Chính sách AML/KYC

Chính sách AML/KYC này (“Chính sách”) mô tả cách tiếp cận của F-Tech, được đăng ký tại Kazakhstan (“Công ty”, “chúng tôi”, “của chúng tôi”), trong việc phòng, chống rửa tiền, tài trợ khủng bố, né tránh lệnh trừng phạt, gian lận và các hoạt động bất hợp pháp hoặc bị cấm khác khi sử dụng trang web https://kashbi.io, ứng dụng KashBi, bot Telegram, Telegram Mini App, phiên bản web, API, ví crypto-fiat, nền tảng P2P và các dịch vụ liên quan khác của Công ty, gọi chung là “Nền tảng”.

Chính sách này là một phần của Điều khoản sử dụng và được áp dụng cùng với Chính sách quyền riêng tư, quy tắc giao dịch P2P, quy tắc phí, cảnh báo rủi ro và các tài liệu khác của Công ty.

Bằng việc sử dụng Nền tảng, tạo tài khoản, nạp số dư, rút tài sản số, tạo hoặc chấp nhận giao dịch P2P, thực hiện xác minh hoặc tương tác với Nền tảng theo bất kỳ cách nào khác, người dùng xác nhận rằng họ đã đọc Chính sách này và đồng ý tuân thủ các quy định của Chính sách.

Nếu người dùng không đồng ý với Chính sách này, người dùng phải ngừng sử dụng Nền tảng.

1. Mục đích và phạm vi áp dụng

1.1. Mục đích của Chính sách

Mục đích của Chính sách này là thiết lập các nguyên tắc, quy tắc và biện pháp chính nhằm:

- ngăn chặn việc sử dụng Nền tảng để rửa tiền;
- ngăn chặn tài trợ khủng bố;
- ngăn chặn việc né tránh lệnh trừng phạt;
- ngăn chặn gian lận, lừa đảo, phishing và các hoạt động trái pháp luật khác;
- xác định và đánh giá người dùng, giao dịch, địa chỉ và khu vực pháp lý có rủi ro cao;
- giám sát các giao dịch liên quan đến tài sản số và giao dịch P2P;
- tuân thủ các yêu cầu pháp luật hiện hành, yêu cầu của đối tác, nhà cung cấp dịch vụ AML/KYC, ngân hàng, nhà cung cấp dịch vụ thanh toán và cơ quan có thẩm quyền;
- bảo vệ người dùng, Công ty, Nền tảng và uy tín kinh doanh của Công ty.

1.2. Phạm vi áp dụng

Chính sách này áp dụng cho tất cả người dùng của Nền tảng, bao gồm người dùng của:

- ví crypto-fiat;
- nền tảng P2P;
- Telegram Mini App;
- bot Telegram;
- phiên bản web;
- chức năng nạp và rút tài sản số;

- chuyển khoản nội bộ;
- các giao dịch fiat ngoài P2P, nếu các chức năng đó khả dụng;
- dịch vụ hỗ trợ và giải quyết tranh chấp.

1.3. Cách tiếp cận dựa trên rủi ro

Công ty áp dụng cách tiếp cận dựa trên rủi ro. Điều này có nghĩa là KYC, kiểm tra AML, hạn mức, yêu cầu tài liệu, thẩm định tăng cường, giám sát, hạn chế và các biện pháp khác được áp dụng tương ứng với mức độ rủi ro của người dùng, giao dịch, khu vực pháp lý, phương thức thanh toán, tài sản số, địa chỉ blockchain, hành vi của người dùng và các yếu tố khác.

Nền tảng được định vị theo hướng privacy-first: Công ty nỗ lực giảm thiểu việc thu thập dữ liệu cá nhân và không yêu cầu giấy tờ định danh khi không cần thiết. Đồng thời, privacy-first không có nghĩa là ẩn danh hoàn toàn và không loại trừ việc xử lý dữ liệu, xác minh người dùng, kiểm tra giao dịch, hạn chế giao dịch hoặc chuyển thông tin cho cơ quan có thẩm quyền khi điều đó được yêu cầu hoặc được pháp luật cho phép, theo quy tắc của Nền tảng, yêu cầu của đối tác hoặc Chính sách này.

2. Thuật ngữ và định nghĩa

2.1. AML

AML là các biện pháp phòng, chống rửa tiền, bao gồm việc phát hiện, ngăn chặn, điều tra và hạn chế các giao dịch liên quan đến nguồn tiền có nguồn gốc bất hợp pháp.

2.2. KYC

KYC là quy trình “Know Your Customer” hoặc “hiểu khách hàng của bạn”, bao gồm nhận dạng, xác minh và đánh giá người dùng khi quy trình đó cần thiết dựa trên rủi ro, hạn mức, giao dịch, pháp luật hiện hành hoặc yêu cầu của đối tác.

2.3. CDD

CDD là thẩm định khách hàng, bao gồm việc thu thập và phân tích thông tin về người dùng, hoạt động của họ, nguồn tiền, mục đích giao dịch và hồ sơ rủi ro.

2.4. EDD

EDD là thẩm định tăng cường được áp dụng đối với người dùng, giao dịch hoặc tình huống có rủi ro cao hơn. EDD có thể bao gồm yêu cầu tài liệu bổ sung, xác nhận nguồn tiền, phân tích giao dịch mở rộng, kiểm tra nguồn mở, kiểm tra lệnh trừng phạt và PEP, cũng như phê duyệt việc tiếp tục cung cấp dịch vụ ở cấp người có trách nhiệm của Công ty.

2.5. KYT

KYT là quy trình “Know Your Transaction” hoặc “hiểu giao dịch của bạn”, bao gồm việc phân tích giao dịch, địa chỉ blockchain, nguồn tiền, hành vi của người dùng, ví liên quan, mô hình P2P và các dữ liệu khác liên quan đến một giao dịch cụ thể.

2.6. PEP

PEP là người có ảnh hưởng chính trị, cũng như thành viên gia đình và những người có liên hệ chặt chẽ với người đó, nếu những người này cần được chú ý tăng cường từ góc độ rủi ro tham nhũng, lệnh trừng phạt, uy tín hoặc các rủi ro khác.

2.7. Lệnh trừng phạt

Lệnh trừng phạt là các biện pháp hạn chế kinh tế, tài chính, thương mại, cá nhân, lãnh thổ hoặc các biện pháp hạn chế khác do quốc gia, tổ chức quốc tế, cơ quan có thẩm quyền áp đặt hoặc được áp dụng thông qua các đối tác của Công ty.

2.8. Khu vực pháp lý bị cấm

Khu vực pháp lý bị cấm là quốc gia, vùng lãnh thổ hoặc khu vực mà Công ty hạn chế hoặc cấm cung cấp dịch vụ do pháp luật, lệnh trừng phạt, rủi ro AML cao, yêu cầu của đối tác, quy tắc nội bộ về quản lý rủi ro hoặc các hoàn cảnh khác.

Danh sách các khu vực pháp lý bị cấm không nhất thiết được công bố trong Chính sách này và có thể được xác định trong giao diện Nền tảng, quy tắc nội bộ của Công ty, tài liệu của đối tác hoặc thông báo riêng.

2.9. Hoạt động đáng ngờ

Hoạt động đáng ngờ là giao dịch, hành vi, nguồn tiền, giao dịch P2P, địa chỉ, phương thức thanh toán, tài khoản hoặc yếu tố khác có thể cho thấy rửa tiền, tài trợ khủng bố, né tránh lệnh trừng phạt, gian lận, lừa đảo, sử dụng dữ liệu của người khác, sử dụng nhiều tài khoản, hoạt động bất hợp pháp hoặc rủi ro không thể chấp nhận khác.

2.10. Red flags / dấu hiệu cảnh báo

Red flags là các dấu hiệu hoặc chỉ báo có thể cho thấy rủi ro gia tăng hoặc nhu cầu kiểm tra bổ sung.

3. Tổ chức kiểm soát AML/KYC

3.1. Người chịu trách nhiệm

Công ty có thể chỉ định một người chịu trách nhiệm hoặc một nhóm chịu trách nhiệm triển khai các quy trình AML/KYC, quản lý rủi ro, giám sát giao dịch, xem xét hoạt động đáng ngờ, tương tác với cơ quan có thẩm quyền và duy trì các quy tắc nội bộ.

3.2. Quy tắc nội bộ

Công ty xây dựng và áp dụng các quy tắc nội bộ, hướng dẫn, tiêu chí rủi ro, red flags, quy trình xác minh, hạn mức, kịch bản giám sát và quy tắc ra quyết định.

Các tài liệu nội bộ đó là thông tin bảo mật của Công ty và không phải tiết lộ cho người dùng nếu việc tiết lộ có thể làm suy giảm hiệu quả kiểm soát, an ninh của Nền tảng, việc tuân thủ pháp luật, quyền của bên thứ ba hoặc lợi ích của cuộc điều tra.

3.3. Cập nhật quy trình

Công ty có thể cập nhật các quy trình AML/KYC dựa trên:

- thay đổi pháp luật;
- sản phẩm và chức năng mới;
- mô hình gian lận mới;
- khuyến nghị của FATF và các tiêu chuẩn quốc tế khác;
- yêu cầu của đối tác;
- kết quả kiểm tra nội bộ;

- sự cố an ninh;
- thay đổi chế độ trừng phạt;
- các hình thái mới của rửa tiền và tài trợ khủng bố.

4. Đánh giá rủi ro

4.1. Đánh giá rủi ro chung

Công ty có thể tiến hành đánh giá định kỳ các rủi ro AML/KYC liên quan đến Nền tảng, người dùng, sản phẩm, tài sản số, khu vực pháp lý, kênh truy cập, giao dịch P2P, phương thức thanh toán, giao dịch fiat ngoài P2P, mạng blockchain và nhà cung cấp dịch vụ.

4.2. Yếu tố rủi ro

Khi đánh giá rủi ro, Công ty có thể xem xét:

- quốc gia cư trú, quốc tịch, vị trí hoặc địa lý theo IP của người dùng;
- loại tài khoản và phương thức đăng ký;
- lịch sử giao dịch;
- số tiền và tần suất giao dịch;
- tài sản số và mạng được sử dụng;
- địa chỉ blockchain của người gửi và người nhận;
- mối liên hệ của địa chỉ với mixer, thị trường darknet, hack, ransomware, dự án scam, địa chỉ bị trừng phạt hoặc các nguồn rủi ro cao khác;
- việc sử dụng giao dịch P2P;
- phương thức thanh toán fiat đã chọn;
- hành vi trong tranh chấp;
- khiếu nại từ người dùng khác;
- sử dụng nhiều tài khoản hoặc liên hệ với các tài khoản đã bị chặn trước đó;
- sử dụng VPN, proxy hoặc phương tiện khác để che giấu vị trí;
- từ chối cung cấp thông tin;
- dữ liệu không nhất quán;
- trạng thái PEP;
- trùng khớp với danh sách trừng phạt;
- adverse media và các yếu tố uy tín khác;
- yêu cầu của đối tác và cơ quan có thẩm quyền.

4.3. Danh mục rủi ro

Công ty có thể gán danh mục rủi ro nội bộ cho người dùng, giao dịch, địa chỉ hoặc thỏa thuận, ví dụ như rủi ro thấp, trung bình, cao hoặc không thể chấp nhận.

Danh mục rủi ro có thể ảnh hưởng đến:

- các chức năng khả dụng;
- hạn mức;
- nhu cầu KYC;

- nhu cầu EDD;
- tốc độ xử lý giao dịch;
- khả năng rút tiền;
- quyền truy cập P2P;
- nhu cầu kiểm tra thủ công;
- khả năng bị đóng băng hoặc từ chối dịch vụ.

Công ty không có nghĩa vụ tiết lộ cho người dùng danh mục rủi ro nội bộ, phương pháp tính toán, tiêu chí chính xác hoặc kết quả scoring.

5. KYC/CDD: xác minh người dùng

5.1. Cách tiếp cận chung

Công ty không yêu cầu xác minh KYC đầy đủ đối với tất cả người dùng theo mặc định, trừ khi pháp luật, giao diện, yêu cầu của đối tác hoặc một chức năng cụ thể quy định khác. Việc xác minh được áp dụng trên cơ sở dựa trên rủi ro.

5.2. Khi nào có thể cần KYC

Công ty có thể yêu cầu KYC hoặc thông tin bổ sung trong các trường hợp sau:

- đạt hạn mức;
- giao dịch có giá trị lớn;
- giao dịch bất thường;
- hoạt động đáng ngờ;
- mở tranh chấp;
- yêu cầu rút tiền;
- trùng khớp AML liên quan đến địa chỉ hoặc giao dịch;
- liên hệ với khu vực pháp lý rủi ro cao;
- sử dụng chức năng fiat ngoài P2P;
- yêu cầu của đối tác thanh toán, ngân hàng, nhà cung cấp dịch vụ trao đổi hoặc nhà cung cấp AML/KYC;
- yêu cầu của cơ quan có thẩm quyền;
- khôi phục quyền truy cập tài khoản;
- nghi ngờ sử dụng nhiều tài khoản, gian lận hoặc sử dụng dữ liệu của người khác;
- các hoàn cảnh khác cần xác minh.

5.3. Dữ liệu có thể được yêu cầu

Tùy thuộc vào mức độ rủi ro, Công ty có thể yêu cầu:

- họ, tên, tên đệm hoặc tên đầy đủ khác;
- ngày sinh;
- quốc tịch;
- quốc gia cư trú;
- địa chỉ cư trú;

- email;
- số điện thoại;
- giấy tờ tùy thân;
- ảnh, selfie, xác minh video hoặc liveness check;
- bằng chứng địa chỉ;
- bằng chứng nguồn tiền;
- bằng chứng nguồn tài sản;
- xác nhận mục đích giao dịch;
- sao kê, biên lai, chứng từ hoặc xác nhận thanh toán;
- tài liệu liên quan đến giao dịch P2P;
- thông tin về liên hệ với PEP;
- các tài liệu hoặc giải thích khác cần thiết để đánh giá rủi ro.

5.4. Xác minh dữ liệu

Công ty có thể xác minh dữ liệu được cung cấp:

- thủ công;
- bằng hệ thống tự động;
- thông qua nhà cung cấp AML/KYC bên ngoài;
- thông qua danh sách trừng phạt và PEP;
- thông qua nguồn mở;
- thông qua phân tích blockchain;
- thông qua thông tin nhận được từ đối tác, người dùng, ngân hàng, nhà cung cấp thanh toán hoặc cơ quan có thẩm quyền.

5.5. Nghĩa vụ hợp tác của người dùng

Người dùng phải cung cấp thông tin và tài liệu được yêu cầu một cách kịp thời, chính xác và đầy đủ.

Nếu người dùng từ chối cung cấp dữ liệu, cung cấp thông tin sai lệch hoặc không nhất quán, không trả lời yêu cầu hoặc cố gắng né tránh xác minh, Công ty có thể hạn chế chức năng, đình chỉ giao dịch, đóng băng tài sản, hủy giao dịch, từ chối dịch vụ hoặc đóng tài khoản.

5.6. Xác minh lại

Công ty có thể yêu cầu lại tài liệu hoặc thông tin, ngay cả khi người dùng đã từng vượt qua xác minh trước đó, nếu:

- dữ liệu của người dùng thay đổi;
- giấy tờ tùy thân hết hạn;
- hoạt động của người dùng thay đổi;
- xuất hiện rủi ro mới;
- người dùng đạt hạn mức mới;
- chức năng mới được mở;
- yêu cầu pháp luật hoặc đối tác thay đổi;

- phát sinh tranh chấp hoặc hoạt động đáng ngờ.

6. Thẩm định tăng cường EDD

6.1. Khi nào EDD được áp dụng

Công ty có thể áp dụng EDD nếu người dùng, giao dịch, địa chỉ, giao dịch P2P, khu vực pháp lý hoặc hành vi có rủi ro cao hơn.

EDD có thể được áp dụng, đặc biệt nếu:

- người dùng là PEP hoặc có liên quan đến PEP;
- người dùng liên quan đến khu vực pháp lý rủi ro cao;
- giao dịch có giá trị lớn, phức tạp, bất thường hoặc không thể giải thích về mặt kinh tế;
- tiền đến từ địa chỉ blockchain rủi ro cao;
- giao dịch liên quan đến mixer, thị trường darknet, hack, ransomware, scam, địa chỉ bị trừng phạt hoặc các red flags khác;
- người dùng thường xuyên mở hoặc thua tranh chấp;
- có dấu hiệu sử dụng nhiều tài khoản;
- có dấu hiệu sử dụng thông tin thanh toán hoặc tài khoản của người khác;
- người dùng không thể giải thích nguồn tiền;
- người dùng trả lời mâu thuẫn;
- cần xác nhận theo yêu cầu của đối tác hoặc cơ quan có thẩm quyền.

6.2. Biện pháp EDD

EDD có thể bao gồm:

- yêu cầu tài liệu bổ sung;
- xác nhận nguồn tiền;
- xác nhận nguồn tài sản;
- xác nhận mục đích giao dịch;
- kiểm tra nguồn mở;
- kiểm tra adverse media;
- phân tích chuyên sâu lịch sử blockchain;
- giảm hạn mức;
- tạm thời đóng băng tiền;
- phê duyệt thủ công giao dịch;
- từ chối giao dịch;
- chấm dứt dịch vụ.

6.3. Kết quả EDD

Theo kết quả EDD, Công ty có thể:

- cho phép giao dịch;
- cho phép giao dịch với hạn mức hoặc điều kiện;
- yêu cầu thông tin bổ sung;

- từ chối giao dịch;
- hoàn trả tiền, nếu được phép và có thể thực hiện;
- đóng băng tiền;
- hạn chế tài khoản;
- đóng tài khoản;
- chuyển thông tin cho cơ quan có thẩm quyền nếu được yêu cầu hoặc được pháp luật cho phép.

7. KYT và giám sát giao dịch

7.1. Giám sát chung

Công ty có thể thực hiện giám sát liên tục hoặc chọn lọc đối với các hoạt động của người dùng, bao gồm:

- nạp tài sản số;
- rút tài sản số;
- chuyển khoản nội bộ;
- giao dịch P2P;
- giao dịch fiat ngoài P2P, nếu các chức năng đó khả dụng;
- các nỗ lực thực hiện giao dịch;
- giao dịch bị hủy;
- giao dịch liên quan đến tranh chấp hoặc khiếu nại.

7.2. Phân tích blockchain

Công ty có thể sử dụng phân tích blockchain để đánh giá rủi ro của địa chỉ, giao dịch, cụm địa chỉ, nguồn tiền và các thực thể liên quan.

Việc kiểm tra có thể xem xét mối liên hệ với:

- địa chỉ bị trừng phạt;
- thị trường darknet;
- mixer và dịch vụ che giấu;
- ransomware;
- hack và tiền bị đánh cắp;
- dự án scam;
- mô hình gian lận;
- dịch vụ bất hợp pháp;
- sàn giao dịch hoặc dịch vụ đổi tiền rủi ro cao;
- các nguồn rủi ro cao khác.

7.3. Giám sát P2P

Trong các giao dịch P2P, Công ty có thể phân tích:

- tần suất giao dịch;
- số tiền giao dịch;

- hành vi của các bên;
- số lần hủy;
- số lượng tranh chấp;
- khiếu nại;
- chứng từ thanh toán;
- trùng khớp thông tin thanh toán;
- liên hệ giữa các tài khoản;
- dấu hiệu sử dụng nhiều tài khoản;
- sự không nhất quán trong dữ liệu thanh toán;
- nỗ lực đưa giao dịch ra ngoài quy tắc của Nền tảng;
- sử dụng tài khoản ngân hàng, thẻ hoặc thông tin thanh toán của người khác.

7.4. Hạn mức và trì hoãn

Công ty có thể đặt hạn mức, trì hoãn, kiểm tra thủ công hoặc yêu cầu bổ sung cho từng người dùng, giao dịch, thỏa thuận, địa chỉ, tài sản, phương thức thanh toán hoặc khu vực pháp lý.

Một giao dịch có thể bị trì hoãn hoặc đình chỉ cho đến khi hoàn tất kiểm tra.

8. Red flags: dấu hiệu hoạt động đáng ngờ

Red flags có thể bao gồm, nhưng không giới hạn ở:

- người dùng từ chối cung cấp dữ liệu hoặc tài liệu;
- cung cấp tài liệu giả mạo, bị chỉnh sửa hoặc không nhất quán;
- sử dụng dữ liệu, thẻ, tài khoản hoặc ví của người khác;
- cố gắng sử dụng nhiều tài khoản;
- thường xuyên hủy giao dịch P2P;
- thường xuyên có tranh chấp P2P;
- biên lai, chứng từ hoặc ảnh chụp màn hình thanh toán giả mạo;
- tên người thanh toán không khớp với người dùng;
- nạp và rút tiền nhanh chóng mà không có mục đích kinh tế rõ ràng;
- chia nhỏ giao dịch thành nhiều khoản nhỏ;
- giao dịch không phù hợp với hành vi thông thường của người dùng;
- sử dụng địa chỉ blockchain rủi ro cao;
- liên hệ với mixer, thị trường darknet, hack, ransomware, scam hoặc địa chỉ bị trừng phạt;
- tăng đột biến khối lượng giao dịch;
- cố gắng né tránh hạn mức;
- sử dụng VPN, proxy hoặc phương tiện khác để che giấu vị trí nhằm né tránh hạn chế;
- gây áp lực mạnh lên đối tác giao dịch hoặc bộ phận hỗ trợ;
- từ chối giải thích nguồn tiền;
- cố gắng đưa giao dịch ra ngoài Nền tảng;
- khiếu nại từ người dùng khác;

- thông tin tiêu cực từ nguồn mở;
- trùng khớp với nguồn trừng phạt, PEP hoặc adverse media.

Sự hiện diện của một red flag không phải lúc nào cũng có nghĩa là vi phạm, nhưng có thể là cơ sở để kiểm tra bổ sung, hạn chế giao dịch hoặc áp dụng các biện pháp khác.

9. Lệnh trừng phạt và quan hệ bị cấm

Công ty không thiết lập hoặc tiếp tục quan hệ với người dùng nếu điều đó bị cấm bởi pháp luật, lệnh trừng phạt, yêu cầu của đối tác hoặc quy tắc nội bộ về quản lý rủi ro.

Công ty có thể từ chối dịch vụ, hạn chế tài khoản, đóng băng tài sản hoặc chấm dứt quan hệ nếu người dùng:

- nằm trong danh sách trừng phạt;
- có liên quan đến người nằm trong danh sách trừng phạt;
- ở trong khu vực pháp lý bị cấm;
- hành động vì lợi ích của người bị cấm;
- sử dụng Nền tảng để né tránh lệnh trừng phạt;
- từ chối cung cấp thông tin cần thiết để kiểm tra lệnh trừng phạt.

Công ty có thể thực hiện kiểm tra lệnh trừng phạt khi đăng ký, trước giao dịch, sau giao dịch, khi danh sách trừng phạt thay đổi, khi mở tranh chấp, khi rút tiền hoặc trong các trường hợp khác.

10. Hoạt động bị cấm

Người dùng bị cấm sử dụng Nền tảng cho:

- rửa tiền;
- tài trợ khủng bố;
- né tránh lệnh trừng phạt;
- gian lận, scam, phishing hoặc social engineering;
- mua bán tiền, tài khoản, thẻ, tài liệu hoặc dữ liệu cá nhân bị đánh cắp;
- sử dụng thẻ ngân hàng, tài khoản, ví hoặc thông tin thanh toán của người khác mà không có căn cứ pháp lý;
- buôn bán trái phép ma túy, vũ khí, chất nguy hiểm hoặc hàng hóa bị cấm khác;
- cờ bạc bất hợp pháp;
- dịch vụ tài chính bất hợp pháp;
- hoạt động darknet;
- tài trợ cho hoạt động cực đoan, khủng bố hoặc hoạt động bị cấm khác;
- xâm phạm quyền của bên thứ ba;
- sử dụng tài liệu, biên lai, chứng từ hoặc ảnh chụp màn hình giả mạo;
- sử dụng nhiều tài khoản và né tránh hạn chế;
- bất kỳ hoạt động nào khác mà Công ty cho là bất hợp pháp, rủi ro cao hoặc không thể chấp nhận.

11. Biện pháp của Công ty khi phát hiện rủi ro

Nếu Công ty phát hiện hoạt động đáng ngờ, rủi ro AML/KYC, rủi ro trừng phạt, vi phạm Chính sách này hoặc việc người dùng từ chối hợp tác, Công ty có thể:

- yêu cầu thông tin bổ sung;
- yêu cầu KYC hoặc EDD;
- giảm hạn mức;
- trì hoãn giao dịch;
- từ chối giao dịch;
- hủy giao dịch P2P;
- hạn chế chức năng P2P;
- đóng băng hoặc dự trữ tài sản;
- hạn chế rút tiền;
- tạm thời chặn tài khoản;
- đóng tài khoản;
- hoàn trả tiền cho người gửi, nếu có thể, được phép và không bị pháp luật cấm;
- khấu trừ phí áp dụng, chi phí mạng hoặc chi phí hoàn trả nếu được quy định bởi quy tắc của Nền tảng;
- chuyển thông tin cho cơ quan có thẩm quyền nếu được yêu cầu hoặc được pháp luật cho phép;
- thực hiện các biện pháp hợp lý khác để bảo vệ Nền tảng, người dùng, đối tác và Công ty.

Công ty không có nghĩa vụ thông báo trước cho người dùng về việc áp dụng các biện pháp đó nếu thông báo có thể vi phạm pháp luật, yêu cầu AML/KYC/CTF, quy tắc trừng phạt, lợi ích điều tra, an ninh của Nền tảng hoặc quyền của bên thứ ba.

12. Hoàn trả tiền trong trường hợp bị từ chối AML/KYC

Nếu một giao dịch bị từ chối hoặc dịch vụ bị hạn chế do kết quả kiểm tra AML/KYC, Công ty có thể, nếu có thể và được phép, hoàn trả tài sản số về địa chỉ gốc của người gửi hoặc địa chỉ khác mà Công ty cho là chấp nhận được từ góc độ rủi ro và pháp lý.

Việc hoàn trả có thể không thể thực hiện hoặc bị trì hoãn nếu:

- tiền liên quan đến địa chỉ bị trừng phạt;
- tiền liên quan đến hoạt động phạm tội;
- đã nhận được yêu cầu từ cơ quan có thẩm quyền;
- việc hoàn trả có thể vi phạm pháp luật;
- địa chỉ gốc không khả dụng, có rủi ro cao hoặc không phù hợp về mặt kỹ thuật;
- cần kiểm tra bổ sung;
- tiền đã được dự trữ, đóng băng hoặc liên quan đến tranh chấp.

Từ số tiền hoàn trả có thể bị khấu trừ phí mạng, phí dịch vụ, chi phí xử lý và các chi phí áp dụng khác nếu được quy định trong Điều khoản sử dụng, trang phí https://kashbi.io/information/fees, giao diện Nền tảng hoặc các quy tắc riêng.

Mức phí hoặc khoản thu cụ thể cho việc hoàn trả đó không được ấn định trong Chính sách này và có thể được xác định bởi trang phí https://kashbi.io/information/fees, giao diện Nền tảng hoặc các quy tắc riêng, nếu khoản phí đó được áp dụng.

13. Báo cáo và tương tác với cơ quan có thẩm quyền

Công ty có thể tương tác với cơ quan có thẩm quyền, đơn vị tình báo tài chính, cơ quan thực thi pháp luật, tòa án, cơ quan quản lý, ngân hàng, nhà cung cấp thanh toán và các cá nhân/tổ chức được ủy quyền khác nếu được yêu cầu hoặc được pháp luật cho phép.

Công ty có thể chuyển thông tin về người dùng, tài khoản, giao dịch, giao dịch P2P, tranh chấp, địa chỉ, dữ liệu thanh toán hoặc các hoàn cảnh khác nếu:

- đã nhận được yêu cầu hợp pháp;
- có nghĩa vụ báo cáo hoạt động đáng ngờ;
- cần tuân thủ yêu cầu trừng phạt;
- cần bảo vệ quyền của Công ty, người dùng hoặc bên thứ ba;
- cần ngăn chặn gian lận, rửa tiền hoặc tài trợ khủng bố.

Công ty không có nghĩa vụ thông báo cho người dùng về việc chuyển thông tin đó nếu việc thông báo bị pháp luật cấm, có thể cản trở điều tra, tiết lộ quy trình AML nội bộ hoặc tạo ra rủi ro an ninh.

14. Lưu giữ dữ liệu và hồ sơ

Công ty lưu giữ dữ liệu và hồ sơ liên quan đến AML/KYC, giao dịch, giao dịch P2P, kiểm tra, tranh chấp, hạn chế và báo cáo trong thời hạn được quy định bởi pháp luật hiện hành, yêu cầu của đối tác, quy tắc nội bộ về quản lý rủi ro và Chính sách quyền riêng tư.

Các dữ liệu đó có thể bao gồm:

- dữ liệu KYC;
- tài liệu của người dùng;
- kết quả xác minh;
- trùng khớp với danh sách trừng phạt và PEP;
- hồ sơ rủi ro;
- lịch sử giao dịch;
- địa chỉ blockchain;
- txid/hash giao dịch;
- dữ liệu giao dịch P2P;
- chứng từ thanh toán;
- tài liệu tranh chấp;
- thư từ với bộ phận hỗ trợ;
- quyết định nội bộ về hạn chế;
- hồ sơ yêu cầu từ cơ quan có thẩm quyền.

Việc xóa tài khoản, rút lại sự đồng ý hoặc chấm dứt sử dụng Nền tảng không phải lúc nào cũng có nghĩa là dữ liệu AML/KYC sẽ bị xóa ngay lập tức nếu việc lưu giữ được yêu cầu

hoặc được pháp luật cho phép, theo quy tắc AML/KYC/CTF, để bảo vệ quyền của Công ty, giải quyết tranh chấp hoặc thực hiện yêu cầu của cơ quan có thẩm quyền.

15. Bên thứ ba và nhà cung cấp dịch vụ

Công ty có thể thuê bên thứ ba để thực hiện các quy trình AML/KYC, bao gồm:

- nhà cung cấp xác minh tài liệu;
- nhà cung cấp liveness check;
- nhà cung cấp kiểm tra lệnh trừng phạt;
- nhà cung cấp kiểm tra PEP/adverse media;
- nhà cung cấp phân tích blockchain;
- đối tác thanh toán;
- ngân hàng, đơn vị xử lý và nhà cung cấp dịch vụ trao đổi;
- cố vấn pháp lý, tuân thủ và kiểm toán;
- nhà cung cấp hạ tầng và an ninh.

Nhà cung cấp có thể được nêu theo danh mục mà không nêu tên cụ thể, trừ khi pháp luật, hợp đồng với nhà cung cấp hoặc chính sách riêng của Công ty yêu cầu khác.

Công ty có thể kiểm tra đối tác và nhà cung cấp về lệnh trừng phạt, uy tín, giấy phép, phê duyệt, rủi ro và khả năng tuân thủ các yêu cầu về an ninh và bảo mật.

16. Nghĩa vụ của người dùng

Người dùng cam kết:

- không sử dụng Nền tảng cho hoạt động bị cấm;
- cung cấp thông tin chính xác;
- trả lời kịp thời các yêu cầu của Công ty;
- cung cấp tài liệu và giải thích nếu được yêu cầu;
- chỉ sử dụng tiền thuộc sở hữu hợp pháp của mình;
- không sử dụng thẻ ngân hàng, tài khoản, ví hoặc thông tin thanh toán của người khác mà không có căn cứ pháp lý;
- không cung cấp tài liệu, biên lai, ảnh chụp màn hình hoặc chứng từ giả mạo;
- không né tránh hạn mức, kiểm tra, hạn chế trừng phạt hoặc quy tắc của Nền tảng;
- không tạo nhiều tài khoản để né tránh hạn chế;
- tuân thủ pháp luật hiện hành;
- tự đánh giá tính hợp pháp của các giao dịch của mình tại quốc gia cư trú.

Việc từ chối hợp tác, né tránh xác minh, cung cấp thông tin sai lệch hoặc cố gắng né tránh kiểm soát AML/KYC có thể dẫn đến hạn chế hoặc chấm dứt dịch vụ.

17. Bảo mật quy trình AML/KYC

Người dùng hiểu rằng Công ty không tiết lộ:

- tiêu chí rủi ro chính xác;

- red flags nội bộ;
- ngưỡng giám sát;
- thuật toán scoring;
- nguồn dữ liệu AML;
- chi tiết điều tra;
- lý do nộp báo cáo cho cơ quan có thẩm quyền;
- chi tiết quyết định nội bộ;
- thông tin mà việc tiết lộ có thể vi phạm pháp luật, an ninh hoặc hiệu quả của kiểm soát AML/KYC.

18. Thay đổi Chính sách

Công ty có thể thay đổi Chính sách này bất kỳ lúc nào. Phiên bản hiện hành được công bố trên trang web https://kashbi.io hoặc trong giao diện Nền tảng.

Việc tiếp tục sử dụng Nền tảng sau khi phiên bản cập nhật được công bố có nghĩa là người dùng đồng ý với phiên bản mới của Chính sách, trừ khi pháp luật hiện hành quy định khác.

19. Phiên bản ngôn ngữ

Chính sách này có thể được công bố bằng tiếng Nga, tiếng Kazakhstan, tiếng Anh và các ngôn ngữ khác.

Nếu pháp luật hiện hành yêu cầu ưu tiên một phiên bản ngôn ngữ cụ thể, phiên bản đó sẽ được áp dụng. Trong tất cả các trường hợp khác, nếu có sự khác biệt giữa các phiên bản ngôn ngữ, phiên bản tiếng Nga sẽ được ưu tiên áp dụng.

20. Liên hệ

Đối với các câu hỏi liên quan đến Chính sách này, người dùng có thể liên hệ:

- Công ty: F-Tech
- Quốc gia đăng ký: Kazakhstan
- Trang web: https://kashbi.io
- Ứng dụng: KashBi
- Email: legal@kashbi.io
- Telegram: kashbi_support
- Địa chỉ pháp lý: 44/1 Al-Farabi Avenue, Apartment 207