Política AML/KYC

A presente Política AML/KYC (a “Política”) descreve a abordagem da F-Tech, registrada no Kazakhstan (a “Empresa”, “nós”, “nos”, “nosso”), para prevenir lavagem de dinheiro, financiamento do terrorismo, evasão de sanções, fraude e outras atividades ilegais ou proibidas ao utilizar o site https://kashbi.io, o aplicativo KashBi, o bot do Telegram, o Telegram Mini App, a versão web, a API, a carteira cripto-fiat, a plataforma P2P e outros serviços relacionados da Empresa, denominados em conjunto como a “Plataforma”.

A presente Política faz parte dos Termos de Uso e aplica-se em conjunto com a Política de Privacidade, as regras de transações P2P, as regras de comissões, os avisos de risco e outros documentos da Empresa.

Ao utilizar a Plataforma, criar uma conta, depositar fundos no saldo, retirar ativos digitais, criar ou aceitar uma transação P2P, passar por verificação ou interagir de qualquer outra forma com a Plataforma, o usuário confirma que leu esta Política e concorda em cumprir suas disposições.

Se o usuário não concordar com a presente Política, deverá deixar de utilizar a Plataforma.

1. Finalidade e âmbito de aplicação

1.1. Finalidade da Política

A finalidade da presente Política é estabelecer os principais princípios, regras e medidas voltados a:

- prevenir o uso da Plataforma para lavagem de dinheiro;
- prevenir o financiamento do terrorismo;
- prevenir a evasão de sanções;
- prevenir fraude, golpes, phishing e outras atividades ilícitas;
- identificar e avaliar usuários, operações, endereços e jurisdições de alto risco;
- monitorar operações com ativos digitais e transações P2P;
- cumprir requisitos legais aplicáveis, requisitos de parceiros, fornecedores de serviços AML/KYC, bancos, provedores de pagamento e autoridades competentes;
- proteger os usuários, a Empresa, a Plataforma e a reputação comercial da Empresa.

1.2. Âmbito de aplicação

A presente Política aplica-se a todos os usuários da Plataforma, incluindo usuários de:

- carteira cripto-fiat;
- plataforma P2P;
- Telegram Mini App;
- bot do Telegram;
- versão web;
- funções de depósito e retirada de ativos digitais;

- transferências internas;
- operações fiat fora de P2P, se tais funções estiverem disponíveis;
- suporte e resolução de disputas.

1.3. Abordagem baseada em risco

A Empresa aplica uma abordagem baseada em risco. Isso significa que KYC, verificações AML, limites, solicitações de documentos, diligência devida reforçada, monitoramento, restrições e outras medidas são aplicadas proporcionalmente ao nível de risco do usuário, da operação, da jurisdição, do método de pagamento, do ativo digital, do endereço blockchain, do comportamento do usuário e de outros fatores.

A Plataforma é posicionada como privacy-first: a Empresa busca minimizar a coleta de dados pessoais e não solicitar documentos de identificação sem necessidade. Ao mesmo tempo, privacy-first não significa anonimato total e não exclui o tratamento de dados, a verificação do usuário, a análise de transações, a restrição de operações ou a transmissão de informações a autoridades competentes quando isso for exigido ou permitido por lei, pelas regras da Plataforma, pelos requisitos de parceiros ou por esta Política.

2. Termos e definições

2.1. AML

AML significa medidas de combate à lavagem de dinheiro, incluindo a detecção, prevenção, investigação e restrição de operações relacionadas a fundos de origem ilícita.

2.2. KYC

KYC significa o procedimento “Know Your Customer” ou “conheça seu cliente”, incluindo a identificação, verificação e avaliação de um usuário quando tal procedimento for exigido em razão de risco, limites, uma operação, legislação aplicável ou requisitos de parceiros.

2.3. CDD

CDD significa diligência devida do cliente, incluindo a coleta e análise de informações sobre o usuário, sua atividade, origem dos fundos, finalidade das operações e perfil de risco.

2.4. EDD

EDD significa diligência devida reforçada aplicada a usuários, operações ou situações de maior risco. A EDD pode incluir solicitações de documentos adicionais, confirmação da origem dos fundos, análise ampliada de transações, verificação de fontes abertas, verificações de sanções e PEP, bem como aprovação da continuidade do atendimento por pessoas responsáveis da Empresa.

2.5. KYT

KYT significa o procedimento “Know Your Transaction” ou “conheça sua transação”, incluindo a análise de operações, endereços blockchain, fontes de fundos, comportamento do usuário, carteiras relacionadas, padrões P2P e outros dados relativos a uma operação específica.

2.6. PEP

PEP significa pessoa politicamente exposta, bem como seus familiares e pessoas estreitamente relacionadas a tal pessoa, quando tais pessoas exigirem atenção reforçada sob a perspectiva de riscos de corrupção, sanções, reputação ou outros riscos.

2.7. Sanções

Sanções significam medidas restritivas econômicas, financeiras, comerciais, pessoais, territoriais ou outras impostas por Estados, organizações internacionais, autoridades competentes ou aplicáveis por meio dos parceiros da Empresa.

2.8. Jurisdição proibida

Jurisdição proibida significa um país, território ou região em relação ao qual a Empresa restringe ou proíbe a prestação de serviços por motivo de lei, sanções, alto risco AML, requisitos de parceiros, regras internas de gestão de riscos ou outras circunstâncias.

A lista de jurisdições proibidas não é necessariamente publicada nesta Política e pode ser determinada na interface da Plataforma, nas regras internas da Empresa, em documentos de parceiros ou em avisos separados.

2.9. Atividade suspeita

Atividade suspeita significa uma operação, comportamento, origem de fundos, transação P2P, endereço, método de pagamento, conta ou outro fator que possa indicar lavagem de dinheiro, financiamento do terrorismo, evasão de sanções, fraude, golpe, uso de dados de terceiros, uso de múltiplas contas, atividade ilícita ou outro risco inaceitável.

2.10. Red flags / sinais de alerta

Red flags significa sinais ou indicadores que podem apontar risco elevado ou necessidade de revisão adicional.

3. Organização dos controles AML/KYC

3.1. Pessoas responsáveis

A Empresa pode designar uma pessoa responsável ou uma equipe responsável pela implementação dos procedimentos AML/KYC, gestão de riscos, monitoramento de transações, revisão de atividade suspeita, interação com autoridades competentes e manutenção das regras internas.

3.2. Regras internas

A Empresa desenvolve e aplica regras internas, instruções, critérios de risco, red flags, procedimentos de verificação, limites, cenários de monitoramento e regras de tomada de decisão.

Tais documentos internos constituem informação confidencial da Empresa e não estão sujeitos à divulgação aos usuários se tal divulgação puder prejudicar a eficácia dos controles, a segurança da Plataforma, o cumprimento da lei, os direitos de terceiros ou os interesses de uma investigação.

3.3. Atualização de procedimentos

A Empresa pode atualizar os procedimentos AML/KYC levando em consideração:

- alterações na legislação;
- novos produtos e funções;
- novos esquemas de fraude;
- recomendações do FATF e outros padrões internacionais;
- requisitos de parceiros;
- resultados de revisões internas;
- incidentes de segurança;
- alterações em regimes de sanções;
- novas tipologias de lavagem de dinheiro e financiamento do terrorismo.

4. Avaliação de riscos

4.1. Avaliação geral de riscos

A Empresa pode realizar avaliações periódicas dos riscos AML/KYC relacionados à Plataforma, usuários, produtos, ativos digitais, jurisdições, canais de acesso, transações P2P, métodos de pagamento, operações fiat fora de P2P, redes blockchain e provedores de serviços.

4.2. Fatores de risco

Ao avaliar o risco, a Empresa pode considerar:

- país de residência, cidadania, localização ou geografia baseada em IP do usuário;
- tipo de conta e método de registro;
- histórico de operações;
- valores e frequência das operações;
- ativos digitais e redes utilizados;
- endereços blockchain de remetentes e destinatários;
- vínculos de endereços com mixers, mercados darknet, hacks, ransomware, projetos scam, endereços sancionados ou outras fontes de alto risco;
- uso de transações P2P;
- métodos de pagamento fiat selecionados;
- comportamento em disputas;
- reclamações de outros usuários;
- uso de múltiplas contas ou vínculos com contas anteriormente bloqueadas;
- uso de VPNs, proxies ou outros meios de ocultar a localização;
- recusa em fornecer informações;
- inconsistência de dados;
- status de PEP;
- correspondências com sanções;
- adverse media e outros fatores reputacionais;

- requisitos de parceiros e autoridades competentes.

4.3. Categorias de risco

A Empresa pode atribuir categorias internas de risco a usuários, operações, endereços ou transações, como risco baixo, médio, alto ou inaceitável.

A categoria de risco pode afetar:

- funções disponíveis;
- limites;
- necessidade de KYC;
- necessidade de EDD;
- velocidade de processamento das operações;
- disponibilidade de retirada;
- acesso ao P2P;
- necessidade de revisão manual;
- probabilidade de congelamento ou recusa de serviço.

A Empresa não é obrigada a divulgar ao usuário a categoria interna de risco, a metodologia de cálculo, os critérios exatos ou os resultados de scoring.

5. KYC/CDD: verificação de usuários

5.1. Abordagem geral

A Empresa não exige verificação KYC completa de todos os usuários por padrão, salvo se previsto de outra forma por lei, pela interface, por requisitos de parceiros ou por uma função específica. A verificação é aplicada com base em risco.

5.2. Quando KYC pode ser exigido

A Empresa pode solicitar KYC ou informações adicionais nos seguintes casos:

- atingimento de limites;
- operação de grande valor;
- operação incomum;
- atividade suspeita;
- abertura de disputa;
- solicitação de retirada;
- correspondência AML relacionada a um endereço ou transação;
- vínculo com jurisdição de alto risco;
- uso de função fiat fora de P2P;
- requisito de parceiro de pagamento, banco, provedor de câmbio ou provedor AML/KYC;
- solicitação de autoridade competente;
- recuperação de acesso à conta;
- suspeita de uso de múltiplas contas, fraude ou uso de dados de terceiros;
- outras circunstâncias que exijam verificação.

5.3. Quais dados podem ser solicitados

Dependendo do nível de risco, a Empresa pode solicitar:

- nome, sobrenome, patronímico ou outro nome completo;
- data de nascimento;
- cidadania;
- país de residência;
- endereço residencial;
- email;
- número de telefone;
- documento de identidade;
- fotografia, selfie, verificação por vídeo ou prova de vida;
- comprovante de endereço;
- comprovação da origem dos fundos;
- comprovação da origem do patrimônio;
- confirmação da finalidade da operação;
- extrato, recibo, comprovante ou confirmação de pagamento;
- documentos relacionados a uma transação P2P;
- informações sobre conexão com PEP;
- outros documentos ou explicações necessários para avaliar o risco.

5.4. Verificação de dados

A Empresa pode verificar os dados fornecidos:

- manualmente;
- usando sistemas automatizados;
- por meio de provedores externos AML/KYC;
- por meio de listas de sanções e PEP;
- por meio de fontes abertas;
- por meio de análise blockchain;
- por meio de informações recebidas de parceiros, usuários, bancos, provedores de pagamento ou autoridades competentes.

5.5. Obrigação do usuário de cooperar

O usuário deve fornecer as informações e documentos solicitados de forma tempestiva, correta e completa.

Se o usuário se recusar a fornecer dados, fornecer informações falsas ou contraditórias, não responder às solicitações ou tentar contornar a verificação, a Empresa poderá restringir funções, suspender operações, congelar ativos, cancelar transações, recusar o serviço ou encerrar a conta.

5.6. Reverificação

A Empresa pode solicitar documentos ou informações novamente, mesmo que o usuário já tenha passado por verificação anteriormente, se:

- os dados do usuário tiverem mudado;
- o documento tiver expirado;
- a atividade do usuário tiver mudado;
- novos riscos tiverem surgido;
- o usuário tiver atingido novos limites;
- uma nova função tiver sido disponibilizada;
- requisitos legais ou de parceiros tiverem mudado;
- tiver surgido uma disputa ou atividade suspeita.

6. Diligência devida reforçada EDD

6.1. Quando a EDD se aplica

A Empresa pode aplicar EDD se um usuário, operação, endereço, transação P2P, jurisdição ou comportamento apresentar risco elevado.

A EDD pode ser aplicada, em particular, se:

- o usuário for PEP ou estiver relacionado a PEP;
- o usuário estiver relacionado a uma jurisdição de alto risco;
- a operação for grande, complexa, incomum ou economicamente inexplicável;
- os fundos vierem de um endereço blockchain de alto risco;
- a operação estiver relacionada a mixers, mercados darknet, hacks, ransomware, scam, endereços sancionados ou outros sinais de alerta;
- o usuário abrir ou perder disputas com frequência;
- houver sinais de uso de múltiplas contas;
- houver sinais de uso de dados de pagamento ou conta de terceiros;
- o usuário não puder explicar a origem dos fundos;
- o usuário responder de forma contraditória às perguntas;
- for necessária confirmação a pedido de parceiro ou autoridade competente.

6.2. Medidas de EDD

A EDD pode incluir:

- solicitação de documentos adicionais;
- confirmação da origem dos fundos;
- confirmação da origem do patrimônio;
- confirmação da finalidade da operação;
- verificação de fontes abertas;
- verificação de adverse media;
- análise aprofundada do histórico blockchain;

- redução de limites;
- congelamento temporário de fundos;
- aprovação manual de operação;
- recusa de operação;
- encerramento do serviço.

6.3. Resultados da EDD

Como resultado da EDD, a Empresa pode:

- permitir a operação;
- permitir a operação com limites ou condições;
- solicitar informações adicionais;
- recusar a operação;
- devolver fundos, quando permitido e possível;
- congelar fundos;
- restringir a conta;
- encerrar a conta;
- transmitir informações a autoridades competentes quando exigido ou permitido por lei.

7. KYT e monitoramento de transações

7.1. Monitoramento geral

A Empresa pode realizar monitoramento contínuo ou seletivo das operações dos usuários, incluindo:

- depósitos de ativos digitais;
- retiradas de ativos digitais;
- transferências internas;
- transações P2P;
- operações fiat fora de P2P, se tais funções estiverem disponíveis;
- tentativas de operação;
- operações canceladas;
- operações relacionadas a disputas ou reclamações.

7.2. Análise blockchain

A Empresa pode utilizar análise blockchain para avaliar o risco de endereços, transações, clusters de endereços, fontes de fundos e entidades relacionadas.

A revisão pode levar em conta vínculos com:

- endereços sancionados;
- mercados darknet;
- mixers e serviços de ofuscação;
- ransomware;
- hacks e fundos roubados;

- projetos scam;
- esquemas fraudulentos;
- serviços ilegais;
- exchanges ou casas de câmbio de alto risco;
- outras fontes de risco elevado.

7.3. Monitoramento P2P

Em transações P2P, a Empresa pode analisar:

- frequência das transações;
- valores das transações;
- comportamento das partes;
- número de cancelamentos;
- número de disputas;
- reclamações;
- comprovantes de pagamento;
- correspondências de dados de pagamento;
- vínculos entre contas;
- sinais de uso de múltiplas contas;
- inconsistências nos dados de pagamento;
- tentativas de levar uma transação para fora das regras da Plataforma;
- uso de contas bancárias, cartões ou dados de pagamento de terceiros.

7.4. Limites e atrasos

A Empresa pode estabelecer limites, atrasos, revisões manuais ou requisitos adicionais para usuários, operações, transações, endereços, ativos, métodos de pagamento ou jurisdições específicos.

Uma operação pode ser atrasada ou suspensa até que a revisão seja concluída.

8. Red flags: sinais de atividade suspeita

Red flags podem incluir, entre outros:

- recusa do usuário em fornecer dados ou documentos;
- apresentação de documentos falsificados, alterados ou contraditórios;
- uso de dados, cartões, contas ou carteiras de terceiros;
- tentativa de utilizar várias contas;
- cancelamentos frequentes de transações P2P;
- disputas frequentes em transações P2P;
- recibos, comprovantes ou capturas de tela de pagamento falsificados;
- divergência entre o nome do pagador e o usuário;
- entrada e saída rápida de fundos sem finalidade econômica aparente;
- estruturação de operações em vários valores menores;

- operações incompatíveis com o comportamento habitual do usuário;
- uso de endereços blockchain de alto risco;
- vínculos com mixers, mercados darknet, hacks, ransomware, scams ou endereços sancionados;
- aumento brusco do volume de operações;
- tentativas de contornar limites;
- uso de VPNs, proxies ou outros meios de ocultar a localização para contornar restrições;
- pressão agressiva sobre a contraparte ou o suporte;
- recusa em explicar a origem dos fundos;
- tentativa de levar uma transação para fora da Plataforma;
- reclamações de outros usuários;
- informações negativas de fontes abertas;
- correspondências com fontes de sanções, PEP ou adverse media.

A presença de uma única red flag nem sempre significa violação, mas pode servir como base para revisão adicional, restrição de uma operação ou outras medidas.

9. Sanções e relações proibidas

A Empresa não estabelece nem mantém relações com usuários quando isso for proibido por lei, sanções, requisitos de parceiros ou regras internas de gestão de riscos.

A Empresa pode recusar serviço, restringir uma conta, congelar ativos ou encerrar a relação se o usuário:

- estiver incluído em uma lista de sanções;
- estiver relacionado a uma pessoa incluída em uma lista de sanções;
- estiver em uma jurisdição proibida;
- agir no interesse de uma pessoa proibida;
- utilizar a Plataforma para evadir sanções;
- recusar-se a fornecer informações necessárias para a verificação de sanções.

A Empresa pode realizar verificações de sanções no registro, antes de uma operação, após uma operação, quando listas de sanções forem alteradas, na abertura de uma disputa, na retirada de fundos ou em outros casos.

10. Atividade proibida

É proibido ao usuário utilizar a Plataforma para:

- lavagem de dinheiro;
- financiamento do terrorismo;
- evasão de sanções;
- fraude, scams, phishing ou engenharia social;
- comércio de fundos, contas, cartões, documentos ou dados pessoais roubados;
- uso de cartões bancários, contas, carteiras ou dados de pagamento de terceiros sem

base legal;

- tráfico ilegal de drogas, armas, substâncias perigosas ou outros bens proibidos;
- jogos de azar ilegais;
- serviços financeiros ilegais;
- atividade em darknet;
- financiamento de atividades extremistas, terroristas ou outras atividades proibidas;
- violação de direitos de terceiros;
- uso de documentos, recibos, comprovantes ou capturas de tela falsificados;
- uso de múltiplas contas e contorno de restrições;
- qualquer outra atividade que a Empresa considere ilegal, de alto risco ou inaceitável.

11. Medidas da Empresa ao detectar risco

Se a Empresa detectar atividade suspeita, risco AML/KYC, risco de sanções, violação desta Política ou recusa do usuário em cooperar, a Empresa poderá:

- solicitar informações adicionais;
- solicitar KYC ou EDD;
- reduzir limites;
- atrasar uma operação;
- recusar uma operação;
- cancelar uma transação P2P;
- restringir funções P2P;
- congelar ou reservar ativos;
- restringir retiradas;
- bloquear temporariamente a conta;
- encerrar a conta;
- devolver fundos ao remetente, quando possível, permitido e não proibido por lei;
- reter comissões aplicáveis, custos de rede ou custos de devolução quando previstos pelas regras da Plataforma;
- transmitir informações a autoridades competentes quando exigido ou permitido por lei;
- adotar outras medidas razoáveis para proteger a Plataforma, os usuários, os parceiros e a Empresa.

A Empresa não é obrigada a notificar o usuário previamente sobre a aplicação de tais medidas se a notificação puder violar a lei, requisitos AML/KYC/CTF, regras de sanções, interesses de investigação, segurança da Plataforma ou direitos de terceiros.

12. Devolução de fundos em caso de recusa AML/KYC

Se uma operação for rejeitada ou o serviço for restringido como resultado de revisão AML/KYC, a Empresa poderá, quando possível e permitido, devolver os ativos digitais ao endereço original do remetente ou a outro endereço que a Empresa considere aceitável sob a perspectiva de risco e legalidade.

A devolução pode ser impossível ou atrasada se:

- os fundos estiverem vinculados a um endereço sancionado;
- os fundos estiverem vinculados a atividade criminosa;
- tiver sido recebida solicitação de autoridade competente;
- a devolução puder violar a lei;
- o endereço original estiver indisponível, for de alto risco ou tecnicamente inadequado;
- for necessária revisão adicional;
- os fundos já estiverem reservados, congelados ou relacionados a uma disputa.

Do valor da devolução podem ser retidas comissões de rede, comissões de serviço, custos de processamento e outros custos aplicáveis, se previstos nos Termos de Uso, na página de comissões https://kashbi.io/information/fees, na interface da Plataforma ou em regras separadas.

O valor específico de qualquer comissão ou cobrança por tal devolução não é fixado nesta Política e pode ser determinado na página de comissões https://kashbi.io/information/fees, na interface da Plataforma ou em regras separadas, se tal cobrança se aplicar.

13. Relatórios e interação com autoridades

A Empresa pode interagir com autoridades competentes, unidades de inteligência financeira, autoridades policiais, tribunais, reguladores, bancos, provedores de pagamento e outras pessoas autorizadas quando exigido ou permitido por lei.

A Empresa pode transmitir informações sobre usuário, conta, transação, transação P2P, disputa, endereço, dados de pagamento ou outras circunstâncias se:

- tiver sido recebida solicitação legal;
- houver obrigação de reportar atividade suspeita;
- for necessário cumprir requisitos de sanções;
- for necessário proteger os direitos da Empresa, dos usuários ou de terceiros;
- for necessário prevenir fraude, lavagem de dinheiro ou financiamento do terrorismo.

A Empresa não é obrigada a notificar o usuário sobre tal transmissão se a notificação for proibida por lei, puder prejudicar uma investigação, revelar procedimentos internos AML ou criar risco de segurança.

14. Retenção de dados e registros

A Empresa retém dados e registros relacionados a AML/KYC, transações, transações P2P, revisões, disputas, restrições e relatórios pelo período previsto pela legislação aplicável, pelos requisitos de parceiros, pelas regras internas de gestão de riscos e pela Política de Privacidade.

Tais dados podem incluir:

- dados KYC;
- documentos do usuário;
- resultados de verificações;

- correspondências com sanções e PEP;
- perfil de risco;
- histórico de operações;
- endereços blockchain;
- txid/hash de transações;
- dados de transações P2P;
- comprovantes de pagamento;
- materiais de disputas;
- correspondência com o suporte;
- decisões internas sobre restrições;
- registros de solicitações de autoridades competentes.

A exclusão de uma conta, a retirada de consentimento ou a cessação do uso da Plataforma nem sempre implica exclusão imediata dos dados AML/KYC quando sua retenção for exigida ou permitida por lei, regras AML/KYC/CTF, proteção dos direitos da Empresa, resolução de disputas ou cumprimento de solicitações de autoridades competentes.

15. Terceiros e prestadores de serviços

A Empresa pode contratar terceiros para executar procedimentos AML/KYC, incluindo:

- fornecedores de verificação de documentos;
- fornecedores de prova de vida;
- fornecedores de screening de sanções;
- fornecedores de screening PEP/adverse media;
- fornecedores de análise blockchain;
- parceiros de pagamento;
- bancos, processadores e provedores de câmbio;
- consultores jurídicos, de compliance e auditoria;
- fornecedores de infraestrutura e segurança.

Os provedores podem ser indicados por categorias sem nomes específicos, salvo se exigido de outra forma por lei, contrato com o provedor ou política separada da Empresa.

A Empresa pode verificar parceiros e provedores quanto a sanções, reputação, licenças, autorizações, riscos e capacidade de cumprir requisitos de segurança e confidencialidade.

16. Obrigações do usuário

O usuário compromete-se a:

- não utilizar a Plataforma para atividade proibida;
- fornecer informações verdadeiras;
- responder tempestivamente às solicitações da Empresa;
- fornecer documentos e explicações quando solicitados;

- utilizar apenas fundos que lhe pertençam legalmente;
- não utilizar cartões bancários, contas, carteiras ou dados de pagamento de terceiros sem base legal;
- não fornecer documentos, recibos, capturas de tela ou comprovantes falsificados;
- não contornar limites, verificações, restrições de sanções ou regras da Plataforma;
- não criar múltiplas contas para contornar restrições;
- cumprir a legislação aplicável;
- avaliar de forma independente a legalidade de suas operações em seu país de residência.

A recusa em cooperar, a evasão de verificação, o fornecimento de informações falsas ou a tentativa de contornar controles AML/KYC pode resultar em restrição ou encerramento do serviço.

17. Confidencialidade dos procedimentos AML/KYC

O usuário entende que a Empresa não divulga:

- critérios exatos de risco;
- red flags internas;
- limites de monitoramento;
- algoritmos de scoring;
- fontes de dados AML;
- detalhes de investigações;
- razões para apresentar relatório a autoridades competentes;
- detalhes de decisões internas;
- informações cuja divulgação possa violar a lei, a segurança ou a eficácia dos controles AML/KYC.

18. Alterações à Política

A Empresa pode alterar esta Política a qualquer momento. A versão vigente é publicada no site https://kashbi.io ou na interface da Plataforma.

O uso continuado da Plataforma após a publicação de uma versão atualizada significa o consentimento do usuário com a nova versão da Política, salvo disposição em contrário da legislação aplicável.

19. Versões linguísticas

A presente Política pode ser publicada em russo, cazaque, inglês e outros idiomas.

Se a legislação aplicável exigir prioridade de uma determinada versão linguística, essa versão será aplicada. Nos demais casos, em caso de divergências entre versões linguísticas, prevalecerá a versão russa.

20. Contatos

Para questões relacionadas à presente Política, o usuário pode entrar em contato:

- Empresa: F-Tech
- País de registro: Kazakhstan
- Site: https://kashbi.io
- Aplicativo: KashBi
- Email: legal@kashbi.io
- Telegram: kashbi_support
- Endereço legal: 44/1 Al-Farabi Avenue, Apartment 207