سياسة AML/KYC

توضح سياسة AML/KYC هذه)"السياسة"(نهج F-Tech، المسجلة في Kazakhstan)"الشركة"، "نحن"، "لنا"، "خاصتنا"(، في منع غسل الأموال، وتمويل الإرهاب، والتهرب من العقوبات، والاحتيال، وغيرها من الأنشطة غير القانونية أو المحظورة عند استخدام الموقع الإلكتروني https://kashbi.net، وتطبيق KashBi، وروبوت Telegram، وTelegram Mini App، والنسخة الويب، وواجهة API، ومحفظة العملات الرقمية/العملات الورقية، ومنصة P2P، والخدمات الأخرى ذات الصلة التابعة للشركة، ويشار إليها مجتمعة باسم "المنصة".

تشكل هذه السياسة جزءاً من شروط الاستخدام، وتطبق مع سياسة الخصوصية، وقواعد معاملات P2P، وقواعد الرسوم، وتحذيرات المخاطر، وغيرها من مستندات الشركة.

باستخدام المنصة، أو إنشاء حساب، أو إيداع رصيد، أو سحب أصول رقمية، أو إنشاء أو قبول معاملة P2P، أو الخضوع للتحقق، أو التفاعل مع المنصة بأي طريقة أخرى، يؤكد المستخدم أنه قرأ هذه السياسة ويوافق على الالتزام بأحكامها.

إذا لم يوافق المستخدم على هذه السياسة، فيجب عليه التوقف عن استخدام المنصة.

1. الغرض ونطاق التطبيق

1.1. الغرض من السياسة

تهدف هذه السياسة إلى وضع المبادئ والقواعد والتدابير الرئيسية الهادفة إلى:

- منع استخدام المنصة في غسل الأموال؛
- منع تمويل الإرهاب؛
- منع التهرب من العقوبات؛
- منع الاحتيال، وعمليات النصب، والتصيد الاحتيلاي، وغيرها من الأنشطة غير المشروعة؛
- تحديد وتقييم المستخدمين والعمليات والعناوين والولايات القضائية علاية المخاطر؛
- مراقبة العمليات المتعلقة بالأصول الرقمية ومعاملات P2P؛
- الامتثال للمتطلبات القانونية المعمول بها، ومتطلبات الشركاء، ومقدمي خدمات AML/KYC، والبنوك، ومزودي خدمات الدفع، والسلطات المختصة؛
- حماية المستخدمين، والشركة، والمنصة، والسمعة التجارية للشركة.

1.2. نطاق التطبيق

تنطبق هذه السياسة على جميع مستخدمي المنصة، بمن فيهم مستخدمو:

- محفظة العملات الرقمية/العملات الورقية؛
- منصة P2P؛
- Telegram Mini App؛
- روبوت Telegram؛
- النسخة الويب؛
- وظائف إيداع وسحب الأصول الرقمية؛
- التحويلات الداخلية؛
- العمليات بلاعملات الورقية خارج P2P، إذا كانت هذه الوظائف متاحة؛
- خدمات الدعم وتسوية النزاعات.

1.3. النهج القائم على المخاطر

تطبق الشركة نهجاً قائماً على المخاطر. وهذا يعني أن KYC، وفحوصات AML، والحدود، وطلبات المستندات، والعناية الواجبة المعززة، والمراقبة، والقيود، وغيرها من التدابير تطبق بما يتناسب مع مستوى مخاطر المستخدم، والعملية، والولاية القضائية، وطريقة الدفع، والأصل الرقمي، وعنوان البلوكشين، وسلوك المستخدم، وغيرها من العوامل.

تتبنى المنصة مبدأ privacy-first: تسعى الشركة إلى تقليل جمع البيانات الشخصية إلى الحد الأدنى وعدم طلب مستندات الهوية دون ضرورة. وفي الوقت نفسه، لا يعني privacy-first إخفاء الهوية بالكامل، ولا يستبعد معالجة البيانات، أو التحقق من المستخدم، أو فحص المعاملات، أو تقييد العمليات، أو نقل المعلومات إلى السلطات المختصة عندما يكون ذلك مطلوباً أو مسموحاً به بموجب القانون، أو قواعد المنصة، أو متطلبات الشركاء، أو هذه السياسة.

2. المصطلحات والتعاريف

2.1. AML

AML يعني تدابير مكافحة غسل الأموال، بما في ذلك اكتشاف ومنع والتحقيق في وتقييد العمليات المرتبطة بأموال ذات مصدر غير مشروع.

2.2. KYC

KYC يعني إجراء "اعرف عميلك"، ويشمل تحديد هوية المستخدم والتحقق منها وتقييمه عندما يكون هذا الإجراء مطلوباً بالنظر إلى المخاطر أو الحدود أو العملية أو القانون المعمول به أو متطلبات الشركاء.

2.3. CDD

CDD يعني العناية الواجبة بالعميل، ويشمل جمع وتحليل المعلومات المتعلقة بالمستخدم ونشاطه ومصدر أمواله وأغراض عملياته وملف المخاطر الخاص به.

2.4. EDD

EDD يعني العناية الواجبة المعززة المطبقة على المستخدمين أو العمليات أو الحالات ذات المخاطر المرتفعة. وقد يشمل EDD طلب مستندات إضافية، وتأكيد مصدر الأموال، وتحليلا موسعاً للمعاملات، وفحص المصادر المفتوحة، وفحوصات العقوبات وPEP، وكذلك الموافقة على استمرار تقديم الخدمة على مستوى الأشخاص المسؤولين في الشركة.

2.5. KYT

KYT يعني إجراء "اعرف معاملتك"، ويشمل تحليل العمليات، وعناوين البلوكشين، ومصادر الأموال، وسلوك المستخدم، والمحافظ المرتبطة، وأنماط P2P، والبيانات الأخرى المتعلقة بعملية معينة.

2.6. PEP

PEP يعني الشخص السياسي المعرض للمخاطر، وكذلك أفراد أسرته والأشخاص المرتبطين به ارتباطاً وثيقاً، عندما تتطلب هذه الأشخاص اهتماماً معززاً من منظور مخاطر الفساد أو العقوبات أو السمعة أو غيرها من المخاطر.

2.7. العقوبات

العقوبات تعني التدابير التقييدية الاقتصادية أو الملاية أو التجارية أو الشخصية أو الإقليمية أو غيرها، المفروضة من قبل الدول أو المنظمات الدولية أو السلطات المختصة، أو المطبقة من خلال شركاء الشركة.

2.8. الولاية القضائية المحظورة

الولاية القضائية المحظورة تعني دولة أو إقليماً أو منطقة تقيد الشركة أو تحظر تقديم الخدمة بشأنها بسبب القانون أو العقوبات أو ارتفاع مخاطر AML أو متطلبات الشركاء أو قواعد إدارة المخاطر الداخلية أو ظروف أخرى.

لا يلزم بالضرورة نشر قائمة الولايات القضائية المحظورة في هذه السياسة، وقد تحدد في واجهة المنصة، أو القواعد الداخلية للشركة، أو مستندات الشركاء، أو إشعارات منفصلة.

2.9. النشاط المشبوه

النشاط المشبوه يعني عملية أو سلوكاً أو مصدر أموال أو معاملة P2P أو عنواناً أو طريقة دفع أو حساباً أو عاملا آخر قد يشير إلى غسل الأموال، أو تمويل الإرهاب، أو التهرب من العقوبات، أو الاحتيال، أو النصب، أو استخدام بيانات الغير، أو تعدد الحسابات، أو نشاط غير قانوني، أو أي مخاطر أخرى غير مقبولة.

2.10. Red flags / مؤشرات التحذير

Red flags تعني علامات أو مؤشرات قد تدل على ارتفاع المخاطر أو الحاجة إلى مراجعة إضافية.

3. تنظيم ضوابط AML/KYC

3.1. الأشخاص المسؤولون

يجوز للشركة تعيين شخص مسؤول أو فريق مسؤول عن تنفيذ إجراءات AML/KYC، وإدارة المخاطر، ومراقبة المعاملات، ومراجعة الأنشطة المشبوهة، والتفاعل مع السلطات المختصة، وصيانة القواعد الداخلية.

3.2. القواعد الداخلية

تطور الشركة وتطبق قواعد داخلية، وتعليمات، ومعايير مخاطر، وred flags، وإجراءات تحقق، وحدوداً، وسيناريوهات مراقبة، وقواعد اتخاذ القرار.

تعد هذه المستندات الداخلية معلومات سرية للشركة ولا تخضع للإفصاح للمستخدمين إذا كان هذا الإفصاح قد يضر بفعالية الضوابط، أو أمن المنصة، أو الامتثال للقانون، أو حقوق الأطراف الثالثة، أو مصالح التحقيق.

3.3. تحديث الإجراءات

يجوز للشركة تحديث إجراءات AML/KYC مع مراعاة:

- التغييرات في التشريعات؛
- المنتجات والوظائف الجديدة؛
- مخططات الاحتيال الجديدة؛
- توصيات FATF وغيرها من المعايير الدولية؛
- متطلبات الشركاء؛
- نتائج المراجعات الداخلية؛
- حوادث الأمن؛
- التغييرات في أنظمة العقوبات؛
- الأنماط الجديدة لغسل الأموال وتمويل الإرهاب.

4. تقييم المخاطر

4.1. تقييم المخاطر العام

يجوز للشركة إجراء تقييم منتظم لمخاطر AML/KYC المتعلقة بالمنصة، والمستخدمين، والمنتجات، والأصول الرقمية، والولايات القضائية، وقنوات الوصول، ومعاملات P2P، وطرق الدفع، والعمليات بالعملات الورقية خارج P2P، وشبكات البلوكشين، ومقدمي الخدمات.

4.2. عوامل المخاطر

عند تقييم المخاطر، يجوز للشركة أن تأخذ في الاعتبار:

- بلد إقامة المستخدم أو جنسيته أو موقعه أو الجغرافيا المستندة إلى IP؛

- نوع الحساب وطريقة التسجيل؛
- سجل العمليات؛
- مبلغ العمليات وتكرارها؛
- الأصول الرقمية والشبكات المستخدمة؛
- عناوين البلوكشين للمرسلين والمستلمين؛
- ارتباط العناوين بالاختلاطات، أو أسواق الدارك نت، أو الاختراقات، أو ransomware، أو مشاريع scam، أو العناوين الخاضعة للعقوبات، أو غيرها من المصادر عالية المخاطر؛
- استخدام معاملات P2P؛
- طرق الدفع بالعملات الورقية المختارة؛
- السلوك في النزاعات؛
- الشكاوى من المستخدمين الآخرين؛
- تعدد الحسابات أو الارتباط بحسابات محظورة سابقاً؛
- استخدام VPN أو proxy أو وسائل أخرى لإخفاء الموقع؛
- رفض تقديم المعلومات؛
- عدم اتساق البيانات؛
- حالة PEP؛
- التطابق مع العقوبات؛
- adverse media وغيرها من عوامل السمعة؛
- متطلبات الشركاء والسلطات المختصة.

4.3. فئات المخاطر

يجوز للشركة تعيين فئات مخاطر داخلية للمستخدمين أو العمليات أو العناوين أو المعاملات، مثل مخاطر منخفضة أو متوسطة أو عالية أو غير مقبولة.

قد تؤثر فئة المخاطر على:

- الوظائف المتاحة؛
- الحدود؛
- الحاجة إلى KYC؛
- الحاجة إلى EDD؛
- سرعة معالجة العمليات؛
- إمكانية السحب؛
- الوصول إلى P2P؛
- الحاجة إلى مراجعة يدوية؛
- احتمال التجميد أو رفض الخدمة.

لا تلتزم الشركة بالإفصاح للمستخدم عن فئة المخاطر الداخلية أو منهجية الحساب أو المعايير الدقيقة أو نتائج التقييم.

5. KYC/CDD: التحقق من المستخدمين

5.1. النهج العام

لا تطلب الشركة التحقق الكامل من KYC من جميع المستخدمين افتراضياً، ما لم ينص القانون أو الواجهة أو متطلبات الشركاء أو وظيفة معينة على خلاف ذلك. يطبق التحقق على أساس قائم على المخاطر.

5.2. متى قد يكون KYC مطلوباً

يجوز للشركة طلب KYC أو معلومات إضافية في الحالات التلاية:

- الوصول إلى الحدود؛
- عملية كبيرة؛
- عملية غير معتادة؛
- نشاط مشبوه؛
- فتح نزاع؛
- طلب سحب؛
- تطابق AML متعلق بعنوان أو معاملة؛
- ارتباط بولاية قضائية علاية المخاطر؛
- استخدام وظيفة عملة ورقية خارج P2P؛
- متطلب من شريك دفع أو بنك أو مزود صرف أو مزود AML/KYC؛
- طلب من سلطة مختصة؛
- استعادة الوصول إلى الحساب؛
- الاشتباه في تعدد الحسابات أو الاحتيال أو استخدام بيانات الغير؛
- ظروف أخرى تتطلب التحقق.

5.3. البيانات التي قد تطلب

وفقاً لمستوى المخاطر، يجوز للشركة طلب:

- الاسم الأول، واسم العائلة، والاسم الأبوي أو أي اسم كامل آخر؛
- تاريخ الميلاد؛
- الجنسية؛
- بلد الإقامة؛
- عنوان السكن؛
- البريد الإلكتروني؛
- رقم الهاتف؛
- وثيقة الهوية؛
- صورة، أو صورة ذاتية، أو تحقق بالفيديو، أو فحص liveness؛
- إثبات العنوان؛
- إثبات مصدر الأموال؛
- إثبات مصدر الثروة؛
- تأكيد غرض العملية؛
- كشف حساب أو إيصال أو مستند أو تأكيد دفع؛
- مستندات متعلقة بمعاملة P2P؛
- معلومات حول الارتباط بـ PEP؛
- مستندات أو توضيحات أخرى ضرورية لتقييم المخاطر.

5.4. التحقق من البيانات

يجوز للشركة التحقق من البيانات المقدمة:

- يدوياً؛
- باستخدام أنظمة آلية؛
- من خلال مزودي AML/KYC خارجيين؛
- من خلال قوائم العقوبات وPEP؛
- من خلال المصادر المفتوحة؛
- من خلال تحليلات البلوكشين؛
- من خلال المعلومات المستلمة من الشركاء أو المستخدمين أو البنوك أو مزودي الدفع أو السلطات المختصة.

5.5. واجب المستخدم في التعاون

يجب على المستخدم تقديم المعلومات والمستندات المطلوبة في الوقت المناسب وبشكل دقيق وكامل.

إذا رفض المستخدم تقديم البيانات، أو قدم معلومات كاذبة أو متناقضة، أو لم يرد على الطلبات، أو حاول التحايل على التحقق، فيجوز للشركة تقييد الوظائف، أو تعليق العمليات، أو تجميد الأصول، أو إلغاء المعاملات، أو رفض الخدمة، أو إغلاق الحساب.

5.6. إعادة التحقق

يجوز للشركة طلب المستندات أو المعلومات مرة أخرى، حتى إذا كان المستخدم قد اجتاز التحقق سابقاً، إذا:

- تغيرت بيانات المستخدم؛
- انتهت صلاحية وثيقة الهوية؛
- تغير نشاط المستخدم؛
- ظهرت مخاطر جديدة؛
- وصل المستخدم إلى حدود جديدة؛
- أصبحت وظيفة جديدة متاحة؛
- تغيرت المتطلبات القانونية أو متطلبات الشركاء؛
- نشأ نزاع أو نشاط مشبوه.

6. العناية الواجبة المعززة EDD

6.1. متى يطبق EDD

يجوز للشركة تطبيق EDD إذا كان المستخدم أو العملية أو العنوان أو معاملة P2P أو الولاية القضائية أو السلوك يمثل مخاطر مرتفعة.

قد يطبق EDD، على وجه الخصوص، إذا:

- كان المستخدم PEP أو مرتبطًا بـ PEP؛
- كان المستخدم مرتبطاً بولاية قضائية علاية المخاطر؛
- كانت العملية كبيرة أو معقدة أو غير معتادة أو غير قابلة للتفسير اقتصادياً؛
- وردت الأموال من عنوان بلوكشين علاي المخاطر؛
- كانت العملية مرتبطة بلاخلاطات، أو أسواق الدارك نت، أو الاختراقات، أو ransomware، أو scam، أو عناوين خاضعة للعقوبات، أو red flags أخرى؛
- كان المستخدم يفتح النزاعات أو يخسرها بشكل متكرر؛
- ظهرت مؤشرات على تعدد الحسابات؛
- ظهرت مؤشرات على استخدام بيانات دفع أو حساب يخص الغير؛
- لم يتمكن المستخدم من شرح مصدر الأموال؛

- قدم المستخدم إجابات متناقضة؛
- كان التأكيد مطلوباً بناءً على طلب شريك أو سلطة مختصة.

6.2. تدابير EDD

قد يشمل EDD:

- طلب مستندات إضافية؛
- تأكيد مصدر الأموال؛
- تأكيد مصدر الثروة؛
- تأكيد غرض العملية؛
- فحص المصادر المفتوحة؛
- فحص adverse media؛
- تحليلا معمقاً لتاريخ البلوكشين؛
- تخفيض الحدود؛
- تجميداً مؤقتاً للأموال؛
- موافقة يدوية على العملية؛
- رفض العملية؛
- إنهاء الخدمة.

6.3. نتائج EDD

نتيجة لـ EDD، يجوز للشركة:

- السماح بالعملية؛
- السماح بالعملية مع حدود أو شروط؛
- طلب معلومات إضافية؛
- رفض العملية؛
- إعادة الأموال، إذا كان ذلك مسموحاً وممكناً؛
- تجميد الأموال؛
- تقييد الحساب؛
- إغلاق الحساب؛
- نقل المعلومات إلى السلطات المختصة عندما يكون ذلك مطلوباً أو مسموحاً به بموجب القانون.

7. KYT ومراقبة المعاملات

7.1. المراقبة العامة

يجوز للشركة إجراء مراقبة مستمرة أو انتقائية لعمليات المستخدمين، بما في ذلك:

- إيداعات الأصول الرقمية؛
- سحوبات الأصول الرقمية؛
- التحويلات الداخلية؛
- معاملات P2P؛
- العمليات بالعملات الورقية خارج P2P، إذا كانت هذه الوظائف متاحة؛
- محاولات العمليات؛

- العمليات الملغاة؛
- العمليات المتعلقة بالنزاعات أو الشكاوى.

7.2. تحليلات البلوكشين

يجوز للشركة استخدام تحليلات البلوكشين لتقييم مخاطر العناوين، والمعاملات، ومجموعات العناوين، ومصادر الأموال، والكيانات ذات الصلة.

قد يأخذ الفحص في الاعتبار الارتباط بـ:

- العناوين الخاضعة للعقوبات؛
- أسواق الدارك نت؛
- الخلاطات وخدمات الإخفاء؛
- ransomware؛
- الاختراقات والأموال المسروقة؛
- مشاريع scam؛
- مخططات الاحتيال؛
- الخدمات غير القانونية؛
- البورصات أو خدمات الصرف علاية المخاطر؛
- مصادر أخرى مرتفعة المخاطر.

7.3. مراقبة P2P

في معاملات P2P، يجوز للشركة تحليل:

- تكرار المعاملات؛
- مبلاغ المعاملات؛
- سلوك الأطراف؛
- عدد الإلغاءات؛
- عدد النزاعات؛
- الشكاوى؛
- إثباتات الدفع؛
- تطابق بيانات الدفع؛
- الروابط بين الحسابات؛
- مؤشرات تعدد الحسابات؛
- عدم اتساق بيانات الدفع؛
- محاولات نقل المعاملة خارج قواعد المنصة؛
- استخدام حسابات مصرفية أو بطاقات أو بيانات دفع تخص الغير.

7.4. الحدود والتأخيرات

يجوز للشركة وضع حدود أو تأخيرات أو مراجعات يدوية أو متطلبات إضافية لمستخدمين أو عمليات أو معاملات أو عناوين أو أصول أو طرق دفع أو ولايات قضائية معينة.

قد يتم تأخير العملية أو تعليقها حتى اكتمال المراجعة.

8. Red flags: مؤشرات النشاط المشبوه

قد تشمل red flags، من بين أمور أخرى:

- رفض المستخدم تقديم البيانات أو المستندات؛
- تقديم مستندات مزورة أو معدلة أو متناقضة؛
- استخدام بيانات أو بطاقات أو حسابات أو محافظ تخص الغير؛
- محاولة استخدام عدة حسابات؛
- الإلغاء المتكرر لمعاملات P2P؛
- النزاعات المتكررة في معاملات P2P؛
- إيصالات أو مستندات أو لقطات شاشة دفع مزورة؛
- عدم تطابق اسم الدافع مع المستخدم؛
- الإيداع والسحب السريع للأموال دون غرض اقتصادي واضح؛
- تقسيم العمليات إلى عدة مبلاغ صغيرة؛
- عمليات لا تتوافق مع السلوك المعتاد للمستخدم؛
- استخدام عناوين بلوكشين علاية المخاطر؛
- الارتباط بلاخلاطات أو أسواق الدارك نت أو الاختراقات أو ransomware أو scam أو العناوين الخاضعة للعقوبات؛
- زيادة حادة في حجم العمليات؛
- محاولات التحايل على الحدود؛
- استخدام VPN أو proxy أو وسائل أخرى لإخفاء الموقع بهدف التحايل على القيود؛
- ضغط عدواني على الطرف المقابل أو الدعم؛
- رفض شرح مصدر الأموال؛
- محاولة نقل معاملة خارج المنصة؛
- شكاوى من مستخدمين آخرين؛
- معلومات سلبية من المصادر المفتوحة؛
- تطابق مع مصادر العقوبات أو PEP أو adverse media.

لا يعني وجود red flag واحد دائماً حدوث مخلافة، لكنه قد يشكل أساساً لمراجعة إضافية أو تقييد عملية أو اتخاذ تدابير أخرى.

9. العقوبات والعلاقات المحظورة

لا تنشئ الشركة ولا تواصل علاقات مع المستخدمين إذا كان ذلك محظوراً بموجب القانون أو العقوبات أو متطلبات الشركاء أو قواعد إدارة المخاطر الداخلية.

يجوز للشركة رفض الخدمة أو تقييد الحساب أو تجميد الأصول أو إنهاء العلاقة إذا كان المستخدم:

- مدرجاً في قائمة عقوبات؛
- مرتبطاً بشخص مدرج في قائمة عقوبات؛
- موجوداً في ولاية قضائية محظورة؛
- يتصرف لمصلحة شخص محظور؛
- يستخدم المنصة للتهرب من العقوبات؛
- يرفض تقديم المعلومات اللازمة لفحص العقوبات.

يجوز للشركة إجراء فحوصات العقوبات عند التسجيل، أو قبل العملية، أو بعد العملية، أو عند تغيير قوائم العقوبات، أو عند فتح نزاع، أو عند سحب الأموال، أو في حالات أخرى.

10. النشاط المحظور

يحظر على المستخدم استخدام المنصة من أجل:

- غسل الأموال؛
- تمويل الإرهاب؛
- التهرب من العقوبات؛
- الاحتيال أو scam أو التصيد الاحتيلاي أو الهندسة الاجتماعية؛
- تداول الأموال أو الحسابات أو البطاقات أو المستندات أو البيانات الشخصية المسروقة؛
- استخدام بطاقات مصرفية أو حسابات أو محافظ أو بيانات دفع تخص الغير دون أساس قانوني؛
- الاتجار غير المشروع بلامخدرات أو الأسلحة أو المواد الخطرة أو غيرها من السلع المحظورة؛
- المقامرة غير القانونية؛
- الخدمات الملاية غير القانونية؛
- نشاط الدارك نت؛
- تمويل الأنشطة المتطرفة أو الإرهابية أو غيرها من الأنشطة المحظورة؛
- انتهاك حقوق الأطراف الثلاثة؛
- استخدام مستندات أو إيصالات أو مستندات دفع أو لقطات شاشة مزورة؛
- تعدد الحسابات والتحايل على القيود؛
- أي نشاط آخر تعتبره الشركة غير قانوني أو علاي المخاطر أو غير مقبول.

11. تدابير الشركة عند اكتشاف المخاطر

إذا اكتشفت الشركة نشاطاً مشبوهاً، أو مخاطر AML/KYC، أو مخاطر عقوبات، أو خرقاً لهذه السياسة، أو رفض المستخدم التعاون، فيجوز للشركة:

- طلب معلومات إضافية؛
- طلب KYC أو EDD؛
- تخفيض الحدود؛
- تأخير عملية؛
- رفض عملية؛
- إلغاء معاملة P2P؛
- تقييد وظائف P2P؛
- تجميد أو حجز الأصول؛
- تقييد السحوبات؛
- حظر الحساب مؤقتاً؛
- إغلاق الحساب؛
- إعادة الأموال إلى المرسل، عندما يكون ذلك ممكناً ومسموحاً وغير محظور قانوناً؛
- اقتطاع الرسوم المطبقة أو تكلايف الشبكة أو تكلايف الإرجاع عندما تنص قواعد المنصة على ذلك؛
- نقل المعلومات إلى السلطات المختصة عندما يكون ذلك مطلوباً أو مسموحاً به بموجب القانون؛
- اتخاذ تدابير معقولة أخرى لحماية المنصة، والمستخدمين، والشركاء، والشركة.

لا تلتزم الشركة بإخطار المستخدم مسبقاً بهذه التدابير إذا كان الإخطار قد يخلاف القانون، أو متطلبات AML/KYC/CTF، أو قواعد العقوبات، أو مصلاح التحقيق، أو أمن المنصة، أو حقوق الأطراف الثلاثة.

12. إعادة الأموال في حالة رفض AML/KYC

إذا تم رفض عملية أو تقييد الخدمة نتيجة مراجعة AML/KYC، فيجوز للشركة، حيثما كان ذلك ممكناً ومسموحاً، إعادة الأصول الرقمية إلى عنوان المرسل الأصلي أو إلى عنوان آخر تعتبره الشركة مقبولاا من منظور المخاطر والقانون.

قد تكون الإعادة مستحيلة أو مؤجلة إذا:

- كانت الأموال مرتبطة بعنوان خاضع للعقوبات؛
- كانت الأموال مرتبطة بنشاط إجرامي؛
- تم استلام طلب من سلطة مختصة؛
- قد تخلاف الإعادة القانون؛
- كان العنوان الأصلي غير متاح أو علاي المخاطر أو غير مناسب تقنياً؛
- كانت هناك حاجة إلى مراجعة إضافية؛
- كانت الأموال محجوزة أو مجمدة بلافعل أو مرتبطة بنزاع.

قد يتم اقتطاع رسوم الشبكة، ورسوم الخدمة، وتكلايف المعلاجة، وغيرها من التكلايف المطبقة من مبلغ الإعادة إذا نصت شروط الاستخدام أو صفحة الرسوم https://kashbi.net/information/fees أو واجهة المنصة أو قواعد منفصلة على ذلك.

لا يحدد مبلغ أي رسم أو تكلفة لهذه الإعادة في هذه السياسة، وقد يحدد في صفحة الرسوم https://kashbi.net/information/fees أو واجهة المنصة أو قواعد منفصلة، إذا كان هذا الرسم مطبقاً.

13. الإبلاغ والتفاعل مع السلطات

يجوز للشركة التفاعل مع السلطات المختصة، ووحدات الاستخبارات الملاية، وسلطات إنفاذ القانون، والمحاكم، والجهات التنظيمية، والبنوك، ومزودي خدمات الدفع، وغيرهم من الأشخاص المفوضين عندما يكون ذلك مطلوباً أو مسموحاً به بموجب القانون.

يجوز للشركة نقل معلومات عن المستخدم أو الحساب أو المعاملة أو معاملة P2P أو النزاع أو العنوان أو بيانات الدفع أو ظروف أخرى إذا:

- تم استلام طلب قانوني؛
- وجدت التزام بالإبلاغ عن نشاط مشبوه؛
- كان من الضروري الامتثال لمتطلبات العقوبات؛
- كان من الضروري حماية حقوق الشركة أو المستخدمين أو الأطراف الثلاثة؛
- كان ذلك مطلوباً لمنع الاحتيال أو غسل الأموال أو تمويل الإرهاب.

لا تلتزم الشركة بإخطار المستخدم بهذا النقل إذا كان الإخطار محظوراً بموجب القانون، أو قد يعيق التحقيق، أو يكشف إجراءات AML الداخلية، أو يخلق مخاطر أمنية.

14. الاحتفاظ بلابيانات والسجلات

تحتفظ الشركة بلابيانات والسجلات المتعلقة بـ AML/KYC، والمعاملات، ومعاملات P2P، والمراجعات، والنزاعات، والقيود، والإبلاغ، طوال المدة المنصوص عليها في القانون المعمول به، ومتطلبات الشركاء، وقواعد إدارة المخاطر الداخلية، وسياسة الخصوصية.

قد تشمل هذه البيانات:

- بيانات KYC؛
- مستندات المستخدم؛
- نتائج التحقق؛
- التطابقات مع العقوبات وPEP؛
- ملف المخاطر؛
- سجل العمليات؛
- عناوين البلوكشين؛
- txid/hash للمعاملات؛
- بيانات معاملات P2P؛
- إثباتات الدفع؛
- مواد النزاعات؛
- المراسلات مع الدعم؛
- القرارات الداخلية بشأن القيود؛
- سجلات طلبات السلطات المختصة.

لا يعني حذف الحساب أو سحب الموافقة أو إنهاء استخدام المنصة دائماً حذف بيانات AML/KYC فوراً، إذا كان الاحتفاظ بها مطلوباً أو مسموحاً به بموجب القانون أو قواعد AML/KYC/CTF أو لحماية حقوق الشركة أو حل النزاعات أو الامتثال لطلبات السلطات المختصة.

15. الأطراف الثلاثة ومقدمو الخدمات

يجوز للشركة الاستعانة بأطراف ثلاثة لتنفيذ إجراءات AML/KYC، بما في ذلك:

- مقدمو التحقق من المستندات؛
- مقدمو فحص liveness؛
- مقدمو فحص العقوبات؛
- مقدمو فحص PEP/adverse media؛
- مقدمو تحليلات البلوكشين؛
- شركاء الدفع؛
- البنوك، والمعالجات، ومزودو الصرف؛
- المستشارون القانونيون ومستشارو الامتثال والتدقيق؛
- مقدمو البنية التحتية والأمن.

يجوز وصف مقدمي الخدمات حسب الفئات دون أسماء محددة، ما لم يتطلب القانون أو العقد مع المزود أو سياسة منفصلة للشركة خلاف ذلك.

يجوز للشركة فحص الشركاء ومقدمي الخدمات من حيث العقوبات، والسمعة، والتراخيص، والتصاريح، والمخاطر، والقدرة على الامتثال لمتطلبات الأمن والسرية.

16. التزامات المستخدم

يتعهد المستخدم بما يلي:

- عدم استخدام المنصة في نشاط محظور؛

- تقديم معلومات صحيحة؛
- الرد في الوقت المناسب على طلبات الشركة؛
- تقديم المستندات والتوضيحات عند طلبها؛
- استخدام الأموال التي يملكها قانوناً فقط؛
- عدم استخدام بطاقات مصرفية أو حسابات أو محافظ أو بيانات دفع تخص الغير دون أساس قانوني؛
- عدم تقديم مستندات أو إيصالات أو لقطات شاشة أو مستندات دفع مزورة؛
- عدم التحايل على الحدود أو الفحوصات أو قيود العقوبات أو قواعد المنصة؛
- عدم إنشاء حسابات متعددة للتحايل على القيود؛
- الامتثال للقانون المعمول به؛
- تقييم قانونية عملياته في بلد إقامته بشكل مستقل.

قد يؤدي رفض التعاون، أو التهرب من التحقق، أو تقديم معلومات كاذبة، أو محاولة التحايل على ضوابط AML/KYC، إلى تقييد الخدمة أو إنهائها.

17. سرية إجراءات AML/KYC

يدرك المستخدم أن الشركة لا تفصح عن:

- معايير المخاطر الدقيقة؛
- red flags الداخلية؛
- حدود المراقبة؛
- خوارزميات التقييم؛
- مصادر بيانات AML؛
- تفاصيل التحقيقات؛
- أسباب تقديم تقرير إلى السلطات المختصة؛
- تفاصيل القرارات الداخلية؛
- المعلومات التي قد يؤدي الإفصاح عنها إلى مخالفة القانون أو الأمن أو فعالية ضوابط AML/KYC.

18. تغييرات السياسة

يجوز للشركة تعديل هذه السياسة في أي وقت. تنشر النسخة الحلاية على الموقع الإلكتروني https://kashbi.net أو في واجهة المنصة.

يشكل استمرار استخدام المنصة بعد نشر نسخة محدثة موافقة المستخدم على النسخة الجديدة من السياسة، ما لم ينص القانون المعمول به على خلاف ذلك.

19. النسخ اللغوية

يجوز نشر هذه السياسة بلالغة الروسية والكازاخية والإنجليزية ولغات أخرى.

إذا كان القانون المعمول به يتطلب أولوية نسخة لغوية معينة، فتطبق تلك النسخة. وفي جميع الحالات الأخرى، في حال وجود تعارض بين النسخ اللغوية، تكون النسخة الروسية هي السائدة.

20. جهات الاتصال

للاستفسارات المتعلقة بهذه السياسة، يمكن للمستخدم التواصل عبر:

- الشركة: F-Tech
- بلد التسجيل: Kazakhstan
- الموقع الإلكتروني: https://kashbi.net
- التطبيق: KashBi
- Email: legal@kashbi.net
- Telegram: kashbi_support
- العنوان القانوني: Al-Farabi Avenue, Apartment 207 44/1