

Kebijakan AML/KYC

Kebijakan AML/KYC ini (“Kebijakan”) menjelaskan pendekatan F-Tech, yang terdaftar di Kazakhstan (“Perusahaan”, “kami”, “kita”, “milik kami”), dalam mencegah pencucian uang, pendanaan terorisme, penghindaran sanksi, penipuan, dan aktivitas ilegal atau terlarang lainnya saat menggunakan situs web <https://kashbi.io>, aplikasi KashBi, bot Telegram, Telegram Mini App, versi web, API, dompet kripto-fiat, platform P2P, dan layanan terkait lainnya milik Perusahaan, yang secara bersama-sama disebut sebagai “Platform”.

Kebijakan ini merupakan bagian dari Syarat Penggunaan dan berlaku bersama dengan Kebijakan Privasi, aturan transaksi P2P, aturan biaya, peringatan risiko, dan dokumen Perusahaan lainnya.

Dengan menggunakan Platform, membuat akun, mengisi saldo, menarik aset digital, membuat atau menerima transaksi P2P, menjalani verifikasi, atau berinteraksi dengan Platform dengan cara lain, pengguna menyatakan bahwa ia telah membaca Kebijakan ini dan setuju untuk mematuhi ketentuannya.

Jika pengguna tidak setuju dengan Kebijakan ini, pengguna harus berhenti menggunakan Platform.

1. Tujuan dan Ruang Lingkup

1.1. Tujuan Kebijakan

Tujuan Kebijakan ini adalah untuk menetapkan prinsip, aturan, dan langkah-langkah utama yang ditujukan untuk:

- mencegah penggunaan Platform untuk pencucian uang;
- mencegah pendanaan terorisme;
- mencegah penghindaran sanksi;
- mencegah penipuan, scam, phishing, dan aktivitas melanggar hukum lainnya;
- mengidentifikasi dan menilai pengguna, operasi, alamat, dan yurisdiksi berisiko tinggi;
- memantau operasi dengan aset digital dan transaksi P2P;
- mematuhi persyaratan hukum yang berlaku, persyaratan mitra, penyedia layanan AML/KYC, bank, penyedia pembayaran, dan otoritas yang berwenang;
- melindungi pengguna, Perusahaan, Platform, dan reputasi bisnis Perusahaan.

1.2. Ruang Lingkup Penerapan

Kebijakan ini berlaku untuk semua pengguna Platform, termasuk pengguna:

- dompet kripto-fiat;
- platform P2P;
- Telegram Mini App;
- bot Telegram;
- versi web;

- fungsi deposit dan penarikan aset digital;
- transfer internal;
- operasi fiat di luar P2P, jika fungsi tersebut tersedia;
- layanan dukungan dan penyelesaian sengketa.

1.3. Pendekatan Berbasis Risiko

Perusahaan menerapkan pendekatan berbasis risiko. Ini berarti bahwa KYC, pemeriksaan AML, limit, permintaan dokumen, enhanced due diligence, pemantauan, pembatasan, dan langkah-langkah lain diterapkan secara proporsional dengan tingkat risiko pengguna, operasi, yurisdiksi, metode pembayaran, aset digital, alamat blockchain, perilaku pengguna, dan faktor lainnya.

Platform diposisikan sebagai privacy-first: Perusahaan berupaya meminimalkan pengumpulan data pribadi dan tidak meminta dokumen identitas tanpa kebutuhan. Pada saat yang sama, privacy-first tidak berarti anonimitas penuh dan tidak mengecualikan pemrosesan data, verifikasi pengguna, pemeriksaan transaksi, pembatasan operasi, atau penyampaian informasi kepada otoritas yang berwenang apabila diwajibkan atau diizinkan oleh hukum, aturan Platform, persyaratan mitra, atau Kebijakan ini.

2. Istilah dan Definisi

2.1. AML

AML berarti langkah-langkah untuk memberantas pencucian uang, termasuk deteksi, pencegahan, investigasi, dan pembatasan operasi yang terkait dengan dana yang berasal dari sumber ilegal.

2.2. KYC

KYC berarti prosedur “Know Your Customer” atau “kenali pelanggan Anda”, yang mencakup identifikasi, verifikasi, dan penilaian pengguna jika prosedur tersebut diperlukan dengan mempertimbangkan risiko, limit, operasi, hukum yang berlaku, atau persyaratan mitra.

2.3. CDD

CDD berarti customer due diligence atau uji tuntas pelanggan, yang mencakup pengumpulan dan analisis informasi mengenai pengguna, aktivitasnya, sumber dana, tujuan operasi, dan profil risiko.

2.4. EDD

EDD berarti enhanced due diligence atau uji tuntas yang ditingkatkan yang diterapkan kepada pengguna, operasi, atau situasi dengan risiko lebih tinggi. EDD dapat mencakup permintaan dokumen tambahan, konfirmasi sumber dana, analisis transaksi yang diperluas, pemeriksaan sumber terbuka, pemeriksaan sanksi dan PEP, serta persetujuan atas kelanjutan layanan oleh pihak yang bertanggung jawab di Perusahaan.

2.5. KYT

KYT berarti prosedur “Know Your Transaction” atau “kenali transaksi Anda”, yang mencakup analisis operasi, alamat blockchain, sumber dana, perilaku pengguna, dompet terkait, pola P2P, dan data lain yang berkaitan dengan operasi tertentu.

2.6. PEP

PEP berarti politically exposed person atau orang yang memiliki kedudukan politik penting, serta anggota keluarganya dan orang yang memiliki hubungan dekat dengan orang tersebut, jika orang-orang tersebut memerlukan perhatian lebih tinggi dari perspektif risiko korupsi, sanksi, reputasi, atau risiko lainnya.

2.7. Sanksi

Sanksi berarti tindakan pembatasan ekonomi, keuangan, perdagangan, personal, teritorial, atau pembatasan lainnya yang ditetapkan oleh negara, organisasi internasional, otoritas yang berwenang, atau yang berlaku melalui mitra Perusahaan.

2.8. Yurisdiksi Terlarang

Yurisdiksi terlarang berarti negara, wilayah, atau kawasan tempat Perusahaan membatasi atau melarang layanan karena hukum, sanksi, risiko AML yang tinggi, persyaratan mitra, aturan internal manajemen risiko, atau keadaan lain.

Daftar yurisdiksi terlarang tidak harus dipublikasikan dalam Kebijakan ini dan dapat ditentukan dalam antarmuka Platform, aturan internal Perusahaan, dokumen mitra, atau pemberitahuan terpisah.

2.9. Aktivitas Mencurigakan

Aktivitas mencurigakan berarti operasi, perilaku, sumber dana, transaksi P2P, alamat, metode pembayaran, akun, atau faktor lain yang dapat mengindikasikan pencucian uang, pendanaan terorisme, penghindaran sanksi, penipuan, scam, penggunaan data orang lain, multi-accounting, aktivitas ilegal, atau risiko lain yang tidak dapat diterima.

2.10. Red flags / tanda peringatan

Red flags berarti tanda atau indikator yang dapat menunjukkan risiko yang meningkat atau perlunya pemeriksaan tambahan.

3. Organisasi Kontrol AML/KYC

3.1. Pihak yang Bertanggung Jawab

Perusahaan dapat menunjuk orang yang bertanggung jawab atau tim yang bertanggung jawab atas pelaksanaan prosedur AML/KYC, manajemen risiko, pemantauan transaksi, peninjauan aktivitas mencurigakan, interaksi dengan otoritas yang berwenang, dan pemeliharaan aturan internal.

3.2. Aturan Internal

Perusahaan menyusun dan menerapkan aturan internal, instruksi, kriteria risiko, red flags, prosedur verifikasi, limit, skenario pemantauan, dan aturan pengambilan keputusan.

Dokumen internal tersebut merupakan informasi rahasia Perusahaan dan tidak wajib diungkapkan kepada pengguna jika pengungkapan tersebut dapat merusak efektivitas kontrol, keamanan Platform, kepatuhan terhadap hukum, hak pihak ketiga, atau kepentingan investigasi.

3.3. Pembaruan Prosedur

Perusahaan dapat memperbarui prosedur AML/KYC dengan mempertimbangkan:

- perubahan peraturan perundang-undangan;
- produk dan fungsi baru;
- skema penipuan baru;
- rekomendasi FATF dan standar internasional lainnya;
- persyaratan mitra;
- hasil pemeriksaan internal;
- insiden keamanan;
- perubahan rezim sanksi;
- tipologi baru pencucian uang dan pendanaan terorisme.

4. Penilaian Risiko

4.1. Penilaian Risiko Umum

Perusahaan dapat melakukan penilaian berkala atas risiko AML/KYC yang terkait dengan Platform, pengguna, produk, aset digital, yurisdiksi, kanal akses, transaksi P2P, metode pembayaran, operasi fiat di luar P2P, jaringan blockchain, dan penyedia layanan.

4.2. Faktor Risiko

Dalam menilai risiko, Perusahaan dapat mempertimbangkan:

- negara tempat tinggal, kewarganegaraan, lokasi, atau geografi berbasis IP pengguna;
- jenis akun dan metode pendaftaran;
- riwayat operasi;
- jumlah dan frekuensi operasi;
- aset digital dan jaringan yang digunakan;
- alamat blockchain pengirim dan penerima;
- hubungan alamat dengan mixer, pasar darknet, peretasan, ransomware, proyek scam, alamat yang terkena sanksi, atau sumber berisiko tinggi lainnya;
- penggunaan transaksi P2P;
- metode pembayaran fiat yang dipilih;
- perilaku dalam sengketa;
- keluhan dari pengguna lain;
- multi-accounting atau hubungan dengan akun yang sebelumnya diblokir;
- penggunaan VPN, proxy, atau sarana lain untuk menyembunyikan lokasi;
- penolakan untuk memberikan informasi;
- ketidakkonsistenan data;
- status PEP;
- kecocokan dengan daftar sanksi;
- adverse media dan faktor reputasi lainnya;
- persyaratan mitra dan otoritas yang berwenang.

4.3. Kategori Risiko

Perusahaan dapat menetapkan kategori risiko internal kepada pengguna, operasi, alamat, atau transaksi, misalnya risiko rendah, sedang, tinggi, atau tidak dapat diterima.

Kategori risiko dapat memengaruhi:

- fungsi yang tersedia;
- limit;
- kebutuhan KYC;
- kebutuhan EDD;
- kecepatan pemrosesan operasi;
- ketersediaan penarikan;
- akses ke P2P;
- kebutuhan pemeriksaan manual;
- kemungkinan pembekuan atau penolakan layanan.

Perusahaan tidak berkewajiban untuk mengungkapkan kepada pengguna kategori risiko internal, metodologi perhitungan, kriteria tepat, atau hasil scoring.

5. KYC/CDD: Verifikasi Pengguna

5.1. Pendekatan Umum

Perusahaan tidak mewajibkan verifikasi KYC penuh bagi semua pengguna secara default, kecuali ditentukan lain oleh hukum, antarmuka, persyaratan mitra, atau fungsi tertentu. Verifikasi diterapkan berdasarkan risiko.

5.2. Kapan KYC Dapat Diperlukan

Perusahaan dapat meminta KYC atau informasi tambahan dalam hal berikut:

- tercapainya limit;
- operasi bernilai besar;
- operasi yang tidak biasa;
- aktivitas mencurigakan;
- pembukaan sengketa;
- permintaan penarikan;
- kecocokan AML terkait alamat atau transaksi;
- hubungan dengan yurisdiksi berisiko tinggi;
- penggunaan fungsi fiat di luar P2P;
- persyaratan dari mitra pembayaran, bank, penyedia pertukaran, atau penyedia AML/KYC;
- permintaan dari otoritas yang berwenang;
- pemulihan akses akun;
- dugaan multi-accounting, penipuan, atau penggunaan data orang lain;
- keadaan lain yang memerlukan verifikasi.

5.3. Data yang Dapat Diminta

Tergantung pada tingkat risiko, Perusahaan dapat meminta:

- nama depan, nama belakang, patronimik, atau nama lengkap lainnya;
- tanggal lahir;
- kewarganegaraan;
- negara tempat tinggal;
- alamat tempat tinggal;
- email;
- nomor telepon;
- dokumen identitas;
- foto, selfie, verifikasi video, atau liveness check;
- bukti alamat;
- bukti sumber dana;
- bukti sumber kekayaan;
- konfirmasi tujuan operasi;
- rekening koran, tanda terima, bukti, atau konfirmasi pembayaran;
- dokumen terkait transaksi P2P;
- informasi tentang hubungan dengan PEP;
- dokumen atau penjelasan lain yang diperlukan untuk menilai risiko.

5.4. Verifikasi Data

Perusahaan dapat memverifikasi data yang diberikan:

- secara manual;
- menggunakan sistem otomatis;
- melalui penyedia AML/KYC eksternal;
- melalui daftar sanksi dan PEP;
- melalui sumber terbuka;
- melalui analitik blockchain;
- melalui informasi yang diterima dari mitra, pengguna, bank, penyedia pembayaran, atau otoritas yang berwenang.

5.5. Kewajiban Pengguna untuk Bekerja Sama

Pengguna wajib memberikan informasi dan dokumen yang diminta secara tepat waktu, akurat, dan lengkap.

Jika pengguna menolak memberikan data, memberikan informasi palsu atau tidak konsisten, tidak menanggapi permintaan, atau mencoba menghindari verifikasi, Perusahaan dapat membatasi fungsi, menangguhkan operasi, membekukan aset, membatalkan transaksi, menolak layanan, atau menutup akun.

5.6. Verifikasi Ulang

Perusahaan dapat meminta dokumen atau informasi kembali, meskipun pengguna sebelumnya telah melewati verifikasi, jika:

- data pengguna berubah;
- dokumen identitas kedaluwarsa;
- aktivitas pengguna berubah;
- muncul risiko baru;
- pengguna mencapai limit baru;
- fungsi baru tersedia;
- persyaratan hukum atau mitra berubah;
- timbul sengketa atau aktivitas mencurigakan.

6. Enhanced Due Diligence (EDD)

6.1. Kapan EDD Diterapkan

Perusahaan dapat menerapkan EDD jika pengguna, operasi, alamat, transaksi P2P, yurisdiksi, atau perilaku memiliki risiko yang lebih tinggi.

EDD dapat diterapkan, khususnya jika:

- pengguna merupakan PEP atau terkait dengan PEP;
- pengguna terkait dengan yurisdiksi berisiko tinggi;
- operasi bernilai besar, kompleks, tidak biasa, atau tidak dapat dijelaskan secara ekonomi;
- dana berasal dari alamat blockchain berisiko tinggi;
- operasi terkait dengan mixer, pasar darknet, peretasan, ransomware, scam, alamat yang terkena sanksi, atau red flags lainnya;
- pengguna sering membuka atau kalah dalam sengketa;
- terdapat tanda multi-accounting;
- terdapat tanda penggunaan detail pembayaran atau akun milik orang lain;
- pengguna tidak dapat menjelaskan sumber dana;
- pengguna memberikan jawaban yang saling bertentangan;
- diperlukan konfirmasi atas permintaan mitra atau otoritas yang berwenang.

6.2. Langkah-Langkah EDD

EDD dapat mencakup:

- permintaan dokumen tambahan;
- konfirmasi sumber dana;
- konfirmasi sumber kekayaan;
- konfirmasi tujuan operasi;
- pemeriksaan sumber terbuka;
- pemeriksaan adverse media;

- analisis mendalam atas riwayat blockchain;
- penurunan limit;
- pembekuan dana sementara;
- persetujuan manual atas operasi;
- penolakan operasi;
- penghentian layanan.

6.3. Hasil EDD

Sebagai hasil EDD, Perusahaan dapat:

- mengizinkan operasi;
- mengizinkan operasi dengan limit atau syarat;
- meminta informasi tambahan;
- menolak operasi;
- mengembalikan dana, jika diperbolehkan dan memungkinkan;
- membekukan dana;
- membatasi akun;
- menutup akun;
- menyampaikan informasi kepada otoritas yang berwenang jika diwajibkan atau diizinkan oleh hukum.

7. KYT dan Pemantauan Transaksi

7.1. Pemantauan Umum

Perusahaan dapat melakukan pemantauan berkelanjutan atau selektif terhadap operasi pengguna, termasuk:

- deposit aset digital;
- penarikan aset digital;
- transfer internal;
- transaksi P2P;
- operasi fiat di luar P2P, jika fungsi tersebut tersedia;
- percobaan operasi;
- operasi yang dibatalkan;
- operasi yang terkait dengan sengketa atau keluhan.

7.2. Analitik Blockchain

Perusahaan dapat menggunakan analitik blockchain untuk menilai risiko alamat, transaksi, kluster alamat, sumber dana, dan entitas terkait.

Pemeriksaan dapat mempertimbangkan hubungan dengan:

- alamat yang terkena sanksi;
- pasar darknet;
- mixer dan layanan obfuscation;

- ransomware;
- peretasan dan dana curian;
- proyek scam;
- skema penipuan;
- layanan ilegal;
- bursa atau penukar berisiko tinggi;
- sumber risiko tinggi lainnya.

7.3. Pemantauan P2P

Dalam transaksi P2P, Perusahaan dapat menganalisis:

- frekuensi transaksi;
- jumlah transaksi;
- perilaku para pihak;
- jumlah pembatalan;
- jumlah sengketa;
- keluhan;
- bukti pembayaran;
- kecocokan detail pembayaran;
- hubungan antar akun;
- tanda multi-accounting;
- ketidaksesuaian data pembayaran;
- upaya membawa transaksi keluar dari aturan Platform;
- penggunaan rekening bank, kartu, atau detail pembayaran milik orang lain.

7.4. Limit dan Penundaan

Perusahaan dapat menetapkan limit, penundaan, pemeriksaan manual, atau persyaratan tambahan untuk pengguna, operasi, transaksi, alamat, aset, metode pembayaran, atau yurisdiksi tertentu.

Suatu operasi dapat ditunda atau ditangguhkan sampai pemeriksaan selesai.

8. Red Flags: Tanda Aktivitas Mencurigakan

Red flags dapat mencakup, antara lain:

- penolakan pengguna untuk memberikan data atau dokumen;
- penyampaian dokumen palsu, diubah, atau tidak konsisten;
- penggunaan data, kartu, akun, atau dompet milik orang lain;
- upaya menggunakan beberapa akun;
- pembatalan transaksi P2P yang sering;
- sengketa P2P yang sering;
- tanda terima, bukti, atau tangkapan layar pembayaran palsu;
- ketidaksesuaian antara nama pembayar dan pengguna;

- deposit dan penarikan dana secara cepat tanpa tujuan ekonomi yang jelas;
- pemecahan operasi menjadi beberapa jumlah kecil;
- operasi yang tidak sesuai dengan perilaku biasa pengguna;
- penggunaan alamat blockchain berisiko tinggi;
- hubungan dengan mixer, pasar darknet, peretasan, ransomware, scam, atau alamat yang terkena sanksi;
- peningkatan volume operasi secara tiba-tiba;
- upaya menghindari limit;
- penggunaan VPN, proxy, atau sarana lain untuk menyembunyikan lokasi guna menghindari pembatasan;
- tekanan agresif terhadap pihak lawan atau dukungan;
- penolakan menjelaskan sumber dana;
- upaya membawa transaksi keluar dari Platform;
- keluhan dari pengguna lain;
- informasi negatif dari sumber terbuka;
- kecocokan dengan sumber sanksi, PEP, atau adverse media.

Keberadaan satu red flag tidak selalu berarti pelanggaran, tetapi dapat menjadi dasar untuk pemeriksaan tambahan, pembatasan operasi, atau langkah lainnya.

9. Sanksi dan Hubungan Terlarang

Perusahaan tidak menjalin atau melanjutkan hubungan dengan pengguna jika hal tersebut dilarang oleh hukum, sanksi, persyaratan mitra, atau aturan internal manajemen risiko.

Perusahaan dapat menolak layanan, membatasi akun, membekukan aset, atau mengakhiri hubungan jika pengguna:

- termasuk dalam daftar sanksi;
- terkait dengan orang yang termasuk dalam daftar sanksi;
- berada di yurisdiksi terlarang;
- bertindak untuk kepentingan orang yang dilarang;
- menggunakan Platform untuk menghindari sanksi;
- menolak memberikan informasi yang diperlukan untuk pemeriksaan sanksi.

Perusahaan dapat melakukan pemeriksaan sanksi saat pendaftaran, sebelum operasi, setelah operasi, saat daftar sanksi berubah, saat sengketa dibuka, saat penarikan dana, atau dalam kasus lain.

10. Aktivitas Terlarang

Pengguna dilarang menggunakan Platform untuk:

- pencucian uang;
- pendanaan terorisme;
- penghindaran sanksi;

- penipuan, scam, phishing, atau social engineering;
- perdagangan dana, akun, kartu, dokumen, atau data pribadi curian;
- penggunaan kartu bank, akun, dompet, atau detail pembayaran milik orang lain tanpa dasar hukum;
- peredaran ilegal narkoba, senjata, zat berbahaya, atau barang terlarang lainnya;
- perjudian ilegal;
- layanan keuangan ilegal;
- aktivitas darknet;
- pendanaan aktivitas ekstremis, teroris, atau aktivitas terlarang lainnya;
- pelanggaran hak pihak ketiga;
- penggunaan dokumen, tanda terima, bukti, atau tangkapan layar palsu;
- multi-accounting dan penghindaran pembatasan;
- aktivitas lain yang dianggap ilegal, berisiko tinggi, atau tidak dapat diterima oleh Perusahaan.

11. Langkah-Langkah Perusahaan Saat Risiko Terdeteksi

Jika Perusahaan mendeteksi aktivitas mencurigakan, risiko AML/KYC, risiko sanksi, pelanggaran Kebijakan ini, atau penolakan pengguna untuk bekerja sama, Perusahaan dapat:

- meminta informasi tambahan;
- meminta KYC atau EDD;
- menurunkan limit;
- menunda operasi;
- menolak operasi;
- membatalkan transaksi P2P;
- membatasi fungsi P2P;
- membekukan atau mencadangkan aset;
- membatasi penarikan;
- memblokir akun sementara;
- menutup akun;
- mengembalikan dana kepada pengirim, jika memungkinkan, diperbolehkan, dan tidak dilarang oleh hukum;
- menahan biaya yang berlaku, biaya jaringan, atau biaya pengembalian jika diatur oleh aturan Platform;
- menyampaikan informasi kepada otoritas yang berwenang jika diwajibkan atau diizinkan oleh hukum;
- mengambil langkah wajar lainnya untuk melindungi Platform, pengguna, mitra, dan Perusahaan.

Perusahaan tidak berkewajiban untuk memberi tahu pengguna terlebih dahulu mengenai penerapan langkah-langkah tersebut jika pemberitahuan dapat melanggar hukum, persyaratan AML/KYC/CTF, aturan sanksi, kepentingan investigasi, keamanan Platform,

atau hak pihak ketiga.

12. Pengembalian Dana dalam Hal Penolakan AML/KYC

Jika suatu operasi ditolak atau layanan dibatasi sebagai hasil pemeriksaan AML/KYC, Perusahaan dapat, jika memungkinkan dan diperbolehkan, mengembalikan aset digital ke alamat pengirim asal atau ke alamat lain yang dianggap dapat diterima oleh Perusahaan dari perspektif risiko dan hukum.

Pengembalian dapat tidak memungkinkan atau tertunda jika:

- dana terkait dengan alamat yang terkena sanksi;
- dana terkait dengan aktivitas kriminal;
- terdapat permintaan dari otoritas yang berwenang;
- pengembalian dapat melanggar hukum;
- alamat asal tidak tersedia, berisiko tinggi, atau secara teknis tidak sesuai;
- diperlukan pemeriksaan tambahan;
- dana sudah dicadangkan, dibekukan, atau terkait dengan sengketa.

Dari jumlah pengembalian dapat dipotong biaya jaringan, biaya layanan, biaya pemrosesan, dan biaya lain yang berlaku jika diatur dalam Syarat Penggunaan, halaman biaya <https://kashbi.io/information/fees>, antarmuka Platform, atau aturan terpisah.

Jumlah spesifik biaya atau tagihan untuk pengembalian tersebut tidak ditetapkan dalam Kebijakan ini dan dapat ditentukan oleh halaman biaya <https://kashbi.io/information/fees>, antarmuka Platform, atau aturan terpisah, jika biaya tersebut berlaku.

13. Pelaporan dan Interaksi dengan Otoritas

Perusahaan dapat berinteraksi dengan otoritas yang berwenang, unit intelijen keuangan, otoritas penegak hukum, pengadilan, regulator, bank, penyedia pembayaran, dan pihak berwenang lainnya jika diwajibkan atau diizinkan oleh hukum.

Perusahaan dapat menyampaikan informasi tentang pengguna, akun, transaksi, transaksi P2P, sengketa, alamat, data pembayaran, atau keadaan lain jika:

- permintaan yang sah telah diterima;
- terdapat kewajiban untuk melaporkan aktivitas mencurigakan;
- diperlukan untuk mematuhi persyaratan sanksi;
- diperlukan untuk melindungi hak Perusahaan, pengguna, atau pihak ketiga;
- diperlukan untuk mencegah penipuan, pencucian uang, atau pendanaan terorisme.

Perusahaan tidak berkewajiban untuk memberi tahu pengguna mengenai penyampaian tersebut jika pemberitahuan dilarang oleh hukum, dapat menghambat investigasi, mengungkap prosedur AML internal, atau menimbulkan risiko keamanan.

14. Penyimpanan Data dan Catatan

Perusahaan menyimpan data dan catatan yang terkait dengan AML/KYC, transaksi, transaksi P2P, pemeriksaan, sengketa, pembatasan, dan pelaporan selama jangka waktu yang ditentukan oleh hukum yang berlaku, persyaratan mitra, aturan internal manajemen risiko, dan Kebijakan Privasi.

Data tersebut dapat mencakup:

- data KYC;
- dokumen pengguna;
- hasil verifikasi;
- kecocokan sanksi dan PEP;
- profil risiko;
- riwayat operasi;
- alamat blockchain;
- txid/hash transaksi;
- data transaksi P2P;
- bukti pembayaran;
- materi sengketa;
- korespondensi dengan dukungan;
- keputusan internal mengenai pembatasan;
- catatan permintaan dari otoritas yang berwenang.

Penghapusan akun, penarikan persetujuan, atau penghentian penggunaan Platform tidak selalu berarti penghapusan langsung data AML/KYC jika penyimpanannya diwajibkan atau diizinkan oleh hukum, aturan AML/KYC/CTF, perlindungan hak Perusahaan, penyelesaian sengketa, atau pemenuhan permintaan dari otoritas yang berwenang.

15. Pihak Ketiga dan Penyedia Layanan

Perusahaan dapat melibatkan pihak ketiga untuk melaksanakan prosedur AML/KYC, termasuk:

- penyedia verifikasi dokumen;
- penyedia liveness check;
- penyedia screening sanksi;
- penyedia screening PEP/adverse media;
- penyedia analitik blockchain;
- mitra pembayaran;
- bank, pemroses, dan penyedia pertukaran;
- penasihat hukum, kepatuhan, dan audit;
- penyedia infrastruktur dan keamanan.

Penyedia dapat disebutkan berdasarkan kategori tanpa nama spesifik, kecuali diwajibkan lain oleh hukum, perjanjian dengan penyedia, atau kebijakan terpisah Perusahaan.

Perusahaan dapat memeriksa mitra dan penyedia terkait sanksi, reputasi, lisensi, izin, risiko, dan kemampuan untuk mematuhi persyaratan keamanan dan kerahasiaan.

16. Kewajiban Pengguna

Pengguna berjanji untuk:

- tidak menggunakan Platform untuk aktivitas terlarang;
- memberikan informasi yang benar;
- menanggapi permintaan Perusahaan tepat waktu;
- memberikan dokumen dan penjelasan jika diminta;
- hanya menggunakan dana yang secara sah menjadi miliknya;
- tidak menggunakan kartu bank, akun, dompet, atau detail pembayaran milik orang lain tanpa dasar hukum;
- tidak memberikan dokumen, tanda terima, tangkapan layar, atau bukti palsu;
- tidak menghindari limit, pemeriksaan, pembatasan sanksi, atau aturan Platform;
- tidak membuat beberapa akun untuk menghindari pembatasan;
- mematuhi hukum yang berlaku;
- secara mandiri menilai legalitas operasinya di negara tempat tinggalnya.

Penolakan untuk bekerja sama, penghindaran verifikasi, pemberian informasi palsu, atau upaya menghindari kontrol AML/KYC dapat mengakibatkan pembatasan atau penghentian layanan.

17. Kerahasiaan Prosedur AML/KYC

Pengguna memahami bahwa Perusahaan tidak mengungkapkan:

- kriteria risiko yang tepat;
- red flags internal;
- ambang batas pemantauan;
- algoritma scoring;
- sumber data AML;
- rincian investigasi;
- alasan penyampaian laporan kepada otoritas yang berwenang;
- rincian keputusan internal;
- informasi yang pengungkapannya dapat melanggar hukum, keamanan, atau efektivitas kontrol AML/KYC.

18. Perubahan Kebijakan

Perusahaan dapat mengubah Kebijakan ini kapan saja. Versi terbaru dipublikasikan di situs web <https://kashbi.io> atau di antarmuka Platform.

Penggunaan Platform secara berkelanjutan setelah publikasi versi yang diperbarui berarti persetujuan pengguna terhadap versi baru Kebijakan, kecuali ditentukan lain oleh hukum yang berlaku.

19. Versi Bahasa

Kebijakan ini dapat dipublikasikan dalam bahasa Rusia, Kazakh, Inggris, dan bahasa lainnya.

Jika hukum yang berlaku mensyaratkan prioritas versi bahasa tertentu, versi tersebut akan berlaku. Dalam semua kasus lainnya, jika terdapat perbedaan antara versi bahasa, versi bahasa Rusia yang berlaku.

20. Kontak

Untuk pertanyaan mengenai Kebijakan ini, pengguna dapat menghubungi:

- Perusahaan: F-Tech
- Negara pendaftaran: Kazakhstan
- Situs web: <https://kashbi.io>
- Aplikasi: KashBi
- Email: legal@kashbi.io
- Telegram: [kashbi_support](#)
- Alamat hukum: 44/1 Al-Farabi Avenue, Apartment 207