京东肯特瑞基金销售有限公司

反洗钱与反恐怖融资内控制度

V2.0

文件编码：KTR-HG-A-01-2022V2

编制部门：反洗钱部

审核部门：内控监察部

发布日期：2022.06.30

生效日期：2022.06.30

历史记录

文件编码	编制部门	审核部门	签发人	签发日期	更改主要内容
KTR-HG-A-01-2021V1	反洗钱部	内控监察部	李骏	2021.09.03	首次正式发布
KTR-HG-A-01-2022V2	反洗钱部	内控监察部	邹保威	2022.06	1.完善反洗钱绩效考核、反洗钱协同相关机制。 2.完善客户身份重新识别相关内容。 3.完善法人风险自评估相关内容。

目 录

1.目的

为依法履行反洗钱和 反恐怖融资（以下统一简称“反洗钱”）义务，指导京东肯特瑞基金销售有限公司（以下简称“肯特瑞”或“公司”）所有相关业务部门、职能部门、分（子）公司，以及所有相关员工依法合规展业，缓释公司所面临的洗钱风险、合规风险和潜在的声誉风险，确保公司可持续发展，特制定本内控制度。

2.适用范围

2.1 本内控制度不仅适用于反洗钱、反恐怖融资，也根据相关监管规定适用于反逃税，反扩散融资等纳入反洗钱监管框架的相关违法犯罪的防控。

2.2 公司所有员工必须自觉遵守反洗钱法律法规及本政策的相关规定，充分认识到洗钱犯罪对社会、公司、客户及员工本人所带来的危害，提升反洗钱意识，避免为犯罪分子所利用。

3.法律依据及定义

3.1 本内控制度主要依据以下中国反洗钱法律法规以及京东科技反洗钱政策：

- 《中华人民共和国反洗钱法》
- 《中华人民共和国反恐怖主义法》
- 《金融机构反洗钱和反恐怖融资监督管理办法》
- 《金融机构客户身份识别和客户身份资料及交易记录保存管理办法》

- 《金融机构大额交易和可疑交易报告管理办法》
- 《涉及恐怖活动资产冻结管理办法》
- 《证券期货业反洗钱工作实施办法》
- 《基金管理公司反洗钱工作指引》
- 《基金管理公司反洗钱客户风险等级划分标准指引》
- 《法人金融机构洗钱和恐怖融资风险管理指引（试行）》
- 《互联网金融从业机构反洗钱和反恐怖融资管理办法》
- 《法人金融机构洗钱和恐怖融资风险自评估指引》

3.2 相关定义

3.2.1 洗钱：是指将违法犯罪所得及其产生的收益，通过各种手段掩饰、隐瞒资金的来源和性质，使其在形式上合法化的行为。

3.2.2 恐怖融资：恐怖组织、恐怖分子募集、占有、使用资金或者其他形式财产；以资金或者其他形式财产协助恐怖组织、恐怖分子以及恐怖主义、恐怖活动犯罪；为恐怖主义和实施恐怖活动犯罪占有、使用以及募集资金或者其他形式财产；为恐怖组织、恐怖分子占有、使用以及募集资金或者其他形式财产。

3.2.3 大规模杀伤性武器扩散融资：是指为转移、出口核生化武器及其运载工具和相关材料提供金融服务，主要是为扩散敏感物品的交易提供融资，也包括为涉及扩散的个人或实体提供其他金融支持。根据 FATF 在其犯罪类型研究报告中的定义，扩散指转移、出口核生化武器及其运载工具和相关材料，包括技术、物

品、软件、服务或专业知识。

3.2.4 逃税：指纳税人违反税法规定不缴或少缴税款的非法行为，主要表现有：伪造、涂改、销毁账册、票据或记账凭证，虚报、多报费用和成本，少报或不报应纳税所得额或收入额，隐匿财产或采用不正当手段骗回已纳税款等。

4.反洗钱管理原则

为确保反洗钱相关法律法规有效执行，切实防范洗钱风险，肯特瑞遵循以下原则履行相应的反洗钱义务。

4.1 全面性原则。公司对洗钱和恐怖融资风险（以下统一简称“洗钱风险”）实施全面管理，将洗钱风险管理贯穿于反洗钱决策、执行和监督全过程，全面覆盖所有须纳入反洗钱管理范畴的业务活动和管理流程，全面覆盖所有相关业务条线和职能部门。

4.2 独立性原则。公司结合业务实际，使得洗钱风险管理在组织架构、制度、流程、人员安排、报告路线等方面保持独立，确保决策和洗钱风险控制有效。公司反洗钱工作由反洗钱部全面统筹。

4.3 匹配性原则。公司依据业务风险特征、管理模式、业务规模、产品复杂程度等因素，投入相应的资源来管理洗钱风险，建立相匹配的反洗钱内控机制，并根据内外部情况的变化进行及时、合理调整。

4.4 有效性原则。为有效控制洗钱风险，公司各业务部门、职能部门应在反洗钱法律法规及京东科技反洗钱政策指引下，将洗钱风险管理的具体要求嵌入日常业务流程，及时根据业务和风险变化进行制度流程更新，并根据实际风险状况采

取有针对性的措施，有效控制洗钱风险。

5.职责与分工

5.1 京东科技风险和内控合规管理委员会（以下简称“风委会”）

京东科技成立了高级管理层组成的“风委会”，是集团反洗钱工作的最高管理和决策机构。肯特瑞作为京东科技全资控股子公司，按照要求接受其管理。“风委会”应能够及时掌握和了解肯特瑞反洗钱重要工作信息，为反洗钱工作提供资源配给，促进反洗钱工作有序开展，并就肯特瑞反洗钱重大事项进行决策。

5.2 高级管理层

肯特瑞总经理牵头负责公司反洗钱和反恐怖融资管理工作，主要职责如下：

- 推动公司洗钱风险管理文化建设；
- 建立并及时调整公司洗钱风险管理组织架构，明确反洗钱管理部门、业务部门及其他部门在洗钱风险管理中的职责分工和协调机制；
- 制定、调整公司洗钱风险管理策略及其执行机制；
- 审核公司洗钱风险管理制度和程序；
- 及时向风委会报告重大洗钱风险事件；
- 组织落实公司信息系统和数据治理；
- 根据授权对违反洗钱风险管理政策和程序的情况进行处理；
- 其他相关职责。

5.3 反洗钱部

反洗钱部统筹公司洗钱风险管理相关具体工作，推动落实反洗钱法律法规，协调、监督反洗钱政策的实施，主要职责如下：

- 制定和更新肯特瑞洗钱风险管理政策和程序；
- 贯彻落实反洗钱法律法规和监管要求，建立健全反洗钱内控制度和内部检查机制；
- 识别、评估、监测公司洗钱风险，提出控制洗钱风险的措施和建议；
- 持续检查洗钱风险管理策略及洗钱风险管理政策和程序的执行情况，对违反风险管理政策和程序的情况及时预警、报告并提出处理建议；
- 组织开展客户洗钱风险分类管理、业务洗钱风险评估工作、产品洗钱风险评估等风险评估工作，对评估结论提出风险缓释方案或建议；
- 牵头配合反洗钱监管，协调配合反洗钱行政调查及合作机构反洗钱协查；
- 组织或协调相关部门开展反洗钱宣传和培训；
- 其他按监管要求需开展的反洗钱相关工作。

5.4 业务部门

业务部门主要包括公募业务事业群组、私募业务事业群组及清算支持中心等，作为反洗钱第一道防线，承担反洗钱工作的直接责任，主要职责包括但不限于：

- 建立相应的工作机制，按要求将洗钱风险管理要求嵌入产品研发、流程设计、业务管理和具体操作中；

- 按要求开展洗钱风险评估工作，根据反洗钱部意见完善业务操作流程，采取风险缓释措施；
- 采取有效管理机制，确保本业务部门相关客户身份资料和交易记录保存完整；
- 负责本业务部门相关数据治理，以满足监管合规要求和反洗钱工作需要；
- 对日常工作中发现的洗钱风险或线索，及时向反洗钱部报告；
- 配合反洗钱监管、反洗钱行政调查及合作机构协查；
- 开展本业务部门的反洗钱工作自查和整改；
- 负责本业务部门反洗钱合规文化传导，履行员工管理职责；
- 配合反洗钱部开展其它反洗钱工作。

5.5 信息技术管理部

信息技术管理部主要承担的职责包括：

- 根据反洗钱需要，协助开展相关的反洗钱数据治理和管理；
- 根据反洗钱需要，提供反洗钱工作所需的数据支持；
- 根据反洗钱法律法规要求，采取有效措施，确保所保存的客户身份数据和交易数据完整，防止数据丢失、损毁和篡改；
- 根据数据安全和保密要求，对客户、账户、交易信息及其他电子化信息实现符合监管要求的妥善保管和处理；
- 负责管理和维护客户实名流程，保障客户实名验证的有效性；

- 负责根据各业务不同的反洗钱需求，建立符合合规标准的客户身份基本信息登记和验证流程，为各相关业务线反洗钱客户尽职调查提供支撑。

5.6 法律合规部

- 配合开展重大洗钱风险事件处置化解工作；
- 配合反洗钱监管检查工作；
- 配合落实其他反洗钱相关工作。

5.7 人资行政部

人资行政部负责洗钱风险管理相关的人力资源管理工作，主要职责包括：

- 协助反洗钱部结合监管要求和公司反洗钱实际需求，保障反洗钱人力资源；
- 协助反洗钱部选聘符合反洗钱需求的员工；
- 协助反洗钱部制订公司反洗钱培训目标和计划，推进反洗钱培训和教育项目；
- 负责在聘用员工、高级管理人员、洗钱风险管理人员之前，对相关人员是否涉及刑事犯罪，是否存在其他犯罪记录等进行充分的背景调查，评估洗钱风险。

6.反洗钱主要管理活动

6.1 客户尽职调查

6.1.1 客户尽职调查的目的

客户尽职调查是指以“了解你的客户”为原则，针对具有不同洗钱风险的客户、业务关系或交易，采取相应的尽职调查措施，登记客户基本信息、核实客户真实身份、了解客户建立和维持业务关系的目的及性质、了解实际控制客户的自然人和交易的实际受益人的过程。客户尽职调查主要目的主要是：识别客户真实身份、识别不应建立业务关系的客户、了解客户真实交易目的、评估客户洗钱风险、识别客户的交易类型和业务品种等。

6.1.2 客户尽职调查基本要求

6.1.2.1 客户身份识别

客户身份识别的基本要求是登记和留存客户身份基本信息及有效身份证明文件，并通过可靠手段来核实客户身份信息或身份证明文件是否合法、真实、有效。为客户办理以下业务时，应当开展客户身份识别，并登记客户身份基本信息，留存客户有效身份证件或者其他身份证明文件的复印件或者影印件：

- 经纪业务；
- 资产管理业务；
- 向不在本机构开立账户的客户销售各类金融产品且交易金额单笔人民币5万元以上或者外币等值1万美元以上的；
- 融资融券、股票质押、约定购回等信用交易类业务；
- 场外衍生品交易等柜台业务；
- 承销与保荐、上市公司并购重组财务顾问、公司债券受托管理、非上市公众公司推荐、资产证券化等业务；

- 中国人民银行和中国证券监督管理委员会规定的应当开展客户尽职调查的其他证券业务。

自然人客户身份识别与核验：集团建立统一的个人实名认证程序，负责对实名认证个人客户的身份信息进行识别和校验。自然人客户建立金融业务关系时，须根据不同业务线的反洗钱具体要求，通过金融实名认证程序登记必要的客户基本信息[1]，实名认证手段包括公安网信息比对、银行卡绑卡鉴权等，认证不通过的不得建立金融业务关系。

非自然人客户身份识别与核实：集团建立统一的企业实名认证程序，在与单位客户建立金融业务关系时，须通过企业实名认证平台填写客户基本信息[2]，并上传可证明该客户合法真实身份及相关业务资质的证件或文件，经公安网信息比对、工商信息比对、补充人工审核等真实性核验后，方可建立金融业务关系。除履行上述基本的身份识别与核验之外，企业客户还应登记留存符合监管要求的受益所有人信息。

业务部门单独设立客户准入流程的，需采取不低于集团统一实名认证标准的措施，确保客户基础信息登记、客户身份识别和核验机制或措施能够按照行业内反洗钱监管要求及合作证券基金公司协议约定。

6.1.2.2 了解客户

业务部门和相关职能部门应根据反洗钱监管要求以及具体业务流程和实际，采

[1] 个人客户基本信息要素主要包括：客户姓名、国籍、性别、职业、住址、联系方式以及客户有效身份证件的种类、号码和有效期限。

[2] 单位客户基本信息包括：法人、其他组织和个体工商户的“身份基本信息”指名称、住所、经营范围、可证明该客户依法设立或者可依法开展经营、社会活动的执照、证件或者文件的名称、号码和有效期限；法定代表人或负责人和授权办理业务人员的姓名、身份证件或者身份证明文件的种类、号码、有效期限；受益所有人的姓名、地址、身份证件或者身份证明文件的种类、号码、有效期限。

取相应的调查措施，了解客户的更多背景信息，包括但不限于：

- 客户交易的目的和业务性质；
- 客户资金来源和财富来源；
- 客户职业/行业等信息；
- 客户地址/主要运营地；
- 其他必要的信息。

6.1.2.3 持续尽职调查

在与客户业务关系存续期间，业务管理部门应采取措施对客户先前提供的身份证件和基本信息进行持续监控和核实。客户身份证明文件已过有效期的，应在监管要求的合理期限内提示客户更新或补充身份资料或信息。客户未在规定的期限内更新的，应根据监管要求中止为客户办理业务。

在与客户业务关系存续期间，触发以下情况时，业务管理部门应采取有效手段，对客户的身份信息进行重新识别：

- 客户要求变更姓名或者名称、身份证件或者身份证明文件种类、身份证件号码、注册资本、经营范围、法定代表人或者负责人等的；
- 客户行为或者交易情况出现异常的；
- 获得的客户信息与先前已经掌握的相关信息存在不一致或相互矛盾的；
- 先前获得的客户身份资料的真实性、有效性、完整性存在疑点的；
- 基金公司同步的风险客户；

- 反洗钱部认为应重新识别客户身份的其他情形。

6.2 客户资料与交易记录保存

公司各相关部门应遵循安全、准确、完整、保密的原则，妥善保存客户身份资料及交易记录，并应采取严格的管理措施和技术措施，防止客户身份资料和交易记录的缺失、损毁，防止客户身份信息和交易信息泄漏，并应满足反洗钱和反恐怖融资调查和监督管理的需要。

6.2.1 应当保存的资料和记录

各业务部门或相关负责部门须保存的客户身份资料包括记载客户身份信息、身份证件或资料、影像资料，以及反映开展客户尽职调查工作的各种记录和资料。

应保存的交易记录包括：每笔交易的数据信息、业务凭证、账簿以及按照有关规定要求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，确保能够重现每笔交易，实现资金追溯。

6.2.2 保存期限要求

业务部门或相关负责部门应确保客户身份资料自业务关系结束当年或者一次性交易记账当年计起至少保存5年。交易记录自交易记账当年计起至少保存5年。

如客户身份资料和交易记录涉及正在被反洗钱和反恐怖融资调查的可疑交易活动，且反洗钱和反恐怖融资调查工作在前款规定的最低保存期届满时仍未结束的，应将其保存至反洗钱和反恐怖融资调查工作结束。

法律、行政法规和其他规章对客户身份资料和交易记录有更长保存期限要求的，遵守其规定。

涉及破产清算的，应根据监管规定，将客户身份资料和交易记录移交相关指定机构。

6.3 反洗钱名单监控

6.3.1 名单库管理

公司通过外采名单库作为反洗钱监控名单的主要数据源，名单包括但不限于：联合国、FATF等国际组织，以及中国政府及相关部门发布的名单，名单类型包括涉恐、制裁、涉黑、涉毒、经济犯罪、腐败、政治敏感人物等。

根据监管指引和公司风险管理需要，反洗钱名单划分为禁止类和高风险关注类：

- 禁止类名单包括联合国制裁名单、公安部涉恐名单、红通名单等人民银行要求重点监控的名单，一旦发现客户命中该名单，相关部门应配合对其实名和交易进行拦截或账户冻结；
- 高风险关注名单是指存在较大洗钱风险的名单，需根据风险评估加强监控或采取相适应的风险缓释措施。

反洗钱部指定专人负责名单库的更新与维护，更新名单须在确认后的 24 小时内，经反洗钱部负责人审批后进行策略布控。未经审批，任何人不得擅自修改名单库。

反洗钱部确认存在重大洗钱可疑并须退出客户关系的，由相关业务线客户管理、账户管理或其他风险管理部门执行退出程序，并将该客户纳入黑名单管理。

6.3.2 名单筛查

实名环节名单筛查：为降低公司因与受制裁名单发生交易而带来潜在的法律风险，在实名认证环节，系统对客户实名证件号码和反洗钱名单库进行实时扫描和

比对，当证件号码与涉恐、制裁等禁止类型的数据匹配一致时，则进行实名阻断。

回溯性筛查：反洗钱部制定名单回溯匹配逻辑，每日对全量实名客户进行自动筛查。对匹配一致的客户，反洗钱部进行人工复核确认，确系为禁止类的情况，及时向反洗钱监测分析中心报告，并以电子形式或书面形式向所在地中国人民银行或者其分支机构报告，根据监管意见进行跟进处置和控制措施设置。

6.4 反洗钱审核

6.4.1 新业务反洗钱评审

公司新业务、新产品、新渠道、新技术上线运营前，须根据公司新业务评审流程提交反洗钱部进行评审。经反洗钱部评审，该业务、产品、渠道、技术不符合反洗钱合规性要求，或超出本公司洗钱风险控制能力时，不予评审通过。业务部门可通过调整业务模式、修改产品流程、增加必要的风控措施等方式，提升合规性或降低洗钱风险，提交反洗钱部再次进行评审。

6.4.2 协议审核

公司与合作机构签订协议前，业务部门应先对反洗钱相关条款进行评估，确认现有业务流程能否满足协议要求，后将评估意见及合作协议一并提交反洗钱部审核。 经反洗钱部审核，协议反洗钱条款不符合行业内反洗钱监管规定，或双方反洗钱义务分担有失公允的，业务部门应根据反洗钱意见推动协议修改。如特殊原因导致协议无法完全依照反洗钱意见修改，业务部门须征得本部门负责人及法务部门特别审批后才可签署协议。

6.5 客户洗钱风险评估

公司遵循“风险为本”的反洗钱管理原则，根据反洗钱监管指引，结合自身业务性质、规模和业务复杂程度等，综合考虑不同风险维度，设计客户洗钱风险评估模型。

6.5.1 客户洗钱风险评估模型

反洗钱部负责建立客户洗钱风险评估指标和模型，并根据监管当局发布的国家洗钱风险评估结果、风险提示、案件通报等外部可靠信息进行适时调整，以使风险评估结果适应环境变化，更加趋于有效。客户洗钱风险经评估划分为高风险客户、中风险客户和低风险客户三个等级。客户风险评估模型主要参考四个维度的因素：客户特性风险、国家/地域风险、行业/职业风险、使用金融产品风险。

- 客户维度主要考虑客户信息公开程度、建立或维持业务关系的渠道、客户身份证件的种类、核实客户身份的难度、可疑交易命中和报告情况、客户年龄阶段、客户注册存续时间、客户注册行为等因素；
- 国家与地域维度主要考虑当地受反洗钱监控或制裁情况、与当地相关的反洗钱风险提示情况、当地洗钱上游犯罪状况等因素；
- 行业/职业维度主要考虑国际、国内权威建议的高风险行业或职业、客户的行业或产品是否提供匿名服务、客户是否涉及现金密集型行业等因素；
- 金融产品维度主要考虑客户使用我公司高风险金融产品的因素。

6.5.2 直接定义的禁止类客户与高风险客户

除上述模型对客户进行洗钱风险评估以外，公司定义以下直接认定的禁止类客

户与高风险客户，而无论其风险评估模型的评估结果如何。任何情况下各金融主体或相关部门不得与所规定的禁止类客户建立业务关系或提供金融服务，除非获得特别授权。对直接定义或模型评估的高风险客户，应基于反洗钱部意见进行业务合作。

直接定义的禁止类客户包括：

- 列入联合国发布的制裁名单；
- 列入我国政府发布的涉恐名单；
- 无法有效识别和核实客户身份；
- 不受法律监管的境外从事金融相关业务的金融机构和货币服务机构；
- 存在严重洗钱和恐怖融资犯罪事实且已被退出业务关系的；
- 不符合公司洗钱风险容忍度的其他类型客户。

直接定义的高风险客户包括：

- 客户为外国政要或其亲属、关系密切人；
- 客户被列为我国发布或承认的应实施反洗钱监控措施的其他名单；
- 客户实际控制人或受益所有人属前两项所述人员；
- 上报过可疑交易报告的客户；
- 客户拒绝配合依法开展的尽职调查工作；
- 涉及高风险国家或地区的非银行金融机构、慈善机构、非营利性组织、宗教组织等；

- 其他监管要求或公司认为可直接定义为高风险的客户。

6.5.3 客户洗钱风险评估流程

客户通过系统完成相应的实名准入流程后，反洗钱部在5个工作日内完成客户洗钱风险评估，获得客户初次风险评级结果。

为确保客户洗钱风险评级状态的及时性和有效性，反洗钱部对客户洗钱风险采取动态评估方式，在初次评估后，结合客户风险评估模型的指标动态变化，每周进行一次重新评估，以持续修正评级结果，更及时反映客户风险状况。

客户洗钱风险评估工作相关文档和信息须得到妥善保存。

6.5.4 高风险客户、基金公司同步的风险客户管理

对于评级为高风险的客户，由反洗钱部执行强化客户尽职调查程序，进一步了解客户的财富来源和资金来源等，具体参见《高风险客户尽职调查操作手册》。

此外，反洗钱部负责制定高风险客户专项可疑交易监控规则，以强化高风险客户交易监测频率和强度；对上报可疑的高风险客户再次发生交易时进行人脸核验等强化身份识别方式。

建立风险台账，对基金公司同步的风险客户身份重新识别情况、对外反馈信息及后续控制措施进行登记并同步相关业务方及反洗钱部。

6.5.5 产品业务洗钱风险评估

反洗钱部统筹公司存量业务的洗钱风险评估工作，评估因素主要包括：与现金关联程度、是否容易转移资金、是否涉及代理交易，历史可疑交易报告情况、公安调证覆盖情况等。经评估该业务为高风险时，各业务部门与相关职能部门应根据

风险管理部意见，对该业务采取强化的控制措施，包括但不限于：

- 强化客户准入审核；
- 限制交易金额、频次；
- 限制业务范围；
- 加强交易监控。

6.5.6 法人机构洗钱风险评估

反洗钱部结合公司业务实际，考虑业务规模、范围和业务复杂程度，并参考监管机构风险评估报告和风险提示，定期对公司及各金融主体所面临的内外部洗钱和恐怖融资风险进行全面评估。

6.5.6.1 风险评估模型

法人机构洗钱风险评估主要包括三个方面：固有风险评估、控制有效性评估、剩余风险评估。

固有风险评估包括四个维度：一是客户群体固有风险评估，如高风险客户数量和比例、涉刑事查冻扣数量和比例、客户身份信息完整度、核实客户身份的有效性等；二是地域固有风险评估，如当地洗钱上游犯罪形式、权威部门对当地的洗钱风险评估情况、当地涉及刑事查冻扣情况、当地涉及可疑交易报告情况等；三是产品业务固有风险评估，如产品涉及高风险客户情况、产品涉及已知洗钱案例情况、产品本身洗钱便利情况、产品是否交易透名等；四是渠道固有风险评估，如渠道覆盖范围的风险程度、渠道引入的客户规模及风险分布、渠道办理业务的规模及风险分布等。

控制有效性评估包括三个维度：一是反洗钱内控基础与环境，主要评估公司及各金融主体高级管理层履职情况、反洗钱管理架构与机制运转情况、反洗钱管理权限和资源、反洗钱监督有效性等；二是洗钱风险管理机制有效性，主要评估各级管理层对洗钱风险的认识、反洗钱政策制定情况、内控制度的适用性、反洗钱内部协调机制、反洗钱主要管理活动的全面性和有效性等；三是特殊控制措施有效性，主要评估针对地域风险、客户风险、产品业务风险、渠道风险，是否根据不同风险实际，设置有特别的风险缓释措施。

剩余风险通过固有风险评估和控制有效性评估二维矩阵方式，对照整体和不同维度剩余风险登记计量得出。

6.5.6.2 评估要求

- 公司洗钱风险自评估工作在公司负责人领导下，由反洗钱部牵头，各业务部门、内控等部门参与成立评估组，共同制定评估方案，开展独立评估；
- 自评估工作应如实记录存档，评估结果报京东科技风委会及高级管理层审批；
- 京东科技风委会和高级管理层依据自评估结论，制定或持续调整完善洗钱风险管理政策、控制措施和程序，并监督控制措施执行情况；
- 自评估至少每两年进行一次，或当显著影响本公司业务及所面对风险的触发事件发生后，开展评估复核。

7.反洗钱数据

7.1 公司各业务部门或相关部门应当加强本部门的数据管理，建立健全数据质

量控制机制，确保所保存的客户信息和交易记录真实、准确、连续、完整，数据的存储和使用应当符合数据安全标准、满足保密管理要求。

7.2 反洗钱部统筹建立公司级反洗钱数据集市，以满足公司洗钱风险识别、评估和报告的工作需求。对于业务合作中其他金融机构依法正常获取开展反洗钱工作所必需的信息和数据的，各相关部门应依法给予必要的协助。

8.反洗钱文化建设

反洗钱作为一项法律义务，体现社会、公司及员工守法合规的价值要求。反洗钱部牵头公司反洗钱文化建设，定期通过培训宣传等形式，将反洗钱意识纳入日常业务开展中，守好公司价值底线。

8.1 反洗钱培训

8.1.1 公司反洗钱培训一般采用网络培训、课堂培训、书面材料等方式，分别开设新员工入职培训和员工持续培训课程，培训内容主要有反洗钱法律法规、京东科技反洗钱政策和相关制度、反洗钱专业知识和技能等，具体包括但不限于：

- 基金代销机构、公司相关部门及员工本身的法定责任，以及违反反洗钱相关法律规定而可能需要承担的后果；
- 公司在打击洗钱和恐怖融资方面的政策及程序，包括客户尽职调查程序、客户资料和交易记录保存要求等；
- 洗钱与恐怖融资的新方法、新手段和犯罪趋势。

8.1.2 人资行政部协助反洗钱部至少每年制作或更新一次反洗钱基础知识网络

视频课程，作为新员工入职培训课程之一。

8.1.3 反洗钱部不定期对肯特瑞高级管理人员和业务部门员工进行反洗钱专业知识培训，并在培训结束后进行反洗钱知识测试和考核。

8.1.4 反洗钱部负责建立培训档案，保存培训资料、培训签到记录等反洗钱培训工作的记录。

8.2 反洗钱宣传

8.2.1 反洗钱部根据实际情况，以季度为单位开展反洗钱宣传工作，宣传方式包括但不限于：内部刊物宣传、内部办公网络宣传、宣传折页、社区宣传、微信公众号、官方微博等社交媒体等。

8.2.2 反洗钱部负责建立宣传档案，保存宣传照片、宣传手册、网络宣传截图等反洗钱宣传工作的资料。

9.反洗钱内部监督与奖惩

9.1 反洗钱内部检查

反洗钱部建立反洗钱监督检查工作机制，制定计划定期对相关业务部门、职能部门反洗钱工作开展检查，或针对某控制薄弱环节开展专项检查，及早发现风险并采取措施缓释风险。

各部门应积极配合反洗钱监督检查工作，提供检查所需资料、系统、数据或文档，并针对反洗钱检查发现的问题积极予以回应和整改。

9.2 反洗钱审计

公司定期对反洗钱工作开展内部审计,评价肯特瑞反洗钱制度的健全性和有效性，督促各项反洗钱制度的落实和执行，加强对各部门反洗钱工作的监督检查，推进完善反洗钱内部操作规程及工作机制，落实反洗钱相关法律规定的各项要求。反洗钱内部审计包括但不限于以下内容：

- 反洗钱法律法规和监管要求的执行情况；
- 内控制度设计和执行落实的有效性；
- 工作机制和系统有效性；
- 其他洗钱风险管理情况等。

9.3 反洗钱奖惩

9.3.1 为保障肯特瑞反洗钱工作有序开展，有效缓释和控制公司业务面临的洗钱风险和声誉风险，公司将反洗钱开展不力作为重大风险事项纳入各相关部门及相关员工工作考核。

9.3.2 公司对于在工作中自觉履行反洗钱义务、在反洗钱工作领域有显著贡献的部门或员工给予奖励，对违反反洗钱法律法规和本政策及相关制度的行为给予不同程度的惩罚。

10.反洗钱监管事务

10.1 反洗钱监管检查：公司各业务部门和相关责任部门，须积极配合人民银行或其他监管机构对公司开展的现场或非现场检查。具体参见京东科技统一的监管检查流程和机制。

10.2 反洗钱行政调查：公司各业务部门和相关责任部门应当依法协助人民银行、公安机关和国家安全机关的调查、侦查，提供与恐怖活动组织及恐怖活动人员有关的信息、数据以及相关资产情况。

11.反洗钱保密

11.1 各业务部门、职能部门及其员工，对依法履行反洗钱义务获得的客户身份资料和交易信息予以保密，非依法律规定，不得向任何单位和个人提供。

11.2 各业务部门、职能部门及其员工，应对反洗钱相关的调查信息严格保密，包括但不限于：涉及反洗钱可疑交易调查和报告的信息、配合人民银行反洗钱行政调查相关信息、配合侦查机关反洗钱案件调查等相关信息。不得违反规定向任何单位和个人提供或透漏，不得在采取冻结措施前通知资产所有人、控制人或者管理人。

11.3 肯特瑞所有员工均须严格遵守以上反洗钱保密要求，如有违反，将承担相应的行政处罚后果，直至承担刑事责任。

12.反洗钱应急处置

各业务部门、职能部门及其员工，发现反洗钱重大风险、舆情和危机时，应遵循公司报告程序进行报告，并向反洗钱部同步相关情况，以获得及时响应和处置，避免引发声誉风险。具体报告和处置流程参见公司重大风险事件报告和处置管理办法。

13.附则

13.1 本内控制度自发布之日起实施生效，原《京东肯特瑞基金销售有限公司反洗钱与反恐怖融资内控制度》（KTR-HG-A-01-2021V1）同时废止。

13.2 本内控制度中有关反洗钱相关义务标准和具体工作安排以基金代销行业反洗钱监管实际要求为准。

13.3 本内控制度由反洗钱部进行解释。

13.4 凡因违反上述规定并给公司造成任何损失，公司保留追究其法律责任的权利。