独征求投资者单独同意的前提下超出原授权的处理目的和方式使用客户信息,在投资者要求删除其个人信息时,可再次提示投资者存在信息共享的情形,并根据投资者的要求协助转达删除申请。

8.9.5 建立合理合规的删除制度机制

证券公司在开户告知书、App 用户协议、第三方机构合作协议、证券公司个人信息保护政策等环节确保下列事项的明确沟通:

- a) 删除权利告知;
- b) 收到投资者删除请求的处理方式和时限;
- c) 向投资者通知证券公司如何对个人信息进行删除或匿名化处理;
- d) 明确投资者请求删除的渠道;
- e) 告知投资者行使删除权可能对其造成的影响,以助于其作出行使相关权利的判断;
- f) 第三方机构删除投资者个人信息的明确义务和操作机制。

注:删除权的告知应在收集个人信息阶段完成,具体告知规范参见 8.2.1.3 合法性之告知。

8.9.6 请求删除的渠道

证券公司在履行主动删除义务的同时,应为投资者提供请求删除的渠道,如:

- a) 证券公司 App 或官方网站提交删除申请；
- b) 现场或电话提交删除申请；
- c) 被授权人代提交删除申请。

8.9.7 例外情形

证券公司应在提供产品或服务前，向投资者明示删除投资者个人信息的例外情形：

- a) 监管有保存期限法律法规要求的个人信息，包括：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；登记、存管和结算的原始凭证及有关文件和资料；监控档案；做市业务，对报价和成交数据；证券投资顾问业务档案等；
- b) 技术难以实现删除的个人信息，如：云存储的情形下，除非全部清空用户的数据，否则无法删除个人信息的情形等；
- c) 证券公司可关注新技术带来的删除权例外情形。

注：此处的技术难以实现指现有的技术根本无法删除个人信息或者在现有的技术条件下需要付出不合理成本才能删除。

8.9.8 保障措施

证券公司在信息不可删除的情形下，应采取合理措施充分保护投资者个人信息：

- a) 受监管存储期限限制，不可删除的个人信息，应做到明确告知投资者；
- b) 在监管存储要求期限内，应建立安全的个人信息储存系统和健全的硬件设施，确保在技术上妥善保护投资者个人信息；
- c) 停止除存储和采取必要的保护措施之外的处理；
- d) 监管存储期限到期后，证券公司应谨慎评估继续保存的必要性，并对无必要继续保存的投资者个人信息进行及时删除；采取去标识化等脱敏技术手段，降低个人信息对投资者的关联程度。

附录 A
(资料性)
投资者个人信息分类分级参考表

个人信息	子类	说明	敏感	分级
投资者个人基本信息	/	开展证券交易的自然人、法人、非法人组织,以及依法设立的金融产品所涉及的自然人的个人基本信息,包含姓名、性别、民族、出生日期、年龄、联系地址、移动电话、电子邮件、国籍等信息。	/	3
投资者个人身份信息	个人身份证件信息	投资者个人证件类型、证件号码、证件地址、证件有效期、签发机关等。证件类型包括身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等。	是	3
	特定身份信息	残障人士身份信息、犯罪人员身份信息、特定工作信息(如军人、警察)等个人信息。	是	3
投资者个人鉴别信息	投资者账户认证	投资者的账户认证信息,包含投资者用于身份认证的账户密码、数字证书、动态口令、口令保护答案、短信验证码等。	是	4
	个人生物识别信息	用于投资者鉴别的个人生物识别信息。指纹认证信息、人脸认证信息等。	是	4
投资者个人账户信息	开户/账户信息	投资者与业务活动相关的识别信息,包含账户名称、投资者标识、账户类别、账户编码、账户用途、账户状态代码等信息。	是	3
	投资者编码	投资者在证券公司的内部统一编码。	/	2
投资者个人交易信息	成交信息	投资者买卖证券产品的成交相关信息,包含证券账户编码、银行账户编码、市场代码、证券代码、成交金额、成交数量、成交时间、成交价格、成交日期、委托编号、席位代码、经手费、证管费、印花税、佣金等。	是	3
	委托信息	投资者买卖证券产品的委托相关信息,包含证券账户编码、市场代码、证券代码、委托价格、委托数量、委托方向、委托类型、委托时间、委托日期、委托渠道、席位代码等。	是	3
	银证转账	投资者通过三方存管账户进行的资金划转相关信息,包含营业部编码、账户编码、银行代码、发生金额、发生日期、发生时间、渠道代码等。	是	3

	交易业务参数信息	证券产品交易业务规则中定义的，完成交易所需的参数，如账户编码、交易时段、涨跌幅、交易单元等。	/	2
	交易日志信息	投资者行为相关信息，可分为注册登录日志、信息变更日志等多类，包含发生日期、发生时间、来源等信息。	/	3
	其他交易信息	有关规定要求的反映交易真实情况的合同、业务凭证、单据、业务函件和其他资料。	/	3
投资者个人财产信息	持仓信息	投资者持有某一证券、期货、基金等品种的信息，包含证券账户编码、市场代码、证券代码、持仓数量、持仓日期、市值等。	是	3
	银行账务信息	投资者开立的用于交易、结算业务的账户信息，包含开户网点信息、银行账户、币种代码等。	/	3
	资金状况信息	投资者资金账户余额信息，包含币种代码、银行账户、资金余额、个人收入状况等。	是	3
投资者个人信用信息	/	指投资者的信用相关信息，包含信用账户编码、信用等级、信用额度、融资融券偿还情况以及投资者在交易活动中形成的，能够反映其信用状况的其他信息。	是	3
投资者个人合约合同	/	指参与交易活动所产生的契约信息，包含账户编码、流水号、合同号、市场代码、证券代码、证券数量、发生金额、归还日期等。	是	3
投资者个人行为信息	/	投资者在 App、网站中的行为埋点信息、操作日志等。	/	2
投资者衍生信息	/	一般指对投资者交易及行为数据进行处理、分析所形成的反映特定投资者某些情况的信息，包含：投资者分类、投资能力、投资意愿、行为习惯、兴趣偏好等。	/	2
投资者个人设备信息	可变更的唯一设备识别码	AndroidID、、广告标识符（IDFA）、应用开发商标识符（IDFV）、开放匿名设备标识符（OAID）等，以及机型、系统版本、存储位置等在内的描述个人常用设备基本情况的信息。	/	3
	不可变更的唯一设备识别码	包括硬件序列号、设备 MAC 地址、唯一设备识别码（如 IMEI/Open UDID/GUID/SIM 卡 IMSI 信息等）。	/	3

	别码			
	应用软件列表	用户在终端上安装的应用程序列表。	/	3
投资者个人位置信息	粗略位置信息	仅能定位到行政区、县级等的位置信息，如地区代码、城市代码等。	/	2
	行踪轨迹信息	包括精准定位信息、经纬度等。	是	3
个人健康生理信息、医疗信息	健康状况信息	与个人身体健康状况产生的相关信息，如体重、身高、体温、肺活量、血压、血型等。	是	3
	医疗健康信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等。	是	3
个人教育工作信息	/	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等。	/	3
个人其他信息	/	宗教信仰、性取向、婚史、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、网页浏览记录等。	是	3
客户关系信息	/	证劵公司与投资者之间在销售、营销和服务上的交互信息数据。	/	3
客户服务信息	/	指证劵公司开发新投资者及维护老投资者形成的对客户的联系、服务、售后等信息定期管理的记录。	/	3
客户经营关系	/	指证劵公司对投资者交易、持仓和资金情况的分析数据，例如对投资者的盈利、交易量、资产等情况的汇总数据。	/	2
渠道信息	/	指证劵公司对投资者进行营销、客户服务等活动中所使用的信息渠道信息。	/	2
市场营销推广信息	/	证劵公司对投资者进行营销推广活动中产生的数据信息。	/	2

服务机构和人员信息	/	证券公司提供投资者服务的部门基本信息,证券公司提供投资者服务的人员开展业务服务所需的基本信息。	/	2
-----------	---	---	---	---

注：投资者个人信息分类分级参考表中未包含的类型，可参考 GB/T 43697-2024《数据安全技术 数据分类分级规则》附录 B。

附录 B
(资料性)
特定场景中的投资者个人信息保护

B.1 场景一：证券公司营业场所场景下的投资者个人信息保护

B.1.1 概述

证券公司营业场所场景包括：

一般营业场所：出于安全的目的，在办公地等公共场所安装图像采集、个人身份识别设备¹。

客户交易区：根据《关于加强证券期货经营机构客户交易终端信息等客户信息管理的规定(2022 修正)》（证监会公告[2022]43 号）规定²在客户交易区安装监控录像设备。

B.1.2 收集的内容

可能被采集的个人信息种类通常包括人脸图像等。

B.1.3 信息的处理

B.1.3.1 使用

- a) 在营业部等经营场所安装摄像头等采集的影像信息不得使用人脸识别技术进行人脸验证、辨识或者分析；
- b) 应安排专人对监控信息进行管理，对查阅、复制、调取信息资料的人员、时间、用途及去向等情况进行登记；
- c) 公安机关等行政主管部门因执法工作需要查阅、复制或者调取公共安全视频图像信息系统的信息资料或者直接接入监控系统的，应当依据有关法律、法规的规定执行；
- d) 除维护公共安全的目的以外，未经个人单独同意，不得公开或者向他人提供其收集的个人图像、身份识别信息。

B.1.3.2 收集

除落实本规范第 7 章和第 8 章的要求外，其他实施要点如下：

- a) 基于公共安全或监管规定安装监控录像设备，属于可免于同意情形；
- b) 在营业部等公共场所通过设备采集个人信息时，需以显著方式向用户展示个人信息处理规则。显著方式通常是指在醒目位置张贴、播放简短易懂的告知内容，同时告知获取更多相关信息的途径；
- c) 在摄像头安装处张贴告示向用户告知简要的个人信息处理规则；
示例：为保障用户人身财产安全，此处摄像头将记录个人影像信息，我们承诺会保护数据安全，了解详情可拨打电话或扫描二维码；
- d) 注意客户交易区安装的监控录像设备位置，不得从录像设备获取投资者交易密码等资料。

¹部分地方政府曾发布公共安全视频图像信息系统相关规定，如《广东省公共安全视频图像信息系统管理办法》。

²《关于加强证券期货经营机构客户交易终端信息等客户信息管理的规定》第十二条第二款规定：证券期货经营机构应妥善保存交易时段客户交易区的监控录像资料，保存期限不得少于 6 个月。

B.1.3.3 存储

除落实本规范第 7 章和第 8 章的要求外，其他实施要点如下：

- a) 客户交易区的监控录像资料,保存期限不得少于 6 个月;其他位置的监控录像资料,不得低于地方政府规章规定的保存期限;
- b) 监控系统应按当地地方政府规定进行备案。

B.2 场景二：非现场开户场景下人脸识别中的个人信息处理

B.2.1 概述

目前,非现场开户包括见证开户和网上开户。见证开户是指证券公司工作人员面见客户,通过适当的方式或信息技术手段验证客户身份、见证客户签署开户相关协议后,按规定程序为客户办理资金账户开户。网上开户是指证券公司通过网上开户系统,以适当的方式或信息技术手段验证客户身份,并与客户签署开户相关协议后,按规定程序为客户办理资金账户开户。

非现场开户中,投资者身份验证涉及单向视频活体检测以及人脸识别比对等。

B.2.2.收集的内容

可能被采集的个人信息种类通常包括人脸图像、人脸认证信息等。

B.2.3 信息的处理

B.2.3.1 收集

a) 收集人脸识别信息时,应向投资者告知人脸识别信息的相关事项,包括但不限于数据处理者的名称和联系方式、处理规则、必要性依据等,收集开户所必需的信息可以免于同意;收集非开户所必需信息时需取得投资者单独同意;

b) 采用需要投资者主动配合的措施收集人脸识别信息,应在识别过程中持续告知投资者验证目的,并通过语言文字等向投资者进行提示;

注:需要投资者主动配合的措施包括要求投资者直视收集设备并做出目光注视、特定姿势、表情,或者通过标注了人脸识别应用的文字、图示、图标或符号的专用收集通道等。

c) 应仅收集生成人脸识别所需的最小数量、最少种类的人脸图像;

d) 应采取安全措施保证人脸识别数据的真实性、完整性和一致性,防止人脸识别数据在收集过程中泄漏或篡改。

B.2.3.2 使用

a) 处理人脸识别信息应当事前进行个人信息保护影响评估;

b) 应采取数据完整性校验、数据加密等措施保障人脸识别数据传输安全;

c) 人脸信息原始样本应在完成认证功能后,立即删除、不得保存。

B.2.3.3 提供、公开

a) 除非经投资者单独同意或书面同意,不应公开人脸识别数据;

b) 不应向第三方提供或委托处理人脸识别信息。符合法律法规和中国证监会规定下的提供或委托处理,应按照本规范的第7章进行有关评估与告知。公安系统联网验证应属于可免于单独同意情形。

B.2.3.4 存储

a) 因非现场开户所必需收集人脸识别信息,按照监管规定,保存至客户关系终止后20年;

b) 因其他业务需要收集的人脸识别信息,应按照与投资者的约定时限及时删除。

B.2.3.5 评估

a) 事前评估

人脸识别技术使用者处理人脸信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。个人信息保护影响评估主要包括以下内容：

- 1) 是否符合法律、行政法规的规定和国家标准的强制性要求,是否符合伦理道德;
- 2) 处理人脸信息是否具有特定的目的和充分的必要性;
- 3) 是否限于实现目的所必需的准度、精度及距离要求;
- 4) 采取的保护措施是否合法有效并与风险程度相适应;
- 5) 发生或者可能发生人脸信息泄露、篡改、丢失、毁损或者被非法获取、非法利用的风险以及可能造成的危害;
- 6) 可能对个人权益带来的损害和影响, 以及降低不利影响的措施是否有效。

b) 持续评估

在使用人脸识别技术过程中,应当对设备的安全性及处理人脸信息的目的、方式等事项进行持续评估与审计,并记录评估、审计过程和结果,根据检测评估情况改进安全策略,调整置信度阈值,采取有效措施保护图像采集设备、个人身份识别设备免受攻击、侵入、干扰和破坏。

B.3 场景三：代销金融产品场景下的个人信息处理

B.3.1 概述

代销金融产品，是指证券公司接受金融产品发行人的委托，为其销售金融产品或者介绍金融产品购买人的行为。

B.3.2 收集的内容

- a) 投资者基本信息。自然人的姓名、住址或邮寄地址、学历、年龄、联系方式（邮箱及手机号码）、有效身份证件、出生地、出生日期、性别、国籍等基本信息、开展金融相关业务资格证明、机构负责人或者法定代表人信息、经办人身份信息、联系方式；税收居民身份证明；金融账户信息；产品份额持有人、实际控制投资者的自然人和交易的实际受益人等；
- b) 投资者资产状况。收入来源和数额、资产、债务等财务状况及对应的证明文件；
- c) 投资者投资经验。投资相关的学习、工作经历、投资经验（包括投资期限、实际投资产品类型、投资金融产品的数量、参与投资的金融市场情况）及对应的证明文件；
- d) 相关专业资质。包括获得职业资格认证的从事金融相关业务的注册会计师和律师等资格及对应的证明文件；
- e) 投资风险偏好。投资目的、投资期限、品种、期望收益等投资目标；风险偏好及可承受的损失；
- f) 诚信记录。包括征信信息、资本市场相关诚信记录查询；
- g) 适当性管理过程相关录音录像材料；
- h) 投资者购买产品所生成的金融资产相关信息。包括但不限于所持有的份额的数量、净值等信息；份额变动信息，包括认购/申购、赎回、转让、质押、冻结、清算等；
- i) 投资者敏感个人信息。投资者的特定身份、金融账户，部分登录系统的还可能涉及指纹认证信息、人脸认证信息、行踪轨迹等信息；
- j) 法律法规、自律规则规定的投资者相关信息，以及其他必要信息。

B.3.3 信息的处理

除落实本规范第7章和第8章的要求外，其他实施要点如下：

B.3.3.1 收集

证券公司作为代销机构，因适当性管理、洗钱风险管理、账户实名制管理、网络安全管理、投资者资金安全等履行法定职责或者法定义务所必需，或为投资者认购/申购、赎回所必需收集、处理投资者个人信息，属于免于同意的情形。

B.3.3.2 提供

如管理人根据本行业或机构需要要求证券公司提供其自身管理范围之外的信息或者基金合同等文件约定之外的个人信息，宜审慎评估；如不属于法定义务或履行合同所必需的信息，应按照委托处理情形取得投资者单独同意。

B.3.4 代销协议个人信息保护条款要点

确认委托人与证券公司均为个人信息处理者；明确代销场合个人信息处理的目的；明确双方各自在个人信息保护相关的权利义务。要点如下：

示例：《金融产品销售协议之个人信息保护条款》参考要点

甲方：**基金管理有限公司

乙方：**证券股份有限公司

一、个人信息保护

（一）释义

本协议所指的“个人信息”是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

本协议所指的“投资者敏感个人信息”是指一旦泄露或者非法使用，容易导致自然人的尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

本协议所指的“个人信息的处理”包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

（二）个人信息的处理

1.依据法律法规规定及《销售协议》的约定，为配合甲方履行其反洗钱、投资者适当性、反恐怖融资、反贿赂、制裁、非居民金融账户涉税信息(CRS)尽职调查等法定义务，以及履行投资者作为一方当事人的合同所必需之目的，乙方应向甲方提供其处理的投资者个人信息。就此，甲乙双方应当依据法律法规的规定就各自的个人信息处理活动向相关信息主体履行必要的告知义务；

依据法律法规及《销售协议》的约定，为向投资者提供持续信息服务，甲方将向乙方提供相关基金投资者份额确认等信息，将涉及投资者个人信息的处理。

2.依据法律法规规定，为实现向投资者提供服务等本条第1款所述之外的目的，乙方应向甲方提供其处理的投资者个人信息(具体信息种类、处理目的、处理方式见下文第3项)。就此，乙方应当依据法律法规的规定向相关个人履行必要的告知义务，并取得个人的单独同意；

甲方要求乙方提供经相关个人确认后的同意函等证明文件(原件、复印件或扫描件)时，乙方应当及时提供。乙方拒绝提供证明文件(原件、复印件或扫描件)的，视为未取得相关个人的同意，并视为乙方违反《销售协议》之约定，甲方有权据此终止《销售协议》。

为履行《销售协议》而涉及个人信息收集的，甲、乙方应当限于实现处理目的的最小范围，不得过度收集个人信息。

3.为实现2所述之目的，乙方应当向甲方提供的投资者个人信息种类、甲方处理目的、处理方式如下：

（1）列举为实现除履行法定义务及履行个人作为一方当事人合同之外的目的，乙方应当向甲方提供的投资者个人信息；

（2）列举为实现除履行法定义务及履行个人作为一方当事人合同之外的目的，甲方就乙方提供的投资者个人信息的处理目的；

(3) 列举为实现除履行法定义务及履行个人作为一方当事人合同之外的目的，甲方就乙方提供的投资者个人信息的处理方式；

乙方应根据第2项的要求，向个人告知上述个人信息的种类、处理目的和处理方式、信息接收方的名称和联系方式等要素。涉及投资者敏感个人信息的，乙方还应当个人告知处理投资者敏感个人信息的必要性以及对个人权益的影响。

如因甲乙双方业务需求变化等原因导致上述内容变更的，乙方应当重新取得个人同意。

4.乙方依照法律法规要求和《销售协议》约定向甲方提供的投资者个人信息，甲方的处理目的应限于前述目的，处理方式应限于为实现前述目的的最小必要范围。如甲方超出前述范围处理个人信息，应自行取得个人的单独同意。

5.甲、乙方确保双方就个人信息的传输方式、传输手段、处理方式等均符合法律法规的规定，采取必要的技术防护措施，降低个人信息转移或交换或处理过程中的安全风险。

6.如未来法律法规或甲乙双方业务需求发生变化，甲乙双方可就个人信息的处理达成补充协议。签署本协议并不构成甲方与乙方共同处理个人信息，亦不构成甲方委托乙方处理个人信息。未经一方同意，另一方不得与该方为共同个人信息处理者或该方的代理人/受托方名义处理个人信息。

二、违约责任

(一) 甲乙双方应严格遵守《中华人民共和国个人信息保护法》的规定及本协议约定，在各自义务范围内履行投资者个人信息保护义务。

(二) 违反投资者个人信息保护义务的，由甲、乙方各自向投资者承担责任。

三、其他

(一) 除双方另有约定外，本协议适用于甲方已经发行的及今后发行的并经乙方销售的各基金。

(二) 甲乙双方为履行本协议所相互提供的信息以及本协议本身均属保密信息，未经对方书面同意，不得向第三方披露，但法律、法规另有规定或监管部门另有要求的除外。

B.4 场景四：互联网营销场景下自动化决策中的个人信息处理

B.4.1 概述

自动化决策是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。《中华人民共和国个人信息保护法》侧重于销售端的自动化决策，如向个人进行信息推送、商业营销等。

B.4.2 收集的内容

B.4.2.1 投资者填写

- a) 基本信息：申请开户时间、客户姓名、出生日期、客户年龄、有效身份证件的类型和号码、手机号码、电话号码；
- b) 个人背景：兴趣爱好、毕业院校、所处行业、所在单位、婚姻情况、家庭人口数、子女数量、血型、性格类型、偏好、联系方式、邮箱、微信；
- c) 财务背景：个人年收入、家庭年收入、收入来源、家庭资产规模、家庭资产组成、置业情况、金融资产、保险、借贷情况、证券投资比重、负债率、家庭人均年收入、月均还贷支出、家庭月均支出、家庭备用金情况、家庭人口数、赡养负担、配偶具体情况、子女具体情况；
- d) 投资经验：投资风格、投资收益目标、预期回报率、从事投资年限、行业偏好、投资决策方法、投资证券经验、曾参与投资品种。

B.4.2.2 系统生成

- a) 基本信息：开户成功时间、风险等级、风测到期日期、普通账户佣金率、信用账户普通交易佣金率、信用账户信用交易佣金率、开户营业部、风险承受能力；
- b) 客户资产：可用资产、股票资产、理财产品、两融余额；
- c) 客户交易：证券代码/证券名称、成交数量、成交价格、成交金额、实收佣金、柜台净佣金。

B.4.2.3 证券公司填写

行为特征：客户分类、操作方式、投资板块、投资行业、投资题材、持仓偏好、交易习性、活跃程度、资产规模、账户盈亏情况、交易频次、客户年龄层、投资性格、服务偏好、产品偏好、服务内容需求、交易风格、客户操作依据、性格特征。

B.4.3 自动化决策过程

证券公司的信息系统首先对收集的投资者个人信息基础数据进行清洗，过滤明显偏离正常范围的数据，通过既定的满足外规要求和业务需求的规则对基础数据进行加工和分类，形成标签，标签应通过系统间加密流转和自动化加工形成。单个投资者拥有多维度的标签后，形成用户画像。

目前自动化决策更多地运用于经纪、财富管理、资管等业务中。基于用户画像的自动化决策将进行精准营销及产品推荐，需重点关注数据来源的合法合规性、控制信息泄露和滥用的风险。

B.4.4 自动化决策注意事项

自动化决策涉及处理投资者个人信息，应公开或告知投资者个人信息处理规则，明示处理的目的、方式和范围并取得投资者的同意，具体参见 8.2.1.3 合法性之告知和 8.2.1.4 合法性之同意。

证券公司利用投资者个人信息进行自动化决策应当事前进行个人信息保护影响评估，并对处理情况进行记录。

评估点应至少包括但不限于以下内容：

- a) 是否向用户说明了自动化决策的基本原理或运行机制；
- b) 是否定期对自动化决策的效果进行评价；
- c) 是否对自动化决策使用的数据源、算法等持续优化；
- d) 是否向用户提供针对自动化决策结果的投诉渠道；
- e) 是否支持对自动化决策结果的人工复核。

证券公司利用投资者个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对投资者在交易价格等交易条件上实行不合理的差别待遇。向不同特征的投资者推荐同样的产品或服务时，应提供一致的价格。

通过自动化决策方式向投资者进行信息推送、商业营销，应当同时提供不针对投资者特征的选项，让投资者可在通用的信息推送、产品和服务营销以及量身定做的信息推送、产品和服务营销中进行选择；或者向投资者提供便捷的拒绝接受为其量身定做的信息推送、产品和服务营销的方式。

通过自动化决策方式作出对投资者个人权益有重大影响的决定，证券公司应让投资者知晓其有权要求证券公司予以说明，投资者有权拒绝证券公司仅通过自动化决策的方式作出决定。如自动化决策用于内部反洗钱管理，基于客户信息自动划分客户风险等级、进行可疑交易预警；用于适当性管理，经纪业务中运用系统自动化匹配投资者分类与产品或服务分级，并出具适当性匹配意见等对投资者个人权益有重大影响的决定时，证券公司应让投资者知晓其有权要求证券公司予以说明，并有权拒绝证券公司仅通过自动化决策的方式作出决定。

B.5 场景五：证券公司移动互联网应用程序（App）的投资者个人信息保护与合规评估

B.5.1 概述

证券公司涉及投资者个人信息处理的移动互联网应用程序（以下简称 App）主要包括证券交易类 App 与业务办理类 App。证券公司应针对相关 App 建立个人信息保护机制及个人信息处理合规评估机制。

B.5.2 证券公司App个人信息处理内容

B.5.2.1 证券交易类App处理的个人信息内容主要包括：

- a) 个人基本资料：个人姓名、电话号码、出生日期等；
- b) 网络身份标识信息：App 主体账号、内外网 IP 地址等；
- c) 个人财产信息：银行账号、资金账号、密码口令、资产信息、委托交易流水、转账流水等；
- d) 个人上网记录：App 操作记录、订阅信息等；
- e) 个人常用设备信息：MAC 地址、IMEI、IDFV、注册手机号码、App 登录手机号码、设备品牌型号、操作系统版本、App 版本等。

B.5.2.2 业务办理类App处理的个人信息内容主要包括：

- a) 个人基本资料：个人姓名、手机号码、出生日期、民族、国籍、联系地址等；
- b) 个人身份信息：身份证、港澳台证件、护照、驾驶证、军官证等；
- c) 个人生物识别信息：人脸认证信息、双录视频等；
- d) 网络身份标识信息：App 主体账号；
- e) 个人教育工作信息：学历、职业、工作单位、收入等；
- f) 个人上网记录：App 操作记录、订阅信息等；
- g) 个人位置信息：定位信息等。

B.5.3 证券公司App个人信息保护实施要点

证券公司 App 应遵循本规范中投资者个人信息全生命周期保护基本要求，以下具体实施要点可供参考。

B.5.3.1 收集

- a) 投资者在同意个人信息保护政策前，确保 App 不收集任何个人信息；
- b) 证券公司 App 应以最小化、必要性为原则收集个人信息。不得因投资者拒绝非必要个人信息收集，影响投资者使用证券交易、业务办理等基本功能；
- c) 当 App 功能更新引起个人信息收集发生变化时，证券公司应及时更新个人信息保护政策；
- d) 证券公司 App 应根据法律法规要求准确收集记录投资者个人交易终端信息；
- e) 证券公司 App 应建立已收集个人信息清单并在二级菜单中展示，应简洁、清晰列出 App(包括内嵌第三方软件工具开发包 SDK)已经收集到的投资者个人信息基本情况，包括信息种类、使用目的、使用场景等。
- f) 证券公司 App 在后台运行期间，不应收集投资者个人信息。

B.5.3.2 存储

- a) 不得在 App 服务端、客户端等日志中记录未脱敏或未加密的敏感个人信息；
- b) 不得在 App 客户端明文存储密码口令类用户鉴别信息；
- c) 人脸信息原始样本应在完成认证功能后立即删除、不得保存；
- d) 在信息系统中个人生物识别信息应与个人身份信息分开保存。

B.5.3.3 使用

- a) 三方存管银行账号、资产信息等投资者敏感个人信息在 App 客户端默认屏蔽显示；
- b) 证券公司开展 App 测试过程中不得使用未脱敏的投资者敏感个人信息；
- c) App 向投资者提供资讯推送等个性化展示时,应同时为投资者提供简单直观的退出个性化展示的选项；
- d) App 基于投资者个人信息进行自动化决策,如对投资者个人主体权益造成显著影响,证券公司应建立自动化决策结果投诉反馈渠道,由人工审核自动化决策结果并反馈；
- e) 证券公司 App 应建立与第三方共享个人信息清单并在二级菜单中展示,应简洁、清晰列出 App 与第三方共享的投资者个人信息基本情况,包括与第三方共享的个人信息种类、使用目的、使用场景和共享方式等。

B.5.3.4 删除

- a) 投资者主动提出删除个人信息要求时,App 应揭示告知个人信息删除的处理措施与证券法律法规针对相关个人信息必要存储的最小期限；
- b) App 应提供资金账号、证券账号等注册账号的销户功能,销户过程中不得设置不合理与不必要的额外要求。

B.5.3.5 身份鉴别

- a) App 应设置一定强度的密码安全策略,防止投资者设置易于猜测的密码；
- b) App 登录宜支持多种认证方式,包括但不限于密码、短信、图形手势、生物特征等；
- c) 投资者进行鉴别信息修改时应采用合适方式进行身份认证；
- d) 针对银行账号、身份信息等投资者敏感个人信息查询,App 应采用合适方式进行二次认证；
- e) 后台系统直接采信客户终端鉴别结果的,应特别关注客户终端人脸信息保护环节和鉴别结果欺诈问题,并做好风险评估、落实安全管控措施。

B.5.4 证券公司App个人信息保护合规评估生命周期管理

针对 App 的个人信息保护合规评估应涵盖系统需求分析与设计、系统开发与测试、系统上线、系统后续运维等阶段。

B.5.4.1 需求分析与设计阶段

在系统需求分析与设计阶段,App 研发方应梳理投资者个人信息处理内容与事项,设计全面、可行的个人信息保护技术方案。

B.5.4.2 系统开发与测试阶段

App 研发方应根据投资者个人信息保护技术方案进行开发,在测试阶段充分验证投资者个人信息保护相关功能的有效性,并记录测试结果。

B.5.4.3 系统上线阶段

系统上线前，证券公司应针对 App 开展专项个人信息保护合规评估，评估通过后进行系统上线。

B.5.4.4 系统后续运维

当 App 涉及个人信息相关功能发生重要变更时，证券公司应针对变更前后差异内容开展个人信息保护合规评估，评估通过后执行变更。重要变更包括但不限于：

- a) App 变更个人信息收集范围；
- b) App 变更个人信息使用范围；
- c) App 变更隐私协议内容。

证券公司应定期聘请第三方安全检测机构针对 App 进行个人信息保护合规评估。

B.5.5 证券公司App个人信息保护合规评估

证券公司 App 应按照《GB/T 35273—2020 信息安全技术 个人信息安全规范》《App 违法违规收集使用个人信息行为认定方法》等法规、标准接收合规评估，证券公司 App 个人信息保护合规评估典型评估项与违规示例：

B.5.5.1 是否公开收集使用规则、是否进行展示方式的优化。

违规示例：

- a) App 中无个人信息保护隐私政策；
- b) 未向投资者提供 App 个人信息保护政策摘要。

B.5.5.2 是否明示收集使用投资者个人信息的目的、方式和范围。

违规示例：

- a) 未逐一列出 App 收集投资者个人信息的目的、方式和范围；
- b) 收集使用投资者个人信息范围发生变化时，未以适当方式通知投资者。

B.5.5.3 是否存在未经投资者同意收集使用个人信息的情况。

违规示例：

- a) 取得投资者同意前 App 就开始收集投资者个人信息；
- b) 投资者明确不同意个人信息收集后 App 仍收集个人信息。

B.5.5.4 是否存在违反必要原则，收集与证券公司服务无关的投资者个人信息的情况。

违规示例：

- a) 在投资者拒绝非必要个人信息收集时，影响与非必要个人信息无关的功能使用；
- b) App 安装使用期间提前申请超出功能服务范围的个人信息相关权限。

B.5.5.5 是否存在未经投资者同意向第三方提供个人信息的情况。

违规示例：

App 接入第三方应用未经投资者同意直接向第三方应用提供个人信息。

B.5.5.6 是否按法律规定提供删除或更正个人信息功能或未公布投诉、举报方式等信息。

违规示例：

- a) App 未向投资者提供有效的删除个人信息或注销账号的功能；
- b) App 未向投资者公布个人信息安全的投诉反馈通道与方式。

B.5.5.7 App 是否存在频繁自启动和关联启动等情况。

违规示例：

未经投资者同意，App 频繁自启动或关联启动其他 App。

B.5.5.8 是否存在误导投资者下载 App 及开屏信息等侵害投资者权益的情况。

违规示例：

App 开屏信息无法跳过。

B.5.5.9 应用分发平台上的 App 信息是否明示到位。

违规示例：

证券公司自有应用分发平台未明示 App 运行所需权限列表及用途、收集使用个人信息的内容、目的、方式和范围。

B.5.5.10 应用分发平台管理责任是否落实到位。

违规示例：

证券公司自有应用分发平台 App 上架审核不严格、违法违规处理不及时。

B.6 场景六：证券公司信息披露中的投资者个人信息公开与保护

B.6.1 概述

证券公司信息披露涉及投资者个人信息公开的场景包括：

- a) 证券公司在提供证券承销与保荐等投行服务的过程中，根据法律法规、监管规定、自律规则等规定或要求，披露投资者的持股情况等信息；
- b) 证券公司自身在融资过程中，根据法律法规、监管规定、自律规则等规定或要求，披露与投资者相关的重大交易、诉讼（仲裁）等信息。

B.6.2 信息公开的内容

证券公司履行上述信息披露义务时，可能被公开的投资者个人信息种类通常包括个人基本信息、身份信息、交易信息等。

B.6.3 信息公开的实施与保护要点

- a) 严格按照《证券法》等法律法规及证监会、证券交易所发布的信息披露相关内容、格式准则的要求披露投资者个人信息，确保相关信息真实、准确、完整；
- b) 确保披露场所或渠道符合《证券法》等法律法规及证监会、证券交易所的要求；
- c) 设置管理信息披露事务的职能部门，安排专人实施具体工作，并对相关人员开展具体工作进行管理与培训；
- d) 建立信息披露管理制度，明确涉及投资者个人信息公开相关工作的操作规程，建立复核机制，避免因信息公开错误等不当行为给投资者造成不利后果或影响；
- e) 通过客服热线等方式受理投资者对证券公司信息披露存在的疑问或异议，及时对投资者进行解释说明或采取补救措施。

附录 C (资料性)

****个人信息保护政策

****公司(以下简称****或我们)深知个人信息对您的重要性,高度重视个人隐私和信息安全。我们将恪守权责一致、目的明确、选择同意、最少够用、确保安全、主体参与、公开透明的原则,按照法律法规的规定保护您的个人信息及隐私安全。

您浏览****互联网平台或使用我们的互联网平台服务时,我们将按照本《****个人信息保护政策》(以下称“本政策”)处理您的个人信息。如您使用****互联网平台提供的某项或某几项服务有其单独的个人信息保护政策的,该单独的个人信息保护政策将与本个人信息保护政策一起构成一份完整的个人信息保护政策。

本政策发布时间:****年*月。

本政策更新时间:****年*月。

本政策生效时间:****年*月。

根据《常见类型移动互联网应用程序必要个人信息范围规定》,****App属于投资理财类,基本功能服务为“股票、期货、基金、债券等相关投资理财服务”,必要的个人信息包括:

- 1、注册用户移动电话号码,微信号;
- 2、投资理财用户姓名,证件类型和号码,证件有效期限、证件影印件;
- 3、投资理财用户资金账户、银行卡号码或支付账号。

本政策将帮助您了解以下内容:

- 1、我们如何收集和使用您的个人信息
- 2、我们如何使用 Cookie 和同类技术
- 3、我们如何共享、转让、公开披露您的个人信息
- 4、我们如何保护您的个人信息
- 5、您的权利
- 6、我们如何处理敏感个人的个人信息
- 7、本政策如何更新
- 8、如何联系我们

请在使用我们的产品(或服务)前,仔细阅读并理解本政策。

一、我们如何收集和使用您的个人信息

个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息,不包括匿名化后的信息。前述信息的来源包括:您通过****互联网服务渠道或其他合法途径向我们提供的信息;您自行向社会公众公开的信息;您通过合法公开渠道(如合法的新闻报道、政府信息公开等)披露或合法留存于第三方的信息等。****仅会出于本政策所述的以下目的,收集和使用您的个人信息:

1、基本业务功能

为实现 App 的业务功能,我们可能需要向您收集以下个人信息。若您拒绝收集,则无法使用相应服务。

1.1、为了完成注册及接收推送

为了您能使用注册功能,且注册后的账户可以使用积分、礼券、进行收藏操作,并接受我们的推送服务,您需要向我们提供您的手机号码,我们会向您发送短信验证码,以验证您的身份。

1.2、为了办理开户

为了您能开通资金账户、证券账户、理财账户,我们会根据监管机构要求收集您的个人身份信息、个人账户信息及办理网上开户业务所需要的其他信息,包括您的个人基本信息,包括姓名、性别、出生日期、手机号码、国籍、邮箱、住址;个人身份信息,包括身份证件类型、身份证件号码、地址、签发

机关、有效期、身份证彩色照片；个人鉴别信息，包括密码信息；个人生物识别信息（指纹认证信息、人脸认证信息、个人视频、个人照片）；个人教育工作信息，包括职业、学历；开户行名称、银行卡卡号、征信信息；风险测评所采集的相关信息（参见第3条）；其他业务要求采集的信息。

根据中国证券登记结算有限公司、沪深交易所、北交所、基金公司及三方存管银行相关机构要求，我们将您填写的个人信息报送至以上机构，以便根据您的申请为您开通资金账户、股东账户、OTC账户、基金账户、建立三方存管、查询及各业务权限开通。

1.3、为了风险测评

当您使用“风险测评”功能时，需要确认您的个人基本信息（姓名、职业、年龄、学历、家庭信息、联系方式）、财务状况、投资经验、投资目标。“风险测评”收集这些信息是用于对您的风险承受能力进行评估，如您拒绝授权此类信息的，我们可能无法为您提供风险评估结果及与此相关的投资服务，但不影响我们为您提供的其他服务的正常使用。

1.4、为了身份验证

当您在开户、交易、业务办理过程中，需要进行身份验证时，我们将会在获取您授权的情况下采集您的生物信息（指纹认证信息/人脸认证信息/视频/照片）。在您的设备上完成对应信息验证后，我们仅接收验证结果，并在法律法规规定时间范围内安全存储相关验证信息。

1.5、为了登录交易账户

在您进行交易登录时，根据证券法及监管要求需记录您的IMEI、UUID、IP地址、MAC地址、IP端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC终端设备名、PC终端设备序列号、CPU序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易终端软件名称及版本，并生成登录日志进行存储。

1.6、为了资产查询及转账

为了您能使用银证转账和资产信息查询，需获取您的IMEI、UUID、IP地址、MAC地址、IP端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC终端设备名、PC终端设备序列号、CPU序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易终端软件名称及版本、交易账号、姓名、身份证件类型、身份证件号码、身份证件有效期、银行卡卡号、银行预留手机号码信息。

1.7、为了交易及业务办理

当您使用股票、信用、期权、理财产品交易及业务办理时，根据证券法及监管要求需记录您的IMEI、UUID、IP地址、MAC地址、IP端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC终端设备名、PC终端设备序列号、CPU序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易软件版本、证券账号、姓名、身份证信息、身份证件照片、性别、生日、民族、国籍、税收身份及税号，生成交易日志并按照监管要求进行存储。

1.8、为了使用行情软件、投顾服务、投资工具及协议签署

当您使用行情、投资工具、投顾服务时，我们会记录您的设备信息，包括：IMEI、UUID、IP地址、MAC地址、IP端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC终端设备名、PC终端设备序列号、CPU序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易软件版本进行相关校验。当您使用的产品功能涉及到您与****签署投资顾问服务协议、产品风险揭示书、适当性匹配，我们将会使用您的账户登录功能对身份信息进行验证，确保协议签署的有效性。

1.9、为了发送必要的通知

为了履行法定和约定的通知义务，我们会将您的电话号码提供给我们合作的通信运营商，这类提供是为提供服务所必须进行的。否则，您将无法收到必要的通知，您将存在资金损失的风险。

2、扩展业务功能

2.1、为了保障账户、资金和服务安全

为保障我们能正常地向您提供服务,维护我们服务的正常运行和改进优化我们的服务体验以及保障您的账户、资金安全,预防您的账户被他人不法侵害,我们会收集您的账户信息、IMEI、UUID、IP地址、MAC地址、IP端口号、硬盘序列号、硬盘分区信息、系统盘卷标号、PC终端设备名、PC终端设备序列号、CPU序列号、ICCID、IDFV、IMSI、AndroidID、IDFA、设备传感器、应用安装列表、实际使用手机号码、注册手机号码、操作系统版本、交易终端软件名称及版本、位置信息,这类信息是为提供服务必须收集的基础信息。如您选择关闭收集位置功能,我们将停止对您的位置信息的收集;这样做不会影响您进行交易,但可能会影响我们对安全状况的判断效果。

2.2、为您提供个性化服务及改进服务质量

为改进服务质量、防范风险、提升您的服务体验,或为您推荐更优质或更适合的服务,我们会收集您使用****互联网平台服务时的搜索记录、浏览信息。(还会向我们的关联公司和合作伙伴收集其合法留存的您的行为信息,用于向您展示和推荐更适合的****互联网平台服务)。

为了客户服务,我们会使用您提供的个人信息,包括联系方式、姓名、性别、年龄、资金账号、投资信息,以及您使用的服务类别和方式、使用服务时的操作信息、交易信息。

当您需要在微信上接收****互联网平台服务的推送消息,您可以将****资金账户与您的微信账号进行绑定,通过微信及时接收****互联网的推送消息。如您不再想要接受微信推送消息,您可以前往****微信服务号退订消息的推送设置。

为提升处理效率、降低处理成本、提高处理准确性,我们可能会委托具备相关能力的****关联公司提供这方面的服务,并且我们会要求该公司遵守严格的保密义务,禁止其将该信息用于未经您授权的用途。在特定场景下本平台需要使用设备定位、相机、麦克风情况下,本平台会在获取您的授权情况下调用相应功能。您可以随时关闭相关的授权。本平台不会在超出功能范围之外向您索取相关的授权。

如果您不希望接收到我们为您推送的个性化内容,您可以随时关闭。对于****App,您可以通过“个人中心”里的“个性化推荐”开关进行关闭。

3、其他情形

在法律法规允许的范围内,我们可能会在出现以下任一情形时收集并使用您的个人信息而无需取得您的授权同意:

- (1) 与国家安全、国防安全直接相关的;
- (2) 与公共安全、公共卫生、重大公共利益直接相关的;
- (3) 与犯罪侦查、起诉、审判和判决执行等直接相关的;
- (4) 出于维护个人信息主体或其他人的生命、财产等重大合法权益但又很难得到本人同意的;
- (5) 所收集的个人信息是个人信息主体自行向社会公众公开的;
- (6) 从合法公开披露的信息中收集个人信息的,如合法的新闻报道、政府信息公开等渠道;
- (7) 根据个人信息主体要求签订和履行合同所必需的;
- (8) 用于维护所提供的产品或服务的安全稳定运行所必需的,例如发现、处置产品或服务的故障;
- (9) 个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的;
- (10) 个人信息控制者为学术研究机构,出于公共利益开展统计或学术研究所必要,且其对外提供学术研究或描述的结果时,对结果中所包含的个人信息进行去标识化处理的;
- (11) 法律法规规定的其他情形。

如需将您的个人信息用于本政策未载明的其他用途,我们会以确认协议、具体场景下的文案确认动作等形式再次征求您的同意。

申请的设备权限如下具体所述:

在提供服务过程中,我们会调用您的一些设备权限,以下是调用涉及个人信息的权限对应的业务功能和调用权限的目的。您可以选择是否授权开通以下权限:

1、读写存储空间的权限

由于行情、资讯、应用日志存储功能需要在手机本地读写文件，因此需要获取存储权限。

2、访问相册的权限

当您进行身份认证需要提交证明材料或导入图片上传自选股、向在线客服发送照片时，您可以从本地相册中选择图片上传，因此需要获取访问相册的权限。

3、获取定位的权限

为了您能方便地进行在线办理业务，查询附近的营业部信息及保障账户安全，需要获取您的地理位置信息，因此需要获取访问定位的权限。

4、访问摄像头的权限

为了您可以通过摄像头进行身份校验（身份证识别、人脸识别、视频验证）、银行卡号码识别及其他证明材料采集，需要获取摄像头权限。

5、获取麦克风的权限

为了您能通过麦克风使用视频通话和语音识别功能进行身份验证、在开户或业务办理过程中视频验证、向在线客服发送语音时，需要获取麦克风的权限。

6、获取电话的权限

为了更好的提供服务，满足投资交易的监管要求或当您需要直接拨打客服热线时，我们需要获取您的电话权限。

7、通知权限

应用程序启动时，如果您没有打开通知权限，我们会向您询问是否打开，如果您不提供通知权限，将无法接收到系统消息推送，但不影响您使用软件的其他功能。

8、访问剪切板的权限

为方便您复制账号、卡号、资讯内容，我们需要获取您设备的剪切板权限，并在 App 启动、前后台切换时读取剪切板信息。

二、我们如何使用 Cookie 和同类技术

（一）Cookie

为确保以 html 技术实现的网页正常运转，我们会在您的计算机或移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。

我们不会将 Cookie 用于本政策所述目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。您可以清除设备上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问我们的网站时亲自更改用户设置。如需详细了解如何更改浏览器设置，您可以通过互联网搜索引擎获得不同浏览器的操作方法。

（二）网页信标和像素标签

除 Cookie 外，我们还会在网页上使用网页信标和像素标签等其他同类技术。例如，我们向您发送的短信或电子邮件可能含有链接至我们网站内容的。如果您点击该链接，我们则会跟踪此次点击，帮助我们了解您的产品或服务偏好并改善客户服务。网站信标通常是一种嵌入到网站或电子邮件中的透明图像。借助于电子邮件中的像素标签，我们能够获知电子邮件是否被打开。如果您不希望自己的活动以这种方式被追踪，则可以随时与我们联系进行退订。

（三）Do Not Track（请勿追踪）

很多网络浏览器均设有 Do Not Track 功能，该功能可向网站发布 Do Not Track 请求。目前，主要互联网标准组织尚未设立相关政策来规定网站应如何应对此类请求。但如果您的浏览器启用了 Do Not Track，那么我们的所有网页都会尊重您的选择。

三、我们如何共享、转让、公开披露您的个人信息

我们承诺对您的信息进行保密，不会与任何公司、组织和个人共享、转让、公开披露您的个人信息，以下情况除外：

1、在获取您明确同意的情况下；

2、根据法律法规、法律程序、政府的强制命令或司法裁定及要求共享的范围共享您的个人信息；
3、在您所参与的抽奖、竞赛或类似推广活动中，将您提供的信息用于管理此类活动。在前述情形下，如您中奖，我们可能会将您的手机号码或注册名进行脱敏后公布在中奖名单或竞赛名单中。如该活动系我们和第三方联合推广，我们可能与该第三方共享活动过程中产生的、为完成该等活动所必要的个人信息（如参加活动的用户数、中奖名单、中奖人联系方式），以便第三方能及时向您发放奖品或为您提供服务；

4、为了向您提供更完善、优质的产品和服务，如我们和第三方联合推广，为进行对账等数据统计需求，我们可能与该第三方共享推广过程中完成对账所必要的个人信息。

同时，我们会与合作第三方签署严格的保密协定，要求他们严格按照我们的说明、本政策以及其他任何相关的保密和采取安全措施来处理您的个人信息。我们将要求合作方无权将共享的个人信息用于任何其他用途。如果您拒绝我们的合作方在提供服务时与我们共享我们收集的为提供服务所必需的您的个人信息，将可能导致您无法在我们的平台上使用该服务；

5、在获取您同意的情况下，为了维护和改善我们的服务、处理您的相关交易或根据相关交易及业务规则进行客户账户管理，我们会使用具有相应业务能力的第三方服务 SDK 来为您提供服务，详见《个人信息第三方共享清单》https://*****，个人信息权限清单，详见《系统权限申请与使用》https://*****，个人信息收集与使用，详见《个人信息收集与使用》https://*****；

6、根据法律法规及相关规定要求，我们需要将您在使用****互联网平台过程中的注册信息、交易信息报送给证券交易所、中国证券登记结算有限公司、金融产品发行方等机构，用于完成这些机构对交易过程的确认、结算及监督。

四、我们如何存储及保护您的个人信息

我们收集和产生的个人信息将存储在中华人民共和国境内。

我们承诺将使信息安全保护达到合理的安全水平。我们通过建立数据分类分级制度、数据安全管理办法来管理规范个人信息的存储和使用，并建立数据安全专职岗位、数据安全应急响应机制来推进和保障个人信息安全。为保障您的信息安全，我们致力于使用各种网络安全层软件（SSL）进行加密传输、信息加密存储、严格限制数据中心的访问、使用专用网络通道及网络代理等安全技术及配套的管理体系来防止您的信息被泄露、毁损或者丢失。

我们将按照相关法律法规及行业监管要求的保存期限对您的个人信息进行保存。

请您理解，由于技术水平限制及可能存在的各种恶意手段，实践中我们对您的信息保护仍然可能因我们可控制范围外的因素而存在不确定性。

如我们停止运营，我们将及时停止收集您个人信息的活动，且对所持有的个人信息进行删除或匿名化处理。

五、您的权利

按照中国相关的法律、法规、标准，以及其他国家、地区的通行做法，我们保障您对自己的个人信息行使以下权利：

（一）查询您的个人信息

您有权查询您的个人信息，法律法规规定的例外情况除外。如果您想行使数据访问权，可以通过以下方式自行访问：

用户信息——您可通过个人中心查询及管理您的用户信息，包括绑定微信、手机号码、地址等；

交易相关的账户信息——如果您希望查询或编辑您的账户中的个人资料信息和账户信息、更改您的密码、添加安全信息，您可以通过访问业务办理功能中的账户查询及资料修改模块执行此类操作。

搜索信息：您可以在搜索栏中查询或清除您的搜索历史记录、查看相关数据。

如果您无法通过上述方式查询这些个人信息，您可以随时联络我们的官方客户热线****，或发送电子邮件至*****@*****.com.cn。我们将在 15 个工作日内回复您的访问请求。

对于您在使用我们的产品或服务过程中产生的其他个人信息，只要不需要过多投入，我们会向

您提供。如果您想行使数据访问权，请发送电子邮件至*****@*****.com.cn。

（二）更正您的个人信息

当您发现我们处理的关于您的个人信息有错误时，您有权要求我们做出更正。您可以通过“业务办理”功能提出个人信息更正申请。

如果您无法通过上述链接更正这些个人信息，您可以随时联络我们的官方客户热线*****，或发送电子邮件至*****@*****.com.cn。我们将在 15 个工作日内回复您的访问请求。

（三）删除您的个人信息

在以下情形中，您可以向我们提出删除个人信息的请求：

- 1、如果我们处理个人信息的行为违反法律法规；
- 2、如果我们收集、使用您的个人信息，却未取得您的同意；
- 3、如果我们处理个人信息的行为违反了与您的约定；

当您从我们的服务中删除信息后，我们可能不会立即从备份系统中删除相应的信息，但会在备份更新时删除这些信息。

您可通过电子邮箱*****@*****.com.cn 或拨打客服热线*****申请删除您的个人信息。我们将尽快审核您的申请，并在验证您的用户身份后的十五个工作日内回复。

（四）个人信息副本获取

如您需要您的个人信息的副本，您可以通过本政策提供的方式联系我们，在核实您的身份后，我们将向您提供您在我们的服务中的个人信息副本(包括基本资料、身份信息)，但法律法规另有规定的或本政策另有约定的除外。

（五）撤回同意或改变您授权同意的范围

您总是可以选择是否向我们披露个人信息。每个业务功能需要一些基本的个人信息才能得以完成（见本政策“第一部分”）。您可以通过撤回个人信息授权、关闭设备权限、注销账户等方式改变您授权我们继续收集信息的范围或撤回您的授权。

当撤回授权后，我们无法继续为您提供撤回授权所对应的服务，也不再处理您相应的信息。但您撤回授权的决定，不会影响此前基于您的授权而开展的信息处理。

（六）注销账户

您随时可注销此前注册的****互联网平台账号。在您主动注销之后，我们将停止为您提供服务，并依据您的要求，删除您的个人信息，但法律法规、监管规定、自律规则等另有规定的除外，您在使用****互联网服务期间提供或产生的信息我们仍需按照上述规定要求的时间进行保存，且在该保存的时间内依法配合有关机关的查询。

在 App 中，您可以通过 App 左上角头像—个人资料—手机号码—注销账号进行账号注销。注销后，与该账号有关的积分、礼券、订阅、收藏、消息、自选股等信息将不再保留。

您还可以通过拨打****客户热线进行注销，我们将根据适用法律及相关规定的要求在 15 个工作日内完成核查和处理。

（七）响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。我们可能会先要求您验证自己的身份，然后再处理您的请求。

我们将在十五个工作日内做出答复。于您合理的请求，我们原则上不收取费用，但对多次重复、超出合理限度的请求，我们将视情收取一定成本费用。对于那些无端重复、需要过多技术手段（例如，需要开发新系统或从根本上改变现行惯例）、给他人合法权益带来风险或者非常不切实际（例如，涉及备份磁带上存放的信息）的请求，我们可能会予以拒绝。

在以下情形中，按照法律法规要求，我们将无法响应您的请求：

- 1、与国家安全、国防安全直接相关的；
- 2、与公共安全、公共卫生、重大公共利益直接相关的；

- 3、与犯罪侦查、起诉、审判和判决执行等直接相关的；
- 4、有充分证据表明您存在主观恶意或滥用权利的；
- 5、响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的；
- 6、涉及商业秘密的。

六、我们如何处理敏感个人的个人信息

如您为未成年人，请您的父母或监护人阅读本政策，并请您在取得父母或监护人同意的前提下使用我们的服务或向我们提供您的信息。如您的监护人不同意您按照本政策使用我们的服务或向我们提供信息，请您立即终止使用我们的服务并及时通知我们，以便我们采取相应的措施。****将根据国家相关法律法规的规定保障未成年人的个人信息的保密性及安全性。

七、本政策如何更新

我们的个人信息保护政策可能变更。

未经您明确同意，我们不会削减您按照本个人信息保护政策所应享有的权利。我们会在本页面上发布对本政策所做的任何变更。

对于重大变更，我们还会提供更为显著的通知（包括对于某些服务，我们会通过系统公告发送通知，说明个人信息保护政策的具体变更内容）。

本政策所指的重大变更包括但不限于：

- 1、我们的服务模式发生重大变化。如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；
- 2、我们在所有权结构、组织架构等方面发生重大变化。如业务调整、破产并购等引起的所有者变更等；
- 3、个人信息共享、转让或公开披露的主要对象发生变化；
- 4、您参与个人信息处理方面的权利及其行使方式发生重大变化；

八、如何联系我们

对于您个人信息权利方面的投诉、举报可以通过以下方式与我们联系。

公司名称：*****公司

公司地址：*****

电子邮箱：*****@*****.com.cn

客服热线：*****

我们将尽快审核您提出的问题，并在验证您的用户身份后的十五个工作日内回复。

如果您对我们的回复不满意，特别是您认为我们的个人信息处理行为损害了您的合法权益，双方应通过友好协商解决，协商不成，您还可以通过向*****人民法院提起诉讼的方式寻求解决方案。

参 考 文 献

- [1] 中华人民共和国个人信息保护法（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过）
- [2] 中华人民共和国证券法（2019年12月28日第十三届全国人民代表大会常务委员会第十五次会议第二次修订）
- [3] 证券投资基金经营机构信息技术管理办法（证监会令[第179号] 2021年修正）
- [4] 证券期货业网络和信息安全管理办法（证监会令[第218号]）
- [5] 证券期货业网络安全事件报告与调查处理办法(证监会公告[2021]12号)
- [6] 证券经纪业务管理办法（证监会令[第204号]）
- [7] 数据出境安全评估办法（国家互联网信息办公室令[第11号]）
- [8] AFCA—FTCC std 0003—2022个人金融信息保护指南
- [9] 人脸识别技术应用安全管理办法（国家互联网信息办公室 中华人民共和国公安部令[第19号]）
- [10] 个人信息保护合规审计管理办法（国家互联网信息办公室令[第18号]）
- [11] 个人信息保护法理解与适用（程啸 著）
- [12] 证券公司客户资金账户管理规则（协会第七届理事会第16次会议表决通过2023年6月9日发布并生效）
- [13] 粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引（国家互联网信息办公室 香港创新科技及工业局公告2023年3号）
- [14] 证券期货业已发布标准术语汇编（2004年—2023年）
- [15] 证券公司客户交易终端信息管理技术规范（证保发[2020]9号）
- [16] ISO/IEC 29100:2024 Information technology-Security techniques-Privacy framework
- [17] 网络数据安全条例(中华人民共和国国务院令[第790号], 2024年8月30日国务院第40次常务会议通过)

证券行业应用RPA技术的通用功能和接口规范

T/TSAC 002—2025

(经协会第七届理事会第四十一次会议审议通过, 2025年12月15日发布实施)

(中证协发〔2025〕260号)

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分: 标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利, 本文件的发布机构不承担识别专利的责任。

本文件由国联民生证券股份有限公司提出。

本文件由中国证券业协会归口。

本文件起草单位: 国联民生证券股份有限公司、中国国际金融股份有限公司、兴业证券股份有限公司、上海证券有限责任公司、国新证券股份有限公司、湘财证券股份有限公司、国泰海通证券股份有限公司、东亚前海证券有限责任公司、中银国际证券股份有限公司、华泰证券股份有限公司、西部证券股份有限公司、东北证券股份有限公司、东方证券股份有限公司、华宝证券股份有限公司、申万宏源证券股份有限公司、中泰证券股份有限公司、北京朗思智能科技有限公司、珠海金智维信息科技有限公司、上海弘玑信息技术有限公司、上海容智信息技术有限公司、来也科技(北京)有限公司。

本文件主要起草人: 刘洪松、吴哲锐、程龙、李予涛、褚卫忠、樊建、王飞、李姣、张思睿、吴冰、牟大恩、杨文琦、姜婷婷、孙浅尘、沈一星、曹啸、张校、潘嘉侃、肖金伟、肖雅雯、汪付申、仇进、张佳佳、任荣、姚振、王彦瑞、屈文浩、陈磊、柴亚团、范里鸿。

引 言

机器人流程自动化（Robotic Process Automation，简称RPA）是一种软件技术，它使得企业能够通过软件机器人，也就是“虚拟员工”，来自动执行重复且繁琐的业务流程任务。软件机器人能够模拟人类用户的行为，包括鼠标点击、数据输入及与应用程序的交互等，从而显著提升工作效率、减少人为错误，并优化整个业务流程。

目前，RPA产业已步入一个成熟的发展阶段，其在证券行业的应用也日益广泛。随着证券公司创新应用深度和规模的持续拓展，市场上涌现出众多RPA产品和解决方案。然而，由于不同服务商提供的RPA产品在接口开放性、证券行业软件的兼容性方面存在差异，导致RPA在证券公司部署、升级和维护过程中的成本居高不下。

为了有效管理RPA并降低应用风险，证券公司正逐步构建可以对RPA进行集中调用和研发运维管理的数字员工平台、RPA运营管理平台或超自动化平台等。在这一过程中，规范RPA的接口标准和核心功能显得尤为重要，它将有助于证券公司减少因采用多家RPA产品及在不同产品间切换的成本和风险。而对于RPA服务商而言，这也能够显著降低他们在证券行业的实施成本，实现双赢。

1 范围

本文件规定了RPA通用功能及接口规范。
本文件适用于证券行业RPA应用与系统建设。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 11457—2006 信息技术—软件工程术语
GB/T 32908—2016 非结构化数据访问接口规范
JR/T 0233—2021 证券期货业经营机构内部应用系统日志规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

RPA robotic process automation

RPA即机器人流程自动化,是一种自动化技术。它通过软件机器人来模拟人类用户与计算机的交互过程,实现自动化执行重复性、规则性的业务流程。

3.2

管理平台 management platform

管理平台是指用于管理和监控机器人和流程的中心化系统。它提供了对机器人活动的实时监视、配置和控制的功能。

3.3

机器人 robot

机器人是一种基于软件的自动化工具,能够模拟人类用户的行为和交互,执行开发好的RPA流程,实现业务流程自动化。包含前台机器人、后台机器人等。前台机器人即有人值守机器人,指需要在人工监督下运行的机器人,由用户或特定用户事件触发。后台机器人即无人值守机器人,指无需人工监督即可执行作业的机器人,通常部署在单独的计算机上运行。

3.4

设计器 designer

设计器是一种用于创建和设计RPA流程的软件。

3.5

应用程序编程接口 application programming interface

应用程序编程接口,简称接口,是一组预先定义的函数,它允许应用程序和开发人员在不访问源代

码或理解其内部工作机制的情况下，基于某个软件或硬件访问一组功能。

3.6

许可 license

许可是管理机器人、设计器使用权限的文件。可以激活不同类型、不同数量的机器人、设计器并设定到期时间。

3.7

部门 department

部门是一个组织中按照功能、业务、地域等因素划分出来的一个部分，通常由一组人员组成，负责完成特定的任务或服务。部门之间数据隔离。

3.8

用户 user

用户是使用服务的人员，通常拥有一个用户账号。在部门下可以创建用户账号，用户根据权限可以操控部门下的流程、调度、任务、数据队列、凭据、资产、文件等。

3.9

流程 process

流程是一组需要自动化处理的任务或操作序列。

3.10

流程包 process package

流程包是一个容器，用于存储自动化流程和资源文件。它可以包含多个流程文件、配置文件和其他资源文件。

3.11

调度 trigger

调度是指根据预设的时间表或触发条件，安排机器人执行流程的过程。

3.12

任务 task

任务是流程执行的一个具体实例。

3.13

数据队列 data queue

数据队列是一种用于存储和管理待处理数据的容器。它通常用于需要机器人批量执行任务的场景，以便存储每次执行任务所需的数据参数。

3.14

凭据 credential

凭据是用于验证身份和访问受限资源的信息，如账户、密码等。凭据支持加密存储并供流程执行过

程中进行调用。

3.15

资产 asset

资产是用户创建的变量，用于定义不同类型的参数（如字符串、整型、布尔型等），可供流程在执行过程中进行调用。

3.16

身份验证令牌 token

一种数字凭证，用于验证用户身份或授权用户访问特定资源。

4 缩略语

API：应用程序编程接口（Application Programming Interface）

CPU：中央处理器（Central Processing Unit）

CRM：客户关系管理（Customer Relationship Management）

DDOS：分布式阻断服务（Distributed Denial of Service）

GIT：分布式版本控制系统(Global Information Tracker)

HTTP：超文本传输协议（Hypertext Transfer Protocol）

HTTPS：以安全为目标的HTTP通道(Hypertext Transfer Protocol Secure)

IM：即时通讯（Instant Messaging）

IP：网际互连协议（Internet Protocol）

JSON：一种轻量级的数据交换格式（JavaScript Object Notation）

OA：办公自动化（Office Automation）

REST：表象化状态转变，是一种软件架构风格、设计风格（Representational State Transfer）

ROI：投资回报率（Return On Investment）

RPA：机器人流程自动化（Robotic Process Automation）

SLA：服务等级协议（Service Level Agreement）

SVN：版本管理工具(Subversion)

TA：登记过户（Transfer Agent）

UTF-8：针对Unicode的一种可变长度字符编码(Unicode Transformation Format-8 bits)

5 通用功能

5.1 基本功能

5.1.1 基本架构

基本架构应包含设计器、机器人、管理平台三大核心功能组件。设计器与机器人支持独立部署，无需依赖管理平台。三大功能组件升级时，宜具备向后兼容能力。

5.1.2 设计器

设计器功能包括但不限于以下内容：

- 支持工作控制流、快捷键、浏览器、桌面程序、窗口、Excel 表格、压缩程序、接口、文件操作、

数据抓取、访问数据库、语音识别、图像识别等多种场景开发需求；

- 支持图形化编程和代码编程两种方式；
- 支持脚本智能识别 UI 元素，即使在分辨率变化、窗口位置变动或 UI 遮挡的情况下，也能保持执行的准确性和稳定性；
- 支持自动的版本管理及版本对比；
- 支持自定义组件；
- 支持流程调试功能，包括单步调试，模拟参数执行等；
- 支持通过录制人工操作过程自动创建流程。

5.1.3 机器人

机器人功能包括但不限于以下内容：

- 支持定时触发、人工触发、快捷键触发等多个模式；
- 支持流程运行后，机器人提供运行日志、记录流程进度等；
- 支持系统锁屏状态下，机器人运行不受影响，并具备自动解锁功能，自动解锁完成任务后或遇到异常情况而导致任务终止时，具备自动重新锁屏的能力；
- 支持无屏幕、无远程桌面状态下，机器人运行不受影响；
- 支持多种操作系统，包括 Windows Server、Windows 桌面版，Linux 系统中的 Redhat、CentOS、Debian 和 Ubuntu 等主流版本，以及国产操作系统中的统信、麒麟、中标麒麟、银河麒麟、欧拉等主流版本；
- 支持 secret 密钥认证并通过接口直接控制机器人；
- 支持高密度部署，即在一台服务器上同时部署多个机器人。

5.1.4 管理平台

管理平台功能包括但不限于以下内容：

- 支持统一管理设计器、机器人的许可；
- 支持机器人生命周期管理，可以创建、修改、删除机器人，能够对机器人进行启动、暂停、继续、停止操作；
- 支持机器人池和任务数据队列，可以将一组任务分发给一组机器人完成；
- 支持流程包的上传、下载功能；
- 支持证券行业多种交易日历的配置；
- 支持单节点部署、应用与数据分离式部署、高可用部署等多种部署模式，以满足不同的可用性需求；
- 支持流程、调度、任务、数据队列、凭据、资产、文件、日志等模糊查询。

5.2 调度功能

调度功能包括但不限于以下内容：

- 支持创建调度，能够设置任务的优先级、调度方式（例如：定时调度、数据队列调度）、部门、流程版本、机器人、SLA 时间（例如：最大运行时长、最大等待时间）、执行时间、日历等；
- 支持查看调度任务的当前状态（如运行中、待运行）以及已执行任务的详细情况，例如运行结果和运行日志；
- 支持修改、停用、启用、删除、筛选已创建的调度。

5.3 运维功能

运维功能包括但不限于以下内容：

- 支持对机器人状态、任务执行情况、服务器资源监控触发通知、告警；
- 支持查看机器人服务器的软硬件信息，如操作系统、IP 地址、CPU、磁盘、内存等指标；
- 支持远程对机器人服务器重启、关机和远程桌面连接；

- 支持机器人运行录屏监控和实时监控；
- 支持在管理平台上传、下载机器人安装包并批量升级机器人。

5.4 日志管理功能

日志管理功能包括但不限于以下内容：

- 流程执行日志：记录流程执行的详细步骤和异常信息，用于性能监控和错误追踪；
- 流程执行录屏：支持手动开启或关闭录屏功能，满足审计和隐私保护需求。录制内容加密存储，视频包含时间戳、操作者、机器人标识和步骤描述，便于定位和回溯；
- 流程变更记录：记录管理平台中流程版本变更历史；
- 用户操作日志：记录用户在管理平台的所有操作，包括登录、配置更改、流程管理等，以支持审计；
- 接口调用日志：记录接口调用的关键信息，便于故障排查和问题定位。

5.5 资源管理功能

资源管理功能包括但不限于以下内容：

- 文件管理：提供全面的文件和文件夹管理功能，包括创建、删除、修改和查询，以及文件的上传和下载；
- 参数管理：用于存储业务系统登录凭据和其他敏感信息，同时管理各类资产，如字符串、数值和哈希值；
- 数据队列管理：允许创建、查看、编辑和删除数据队列，支持数据项的导入、导出、筛选和搜索；
- 机器人资源管理：实现机器人的分组管理，并提供查看、停用、启用和删除机器人的权限控制。

5.6 运营功能

运营功能包括但不限于以下内容：

- 流程台账：包括流程名称、部门、业务人员、研发负责人、运维负责人、机器人组、流程包版本等并能够通过以上维度进行统计筛选；
- 任务台账：包括流程名称、部门、机器人、任务类型、许可类型、运行状态、任务优先级、开始时间、结束时间、运行时长等并能够通过以上维度进行统计筛选，展示任务排班计划表；
- 许可台账：记录许可类型、许可状态、部门、机器人等并能够通过以上维度进行统计筛选；
- 机器人台账：记录机器人客户端信息、许可状态、机器人利用率等并能够通过以上维度进行统计筛选；
- ROI 效能台账：显示流程执行成功率，支持按部门、机器人、流程等维度分析节省的时间和成本。

5.7 系统管理功能

系统管理功能包括但不限于以下内容：

- 角色管理：允许创建、导入和导出角色，并设置角色的操作权限，涵盖流程、调度、任务、数据队列、凭据、资产、文件、机器人和日志等；
- 部门管理：支持构建部门架构，并实现基于架构的数据权限隔离；
- 用户管理：支持创建用户和用户组，分配部门归属和角色；
- 许可管理：集中管理许可，包括不同期限的许可，并支持手动回收；
- 登录设置管理：设置登录超时时间、密码安全（如强度、有效期）和登录失败限制，支持双因子（手机验证码+账号密码）认证，并可基于 IP 设置登录白名单和黑名单；
- 日志文件设置管理：定义日志清理和文件备份策略，以及备份存储配置；
- 审计日志管理：提供操作审计日志的筛选和导出功能；
- 消息通知管理：配置邮件、短信、即时通讯等通知方式，并设置消息级别；
- 外部数据对接：支持与外部系统组织架构数据的集成，便于与券商已有系统进行集成。

6 接口规范和列表

6.1 接口规范

6.1.1 接口方法与数据交换

6.1.1.1 通信协议与数据交换格式

为了获得更高的安全性，宜使用HTTPS协议。
宜使用JSON作为数据交换的格式。

6.1.1.2 字符编码

请求及返回结果宜使用UTF-8进行数据编码，确保数据的正确传输和解析。

6.1.1.3 接口访问方法规范

宜使用RESTful接口类型。
宜通过HTTPS的POST协议进行接口调用。

6.1.1.4 请求参数

本文件列示的所有接口的请求参数均由Header参数和Body参数组成。其中Header参数统一定义如表1所示，Body参数则详见6.2、6.3章节各接口的定义。

表 1 Header 参数

参数名称	数据类型	是否必须	详细说明
content-type	application/json;charset=utf-8	是	数据格式为JSON；编码方式为UTF-8
token	string	是	字符令牌
version	string	是	接口版本号
章节6.2.1.1和6.3.1.1中定义接口不包含token参数。			

6.1.1.5 响应结果

本标准列示的所有接口请求的响应结果如表2所示，其中data为返回业务参数，具体详见6.2、6.3章节各接口的定义。

表 2 响应结果

返回参数	数据类型	说明
resultCode	string	业务状态码
message	string	消息内容
data	string	返回业务参数
resultCode详见章节6.1.1.8。		

示例：

```
正常返回：{  
    "resultCode": "00000",  
    "message": "无业务异常。",  
    "data": {
```

```

        "name": "user1"
    }
}
异常返回: {
    "resultCode": "10001",
    "message": "token 无效。",
    "data": {}
}

```

6.1.1.6 HTTP 状态码规范

本标准列示的所有接口统一使用HTTP状态码来表示接口操作的结果。常见的HTTP状态码如表3所示:

表 3 HTTP 状态码

状态码	状态码英文名称	中文描述
200	Ok	请求成功
201	Created	成功创建了新资源
400	Bad Request	参数错误
401	Unauthorized	未许可的访问
403	Forbidden	禁止访问该资源
404	Not Found	请求的资源不存在
409	Conflict	请求与另一个请求冲突
429	Too Many Requests	太多请求
500	Internal Server Error	服务器内部错误

6.1.1.7 业务状态码规范

业务状态码应设计为能够快速溯源且简单易记。字符串类型,长度共5位。其中,正常状态码为00000。对于其他业务状态码,它们由三部分构成:第一位数字代表一级宏观业务错误码;第二至第三位数字代表二级宏观业务错误码;第四至第五位数字则代表三级宏观业务错误码。

具体业务状态码范围请参考下表:

表 4 业务状态码

业务状态码	状态类型
00000	业务正常
1****	通用业务错误码
2****	服务器相关业务错误码
3****	权限相关业务错误码

常见的业务状态码见附录A。

6.1.1.8 接口认证机制

所有接口的安全认证一律采用token认证机制。token为字符串格式。服务端会为每个合法的接口用

户生成一个唯一的token，这个token应具有足够的复杂性和随机性。接口用户在发送接口请求时，需要在请求参数中包含token。服务端接收到请求后，会检查请求中的token是否有效（包括验证token格式、有效期、以及与用户身份的关联）。如果token验证成功，系统认为用户拥有指定的操作权限，并执行相关操作；如果token验证失败，系统将忽略该操作并返回错误信息。

6.1.2 接口的调用监控管理

6.1.2.1 监控指标

在此定义被监控的关键指标以评估接口的性能和健康状态。宜包含：

- 接口调用次数：记录每个接口的调用次数，包括成功和错误的调用；
- 平均响应时间：跟踪每个接口的平均响应时间，用于衡量接口的性能；
- 错误率：计算错误调用与总调用次数之间的比例，以确定接口的可靠性。

6.1.2.2 监控策略

在此明确调用监控的策略和流程，确保接口调用的及时监控和异常处理。宜包含：

- 监控时间范围：规定监控的时间范围，例如每天、每周或每月等，对于内置了交易日历的管理平台，还需要支持每交易日；
- 监控频率：规定监控指标的采集频率，如每分钟、每小时或每天；
- 异常告警机制：定义当监控指标超过预设阈值时的告警方式和操作流程；
- 配置负责人员：配置负责监控和处理异常的人员。

6.1.2.3 日志记录

在此明确接口调用过程中的关键信息应被记录下来，以支持故障排查和问题定位。宜包含：

- 跟踪标识：表示本条功能处理的跟踪标志，全局唯一，伴随着本次业务处理全程；
- 来源标识：表示本次业务调用的来源方。如果来源方是用户操作，可记录用户账户、机器 IP，如果是服务器，记录发起调用的系统服务名称、机器 IP；
- 请求参数：记录接口调用时传递的请求参数，包括请求方式、请求地址、Header 参数、Body 参数等；
- 响应结果：记录接口返回的响应结果，包括 HTTP 状态码、业务状态码、消息内容、返回业务参数等；
- 调用时间：记录接口调用的时间戳，用于性能分析和故障排查；
- 调用者：记录调用接口的用户或系统身份，以便追踪和审核操作行为。

6.1.3 接口的信息安全规范

6.1.3.1 访问控制

在此要求对接口进行严格的访问控制，确保只有许可用户或系统可以进行访问。以下是访问控制规范：

- 强身份验证：使用安全的身份验证机制，例如基于 token 的认证，确保只有经过身份验证的用户才能访问接口；
- 接口授权管理：支持对接口进行分组并提供细分颗粒度的访问许可授权，可以允许不同身份的应用调用者（比如业务程序或运维监控程序）或不同 IP 分别调用不同的接口且不能越权访问其他未经授权的接口，授权接口有且只能访问授权范围内的数据；
- 接口限流管理：为避免产生 DDOS 攻击影响正常接收和响应请求，应提供突发高频请求的流量控制功能。

6.1.3.2 数据加密

在此要求对接口传输的敏感信息进行加密保护，以防止数据泄露和篡改。以下是数据加密规范：

- 传输层加密：使用安全协议（如 HTTPS）对接口的传输进行加密，确保数据在传输过程中的机密性和完整性；
- 数据存储加密：对敏感数据在存储过程中进行加密，采用高强度的加密算法和严格的密钥管理策略，以防止数据泄露。

6.1.3.3 输入验证

在此要求对接口收到的输入进行有效性检查，防止恶意输入和攻击。以下是输入验证规范：

- 参数校验：验证接口的输入参数，包括参数类型、长度、格式等，以防止恶意输入和非法操作；
- 白名单/黑名单：使用白名单和黑名单技术，限制接口接受的输入内容，防止恶意输入和安全漏洞利用。

6.1.4 接口版本管理

6.1.4.1 版本号命名规范

在此要求接口版本采用统一的命名规范，以便开发人员、用户理解和使用。宜使用“主版本号.次版本号.补丁版本号”的格式进行版本号命名，例如1.0.1。版本号详细说明如下：

- 主版本号：标记接口重大改动或不兼容变化，接口发生不兼容改动时递增；
- 次版本号：标记接口功能增强或向后兼容变化，接口新增功能时递增；
- 补丁版本号：标记接口错误修复或小改进，接口进行错误修复时递增。

6.1.4.2 接口变更记录

在此要求记录接口版本的变更记录。以下是变更记录规范：

- 更新日志：编写详细的更新日志，描述每个版本的变更内容、修复的问题和创建的功能等；
- 发布说明：为每个版本提供发布说明文档，介绍新功能的使用方法、已知问题和兼容性信息等。

6.1.4.3 向后兼容性保证

当对接口进行更新时，宜尽量保持向后兼容性，避免破坏现有调用方的功能，以便现有系统和用户能够平滑升级。可以通过添加新的接口方法、增加可选参数等方式来扩展接口功能，而不影响原有调用方式。

6.2 管理平台接口

本章节定义RPA管理平台需提供的接口。

6.2.1 认证接口

功能说明：获取管理平台认证凭证。

请求地址：/api/platform/account/authenticate

Body参数：

表 5 管理平台认证接口 Body 参数

参数名称	数据类型	是否必须	详细说明
username	string	是	用户账号
password	string	是	密码（密文）

返回业务参数：

表 6 管理平台认证接口返回业务参数

参数名称	数据类型	详细说明
token	string	字符令牌
expirationTime	string	token 过期时间，格式为 yyyy-MM-dd HH:mm:ss

6.2.2 部门管理接口

6.2.2.1 创建部门

功能说明：创建部门。

请求地址：/api/platform/department/create

Body参数：

表 7 管理平台创建部门接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depName	string	是	部门名称
parentId	int	是	父级部门 ID

返回业务参数：

表 8 管理平台创建部门接口返回业务参数

参数名称	数据类型	详细说明
depId	int	部门 ID

6.2.2.2 删除部门

功能说明：删除部门及其下属部门。

请求地址：/api/platform/department/delete

Body参数：

表 9 管理平台删除部门接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID

返回业务参数：

无

6.2.2.3 更新部门

功能说明：更新部门信息。

请求地址：/api/platform/department/update

Body参数：

表 10 管理平台更新部门接口 Body 参数

参数名称	数据类型	是否必须	详细说明
------	------	------	------

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID
parentId	int	否	父级部门 ID
depName	string	否	部门名称

返回业务参数：

无

6.2.2.4 查询部门列表

功能说明：获取该部门及其子部门的列表。

请求地址：/api/platform/department/list

Body参数：

表 11 管理平台查询部门列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 12 管理平台查询部门列表接口返回业务参数

参数名称	数据类型	详细说明
departments	array	部门列表 包括字段： depId int 部门 ID， depName string 部门名称， parentId int 父级部门 ID， isDeleted boolean 是否删除

6.2.3 用户管理接口

6.2.3.1 创建用户

功能说明：创建用户。

请求地址：/api/platform/employee/create

Body参数：

表 13 管理平台创建用户接口 Body 参数

参数名称	数据类型	是否必须	详细说明
------	------	------	------

参数名称	数据类型	是否必须	详细说明
employeeName	string	是	员工名称
username	string	是	用户账号
password	string	是	密码（密文）
depId	int	是	部门 ID
email	string	否	邮箱
mobile	string	否	手机号码

返回业务参数：

表 14 管理平台创建用户接口返回业务参数

参数名称	数据类型	详细说明
employeeId	int	员工 ID

6.2.3.2 删除用户

功能说明：删除用户。

请求地址：/api/platform/employee/delete

Body参数：

表 15 管理平台删除用户接口 Body 参数

参数名称	数据类型	是否必须	详细说明
employeeId	int	是	员工 ID

返回业务参数：

无

6.2.3.3 更新用户

功能说明：更新用户信息。

请求地址：/api/platform/employee/update

Body参数：

表 16 管理平台更新用户接口 Body 参数

参数名称	数据类型	是否必须	详细说明
employeeId	int	是	员工 ID
employeeName	string	否	员工名称
username	string	否	用户账号
password	string	否	密码（密文）
email	string	否	邮箱
mobile	string	否	手机号码

返回业务参数：

无

6.2.3.4 查询用户

功能说明：查询用户信息。

请求地址：/api/platform/employee/query

Body参数：

表 17 管理平台查询用户接口 Body 参数

参数名称	数据类型	是否必须	详细说明
employeeId	int	是	员工 ID

返回业务参数：

表 18 管理平台查询用户接口返回业务参数

参数名称	数据类型	详细说明
employeeName	string	员工名称
username	string	用户账号
password	string	密码（密文）
depId	int	部门 ID
email	string	邮箱
mobile	string	手机号码
userStatus	int	用户状态（0-正常 1-已锁定）
isDeleted	boolean	是否删除

6.2.3.5 查询用户列表

功能说明：查询部门下的用户列表。

请求地址：/api/platform/employee/list

Body参数：

表 19 管理平台查询用户列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 20 管理平台查询用户列表接口返回业务参数

参数名称	数据类型	详细说明
users	array	用户列表 包括字段： employeeId int 员工 ID，

参数名称	数据类型	详细说明
		employeeName string 员工名称, username string 用户账号, depId int 部门 ID, userStatus int 用户状态 (0-正常 1-已锁定), isDeleted boolean 是否删除

6.2.4 流程包管理接口

6.2.4.1 创建流程包

功能说明：创建流程包。

请求地址：/api/platform/package/create

Body参数：

表 21 管理平台创建流程包接口 Body 参数

参数名称	数据类型	是否必须	详细说明
packageName	string	是	流程包名称
package	file	是	流程包
packageVersion	string	是	流程包版本
depId	int	是	部门 ID

返回业务参数：

表 22 管理平台创建流程包接口返回业务参数

参数名称	数据类型	详细说明
packageId	int	流程包 ID

6.2.4.2 删除流程包

功能说明：删除流程包。

请求地址：/api/platform/package/delete

Body参数：

表 23 管理平台删除流程包接口 Body 参数

参数名称	数据类型	是否必须	详细说明
packageId	int	是	流程包 ID

返回业务参数：

无

6.2.4.3 查询流程包列表

功能说明：查询部门下的流程包列表。

请求地址：/api/platform/package/query

Body参数：

表 24 管理平台查询流程包列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 25 管理平台查询流程包列表接口返回业务参数

参数名称	数据类型	详细说明
packageList	array	流程包列表 包括字段： packageName string 流程包名称， packageId int 流程包 ID， packageVersion string 流程包版本， packageUrl string 流程包下载地址， depId int 部门 ID， isDeleted boolean 是否删除

6.2.5 流程管理接口

6.2.5.1 创建流程

功能说明：创建流程。

请求地址：/api/platform/process/create

Body参数：

表 26 管理平台创建流程接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processName	string	是	流程名称
remark	string	否	流程备注
depId	int	是	部门 ID
robotGroupId	int	是	机器人组 ID
isRecord	boolean	是	是否录屏

返回业务参数：

表 27 管理平台创建流程接口返回业务参数

参数名称	数据类型	详细说明
processId	int	流程 ID

6.2.5.2 流程激活流程包版本

功能说明：流程激活流程包版本。

请求地址：/api/platform/process/activate-package-version

Body参数：

表 28 管理平台流程激活流程包版本接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID
packageId	int	是	流程包 ID
inParameters	array	否	入参列表 包括字段： name string 参数名， value string 参数值

返回业务参数：

无

6.2.5.3 删除流程

功能说明：删除流程。

请求地址：/api/platform/process/delete

Body参数：

表 29 管理平台删除流程接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID

返回业务参数：

表 30 管理平台删除流程接口返回业务参数

参数名称	数据类型	详细说明
affectedTriggerIds	array	受影响调度 ID 组

6.2.5.4 更新流程

功能说明：更新流程信息。

请求地址：/api/platform/process/update

Body参数：

表 31 管理平台更新流程接口 Body 参数

参数名称	数据类型	是否必须	详细说明
------	------	------	------

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID
processName	string	否	流程名称
remark	string	否	流程备注
robotGroupId	int	否	机器人组 ID
isRecord	boolean	否	是否录屏

返回业务参数：

无

6.2.5.5 查询流程列表

功能说明：查询流程列表。

请求地址：/api/platform/process/list

Body参数：

表 32 管理平台查询流程列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 33 管理平台查询流程列表接口返回业务参数

参数名称	数据类型	详细说明
processes	array	流程列表 包括字段： processId int 流程 ID， depId int 部门 ID， processName string 流程名称， remark string 流程备注， robotGroupId int 机器人组 ID， isRecord boolean 是否录屏， isDeleted boolean 是否删除

6.2.6 调度管理接口

6.2.6.1 创建调度

功能说明：创建调度任务。

请求地址：/api/platform/trigger/create

Body参数：

表 34 管理平台创建调度接口 Body 参数

参数名称	数据类型	是否必须	详细说明
triggerName	string	是	调度名称
description	string	否	调度描述
isActivated	boolean	否	是否激活
depId	int	是	部门 ID
processId	int	是	流程 ID
priority	int	否	优先级（0-高 1-中 2-低）
assignType	int	是	分配类型（0-全部 robot 1-自动分配 2-指定 robot）
robotIds	array	否	机器人 ID 组
robotGroupId	int	否	机器人组 ID
inParameters	array	否	入参列表 包括字段： name string 参数名， value string 参数值
isRecord	boolean	是	是否录屏
isWarn	boolean	否	是否报警
warnType	int	否	报警方式（0-邮件 1-短信 2-IM）
cronExpression	string	是	cron 表达式
isDefineCalendar	boolean	是	是否启用自定义日历
calendarId	int	否	日历 ID
timeZone	string	否	时区
maxRunTime	int	否	任务最长运行时长
maxWaitingTime	int	否	任务最长等待时间

返回业务参数：

表 35 管理平台创建调度接口返回业务参数

参数名称	数据类型	详细说明
triggerId	int	调度 ID

6.2.6.2 删除调度

功能说明：删除调度任务。

请求地址：/api/platform/trigger/delete

Body参数：

表 36 管理平台删除调度接口 Body 参数

参数名称	数据类型	是否必须	详细说明
triggerId	int	是	调度 ID

返回业务参数：

无

6.2.6.3 更新调度

功能说明：更新调度任务。

请求地址：/api/platform/trigger/update

Body参数：

表 37 管理平台修改调度接口 Body 参数

参数名称	数据类型	是否必须	详细说明
triggerId	int	是	调度 ID
triggerName	string	否	调度名称
description	string	否	调度描述
isActivated	boolean	否	是否激活
processId	int	否	流程 ID
priority	int	否	优先级（0-高 1-中 2-低）
assignType	int	否	分配类型（0-全部 robot 1-自动分配 2-指定 robot）
inParameters	array	否	入参列表 包括字段： name string 参数名， value string 参数值
robotIds	array	否	机器人 ID 组
robotGroupId	int	否	机器人组 ID
isRecord	boolean	否	是否录屏
isWarn	boolean	否	是否报警
warnType	int	否	报警方式（0-邮件 1-短信 2-IM）
cronExpression	string	否	cron 表达式
isDefineCalendar	boolean	否	是否启用自定义日历
calendarId	int	否	日历 ID
timeZone	string	否	时区
maxRunTime	int	否	任务最长运行时长
maxWaitingTime	int	否	任务最长等待时间

返回业务参数：

无

6.2.6.4 查询调度

功能说明：查询调度任务。

请求地址：/api/platform/trigger/query

Body参数：

表 38 管理平台查询调度接口 Body 参数

参数名称	数据类型	是否必须	详细说明
triggerId	int	是	调度 ID

返回业务参数：

表 39 管理平台查询调度接口返回业务参数

参数名称	数据类型	详细说明
depId	int	部门 ID
triggerName	string	调度名称
description	string	调度描述
isActivated	boolean	是否激活
processId	int	流程 ID
priority	int	优先级（0-高 1-中 2-低）
assignType	int	分配类型（0-全部 robot 1-自动分配 2-指定 robot）
inParameters	array	入参列表 包括字段： name string 参数名， value string 参数值
robotIds	array	机器人 ID 组
robotGroupId	int	机器人组 ID
isRecord	boolean	是否录屏
isWarn	boolean	是否报警
warnType	int	报警方式（0-邮件 1-短信 2-IM）
cronExpression	string	cron 表达式
isDefineCalendar	boolean	是否启用自定义日历
calendarId	int	日历 ID
timeZone	string	时区
maxRunTime	int	任务最长运行时长
maxWaitingTime	int	任务最长等待时间
isDeleted	boolean	是否删除

6.2.6.5 查询调度列表

功能说明：查询部门下的调度任务列表。

请求地址：/api/platform/trigger/list

Body参数：

表 40 管理平台查询调度列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
isActivated	boolean	否	是否激活
processId	int	否	流程 ID
pageNum	int	否	检索数据所在的页码【默认

参数名称	数据类型	是否必须	详细说明
			1, 即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100, 即默认每页最多显示 100 条数据】

返回业务参数:

表 41 管理平台查询调度列表接口返回业务参数

参数名称	数据类型	详细说明
triggers	array	调度列表 包括字段: triggerId int 调度 ID, triggerName string 调度名称, description string 调度描述, isActive boolean 是否激活, depId int 部门 ID, isDeleted boolean 是否删除

6.2.7 任务管理接口

6.2.7.1 启动任务

功能说明: 启动任务。

请求地址: /api/platform/task/create

Body 参数:

表 42 管理平台启动任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID
totalCount	int	否	创建数量
robotIds	array	否	机器人 ID 组
robotGroupId	int	否	机器人组 ID
priority	int	是	优先级 (0-高 1-中 2-低)
isRecord	boolean	是	是否录屏
isWarn	boolean	否	是否报警
warnType	int	否	报警方式 (0-邮件 1-短信 2-IM)
inParameters	array	否	入参列表 包括字段: name string 参数名, value string 参数值

参数名称	数据类型	是否必须	详细说明
maxRunTime	int	否	任务最长运行时长
maxWaitingTime	int	否	任务最长等待时间

返回业务参数：

表 43 管理平台启动任务接口返回业务参数

参数名称	数据类型	详细说明
taskIds	array	任务 ID 组

6.2.7.2 取消任务

功能说明：取消任务。

请求地址：/api/platform/task/cancel

Body参数：

表 44 管理平台取消任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

无

6.2.7.3 暂停任务

功能说明：暂停正在执行或正在排队中的任务。

请求地址：/api/platform/task/pause

Body参数：

表 45 管理平台暂停任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

无

6.2.7.4 继续任务

功能说明：继续任务。

请求地址：/api/platform/task/resume

Body参数：

表 46 管理平台继续任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

无

6.2.7.5 查询任务

功能说明：查询任务详情。

请求地址：/api/platform/task/query

Body参数：

表 47 管理平台查询任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

表 48 管理平台查询任务接口返回业务参数

参数名称	数据类型	详细说明
createModeType	int	任务创建类型（0-管理平台启动 1-机器人客户端启动 2-api 启动）
depId	int	部门 ID
robotId	int	机器人 ID
processId	int	流程 ID
triggerId	int	调度 ID
taskStatus	string	任务状态（0-成功 1-失败 2-进行中 3-已取消 4-暂停）
isRecord	boolean	是否录屏
recordFileIds	array	录屏文件 ID 组
isWarn	boolean	是否报警
warnType	int	报警方式（0-邮件 1-短信 2-IM）

表48 管理平台查询任务接口返回业务参数（续）

参数名称	数据类型	详细说明
inParameters	array	入参列表 包括字段： name string 参数名， value string 参数值
outParameters	array	出参列表 包括字段： name string 参数名， value string 参数值
priority	int	优先级（0-高 1-中 2-低）
startTime	string	开始时间，格式为 yyyy-MM-dd HH:mm:ss
stopTime	string	结束时间，格式为 yyyy-MM-dd HH:mm:ss
maxRunTime	int	任务最长运行时长
maxWaitingTime	int	任务最长等待时间

6.2.7.6 查询任务列表

功能说明：查询部门下的任务列表。

请求地址：/api/platform/task/list

Body参数：

表 49 管理平台查询任务列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
runningStartTimeRange_startTime	string	否	任务开始运行时间范围_开始时间，格式为 yyyy-MM-dd HH:mm:ss
runningStartTimeRange_endTime	string	否	任务开始运行时间范围_结束时间，格式为 yyyy-MM-dd HH:mm:ss
processId	int	否	流程 ID
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认100，即默认每页最多显示100条数据】

返回业务参数：

表 50 管理平台查询任务列表接口返回业务参数

参数名称	数据类型	详细说明
tasks	array	任务列表 包括字段： taskId int 任务 ID， depId int 部门 ID， robotId int 机器人 ID， processId int 流程 ID， taskStatus int 任务状态（0-成功 1-失败 2-进行中 3-已取消 4-暂停）， startTime string 开始时间，格式为 yyyy-MM-dd HH:mm:ss， endTime string 结束时间，格式为 yyyy-MM-dd HH:mm:ss

6.2.8 数据队列管理接口

6.2.8.1 创建数据队列

功能说明：创建数据队列。

请求地址：/api/platform/data-queue/create

Body参数：

表 51 管理平台创建数据队列接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID
queueName	string	是	数据队列名称
remark	string	否	备注

返回业务参数：

表 52 管理平台创建数据队列接口返回业务参数

参数名称	数据类型	详细说明
queueId	int	数据队列 ID

6.2.8.2 删除数据队列

功能说明：删除数据队列。

请求地址：/api/platform/data-queue/delete

Body参数：

表 53 管理平台删除数据队列接口 Body 参数

参数名称	数据类型	是否必须	详细说明
queueId	int	是	数据队列 ID

返回业务参数：
无

6.2.8.3 查询数据队列

功能说明：查询数据队列。
请求地址：/api/platform/data-queue/query
Body参数：

表 54 管理平台查询数据队列接口 Body 参数

参数名称	数据类型	是否必须	详细说明
queueId	int	是	数据队列 ID

返回业务参数：

表 55 管理平台查询数据队列接口返回业务参数

参数名称	数据类型	详细说明
unconsumedMessageCount	int	未消费消息数
consumedMessageCount	int	消费消息数
unavailableMessageCount	int	未生效消息数
expiredMessageCount	int	过期消息数
consumedMessageSuccessCount	int	消费消息成功数
consumedMessageFailCount	int	消费消息失败数
totalCount	int	总数
isDeleted	boolean	是否删除

6.2.8.4 查询数据队列列表

功能说明：查询部门下的所有数据队列。
请求地址：/api/platform/data-queue/list
Body参数：

表 56 管理平台查询数据队列列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 57 管理平台查询数据队列列表接口返回业务参数

参数名称	数据类型	详细说明
queues	array	数据队列列表 包括字段： queueId int 数据队列 ID， queueName string 数据队列名称， remark string 备注， depId int 部门 ID， isDeleted boolean 是否删除

6.2.9 服务器管理接口

6.2.9.1 创建服务器

功能说明：创建服务器。

请求地址：/api/platform/machine/create

Body 参数：

表 58 管理平台创建服务器接口 Body 参数

参数名称	数据类型	是否必须	详细说明
machineName	string	是	计算机名
remark	string	否	备注

返回业务参数：

表 59 管理平台创建服务器接口返回业务参数

参数名称	数据类型	详细说明
machineId	int	机器 ID

6.2.9.2 删除服务器

功能说明：删除服务器。

请求地址：/api/platform/machine/delete

Body 参数：

表 60 管理平台删除服务器接口 Body 参数

参数名称	数据类型	是否必须	详细说明
machineId	int	是	机器 ID

返回业务参数：

无

6.2.9.3 更新服务器

功能说明：更新服务器设置。

请求地址：/api/platform/machine/update

Body参数：

表 61 管理平台更新服务器接口 Body 参数

参数名称	数据类型	是否必须	详细说明
machineId	int	是	机器 ID
machineName	string	否	计算机名
remark	string	否	备注

返回业务参数：

无

6.2.9.4 查询服务器信息

功能说明：查询服务器信息（包括管理平台、设计器、机器人部署服务器，信息包括计算机名、IP、CPU、硬盘、内存、操作系统版本）。

请求地址：/api/platform/machine/query

Body参数：

表 62 管理平台查询服务器信息接口 Body 参数

参数名称	数据类型	是否必须	详细说明
machineId	int	是	机器 ID
resourceTypes	array	否	需要获取服务器资源信息的类型，为空则返回所有类型的资源信息，目前支持的类型包括： machineName: 计算机名 ip: 机器 IP 地址 cpu: CPU 使用率 disk: 磁盘空间大小和使用率 memory: 内存大小和使用率 systemversion: 操作系统版本

返回业务参数：

表 63 管理平台查询服务器信息接口返回业务参数

参数名称	数据类型	详细说明
resourceInfo	json	返回服务资源信息 machineName string 计算机名, ip string 机器 IP 地址, cpu string CPU 的使用率, disk string 磁盘空间大小和使用率, memory string 内存大小和使用率,

参数名称	数据类型	详细说明
		systemVersion string 操作系统版本
isDeleted	boolean	是否删除

6.2.9.5 查询服务器列表

功能说明：查询服务器列表。

请求地址：/api/platform/machine/list

Body参数：

表 64 管理平台查询服务器列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 65 管理平台查询服务器列表接口返回业务参数

参数名称	数据类型	详细说明
machines	array	机器人列表 包括字段： machineId int 机器 ID， remark string 备注， isDeleted boolean 是否删除

6.2.10 机器人管理接口

6.2.10.1 创建机器人

功能说明：创建机器人。

请求地址：/api/platform/robot/create

Body参数：

表 66 管理平台创建机器人接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID
robotName	string	是	机器人名称
robotType	int	是	机器人类型（0-后台机器人

参数名称	数据类型	是否必须	详细说明
			1-前台机器人)
machineId	int	是	机器 ID
machineName	string	是	计算机名
machineUsername	string	是	计算机用户名
machinePassword	string	否	计算机用户密码 (密文)
remark	string	否	备注
desktopType	int	否	远程连接方式 (0-console 1-RDP/VNC)
resolutionWidth	int	否	分辨率宽度
resolutionHeight	int	否	分辨率高度
resolutionDepth	int	否	分辨率深度
isAutoUnlockEnabled	boolean	否	是否开启屏幕自动解锁
logLevel	string	否	日志等级 (trace,debug,info,warn,error)

返回业务参数:

表 67 管理平台创建机器人接口返回业务参数

参数名称	数据类型	详细说明
robotId	int	机器人 ID

6.2.10.2 删除机器人

功能说明: 删除机器人。

请求地址: /api/platform/robot/delete

Body参数:

表 68 管理平台删除机器人接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotId	int	是	机器人 ID

返回业务参数:

表 69 管理平台删除机器人接口返回业务参数

参数名称	数据类型	详细说明
affectedTriggerIds	array	受影响调度 ID 组

6.2.10.3 更新机器人

功能说明: 更新机器人设置。

请求地址: /api/platform/robot/update

Body参数:

表 70 管理平台更新机器人接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotId	int	是	机器人 ID

表 70 管理平台更新机器人接口 Body 参数（续）

参数名称	数据类型	是否必须	详细说明
robotType	int	否	机器人类型（0-后台机器人 1-前台机器人）
robotName	string	否	机器人名称
machineName	string	否	计算机名
machineUsername	string	否	计算机用户名
machinePassword	string	否	计算机用户密码（密文）
remark	string	否	备注
desktopType	int	否	远程连接方式（0-console 1-RDP/VNC）
resolutionWidth	int	否	分辨率宽度
resolutionHeight	int	否	分辨率高度
resolutionDepth	int	否	分辨率深度
isAutoUnlockEnabled	boolean	否	是否开启屏幕自动解锁
logLevel	string	否	日志等级 (trace,debug,info,warn,error)

返回业务参数：

无

6.2.10.4 查询机器人

功能说明：查询机器人。

请求地址：/api/platform/robot/query

Body参数：

表 71 管理平台查询机器人接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotId	int	是	机器人 ID

返回业务参数：

表 72 管理平台查询机器人接口返回业务参数

参数名称	数据类型	详细说明
robotName	string	机器人名称
robotType	int	机器人类型（0-后台机器人 1-前台机器人）
depId	int	部门 ID
machineId	int	机器 ID
machineName	string	计算机名
machineUsername	string	计算机用户名
machinePassword	string	计算机用户密码（密文）
remark	string	备注
desktopType	int	远程连接方式（0-console 1-RDP/VNC）
resolutionWidth	int	分辨率宽度

参数名称	数据类型	详细说明
resolutionHeight	int	分辨率高度
resolutionDepth	int	分辨率深度
robotOnlineTime	string	机器人在线时长
robotInstallPath	string	机器人安装路径
robotInstallDate	string	机器人安装日期，格式为 yyyy-MM-dd HH:mm:ss

表 72 管理平台查询机器人接口返回业务参数（续）

参数名称	数据类型	详细说明
robotVersion	string	机器人版本
isAutoUnlockEnabled	boolean	是否开启屏幕自动解锁
logLevel	string	日志等级（trace,debug,info,warn,error）
robotStatus	int	机器人状态（0-空闲 1-运行 2-离线）
isDeleted	boolean	是否删除

6.2.10.5 查询机器人列表

功能说明：查询机器人列表。

请求地址：/api/platform/robot/list

Body参数：

表 73 管理平台查询机器人列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
processId	int	否	流程 ID
triggerId	int	否	调度 ID
robotStatus	int	否	机器人状态（0-空闲 1-运行 2-离线）
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 74 管理平台查询机器人列表接口返回业务参数

参数名称	数据类型	详细说明
robots	array	机器人列表 包括字段： robotId int 机器人 ID， depId int 部门 ID， robotType int 机器人类型（0-后台机器人 1-前台机器人） robotName string 机器人名， machineId string 设备 ID， remark string 备注， isDeleted boolean 是否删除

6.2.10.6 创建机器人组

功能说明：创建机器人组。

请求地址：/api/platform/robot-group/create

Body参数：

表 75 管理平台创建机器人组接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID
robotGroupName	string	是	机器人组名称
remark	string	否	备注

返回业务参数：

表 76 管理平台创建机器人接口返回业务参数

参数名称	数据类型	详细说明
robotGroupId	int	机器人组 ID

6.2.10.7 删除机器人组

功能说明：删除机器人组。

请求地址：/api/platform/robot-group/delete

Body参数：

表 77 管理平台删除机器人组接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotGroupId	int	是	机器人组 ID

返回业务参数：

表 78 管理平台删除机器人组接口返回业务参数

参数名称	数据类型	详细说明
affectedProcessIds	array	受影响流程 ID 组
affectedTriggerIds	array	受影响调度 ID 组

6.2.10.8 更新机器人组

功能说明：更新机器人组设置。

请求地址：/api/platform/robot-group/update

Body参数：

表 79 管理平台更新机器人组接口 Body 参数

参数名称	数据类型	是否必须	详细说明
------	------	------	------

参数名称	数据类型	是否必须	详细说明
robotGroupId	int	是	机器人组 ID
robotGroupName	string	否	机器人组名称
remark	string	否	备注

返回业务参数：

无

6.2.10.9 添加机器人到机器人组

功能说明：添加机器人到机器人组。

请求地址：/api/platform/robot-group/append

Body参数：

表 80 管理平台添加机器人到机器人组接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotIds	array	是	机器人 ID 组
robotGroupId	int	是	机器人组 ID

返回业务参数：

无

6.2.10.10 机器人移出机器人组

功能说明：机器人移出机器人组。

请求地址：/api/platform/robot-group/remove

Body参数：

表 81 管理平台机器人移出机器人组接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotIds	array	是	机器人 ID 组
robotGroupId	int	是	机器人组 ID

返回业务参数：

无

6.2.10.11 查询机器人组列表

功能说明：查询机器人组列表。

请求地址：/api/platform/robot-group/list

Body参数：

表 82 管理平台查询机器人组列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID

参数名称	数据类型	是否必须	详细说明
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 83 管理平台查询机器人组列表接口返回业务参数

参数名称	数据类型	详细说明
robotGroups	array	机器人组列表 包括字段： robotGroupId int 机器人组 ID， depId int 部门 ID， robotGroupName string 机器人组名称， robotIds array 机器人 ID 组， remark string 备注， isDeleted boolean 是否删除

6.2.11 日志管理接口

6.2.11.1 查询任务日志

功能说明：查询任务日志。

请求地址：/api/platform/task-log/query

Body参数：

表 84 管理平台查询任务日志接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID
logLevel	string	否	日志等级 (trace,debug,info,warn,error)

返回业务参数：

表 85 管理平台查询任务日志接口返回业务参数

参数名称	数据类型	详细说明
logs	array	日志记录数组 包括字段： logTime string 日志时间，格式为 yyyy-MM-dd HH:mm:ss，

参数名称	数据类型	详细说明
		logLevel string 日志等级 (trace,debug,info,warn,error), message string 日志信息

6.2.11.2 查询任务录屏

功能说明：查询任务的录屏文件。

请求地址：/api/platform/video/query

Body参数：

表 86 管理平台查询任务录屏接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

表 87 管理平台查询任务录屏接口返回业务参数

参数名称	数据类型	详细说明
recordFileInfos	array	录屏文件信息(一个任务可能对应多个录屏) recordFileId int 录屏文件 ID videoStartTime string 录屏开始时间, 格式为 yyyy-MM-dd HH:mm:ss videoEndTime string 录屏结束时间, 格式为 yyyy-MM-dd HH:mm:ss url string 录屏文件下载地址

6.2.12 凭据管理接口

6.2.12.1 创建凭据

功能说明：创建凭据。

请求地址：/api/platform/credential/create

Body参数：

表 88 管理平台创建凭据接口 Body 参数

参数名称	数据类型	是否必须	详细说明
credentialName	string	是	凭据名称
credentialUsername	string	是	凭据账号
credentialPassword	string	是	凭据密码(密文)
remark	string	否	凭据备注
isGlobal	boolean	是	是否为全局凭据
robotIds	array	否	机器人 ID 组

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID

返回业务参数：

表 89 管理平台创建凭据接口返回业务参数

参数名称	数据类型	详细说明
credentialId	int	凭据 ID

6.2.12.2 删除凭据

功能说明：删除凭据

请求地址：/api/platform/credential/delete

Body参数：

表 90 管理平台删除凭据接口 Body 参数

参数名称	数据类型	是否必须	详细说明
credentialId	int	是	凭据 ID

返回业务参数：

无

6.2.12.3 更新凭据

功能说明：更新凭据。

请求地址：/api/platform/credential/update

Body参数：

表 91 管理平台更新凭据接口 Body 参数

参数名称	数据类型	是否必须	详细说明
credentialId	int	是	凭据 ID
credentialName	string	否	凭据名称
credentialUsername	string	否	凭据账号
credentialPassword	string	否	凭据密码（密文）
isGlobal	boolean	否	是否为全局凭据
robotIds	array	否	机器人 ID 组
remark	string	否	凭据备注

返回业务参数：

无

6.2.12.4 查询凭据

功能说明：查询凭据。

请求地址：/api/platform/credential/query

Body参数：

表 92 管理平台查询凭据接口 Body 参数

参数名称	数据类型	是否必须	详细说明
credentialId	int	是	凭据 ID

返回业务参数：

表 93 管理平台查询凭据接口返回业务参数

参数名称	数据类型	详细说明
credentialName	string	凭据名称
credentialUsername	string	凭据账号
credentialPassword	string	凭据密码（密文）
isGlobal	boolean	是否全局
robotIds	array	机器人 ID 组
remark	string	凭据备注
depId	int	部门 ID
isDeleted	boolean	是否删除

6.2.12.5 查询凭据列表

功能说明：查询凭据列表。

请求地址：/api/platform/credential/list

Body参数：

表 94 管理平台查询凭据列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 95 管理平台查询凭据列表接口返回业务参数

参数名称	数据类型	详细说明
credentials	array	凭据列表 包括字段： credentialId int 凭据 ID， credentialName string 凭据名称， depId int 部门 ID， isDeleted boolean 是否删除

6.2.13 资产管理接口

6.2.13.1 创建资产

功能说明：创建资产。

请求地址：/api/platform/asset/create

Body参数：

表 96 管理平台创建资产接口 Body 参数

参数名称	数据类型	是否必须	详细说明
assetName	string	是	资产名称
assetValue	string	是	资产内容
dataType	int	是	资产数据类型（0-文本 1-布尔 2-数值）
isGlobal	boolean	是	是否全局
robotIds	array	否	机器人 ID 组
depId	int	是	部门 ID
remark	int	否	备注

返回业务参数：

表 97 管理平台创建资产接口返回业务参数

参数名称	数据类型	详细说明
assetId	int	资产 ID

6.2.13.2 删除资产

功能说明：删除资产。

请求地址：/api/platform/asset/delete

Body参数：

表 98 管理平台删除资产接口 Body 参数

参数名称	数据类型	是否必须	详细说明
assetId	int	是	资产 ID

返回业务参数：

无

6.2.13.3 更新资产

功能说明：更新资产。

请求地址：/api/platform/asset/update

Body参数：

表 99 管理平台更新资产接口 Body 参数

参数名称	数据类型	是否必须	详细说明
assetId	int	是	资产 ID
assetName	string	否	资产名称
assetValue	string	否	资产内容
isGlobal	boolean	否	是否全局
robotIds	array	否	机器人 ID 组
remark	int	否	备注

返回业务参数：

无

6.2.13.4 查询资产

功能说明：查询资产。

请求地址：/api/platform/asset/query

Body参数：

表 100 管理平台查询资产接口 Body 参数

参数名称	数据类型	是否必须	详细说明
assetId	int	是	资产 ID

返回业务参数：

表 101 管理平台查询资产接口返回业务参数

参数名称	数据类型	详细说明
assetName	string	资产名称
assetValue	string	资产内容
dataType	int	资产数据类型(0-文本 1-布尔 2-数值)
isGlobal	boolean	是否全局
robotIds	array	机器人 ID 组
remark	int	备注
isDeleted	boolean	是否删除
depId	int	部门 ID

6.2.13.5 查询资产列表

功能说明：查询资产列表。

请求地址：/api/platform/asset/list

Body参数：

表 102 管理平台查询资产列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】

参数名称	数据类型	是否必须	详细说明
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 103 管理平台查询资产列表接口返回业务参数

参数名称	数据类型	详细说明
assets	array	资产列表 包括字段： assetId int 资产 ID， assetName string 资产名称， depId int 部门 ID， isDeleted boolean 是否删除

6.2.14 文件管理接口

6.2.14.1 创建文件

功能说明：创建文件。

请求地址：/api/platform/file/create

Body参数：

表 104 管理平台创建文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	是	部门 ID
folderPath	string	是	文件夹路径
fileName	string	是	文件名称
filePassword	string	否	文件的访问密码（密文）。如果文件没有访问密码则不需要提供
file	file	是	上传管理平台的本地文件

返回业务参数：

表 105 管理平台创建文件接口返回业务参数

参数名称	数据类型	详细说明
fileId	int	文件 ID

6.2.14.2 删除文件

功能说明：删除文件。

请求地址：/api/platform/file/delete

Body参数：

表 106 管理平台删除文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
fileId	int	是	文件 ID

返回业务参数：

无

6.2.14.3 更新文件

功能说明：更新文件。

请求地址：/api/platform/file/update

Body参数：

表 107 管理平台更新文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
fileId	int	是	文件 ID
folderPath	string	否	文件夹路径
fileName	string	否	文件名称
filePassword	string	否	文件的访问密码（密文）。 如果文件没有访问密码则不需要提供
file	file	否	上传管理平台的本地文件

返回业务参数：

无

6.2.14.4 查询文件

功能说明：查询文件。

请求地址：/api/platform/file/query

Body参数：

表 108 管理平台查询文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
fileId	int	是	文件 ID

返回业务参数：

表 109 管理平台查询文件接口返回业务参数

参数名称	数据类型	详细说明
fileName	string	文件名称
url	string	文件在管理平台的下载地址
isDeleted	boolean	是否删除
depId	int	部门 ID
folderPath	string	文件夹路径

参数名称	数据类型	详细说明
updateTime	string	文件更新时间，格式为 yyyy-MM-dd HH:mm:ss

6.2.14.5 查询文件列表

功能说明：查询文件列表。

请求地址：/api/platform/file/list

Body参数：

表 110 管理平台查询文件列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
depId	int	否	部门 ID
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 111 管理平台查询文件列表接口返回业务参数

参数名称	数据类型	详细说明
files	array	文件列表 包括字段： fileId int 文件 ID， fileName string 文件名称， folderPath string 文件夹路径， depId int 部门 ID， isDeleted boolean 是否删除

6.2.15 日历管理接口

6.2.15.1 创建日历

功能说明：创建日历信息。

请求地址：/api/platform/calendar/create

Body参数：

表 112 管理平台创建日历接口 Body 参数

参数名称	数据类型	是否必须	详细说明
calendarName	string	是	日历名称

参数名称	数据类型	是否必须	详细说明
nonWorkingDays	array	是	非工作日或非交易日数组

返回业务参数：

表 113 管理平台创建日历接口返回业务参数

参数名称	数据类型	详细说明
calendarId	int	日历 ID

6.2.15.2 删除日历

功能说明：删除日历。

请求地址：/api/platform/calendar/delete

Body 参数：

表 114 管理平台删除日历接口 Body 参数

参数名称	数据类型	是否必须	详细说明
calendarId	int	是	日历 ID

返回业务参数：

无

6.2.15.3 更新日历

功能说明：更新日历信息

请求地址：/api/platform/calendar/update

Body 参数：

表 115 管理平台更新日历接口 Body 参数

参数名称	数据类型	是否必须	详细说明
calendarId	int	是	日历 ID
calendarName	string	否	日历名称
nonWorkingDays	array	否	非工作日或非交易日组

返回业务参数：

无

6.2.15.4 查询日历

功能说明：查询日历信息。

请求地址：/api/platform/calendar/query

Body 参数：

表 116 管理平台查询日历接口 Body 参数

参数名称	数据类型	是否必须	详细说明
calendarId	int	是	日历 ID

返回业务参数：

表 117 管理平台查询日历接口返回业务参数

参数名称	数据类型	详细说明
nonWorkingDays	array	非工作日或非交易日数组
isDeleted	boolean	是否删除

6.2.15.5 查询日历列表

功能说明：查询日历列表。

请求地址：/api/platform/calendar/list

Body参数：

表 118 管理平台查询日历列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 119 管理平台查询日历列表接口返回业务参数

参数名称	数据类型	详细说明
calendars	array	日历列表 包括字段： calendarId int 日历 ID， calendarName string 日历名称， isDeleted boolean 是否删除

6.2.16 许可管理接口

功能说明：查询许可信息。

请求地址：/api/platform/license/info

Body参数：

无

返回业务参数：

表 120 管理平台查询许可信息接口返回业务参数

参数名称	数据类型	详细说明
licenses	array	许可明细 包括字段： type string 许可类型， quantity int 数量， used_quantity int 已使用数量， licenseExpirationTime string 许可到期时间，格式为 yyyy-MM-dd HH:mm:ss

6.3 机器人接口

本章节定义机器人需提供的接口。

6.3.1 机器人管理接口

6.3.1.1 机器人认证

功能说明：获取机器人认证凭证。

请求地址：/api/robot/authenticate

Body参数：

表 121 机器人认证接口 Body 参数

参数名称	数据类型	是否必须	详细说明
secret	string	是	机器人的 secret 密钥, 每个机器人有自己唯一的密钥

返回业务参数：

表 122 机器人认证接口返回业务参数

参数名称	数据类型	详细说明
token	string	字符令牌
expirationTime	string	token 过期时间, 格式为 yyyy-MM-dd HH:mm:ss

6.3.1.2 启动机器人

功能说明：启动本地机器人。

请求地址：/api/robot/start

Body参数：

无

返回业务参数：

无

6.3.1.3 停止机器人

功能说明：停止本地机器人。

请求地址: /api/robot/stop

Body参数:

无

返回业务参数:

无

6.3.1.4 设置机器人

功能说明: 设置本地机器人的配置。

请求地址: /api/robot/config

Body参数:

表 123 机器人设置接口 Body 参数

参数名称	数据类型	是否必须	详细说明
robotConfig	json	是	机器人配置信息 包括字段: machineName string 计算机名, machineUsername string 计算机用户名, machinePassword string 计算机用户密码(密文), desktopType int 远程连接方式(0-console 1-RDP/VNC), resolutionWidth int 分辨率宽度, resolutionHeight int 分辨率高度, resolutionDepth int 分辨率深度, isAutoUnlockEnabled boolean 是否开启屏幕自动解锁, logLevel string 日志等级 (trace,debug,info,warn,error)

返回业务参数:

无

6.3.1.5 查询机器人

功能说明: 查询机器人状态。

请求地址: /api/robot/query

Body参数:

无

返回业务参数：

表 124 机器人查询状态接口返回业务参数

参数名称	数据类型	详细说明
robotInfo	json	机器人信息 包括字段： machineName string 计算机名， machineUsername string 计算机用户名， machinePassword string 计算机用户密码（密文）， desktopType int 远程连接方式（0-console 1-RDP/VNC）， resolutionWidth int 分辨率宽度， resolutionHeight int 分辨率高度， resolutionDepth int 分辨率深度， robotOnlineTime string 机器人在线时长， robotInstallPath string 机器人安装路径， robotInstallDate string 机器人安装日期，格式为 yyyy-MM-dd HH:mm:ss， robotVersion string 机器人版本， isAutoUnlockEnabled boolean 是否开启屏幕自动解锁， logLevel string 日志等级（trace,debug,info,warn,error）， robotStatus int 机器人状态（0-空闲 1-运行 2-离线）

6.3.2 服务器管理接口

功能说明：查询服务器信息（包括计算机名、IP、CPU、硬盘、内存、操作系统版本）。

请求地址：/api/robot/machine/query

Body参数：

表 125 机器人查询服务器资源信息接口 Body 参数

参数名称	数据类型	是否必须	详细说明
resourceTypes	array	否	需要获取服务器资源信息的类型，为空则返回所有信息，目前支持的类型包括： machineName: 计算机名 ip: 机器 IP 地址

参数名称	数据类型	是否必须	详细说明
			cpu: CPU 使用率 disk: 磁盘空间大小和使用率 memory: 内存大小和使用率 systemVersion: 操作系统版本

返回业务参数:

表 126 机器人查询服务器资源信息接口返回业务参数

参数名称	数据类型	详细说明
resourceInfo	json	返回服务资源信息 machineName string 计算机名, ip string 机器 IP 地址, cpu string CPU 的使用率, disk string 磁盘空间大小和使用率, memory string 内存大小和使用率, systemVersion string 操作系统版本

6.3.3 流程包管理接口

6.3.3.1 创建流程包

功能说明: 上传流程包到机器人所在服务器本地目录。

请求地址: /api/robot/package/create

Body参数:

表 127 机器人创建流程包接口 Body 参数

参数名称	数据类型	是否必须	详细说明
packageName	string	是	流程包名称

表 127 机器人创建流程包接口 Body 参数 (续)

参数名称	数据类型	是否必须	详细说明
package	file	是	流程包
packageVersion	string	是	流程包版本

返回业务参数:

表 128 机器人创建流程包接口返回业务参数

参数名称	数据类型	详细说明
packageId	int	流程包 ID

6.3.3.2 删除流程包

功能说明: 删除机器人所在服务器本地流程包。

请求地址: /api/robot/package/delete

Body参数:

表 129 机器人删除流程包接口 Body 参数

参数名称	数据类型	是否必须	详细说明
packageId	int	是	流程包 ID

返回业务参数:

无

6.3.3.3 查询流程包列表

功能说明: 查询机器人所在服务器本地流程包信息。

请求地址: /api/robot/package/query

Body参数:

表 130 机器人查询流程包列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
pageNum	int	否	检索数据所在的页码【默认 1, 即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100, 即默认每页最多显示 100 条数据】

返回业务参数:

表 131 机器人查询流程包列表接口返回业务参数

参数名称	数据类型	详细说明
packages	array	流程包列表 包括字段:

参数名称	数据类型	详细说明
		packageName string 流程包名称, packageId int 流程包 ID, packageVersion string 流程包版本, packagePath string 流程包本地路径, isDeleted boolean 是否删除

6.3.4 流程管理接口

6.3.4.1 创建流程

功能说明：创建流程。

请求地址：/api/robot/process/create

Body参数：

表 132 机器人创建流程接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processName	string	是	流程名称
remark	string	否	流程备注

返回业务参数：

表 133 机器人创建流程接口返回业务参数

参数名称	数据类型	详细说明
processId	int	流程 ID

6.3.4.2 流程激活流程包版本

功能说明：流程激活流程包版本。

请求地址：/api/robot/process/activate-package-version

Body参数：

表 134 机器人流程激活流程包版本接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID
packageId	int	是	流程包 ID
inParameters	array	否	入参列表 包括字段： name string 参数名, value string 参数值

返回业务参数：

无

6.3.4.3 删除流程

功能说明：删除流程。

请求地址：/api/robot/process/delete

Body参数：

表 135 机器人删除流程接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID

返回业务参数：

无

6.3.4.4 更新流程

功能说明：更新流程信息。

请求地址：/api/robot/process/update

Body参数：

表 136 机器人更新流程接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID
processName	string	否	流程名称
remark	string	否	流程备注

返回业务参数：

无

6.3.4.5 查询流程列表

功能说明：查询流程列表。

请求地址：/api/platform/process/list

Body参数：

表 137 机器人查询流程列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100，即默认每页最多显示 100 条数据】

返回业务参数：

表 138 机器人查询流程列表接口返回业务参数

参数名称	数据类型	详细说明
processes	array	流程列表

参数名称	数据类型	详细说明
		包括字段： processId int 流程 ID， processName string 流程名称， remark string 流程备注， isDeleted boolean 是否删除

6.3.5 任务管理接口

6.3.5.1 启动任务

功能说明：启动任务。

请求地址：/api/robot/task/create

Body参数：

表 139 机器人启动任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
processId	int	是	流程 ID
totalCount	int	否	创建数量
priority	int	否	优先级（0-高 1-中 2-低）
isRecord	boolean	是	是否录屏

表 139 机器人启动任务接口 Body 参数 (续)

参数名称	数据类型	是否必须	详细说明
inParameters	array	否	入参列表 包括字段： name string 参数名， value string 参数值
maxRunTime	int	否	任务最长运行时长
maxWaitingTime	int	否	任务最长等待时间

返回业务参数：

表 140 机器人启动任务接口返回业务参数

参数名称	数据类型	详细说明
taskIds	array	任务 ID 组

6.3.5.2 取消任务

功能说明：取消任务。

请求地址：/api/robot/task/cancel

Body参数：

表 141 机器人取消任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

无

6.3.5.3 暂停任务

功能说明：暂停正在执行或正在排队中的任务。

请求地址：/api/robot/task/pause

Body参数：

表 142 机器人暂停任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

无

6.3.5.4 继续任务

功能说明：恢复暂停中的任务。

请求地址：/api/robot/task/resume

Body参数：

表 143 机器人继续任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

无

6.3.5.5 查询任务

功能说明：查询任务的详细信息。

请求地址：/api/robot/task/query

Body参数：

表 144 机器人查询任务接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID

返回业务参数：

表 145 机器人查询任务接口返回业务参数

参数名称	数据类型	详细说明
processId	int	流程 ID
processName	string	流程名称
taskStatus	int	任务状态（0-成功 1-失败 2-进行中 3-已取消 4-暂停）
isRecord	boolean	是否录屏
recordFileIds	array	录屏文件 ID 组
inParameters	array	入参列表 包括字段： name string 参数名， value string 参数值
outParameters	array	出参列表 包括字段： name string 参数名， value string 参数值
priority	int	优先级（0-高 1-中 2-低）
startTime	string	开始时间，格式为 yyyy-MM-dd HH:mm:ss
stopTime	string	结束时间，格式为 yyyy-MM-dd HH:mm:ss
maxRunTime	int	任务最长运行时长
maxWaitingTime	int	任务最长等待时间

6.3.5.6 查询任务列表

功能说明：查询机器人的任务列表。

请求地址：/api/robot/task/list

Body参数：

表 146 机器人查询任务列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
runningStartTimeRange_startTime	string	否	任务开始运行时间范围_开始时间，格式为 yyyy-MM-dd HH:mm:ss
runningStartTimeRange_endTime	string	否	任务开始运行时间范围_结束时间，格式为 yyyy-MM-dd HH:mm:ss

表 146 机器人查询任务列表接口 Body 参数 (续)

参数名称	数据类型	是否必须	详细说明
processId	int	否	流程 ID
pageNum	int	否	检索数据所在的页码【默认 1, 即默认检索第一页的数据】
pageSize	int	否	每页显示的数据条目数【默认 100, 即默认每页最多显示 100 条数据】

返回业务参数:

表 147 机器人查询任务列表接口返回业务参数

参数名称	数据类型	详细说明
tasks	array	任务列表 包括字段: taskId int 任务 ID, processId int 流程 ID, taskStatus int 任务状态 (0-成功 1-失败 2-进行中 3-已取消 4-暂停), isRecord boolean 是否录屏, recordFileIds array 录屏文件 ID 组, startTime string 开始时间, 格式为 yyyy-MM-dd HH:mm:ss, endTime string 结束时间, 格式为 yyyy-MM-dd HH:mm:ss

6.3.6 文件管理接口

6.3.6.1 创建文件

功能说明: 上传文件到机器人所在服务器本地文件目录。

请求地址: /api/robot/file/create

Body参数:

表 148 机器人创建文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
file	file	是	上传文件
folderPath	string	是	文件夹路径
fileName	string	是	文件名称
filePassword	string	否	文件的访问密码 (密文)。如果文件没有访问密码则不需要提供

返回业务参数:

表 149 机器人创建文件接口返回业务参数

参数名称	数据类型	详细说明
fileId	string	文件 ID

6.3.6.2 删除文件

功能说明：删除机器人所在服务器本地目录的指定文件。

请求地址：/api/robot/file/delete

Body参数：

表 150 机器人删除文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
fileId	int	是	文件 ID

返回业务参数：

无

6.3.6.3 更新文件

功能说明：更新文件。

请求地址：/api/robot/file/update

Body参数：

表 151 机器人更新文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
fileId	int	是	文件 ID
fileName	string	否	文件名称
filePassword	string	否	文件的访问密码（密文）。 如果文件没有访问密码则不需要提供
file	file	否	上传文件
folderPath	string	是	文件夹路径

返回业务参数：

无

6.3.6.4 查询文件

功能说明：查询存储文件。

请求地址：/api/robot/file/query

Body参数：

表 152 机器人查询文件接口 Body 参数

参数名称	数据类型	是否必须	详细说明
fileId	int	是	文件 ID

返回业务参数：

表 153 机器人查询文件接口返回业务参数

参数名称	数据类型	详细说明
fileName	string	文件名称
folderPath	string	文件夹路径
updateTime	string	文件更新时间，格式为 yyyy-MM-dd HH:mm:ss

6.3.6.5 查询文件列表

功能说明：获取文件列表。

请求地址：/api/robot/file/list

Body参数：

表 154 机器人查询文件列表接口 Body 参数

参数名称	数据类型	是否必须	详细说明
pageNum	int	否	检索数据所在的页码【默认 1，即默认检索第一页的数 据】
pageSize	int	否	每页显示的数据条目数【默 认 100，即默认每页最多显 示 100 条数据】

返回业务参数：

表 155 机器人查询文件列表接口返回业务参数

参数名称	数据类型	详细说明
files	array	文件列表 包括字段： fileId int 文件 ID， fileName string 文件名称， isDeleted boolean 是否删除

6.3.7 日志管理接口

6.3.7.1 查询任务日志

功能说明：查询任务日志。

请求地址：/api/robot/task-log/query

Body参数：

表 156 机器人查询任务日志接口 Body 参数

参数名称	数据类型	是否必须	详细说明
------	------	------	------

参数名称	数据类型	是否必须	详细说明
taskId	int	是	任务 ID
logLevel	string	否	日志等级 (trace,debug,info,warn,error)

返回业务参数：

表 157 机器人查询任务日志接口返回业务参数

参数名称	数据类型	详细说明
logs	array	日志记录数组 包括字段： logTime string 日志时间，格式为 yyyy-MM-dd HH:mm:ss， logLevel string 日志等级 (trace,debug,info,warn,error)， message string 日志信息

6.3.7.2 查询任务录屏

功能说明：查询任务的录屏文件。

请求地址：/api/robot/video/query

Body参数：

表 158 机器人查询任务录屏接口 Body 参数

参数名称	数据类型	是否必须	详细说明
taskId	string	是	任务 ID

返回业务参数：

表 159 机器人查询任务录屏接口返回业务参数

参数名称	数据类型	详细说明
recordFileInfos	array	录屏文件信息(一个任务可能对应多个录屏) recordFileId int 录屏文件 ID videoStartTime string 录屏开始时间，格式为 yyyy-MM-dd HH:mm:ss videoEndTime string 录屏结束时间，格式为 yyyy-MM-dd HH:mm:ss videoPath string 录屏文件的本地路径

6.3.8 许可管理接口

功能说明：查询机器人的许可信息。

请求地址：/api/robot/license/info

Body参数：

无

返回业务参数：

表 160 机器人查询许可信息接口返回业务参数

参数名称	数据类型	详细说明
licenseExpirationTime	string	许可到期时间，格式为 yyyy-MM-dd HH:mm:ss
type	string	许可类型

7 适配证券行业应用系统

证券公司应用系统是业务流程的核心载体，理所当然成为证券公司RPA应用场景中机器人主要需要操作的信息系统。为扩大RPA产品在证券公司业务场景中的应用范围，降低部署风险，推荐RPA服务商依据表161中的证券行业应用系统清单（包括但不限于清单所列项目）逐步提高产品的适配能力。

表 161 证券行业应用系统清单

系统名称	所属业务
集中交易系统	经纪业务
两融系统	经纪业务
转融通系统	经纪业务
OTC 交易柜台	经纪业务
极速交易系统	经纪业务
法人结算系统	经纪业务
资金结算系统	经纪业务
呼叫中心系统	经纪业务
零售 CRM/智能投顾系统	经纪业务
投资管理系统	资管业务

表 161 证券行业应用系统清单（续）

系统名称	所属业务
投研系统	资管业务
估值系统	资管业务
TA 系统	资管业务
投行底稿管理系统	投行业务
投行质量评价系统	投行业务
发行簿记系统	投行业务
投行项目管理平台	投行业务
全面风险管理系统	风险合规
反洗钱系统	风险合规
信息隔离墙系统	风险合规
财务系统	财务管理
资金管理系统	财务管理
财务报销系统	财务管理
OA 系统	办公管理
邮件系统	办公管理
监管综合报送管理平台	信息披露
资讯终端	资讯服务

适配能力分为四个等级：

- 完全兼容：指通过应用程序内部对象接管技术开发，并已在实际中使用。选择此选项时，应提供投产案例；
- 部分兼容：指部分脚本依赖于鼠标和键盘模拟技术，并已在实际中使用。选择此选项时，应提供投产案例；
- 待验证：指已经开发但尚未经过验证。选择此选项时，投产案例可以不提供；
- 未知：指不清楚是否支持，未实际接触过相关系统。选择此选项时，投产案例可以不提供。

附 录 A
(资料性)
业务状态码示例

A.1 通用业务错误码

表 A.1 通用业务错误码

resultCode	错误信息
10001	token 无效
10002	接口版本信息不支持
10003	用户未注册
10004	用户密码错误
10005	参数为空
10006	参数不全
10007	参数类型错误
10101	任务已取消
10102	任务已停止
10201	文件名称已存在
10202	文件保存失败
10203	文件不存在或文件密码不正确
10301	时间格式不正确
10401	日志等级不存在
11001	机器人状态异常
11002	机器人许可过期

A.2 服务器相关业务错误码

表 A.2 服务器相关业务错误码

resultCode	错误信息
20001	服务器状态异常

A.3 权限相关业务错误码

表 A.3 权限相关业务错误码

resultCode	错误信息
30001	接口调用权限不足