

AML/KYC 政策

本 AML/KYC 政策（以下简称“本政策”）说明 F-Tech（在Kazakhstan注册，以下简称“公司”、“我们”）在用户使用网站 <https://kashbi.io>、应用程序 KashBi、Telegram 机器人、Telegram Mini App、网页版本、API、加密货币-法币钱包、P2P 平台以及公司的其他相关服务（统称为“平台”）时，为防止洗钱、恐怖主义融资、规避制裁、欺诈以及其他非法或被禁止活动而采取的方针。

本政策是《使用条款》的一部分，并与《隐私政策》、P2P 交易规则、费用规则、风险提示以及公司的其他文件共同适用。

用户使用平台、创建账户、充值余额、提取数字资产、创建或接受 P2P 交易、接受验证，或以其他方式与平台互动，即表示用户确认已阅读本政策，并同意遵守本政策的规定。

如果用户不同意本政策，用户应停止使用平台。

1. 目的和适用范围

1.1. 本政策的目的

本政策旨在确立主要原则、规则和措施，以实现以下目的：

- 防止平台被用于洗钱；
- 防止恐怖主义融资；
- 防止规避制裁；
- 防止欺诈、诈骗、网络钓鱼及其他违法活动；
- 识别和评估高风险用户、操作、地址和司法管辖区；
- 监控涉及数字资产的操作和 P2P 交易；
- 遵守适用法律要求、合作伙伴要求、AML/KYC 服务提供商要求、银行要求、支付服务提供商要求以及主管机关要求；
- 保护用户、公司、平台以及公司的商业声誉。

1.2. 适用范围

本政策适用于平台的所有用户，包括以下服务或功能的用户：

- 加密货币-法币钱包；
- P2P 平台；
- Telegram Mini App；
- Telegram 机器人；
- 网页版本；

- 数字资产充值和提现功能；
- 内部转账；
- P2P 之外的法币操作（如该等功能可用）；
- 客服服务和争议处理。

1.3. 基于风险的方法

公司采用基于风险的方法。这意味着 KYC、AML 检查、限额、文件请求、强化尽职调查、监控、限制和其他措施，将根据用户、操作、司法管辖区、支付方式、数字资产、区块链地址、用户行为以及其他因素的风险水平按比例适用。

平台定位为 privacy-first：公司努力尽量减少个人数据收集，并避免在没有必要的情况下要求提供身份证明文件。同时，privacy-first 并不意味着完全匿名，也不排除在法律、平台规则、合作伙伴要求或本政策要求或允许的情况下，对数据进行处理、对用户进行验证、对交易进行审查、限制操作或向主管机关提供信息。

2. 术语和定义

2.1. AML

AML 指反洗钱措施，包括发现、防止、调查和限制与非法来源资金相关的操作。

2.2. KYC

KYC 指“了解你的客户”程序，包括在基于风险、限额、操作、适用法律或合作伙伴要求而有必要时，对用户进行身份识别、验证和评估。

2.3. CDD

CDD 指客户尽职调查，包括收集和分析有关用户、其活动、资金来源、操作目的和风险状况的信息。

2.4. EDD

EDD 指适用于较高风险用户、操作或情形的强化尽职调查。EDD 可包括要求提供额外文件、确认资金来源、扩展交易分析、公开来源核查、制裁和 PEP 筛查，以及由公司负责人层级批准继续提供服务。

2.5. KYT

KYT 指“了解你的交易”程序，包括分析操作、区块链地址、资金来源、用户行为、相关钱包、P2P 模式以及与特定操作相关的其他数据。

2.6. PEP

PEP 指政治公众人物，以及其家庭成员和与其关系密切的人；如果该等人员从腐败、制裁、声誉或其他风险角度需要加强关注，则适用本定义。

2.7. 制裁

制裁指由国家、国际组织、主管机关实施，或通过公司合作伙伴适用的经济、金融、贸易、个人、地域或其他限制性措施。

2.8. 禁止司法管辖区

禁止司法管辖区指公司因法律、制裁、高 AML 风险、合作伙伴要求、内部风险管理规则或其他情况而限制或禁止提供服务的国家、地区或区域。

禁止司法管辖区清单不一定在本政策中公布，可能在平台界面、公司内部规则、合作伙伴文件或单独通知中确定。

2.9. 可疑活动

可疑活动指可能表明洗钱、恐怖主义融资、规避制裁、欺诈、诈骗、使用他人数据、多账户使用、非法活动或其他不可接受风险的操作、行为、资金来源、P2P 交易、地址、支付方式、账户或其他因素。

2.10. Red flags / 风险警示信号

Red flags 指可能表明风险升高或需要额外审查的迹象或指标。

3. AML/KYC 控制组织

3.1. 负责人

公司可以指定负责人或团队，负责实施 AML/KYC 程序、风险管理、交易监控、可疑活动审查、与主管机关互动以及维护内部规则。

3.2. 内部规则

公司制定并适用内部规则、指引、风险标准、red flags、验证程序、限额、监控场景和决策规则。

该等内部文件属于公司的保密信息；如果披露可能损害控制措施的有效性、平台安全、法律合规、第三方权利或调查利益，则不向用户披露。

3.3. 程序更新

公司可以根据以下因素更新 AML/KYC 程序：

- 法律变化；
- 新产品和新功能；
- 新的欺诈模式；
- FATF 建议和其他国际标准；
- 合作伙伴要求；
- 内部审查结果；
- 安全事件；
- 制裁制度变化；
- 洗钱和恐怖主义融资的新类型。

4. 风险评估

4.1. 一般风险评估

公司可以定期评估与平台、用户、产品、数字资产、司法管辖区、访问渠道、P2P 交易、支付方式、P2P 之外的法币操作、区块链网络和服务提供商相关的 AML/KYC 风险。

4.2. 风险因素

在评估风险时，公司可以考虑：

- 用户的居住国、公民身份、位置或基于 IP 的地理信息；
- 账户类型和注册方式；
- 操作历史；
- 操作金额和频率；
- 使用的数字资产和网络；
- 发送方和接收方的区块链地址；
- 地址与混币器、暗网市场、黑客攻击、勒索软件、诈骗项目、受制裁地址或其他高风险来源之间的关联；
- P2P 交易的使用情况；
- 选择的法币支付方式；
- 争议中的行为；
- 其他用户的投诉；
- 多账户使用或与此前被封禁账户的关联；
- 使用 VPN、代理或其他隐藏位置的方式；
- 拒绝提供信息；
- 数据不一致；
- PEP 状态；
- 制裁匹配；
- adverse media 以及其他声誉因素；
- 合作伙伴和主管机关的要求。

4.3. 风险类别

公司可以为用户、操作、地址或交易分配内部风险类别，例如低风险、中风险、高风险或不可接受风险。

风险类别可能影响：

- 可用功能；
- 限额；
- 是否需要 KYC；

- 是否需要 EDD；
- 操作处理速度；
- 提现可用性；
- P2P 访问权限；
- 是否需要人工审查；
- 资产冻结或拒绝服务的可能性。

公司没有义务向用户披露内部风险类别、计算方法、具体标准或评分结果。

5. KYC/CDD：用户验证

5.1. 一般方法

除非法律、界面、合作伙伴要求或特定功能另有规定，公司默认不要求所有用户完成完整 KYC 验证。验证基于风险适用。

5.2. 何时可能需要 KYC

公司可以在以下情况下要求 KYC 或额外信息：

- 达到限额；
- 大额操作；
- 异常操作；
- 可疑活动；
- 开启争议；
- 提现请求；
- 与地址或交易相关的 AML 匹配；
- 与高风险司法管辖区有关联；
- 使用 P2P 之外的法币功能；
- 支付合作伙伴、银行、兑换服务提供商或 AML/KYC 提供商的要求；
- 主管机关的请求；
- 恢复账户访问权限；
- 怀疑多账户使用、欺诈或使用他人数据；
- 其他需要验证的情形。

5.3. 可能要求的数据

根据风险水平，公司可以要求：

- 名、姓、父称或其他完整姓名；
- 出生日期；

- 国籍；
- 居住国；
- 居住地址；
- email；
- 电话号码；
- 身份证明文件；
- 照片、自拍、视频验证或活体检测；
- 地址证明；
- 资金来源证明；
- 财富来源证明；
- 操作目的确认；
- 对账单、收据、凭证或付款确认；
- 与 P2P 交易相关的文件；
- 与 PEP 关联的信息；
- 评估风险所需的其他文件或说明。

5.4. 数据验证

公司可以通过以下方式验证所提供的数据：

- 人工方式；
- 自动化系统；
- 外部 AML/KYC 提供商；
- 制裁和 PEP 名单；
- 公开来源；
- 区块链分析；
- 从合作伙伴、用户、银行、支付服务提供商或主管机关获得的信息。

5.5. 用户合作义务

用户必须及时、准确、完整地提供所要求的信息和文件。

如果用户拒绝提供数据、提供虚假或不一致的信息、不回应请求或试图规避验证，公司可以限制功能、暂停操作、冻结资产、取消交易、拒绝服务或关闭账户。

5.6. 重新验证

即使用户此前已经通过验证，公司也可以在以下情况下再次要求文件或信息：

- 用户数据发生变化；
- 身份证明文件过期；

- 用户活动发生变化；
- 出现新的风险；
- 用户达到新的限额；
- 新功能开放；
- 法律或合作伙伴要求发生变化；
- 出现争议或可疑活动。

6. 强化尽职调查 EDD

6.1. 何时适用 EDD

如果用户、操作、地址、P2P 交易、司法管辖区或行为具有较高风险，公司可以适用 EDD。

尤其在以下情况下，可能适用 EDD：

- 用户为 PEP 或与 PEP 有关联；
- 用户与高风险司法管辖区有关联；
- 操作为大额、复杂、异常或经济上难以解释；
- 资金来自高风险区块链地址；
- 操作与混币器、暗网市场、黑客攻击、勒索软件、诈骗、受制裁地址或其他 red flags 有关；
- 用户频繁发起争议或在争议中败诉；
- 存在多账户使用迹象；
- 存在使用他人支付信息或账户的迹象；
- 用户无法解释资金来源；
- 用户回答相互矛盾；
- 根据合作伙伴或主管机关要求需要确认。

6.2. EDD 措施

EDD 可以包括：

- 要求额外文件；
- 确认资金来源；
- 确认财富来源；
- 确认操作目的；
- 公开来源检查；
- adverse media 检查；
- 深入分析区块链历史；
- 降低限额；

- 临时冻结资金；
- 人工批准操作；
- 拒绝操作；
- 终止服务。

6.3. EDD 结果

根据 EDD 结果，公司可以：

- 允许操作；
- 在限额或条件下允许操作；
- 要求额外信息；
- 拒绝操作；
- 在允许且可行的情况下退还资金；
- 冻结资金；
- 限制账户；
- 关闭账户；
- 在法律要求或允许的情况下向主管机关提供信息。

7. KYT 和交易监控

7.1. 一般监控

公司可以对用户操作进行持续或选择性监控，包括：

- 数字资产充值；
- 数字资产提现；
- 内部转账；
- P2P 交易；
- P2P 之外的法币操作（如该等功能可用）；
- 操作尝试；
- 已取消操作；
- 与争议或投诉相关的操作。

7.2. 区块链分析

公司可以使用区块链分析来评估地址、交易、地址集群、资金来源和相关实体的风险。

审查可能考虑与以下对象的关联：

- 受制裁地址；
- 暗网市场；

- 混币器和混淆服务；
- 勒索软件；
- 黑客攻击和被盗资金；
- 诈骗项目；
- 欺诈模式；
- 非法服务；
- 高风险交易所或兑换商；
- 其他风险升高的来源。

7.3. P2P 监控

在 P2P 交易中，公司可以分析：

- 交易频率；
- 交易金额；
- 各方行为；
- 取消次数；
- 争议次数；
- 投诉；
- 付款证明；
- 支付信息匹配情况；
- 账户关联；
- 多账户使用迹象；
- 支付数据不一致；
- 将交易转移到平台规则之外的尝试；
- 使用第三方银行账户、银行卡或支付信息。

7.4. 限额和延迟

公司可以针对特定用户、操作、交易、地址、资产、支付方式或司法管辖区设置限额、延迟、人工审查或额外要求。

操作可能被延迟或暂停，直至审查完成。

8. Red flags：可疑活动迹象

Red flags 可包括但不限于：

- 用户拒绝提供数据或文件；
- 提供伪造、篡改或相互矛盾的文件；

- 使用他人的数据、银行卡、账户或钱包；
- 试图使用多个账户；
- 频繁取消 P2P 交易；
- P2P 交易中频繁发生争议；
- 伪造收据、凭证或付款截图；
- 付款人姓名与用户不一致；
- 在没有明显经济目的的情况下快速充值和提现；
- 将操作拆分为多笔小额金额；
- 操作与用户通常行为不一致；
- 使用高风险区块链地址；
- 与混币器、暗网市场、黑客攻击、勒索软件、诈骗或受制裁地址有关联；
- 交易量突然大幅增加；
- 试图规避限额；
- 使用 VPN、代理或其他隐藏位置的方式规避限制；
- 对交易对手或客服施加强烈压力；
- 拒绝解释资金来源；
- 试图将交易移出平台；
- 来自其他用户的投诉；
- 公开来源中的负面信息；
- 与制裁、PEP 或 adverse media 来源匹配。

存在一个 red flag 并不一定意味着违规，但可能成为额外审查、限制操作或采取其他措施的依据。

9. 制裁和禁止关系

如果法律、制裁、合作伙伴要求或内部风险管理规则禁止，公司不会与用户建立或继续关系。

如果用户符合以下情况，公司可以拒绝服务、限制账户、冻结资产或终止关系：

- 被列入制裁名单；
- 与制裁名单中的人员有关联；
- 位于禁止司法管辖区；
- 为被禁止人员的利益行事；
- 使用平台规避制裁；
- 拒绝提供制裁筛查所需信息。

公司可以在注册时、操作前、操作后、制裁名单变化时、开启争议时、提现时或其他情况下进行制裁筛查。

10. 禁止活动

用户不得将平台用于：

- 洗钱；
- 恐怖主义融资；
- 规避制裁；
- 欺诈、诈骗、网络钓鱼或社会工程；
- 交易被盗资金、账户、银行卡、文件或个人数据；
- 在没有法律依据的情况下使用他人的银行卡、账户、钱包或支付信息；
- 非法贩卖毒品、武器、危险物质或其他禁止商品；
- 非法赌博；
- 非法金融服务；
- 暗网活动；
- 为极端主义、恐怖主义或其他被禁止活动提供资金；
- 侵犯第三方权利；
- 使用伪造文件、收据、凭证或截图；
- 多账户使用和规避限制；
- 公司认为非法、高风险或不可接受的任何其他活动。

11. 公司在发现风险时采取的措施

如果公司发现可疑活动、AML/KYC 风险、制裁风险、违反本政策或用户拒绝合作，公司可以：

- 要求额外信息；
- 要求 KYC 或 EDD；
- 降低限额；
- 延迟操作；
- 拒绝操作；
- 取消 P2P 交易；
- 限制 P2P 功能；
- 冻结或预留资产；
- 限制提现；
- 临时封锁账户；
- 关闭账户；
- 在可能、允许且不被法律禁止的情况下将资金退回给发送方；

- 在平台规则规定的情况下扣除适用费用、网络费用或退回处理费用；
- 在法律要求或允许的情况下向主管机关提供信息；
- 采取其他合理措施，以保护平台、用户、合作伙伴和公司。

如果通知可能违反法律、AML/KYC/CTF 要求、制裁规则、调查利益、平台安全或第三方权利，公司没有义务提前通知用户采取该等措施。

12. AML/KYC 拒绝情况下的资金退回

如果操作因 AML/KYC 审查而被拒绝，或服务受到限制，公司可以在可能且允许的情况下，将数字资产退回原始发送方地址，或退回公司从风险和法律角度认为可接受的其他地址。

在以下情况下，退回可能无法进行或被延迟：

- 资金与受制裁地址有关联；
- 资金与犯罪活动有关联；
- 已收到主管机关请求；
- 退回可能违反法律；
- 原始地址不可用、高风险或技术上不适用；
- 需要额外审查；
- 资金已被预留、冻结或与争议有关。

如果《使用条款》、费用页面 <https://kashbi.io/information/fees>、平台界面或单独规则有规定，可从退回金额中扣除网络费用、服务费用、处理费用和其他适用费用。

本政策不固定该等退回的具体费用或收费金额；如适用，该金额可由费用页面 <https://kashbi.io/information/fees>、平台界面或单独规则确定。

13. 报告以及与机关互动

在法律要求或允许的情况下，公司可以与主管机关、金融情报机构、执法机关、法院、监管机构、银行、支付服务提供商以及其他授权人员进行互动。

在以下情况下，公司可以提供有关用户、账户、交易、P2P 交易、争议、地址、支付数据或其他情况的信息：

- 收到合法请求；
- 有义务报告可疑活动；
- 需要遵守制裁要求；
- 需要保护公司、用户或第三方的权利；
- 需要防止欺诈、洗钱或恐怖主义融资。

如果通知被法律禁止、可能妨碍调查、披露内部 AML 程序或造成安全风险，公司没有义务就该等信息提

供通知用户。

14. 数据和记录保存

公司将在适用法律、合作伙伴要求、内部风险管理规则和《隐私政策》规定的期限内，保存与 AML/KYC、交易、P2P 交易、审查、争议、限制和报告相关的数据和记录。

该等数据可包括：

- KYC 数据；
- 用户文件；
- 验证结果；
- 制裁和 PEP 匹配；
- 风险档案；
- 操作历史；
- 区块链地址；
- 交易 txid/hash；
- P2P 交易数据；
- 付款证明；
- 争议材料；
- 与客服的通信；
- 关于限制的内部决定；
- 主管机关请求记录。

删除账户、撤回同意或停止使用平台，并不总是意味着立即删除 AML/KYC 数据；如果法律、AML/KYC/CTF 规则、保护公司权利、解决争议或履行主管机关请求要求或允许保存，该等数据可以继续保存。

15. 第三方和服务提供商

公司可以聘请第三方执行 AML/KYC 程序，包括：

- 文件验证提供商；
- 活体检测提供商；
- 制裁筛查提供商；
- PEP/adverse media 筛查提供商；
- 区块链分析提供商；
- 支付合作伙伴；
- 银行、处理机构和兑换服务提供商；
- 法律、合规和审计顾问；

- 基础设施和安全提供商。

除法律、与提供商的合同或公司单独政策另有要求，提供商可以按类别而非具体名称列示。

公司可以对合作伙伴和提供商进行制裁、声誉、许可、授权、风险以及遵守安全和保密要求能力方面的审查。

16. 用户义务

用户承诺：

- 不将平台用于禁止活动；
- 提供真实信息；
- 及时回应公司的请求；
- 在被要求时提供文件和说明；
- 仅使用合法属于自己的资金；
- 不在没有法律依据的情况下使用他人的银行卡、账户、钱包或支付信息；
- 不提供伪造文件、收据、截图或凭证；
- 不规避限额、检查、制裁限制或平台规则；
- 不为规避限制而创建多个账户；
- 遵守适用法律；
- 自行评估其操作在居住国的合法性。

拒绝合作、规避验证、提供虚假信息或试图规避 AML/KYC 控制，可能导致服务受到限制或终止。

17. AML/KYC 程序的保密性

用户理解，公司不会披露：

- 具体风险标准；
- 内部 red flags；
- 监控阈值；
- 评分算法；
- AML 数据来源；
- 调查细节；
- 向主管机关提交报告的原因；
- 内部决定的细节；
- 披露可能违反法律、安全或 AML/KYC 控制有效性的信息。

18. 本政策的变更

公司可以随时修改本政策。最新版本将发布在网站 <https://kashbi.io> 或平台界面中。

除非适用法律另有规定，用户在更新版本发布后继续使用平台，即表示用户同意本政策的新版本。

19. 语言版本

本政策可以以俄语、哈萨克语、英语和其他语言发布。

如果适用法律要求特定语言版本具有优先效力，则适用该语言版本。在其他情况下，如不同语言版本之间存在差异，以俄语版本为准。

20. 联系方式

用户如对本政策有任何问题，可以通过以下方式联系：

- 公司：F-Tech
- 注册国家：Kazakhstan
- 网站：<https://kashbi.io>
- 应用程序：KashBi
- Email：legal@kashbi.io
- Telegram：[kashbi_support](https://t.me/kashbi_support)
- 法定地址：44/1 Al-Farabi Avenue, Apartment 207