AML/KYC Policy

This AML/KYC Policy (the “Policy”) describes the approach of F-Tech, registered in Kazakhstan (the “Company”, “we”, “us”, “our”), to preventing money laundering, terrorist financing, sanctions evasion, fraud, and other illegal or prohibited activities when using the website https://kashbi.io, the KashBi application, the Telegram bot, Telegram Mini App, web version, API, crypto-fiat wallet, P2P platform, and other related services of the Company, collectively referred to as the “Platform”.

This Policy forms part of the Terms of Use and applies together with the Privacy Policy, P2P transaction rules, fee rules, risk warnings, and other documents of the Company.

By using the Platform, creating an account, funding a balance, withdrawing digital assets, creating or accepting a P2P transaction, undergoing verification, or otherwise interacting with the Platform, the user confirms that they have read this Policy and agree to comply with its provisions.

If the user does not agree with this Policy, they must stop using the Platform.

1. Purpose and Scope

1.1. Purpose of the Policy

The purpose of this Policy is to establish the key principles, rules, and measures aimed at:

- preventing the use of the Platform for money laundering;
- preventing terrorist financing;
- preventing sanctions evasion;
- preventing fraud, scams, phishing, and other unlawful activities;
- identifying and assessing high-risk users, transactions, addresses, and jurisdictions;
- monitoring transactions involving digital assets and P2P transactions;
- complying with applicable legal requirements, partner requirements, AML/KYC service provider requirements, bank requirements, payment provider requirements, and requirements of competent authorities;
- protecting users, the Company, the Platform, and the Company’s business reputation.

1.2. Scope of Application

This Policy applies to all users of the Platform, including users of:

- the crypto-fiat wallet;
- the P2P platform;
- Telegram Mini App;
- Telegram bot;
- the web version;
- digital asset deposit and withdrawal functions;
- internal transfers;

- fiat operations outside P2P, where such functions are available;
- support services and dispute resolution.

1.3. Risk-Based Approach

The Company applies a risk-based approach. This means that KYC, AML checks, limits, document requests, enhanced due diligence, monitoring, restrictions, and other measures are applied in proportion to the risk level of the user, transaction, jurisdiction, payment method, digital asset, blockchain address, user behavior, and other factors.

The Platform is positioned as privacy-first: the Company seeks to minimize the collection of personal data and not to request identity documents unnecessarily. At the same time, privacy-first does not mean full anonymity and does not exclude data processing, user verification, transaction screening, transaction restrictions, or disclosure of information to competent authorities where this is required or permitted by law, the Platform rules, partner requirements, or this Policy.

2. Terms and Definitions

2.1. AML

AML means measures for combating money laundering, including the detection, prevention, investigation, and restriction of transactions related to funds of unlawful origin.

2.2. KYC

KYC means the “Know Your Customer” procedure, including the identification, verification, and assessment of a user where such procedure is required in view of risk, limits, a transaction, applicable law, or partner requirements.

2.3. CDD

CDD means customer due diligence, including the collection and analysis of information about a user, their activity, source of funds, purpose of transactions, and risk profile.

2.4. EDD

EDD means enhanced due diligence applied to users, transactions, or situations presenting elevated risk. EDD may include requests for additional documents, confirmation of source of funds, extended transaction analysis, open-source checks, sanctions and PEP screening, and approval of continued servicing at the level of the responsible persons of the Company.

2.5. KYT

KYT means the “Know Your Transaction” procedure, including the analysis of transactions, blockchain addresses, sources of funds, user behavior, related wallets, P2P patterns, and other data relating to a particular transaction.

2.6. PEP

PEP means a politically exposed person, as well as members of their family and persons closely associated with such person, where such persons require enhanced attention from the perspective of corruption, sanctions, reputational, or other risks.

2.7. Sanctions

Sanctions mean economic, financial, trade, personal, territorial, or other restrictive measures imposed by states, international organizations, competent authorities, or applicable through the Company's partners.

2.8. Prohibited Jurisdiction

A prohibited jurisdiction means a country, territory, or region in relation to which the Company restricts or prohibits service due to law, sanctions, high AML risk, partner requirements, internal risk management rules, or other circumstances.

The list of prohibited jurisdictions is not necessarily published in this Policy and may be determined in the Platform interface, the Company's internal rules, partner documents, or separate notices.

2.9. Suspicious Activity

Suspicious activity means a transaction, behavior, source of funds, P2P transaction, address, payment method, account, or other factor that may indicate money laundering, terrorist financing, sanctions evasion, fraud, scam, use of another person's data, multi-accounting, unlawful activity, or any other unacceptable risk.

2.10. Red Flags

Red flags mean signs or indicators that may indicate elevated risk or the need for additional review.

3. Organization of AML/KYC Controls

3.1. Responsible Persons

The Company may appoint a responsible person or team responsible for implementing AML/KYC procedures, risk management, transaction monitoring, review of suspicious activity, interaction with competent authorities, and maintenance of internal rules.

3.2. Internal Rules

The Company develops and applies internal rules, instructions, risk criteria, red flags, verification procedures, limits, monitoring scenarios, and decision-making rules.

Such internal documents constitute confidential information of the Company and are not subject to disclosure to users if such disclosure may impair the effectiveness of controls, Platform security, compliance with law, rights of third parties, or the interests of an investigation.

3.3. Updating Procedures

The Company may update AML/KYC procedures taking into account:

- changes in legislation;
- new products and functions;
- new fraud schemes;
- FATF recommendations and other international standards;
- partner requirements;

- results of internal reviews;
- security incidents;
- changes in sanctions regimes;
- new typologies of money laundering and terrorist financing.

4. Risk Assessment

4.1. General Risk Assessment

The Company may conduct regular assessment of AML/KYC risks related to the Platform, users, products, digital assets, jurisdictions, access channels, P2P transactions, payment methods, fiat operations outside P2P, blockchain networks, and service providers.

4.2. Risk Factors

When assessing risk, the Company may consider:

- the user’s country of residence, citizenship, location, or IP-based geography;
- account type and registration method;
- transaction history;
- transaction amounts and frequency;
- digital assets and networks used;
- blockchain addresses of senders and recipients;
- links between addresses and mixers, darknet markets, hacks, ransomware, scam projects, sanctioned addresses, or other high-risk sources;
- use of P2P transactions;
- selected fiat payment methods;
- behavior in disputes;
- complaints from other users;
- multi-accounting or links to previously blocked accounts;
- use of VPNs, proxies, or other means of concealing location;
- refusal to provide information;
- inconsistency of data;
- PEP status;
- sanctions matches;
- adverse media and other reputational factors;
- requirements of partners and competent authorities.

4.3. Risk Categories

The Company may assign internal risk categories to users, transactions, addresses, or deals, such as low, medium, high, or unacceptable risk.

The risk category may affect:

- available functions;
- limits;

- the need for KYC;
- the need for EDD;
- transaction processing speed;
- withdrawal availability;
- access to P2P;
- the need for manual review;
- the likelihood of freezing or refusal of service.

The Company is not obliged to disclose to the user the internal risk category, calculation methodology, exact criteria, or scoring results.

5. KYC/CDD: User Verification

5.1. General Approach

The Company does not require full KYC verification from all users by default, unless otherwise provided by law, the interface, partner requirements, or a specific function. Verification is applied on a risk-based basis.

5.2. When KYC May Be Required

The Company may request KYC or additional information in the following cases:

- reaching limits;
- a large transaction;
- an unusual transaction;
- suspicious activity;
- opening a dispute;
- a withdrawal request;
- an AML match relating to an address or transaction;
- a link to a high-risk jurisdiction;
- use of a fiat function outside P2P;
- a requirement of a payment partner, bank, exchange provider, or AML/KYC provider;
- a request from a competent authority;
- account access recovery;
- suspicion of multi-accounting, fraud, or use of another person's data;
- other circumstances requiring verification.

5.3. What Data May Be Requested

Depending on the risk level, the Company may request:

- first name, last name, patronymic, or other full name;
- date of birth;
- citizenship;
- country of residence;
- residential address;

- email;
- phone number;
- identity document;
- photograph, selfie, video verification, or liveness check;
- proof of address;
- proof of source of funds;
- proof of source of wealth;
- confirmation of the purpose of a transaction;
- statement, receipt, payment slip, or proof of payment;
- documents relating to a P2P transaction;
- information about a connection with a PEP;
- other documents or explanations necessary to assess risk.

5.4. Verification of Data

The Company may verify the data provided:

- manually;
- using automated systems;
- through external AML/KYC providers;
- through sanctions and PEP lists;
- through open sources;
- through blockchain analytics;
- through information received from partners, users, banks, payment providers, or competent authorities.

5.5. User’s Duty to Cooperate

The user must provide requested information and documents in a timely, accurate, and complete manner.

If the user refuses to provide data, provides false or inconsistent information, fails to respond to requests, or attempts to circumvent verification, the Company may restrict functions, suspend transactions, freeze assets, cancel transactions, refuse service, or close the account.

5.6. Re-Verification

The Company may request documents or information again, even if the user has previously passed verification, if:

- the user’s data has changed;
- the identity document has expired;
- the user’s activity has changed;
- new risks have arisen;
- the user has reached new limits;
- a new function has become available;
- legal or partner requirements have changed;

- a dispute or suspicious activity has arisen.

6. Enhanced Due Diligence (EDD)

6.1. When EDD Applies

The Company may apply EDD if a user, transaction, address, P2P transaction, jurisdiction, or behavior presents elevated risk.

EDD may apply, in particular, if:

- the user is a PEP or is connected with a PEP;
- the user is connected with a high-risk jurisdiction;
- the transaction is large, complex, unusual, or economically inexplicable;
- funds are received from a high-risk blockchain address;
- the transaction is associated with mixers, darknet markets, hacks, ransomware, scams, sanctioned addresses, or other red flags;
- the user frequently opens or loses disputes;
- there are signs of multi-accounting;
- there are signs of using another person’s payment details or account;
- the user cannot explain the source of funds;
- the user gives inconsistent answers;
- confirmation is required at the request of a partner or competent authority.

6.2. EDD Measures

EDD may include:

- requests for additional documents;
- confirmation of source of funds;
- confirmation of source of wealth;
- confirmation of the purpose of a transaction;
- open-source checks;
- adverse media checks;
- in-depth analysis of blockchain history;
- reduction of limits;
- temporary freezing of funds;
- manual approval of a transaction;
- refusal of a transaction;
- termination of service.

6.3. EDD Outcomes

As a result of EDD, the Company may:

- permit the transaction;
- permit the transaction with limits or conditions;
- request additional information;

- refuse the transaction;
- return funds, where permitted and possible;
- freeze funds;
- restrict the account;
- close the account;
- disclose information to competent authorities where required or permitted by law.

7. KYT and Transaction Monitoring

7.1. General Monitoring

The Company may conduct continuous or selective monitoring of user operations, including:

- digital asset deposits;
- digital asset withdrawals;
- internal transfers;
- P2P transactions;
- fiat operations outside P2P, where such functions are available;
- attempted transactions;
- cancelled transactions;
- operations related to disputes or complaints.

7.2. Blockchain Analytics

The Company may use blockchain analytics to assess the risk of addresses, transactions, address clusters, sources of funds, and related entities.

The review may take into account links to:

- sanctioned addresses;
- darknet markets;
- mixers and obfuscation services;
- ransomware;
- hacks and stolen funds;
- scam projects;
- fraudulent schemes;
- illegal services;
- high-risk exchanges or exchangers;
- other sources of elevated risk.

7.3. P2P Monitoring

In P2P transactions, the Company may analyze:

- frequency of transactions;
- transaction amounts;
- behavior of the parties;

- number of cancellations;
- number of disputes;
- complaints;
- proof of payment;
- matching payment details;
- account links;
- signs of multi-accounting;
- inconsistencies in payment data;
- attempts to move a transaction outside the Platform rules;
- use of third-party bank accounts, cards, or payment details.

7.4. Limits and Delays

The Company may set limits, delays, manual reviews, or additional requirements for individual users, transactions, deals, addresses, assets, payment methods, or jurisdictions.

A transaction may be delayed or suspended until the review is completed.

8. Red Flags: Signs of Suspicious Activity

Red flags may include, in particular:

- refusal by the user to provide data or documents;
- provision of forged, altered, or inconsistent documents;
- use of another person's data, cards, accounts, or wallets;
- an attempt to use multiple accounts;
- frequent cancellation of P2P transactions;
- frequent disputes in P2P transactions;
- forged receipts, payment slips, or payment screenshots;
- mismatch between the payer's name and the user;
- rapid deposit and withdrawal of funds without an apparent economic purpose;
- structuring transactions into multiple smaller amounts;
- transactions inconsistent with the user's usual behavior;
- use of high-risk blockchain addresses;
- links to mixers, darknet markets, hacks, ransomware, scams, or sanctioned addresses;
- sharp increase in turnover;
- attempts to circumvent limits;
- use of VPNs, proxies, or other means of concealing location to circumvent restrictions;
- aggressive pressure on a counterparty or support;
- refusal to explain the source of funds;
- attempt to move a transaction outside the Platform;
- complaints from other users;
- negative information from open sources;

- matches with sanctions, PEP, or adverse media sources.

The presence of one red flag does not always mean a violation, but it may serve as a basis for additional review, restriction of a transaction, or other measures.

9. Sanctions and Prohibited Relationships

The Company does not establish or continue relationships with users where this is prohibited by law, sanctions, partner requirements, or internal risk management rules.

The Company may refuse service, restrict an account, freeze assets, or terminate the relationship if the user:

- is included in a sanctions list;
- is connected with a person included in a sanctions list;
- is located in a prohibited jurisdiction;
- acts in the interests of a prohibited person;
- uses the Platform to evade sanctions;
- refuses to provide information necessary for sanctions screening.

The Company may conduct sanctions screening at registration, before a transaction, after a transaction, upon changes to sanctions lists, when a dispute is opened, upon withdrawal of funds, or in other cases.

10. Prohibited Activity

The user is prohibited from using the Platform for:

- money laundering;
- terrorist financing;
- sanctions evasion;
- fraud, scams, phishing, or social engineering;
- trading in stolen funds, accounts, cards, documents, or personal data;
- use of another person’s bank cards, accounts, wallets, or payment details without lawful grounds;
- illegal trafficking in drugs, weapons, hazardous substances, or other prohibited goods;
- illegal gambling;
- illegal financial services;
- darknet activity;
- financing extremist, terrorist, or other prohibited activities;
- infringement of third-party rights;
- use of forged documents, receipts, payment slips, or screenshots;
- multi-accounting and circumvention of restrictions;
- any other activity that the Company considers illegal, high-risk, or unacceptable.

11. Measures Taken by the Company Upon Detection of Risk

If the Company detects suspicious activity, AML/KYC risk, sanctions risk, a breach of this Policy, or a user's refusal to cooperate, the Company may:

- request additional information;
- request KYC or EDD;
- reduce limits;
- delay a transaction;
- refuse a transaction;
- cancel a P2P transaction;
- restrict P2P functions;
- freeze or reserve assets;
- restrict withdrawals;
- temporarily block the account;
- close the account;
- return funds to the sender, where possible, permitted, and not prohibited by law;
- withhold applicable fees, network costs, or return processing costs where provided by the Platform rules;
- disclose information to competent authorities where required or permitted by law;
- take other reasonable measures to protect the Platform, users, partners, and the Company.

The Company is not obliged to notify the user in advance of such measures if the notification may violate law, AML/KYC/CTF requirements, sanctions rules, the interests of an investigation, Platform security, or rights of third parties.

12. Return of Funds Upon AML/KYC Refusal

If a transaction is rejected or service is restricted as a result of an AML/KYC review, the Company may, where possible and permitted, return digital assets to the original sender address or to another address that the Company considers acceptable from a risk and legal perspective.

A return may be impossible or delayed if:

- the funds are linked to a sanctioned address;
- the funds are linked to criminal activity;
- a request has been received from a competent authority;
- the return may violate law;
- the original address is unavailable, high-risk, or technically unsuitable;
- additional review is required;
- the funds are already reserved, frozen, or related to a dispute.

Network fees, service fees, processing costs, and other applicable costs may be withheld from the return amount where provided by the Terms of Use, the fees page https://kashbi.io/information/fees, the Platform interface, or separate rules.

The specific amount of any fee or charge for such return is not fixed in this Policy and may be determined by the fees page https://kashbi.io/information/fees, the Platform interface, or separate rules, if such fee applies.

13. Reporting and Interaction with Authorities

The Company may interact with competent authorities, financial intelligence units, law enforcement authorities, courts, regulators, banks, payment providers, and other authorized persons where required or permitted by law.

The Company may disclose information about a user, account, transaction, P2P transaction, dispute, address, payment data, or other circumstances if:

- a lawful request has been received;
- there is an obligation to report suspicious activity;
- sanctions requirements must be complied with;
- it is necessary to protect the rights of the Company, users, or third parties;
- it is required to prevent fraud, money laundering, or terrorist financing.

The Company is not obliged to notify the user of such disclosure if notification is prohibited by law, may interfere with an investigation, reveal internal AML procedures, or create a security risk.

14. Retention of Data and Records

The Company retains data and records related to AML/KYC, transactions, P2P transactions, reviews, disputes, restrictions, and reporting for the period provided by applicable law, partner requirements, internal risk management rules, and the Privacy Policy.

Such data may include:

- KYC data;
- user documents;
- verification results;
- sanctions and PEP matches;
- risk profile;
- transaction history;
- blockchain addresses;
- transaction txid/hash;
- P2P transaction data;
- proof of payment;
- dispute materials;
- correspondence with support;
- internal decisions on restrictions;
- records of requests from competent authorities.

Deletion of an account, withdrawal of consent, or termination of use of the Platform does not always mean immediate deletion of AML/KYC data where its retention is required or permitted by law, AML/KYC/CTF rules, protection of the Company's rights, dispute resolution, or compliance with requests from competent authorities.

15. Third Parties and Service Providers

The Company may engage third parties to perform AML/KYC procedures, including:

- document verification providers;
- liveness check providers;
- sanctions screening providers;
- PEP/adverse media screening providers;
- blockchain analytics providers;
- payment partners;
- banks, processors, and exchange providers;
- legal, compliance, and audit advisers;
- infrastructure and security providers.

Providers may be described by category without specific names, unless otherwise required by law, an agreement with a provider, or a separate policy of the Company.

The Company may screen partners and providers for sanctions, reputation, licenses, authorizations, risks, and ability to comply with security and confidentiality requirements.

16. User Obligations

The user undertakes to:

- not use the Platform for prohibited activity;
- provide accurate information;
- respond to the Company's requests in a timely manner;
- provide documents and explanations where requested;
- use only funds lawfully belonging to the user;
- not use another person's bank cards, accounts, wallets, or payment details without lawful grounds;
- not provide forged documents, receipts, screenshots, or payment slips;
- not circumvent limits, checks, sanctions restrictions, or Platform rules;
- not create multiple accounts to circumvent restrictions;
- comply with applicable law;
- independently assess the legality of their transactions in their country of residence.

Refusal to cooperate, evasion of verification, provision of false information, or an attempt to circumvent AML/KYC controls may result in restriction or termination of service.

17. Confidentiality of AML/KYC Procedures

The user understands that the Company does not disclose:

- exact risk criteria;
- internal red flags;
- monitoring thresholds;
- scoring algorithms;
- sources of AML data;
- details of investigations;
- reasons for filing a report with competent authorities;
- details of internal decisions;
- information whose disclosure may violate law, security, or the effectiveness of AML/KYC controls.

18. Changes to the Policy

The Company may amend this Policy at any time. The current version is published on the website https://kashbi.io or in the Platform interface.

Continued use of the Platform after publication of an updated version constitutes the user’s consent to the new version of the Policy, unless otherwise provided by applicable law.

19. Language Versions

This Policy may be published in other languages.

If applicable law requires priority of a particular language version, that version shall apply. In all other cases, in the event of discrepancies between language versions, the Russian version shall prevail.

20. Contacts

For questions regarding this Policy, the user may contact:

- Company: F-Tech
- Country of registration: Kazakhstan
- Website: https://kashbi.io
- Application: KashBi
- Email: legal@kashbi.io
- Telegram: kashbi_support
- Legal address: 44/1 Al-Farabi Avenue, Apartment 207