Politics

KYC/AML/CTF

Approved by order No.4B24 dated February 12, 2024.
General Director Abdyrazakov Erkinbek Talipovich

Introduction

ZAO Biateks - company, registered in accordance with the Law on Virtual Assets of the Republic of Kyrgyzstan («**Company**», «**Biatex**», **"we", "our"**). This AML/KYC/CTF Policy ("**AML Policy**") establishes the rules and procedures that the Company follows to detect and prevent any financial crime.

The Company is firmly committed to preventing the use of its operations for money laundering or any activity that facilitates money laundering or the financing of terrorist or criminal activities.

The procedures are the responsibility of the Chief Compliance Officer and his team, collectively referred to as **Compliance Department**. The compliance department is tasked with monitoring compliance with relevant AML/CFT procedures.

In accordance with our AML policy, the Company does not work with Iran, Iraq, Sudan, South Sudan, Syria, North Korea, Republic of Seychelles, Bermuda, Belarus, Cuba, Crimea, Democratic Republic of Congo, Zimbabwe, USA, US territories: US Minor Outlying Islands, Puerto Rico, American Samoa, Guam, Northern Mariana Islands and US Virgin Islands (Santa Cruz, St. John and St. Thomas).

Protection measures

JSC Biatex has implemented protection measures that protect JSC Biatex from participation in any suspicious financial activities, by:

1. Carrying out KYC procedures in relation to Users – individuals and legal entities;
2. Conducting an enterprise-wide risk assessment to determine the Company's risk profile; 3) Implementation of internal procedures, policies and virtual control assets aimed at reducing the risks of money laundering and terrorist financing;
3. Conducting personnel training in the field of AML/CFT;
4. Conducting periodic AML checks;
5. Maintaining and updating information about Users;
6. Reporting suspicious transactions to the appropriate financial authority.

KYC measures

As part of user due diligence, the Company must:

1. Identify the User or his representative and verify the information provided with reliable, independent sources, including using virtual assets of electronic identification and trust services for electronic transactions;
2. Confirm the authenticity of documents and information provided by Users;
3. Investigate Users whose activities have been determined to be suspicious or risky;
4. Request additional and/or updated documents and information from Users when deemed necessary necessary for the Company;
5. Identify Users on an ongoing basis, even if Users have been identified in the past.

Risk factors and risk assessment

In order to conduct due diligence on users, the Company reserves the right to request documents and information, which include, but are not limited to:

1. Name (for individuals), business name and names of directors or others representatives (for legal entities);
2. Date of birth (for individuals), date of registration and company number (for legal entities). persons);
3. Country of residence/citizenship (for individuals)/registration address (for legal entities);
4. Residence address and document confirming residence address;
5. E-mail address;
6. State-issued identification card;
7. Source of virtual assets;
8. Any other document/information requested by the Company.

Levels of User Due Diligence

Levels checks perform the following functions:

1. Providing access to certain types of input and output of virtual assets;
2. Increasing limits on input/output of virtual assets.

The level of verification carried out on the User will affect the number of actions that the User can carry out on Biat Exchange.

KYC verification levels are an integral part of the Biatex AML policy and are available on the website.

Requested information

The requested information and documents form an integral part of the Biatex AML JSC Policy

Certain information will be automatically collected from documents provided by the User. The Company reserves the right to request any additional documents and/or information at any time.

Monitoring Requirements

The company constantly monitors activities to prevent money laundering and terrorism. financing and other illegal activities.
As part of the monitoring requirements, the Company must:

1. Check transactions on the Platform;
2. If necessary, request documents to update/confirm the information collected when submitting the application customer screening measures;
3. If necessary, indicate the source of the User’s virtual assets;
4. Pay special attention to transactions made by Users from high-risk countries.

Detection of suspicious activity

In the event that the Company detects suspicious transactions, as specified in its internal policies and procedures, it shall conduct further inquiries regarding the User's activity and request any additional documents that may be required.

JSC Biatex reserves the right to confirm your identity at any time in order to comply with Anti-Money Laundering Act or any other applicable law.

Reporting suspicious activity

In the event that the User has not provided information and explanation about the suspicious transaction, the full set of requested documents, or has submitted suspicious or unusual documents that the Company cannot verify, and the Company reasonably suspects that the User's actions may be related to money laundering, terrorist financing or other illegal activities, the Company reserves the right to suspend the account of a User suspected of such activity, at its discretion.

If you have additional questions regarding AML/KYC/CTF procedures carried out at Biatex JSC Users please contact us at