AML / KYC POLICY

DESCRIPTION

At Believe551 Ltd., a company incorporated and acting under the laws of the Republic of Seychelles ("*Website*", "*Service*", "*Believe*", "*Company*," "ourselves", "*we*" or "*us*") we are committed to the highest standards of anti-money laundering (the "*AML*") and counter-terrorism financing (the "*CTF*") practices. Our Anti-Money Laundering and Know Your Customer (the "*AML/KYC*") Policy (the "*Policy*" or "*AML/KYC Policy*") is designed to prevent our services from being used for illegal activities, ensuring compliance with relevant laws and regulations. This Policy outlines the steps we take to verify the identity of our clients (the "*Client*", "*you*" or "*your*") and monitor transactions to detect and prevent illicit activities.

Both international and local regulations require the Company to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its Clients.

If you are from any of the high-risk and non-cooperative jurisdictions listed on the website of Financial Action Task Force (FATF), you will not be allowed to register as a Client of this Website or use any service offered by our Website.

By accessing and using our Services and the Website, you acknowledge and declare that you are not located in, or are not a citizen or resident of USA, Afghanistan, North Korea, Crimea and Sevastopol, Democratic Republic of Congo, Eritrea, Libya, Somalia, South Sudan, Sudan, Yemen, Iran, Iraq, Cuba, Syria, Mali, Central African Republic, Guinea-Bissau, Lebanon, UK, countries of the European Union or any other country subject to United Nations Security Council Sanctions List and its equivalent.

We may change this AML/KYC Policy at any time without any notice, effective upon its posting on the Website. Your continued use of the Website and services shall be considered your acceptance to the revised AML/KYC Policy.

For law enforcement requests please direct your official document to our compliance team at: cooperation@believe.exchange.

1. MONITORING TRANSACTIONS

1.1. The purpose of transaction monitoring is to detect and prevent money laundering, terrorist financing, and other illicit activities by identifying and investigating suspicious activities and patterns within financial transactions. This section outlines the procedures and controls

established by us to monitor, detect, and report suspicious transactions in compliance with applicable laws and regulations.

1.2. This policy applies to all transactions conducted through our Services, including but not limited to currency exchanges. It covers all client accounts and activities to ensure comprehensive monitoring across the Company.

1.3. Procedures we implement to monitor the transactions conducted within the Services use are the following:

1.3.1. ***Risk-based approach:*** We apply a risk-based approach to monitoring, giving special attention to high-risk Clients and transactions.

1.3.2. ***Alert generation and review:*** We generate alerts for transactions that meet criteria indicative of suspicious activity, such as structuring, rapid movement of funds, and transactions with high-risk jurisdictions. We assign alerts to qualified compliance personnel for timely review and investigation.

1.3.3. ***Automated monitoring systems:*** We implement and maintain automated transaction monitoring systems to analyze and flag transactions based on predefined criteria and risk parameters. We systems are updated regularly to reflect current regulatory requirements and emerging typologies of illicit activities.

1.3.4. ***Suspicious activity reporting:*** We establish protocols for filing Suspicious Activity Reports (the "SARs") with the appropriate regulatory bodies within the required timeframes. We ensure all reported transactions are documented and filed in accordance with legal requirements and internal policies.

1.3.5. ***Investigative procedures:*** We develop and document procedures for investigating flagged transactions. This may include gathering additional information, analyzing transaction patterns, and interviewing relevant parties if necessary. We maintain thorough records of all investigations, including decisions made and actions taken.

1.3.6. ***Employee training:*** We provide ongoing training to employees involved in transaction monitoring to ensure they are aware of the latest typologies, regulatory requirements, and internal procedures. We also encourage a culture of vigilance and compliance throughout the Company.

1.3.7. ***Data Privacy and Security:*** We ensure that all transaction monitoring activities comply with data privacy and security laws and we implement respective measures to protect the confidentiality and integrity of data used in the monitoring process.

1.3.8. ***Continuous Improvement:*** We review and update transaction monitoring procedures and systems to adapt to new risks, technologies, and regulatory changes on a regular basis.

Also we conduct periodic audits and assessments of the transaction monitoring process to ensure effectiveness and compliance.

2. IDENTIFICATION AND VERIFICATION PROCEDURES

2.1. The main purpose of the identification and verification procedures (the "IVP") is to establish a framework for verifying the identity of Clients and beneficial owners, ensuring compliance with the AML and the KYC regulations. This section outlines the procedures to accurately identify and verify the identity of our Clients to prevent money laundering, terrorist financing, and other illicit activities.
The terms of this section will apply to all new and existing Clients, including individual and corporate clients, across all Services offered and provided by us. It also extends to beneficial owners, agents, and other relevant parties.

2.2. We implement the following procedures to conduct the identification and verification processes:

2.2.1. ***Client identification program (the "CIP")***: We implemented the CIP that mandates the collection of specific information from Clients before establishing a business relationship. The information required to complete the procedure includes, but is not limited to, full name, date of birth, address, and identification number (e.g., Social Security Number, Tax Identification Number).
2.2.2. ***Verification of identity***: We verify the identity of Clients using reliable and independent sources of information, documents, or data. Acceptable documents may include:

- Government-issued photo identification (e.g., passport, driver's license, national ID card);
- Utility bills, bank statements, or other documents confirming the Client's residential address.

2.2.3. ***Enhanced Due Diligence (the "EDD")***: We apply the EDD for high-risk Clients, transactions, and jurisdictions. EDD measures may include:

- Obtaining additional information on the Client and intended nature of the business relationship;
- Conducting more frequent and detailed ongoing monitoring of transactions;
- Verifying the source of funds and wealth.

2.2.4. ***Training and awareness***: We provide regular training to our employees on the IVP, including updates on regulatory changes and best practices. We promote a culture of compliance and vigilance in identifying and mitigating risks associated with Clients onboarding.

2.2.5. ***Record keeping:*** We maintain records of all identification information and verification documents for a minimum period as required by applicable laws and regulations. We ensure that records are easily accessible for regulatory inspections and audits.

2.3. Clients' identification information will be collected, stored, shared and protected strictly in accordance with our Privacy Policy https://believe.exchange/privacy-policy and related regulations.

2.4. Once the Client's identity has been verified, we are able to remove ourselves from potential legal liability in a situation where our Services are used to conduct illegal activity.

2.5. We may always contact the Clients to clarify the information given or ask for additional information which is needed for the IVP, or to address the risks of the case.

2.6. We may refuse to provide the service to the Clients without receiving additional information from them upon the respective request.

3. AUDITING AND REVIEW

3.1. The purpose of the auditing and review procedures is to establish a framework for the regular assessment and evaluation of the AML and the KYC. This ensures the effectiveness, adequacy, and compliance of the program with applicable laws, regulations, and internal policies. This section outlines the procedures for conducting audits, reviews, and ongoing assessments to identify and mitigate risks, enhance controls, and ensure continuous improvement.

3.2. We may conduct the following procedures related to the auditing and review:

3.2.1. ***Internal Audits:*** We conduct regular internal audits of the AML/KYC program to assess compliance with regulatory requirements, internal policies, and procedures. Our cover all areas of the program, including Clients onboarding, transactions monitoring, suspicious activity reporting, and employee training. We develop an audit plan that outlines the scope, objectives, and frequency of audits.
3.2.3. ***Risk-Based Auditing:*** We applied a risk-based approach to auditing, focusing on high-risk areas, Clients, transactions, and jurisdictions.
3.2.4. ***Audit Findings and Reporting:*** We document all audit findings, including identified deficiencies, areas of non-compliance, and recommendations for improvement. We prepare audit reports that summarize the findings and provide actionable recommendations.
3.2.5. ***Corrective Actions:*** We develop and implement corrective action plans to address audit findings and recommendations.
3.2.6. ***Regulatory compliance reviews:*** We conduct regular reviews to ensure compliance with the AML/KYC regulations and guidelines issued by regulatory bodies.
3.2.7. ***Employee Training and awareness:*** We provide ongoing training to employees on the importance of auditing and review processes and ensure they understand their roles and responsibilities in maintaining compliance and supporting audit activities.

4. COMPLIANCE OFFICER

4.1. The Compliance Officer is responsible for overseeing the implementation and enforcement of this AML/KYC Policy, ensuring that we comply with all relevant laws and regulations.

4.2. The main responsibilities of our Compliance Officer shall include but are not limited to the following:
4.2.1 Develop, implement and maintain this AML/KYC Policy and procedures;
4.2.2. Monitor transactions and Clients' activities for suspicious behavior;
4.2.3. Report suspicious activities to the appropriate regulatory authorities;
4.2.4. Coordinate internal audits of the AML/KYC program;
4.2.5. Address audit findings and implement corrective actions;
4.2.6. Ensure that our policies and procedures remain compliant with current regulations;
4.2.7. Conduct regular training sessions for our employees on the AML/KYC regulations and procedures.

4.3. Contact Compliance Officer is: cooperation@believe.exchange

5. CONTACT US

For any questions, concerns, or to report suspicious activities related to our AML/KYC policy, please contact us through the following channels:
EMAIL: cooperation@believe.exchange

Updated: 23 of December, 2024