AML POLICY

This document outlines Anti-Money Laundering and Know Your Customer Policy (the "AML/KYC Policy") of Service Provider. The AML/KYC Policy is designed to ensure that International Service Provider complies with international and local regulations related to preventing illegal activities, such as money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery. In accordance with these regulations, Service Provider has implemented internal procedures and mechanisms to prevent and mitigate the risks of being involved in any kind of illegal activity. The AML/KYC Policy outlines Service Provider compliance policies and procedures and reflects the company's commitment to preventing money laundering, terrorist financing, and other forms of illegal activities.

The AML/KYC Policy requires Service Provider to take action in case of any form of suspicious activity from its users, and to implement effective measures to prevent money laundering, terrorist financing, and other forms of illegal activities. Service Provider is committed to maintaining a culture of compliance and to fostering an environment that promotes transparency, integrity, and accountability in all of its activities.

1. Customer Identification Procedures

1.1. All customers who wish to use the service of Service Provider (hereinafter “We”) must complete a KYC verification process in accordance with our procedures.
1.2. The KYC verification process requires the submission of valid identification documents, including a government-issued ID, proof of address, and in some cases, a selfie or video for facial recognition purposes.
1.3. We reserve the right to reject any application if the KYC verification process is not completed to our satisfaction.
1.4. We maintain accurate and up-to-date customer identification records, including the customer's name, address, date of birth, and identification number.
1.5. We apply risk-based procedures to determine the level of verification required for each customer, based on factors such as the customer's transaction volume and country of residence.
1.6. We may perform additional verification procedures if we have reason to believe that a customer is engaging in suspicious or illegal activity.
1.7. We will maintain records of all customer identification procedures and ensure that they are stored securely and confidentially.
1.8. We will periodically review and update our customer identification procedures to ensure that they remain up-to-date with changing regulations and industry best practices.
1.9. We use third-party service providers to assist with the customer identification process, provided that they meet our standards for reliability and security.
1.10. We may request additional information or documentation from the customer as part of the KYC verification process, and may suspend or terminate the customer's account if the requested information is not provided or is determined to be insufficient or inaccurate.
1.11. The user undertakes to provide all the necessary information and documents for conducting AML and KYC checks within 30 (thirty) days from the day when your verification request has been received.
1.12. In case of failure to provide the requested information or documents within the specified period, the platform administration reserves the right to deactivate the user's account.
1.13. The user understands and agrees that deactivation of the account will lead to permanent blocking of access.

2. Risk Assessment Procedures

2.1. We perform a risk assessment of each customer based on factors such as the customer's country of residence, transaction volume, and other relevant information in accordance with the requirements of international and local legislation for KYC procedures and data collection.

2.2. We may apply enhanced due diligence procedures for higher-risk customers, including those who are politically exposed or involved in high-risk industries.

2.3. We will monitor customer transactions for suspicious activity, including but not limited to large or unusual transactions, transactions involving high-risk countries, and transactions that do not align with the customer's known profile according to the current threshold values of the risk level of regulators at the time of the audit

2.4. We use a risk-based approach to determine the level of due diligence required for each customer, based on the customer's risk profile.

2.5. We may use a variety of risk assessment tools and methods to identify and mitigate potential money laundering and terrorist financing risks, including but not limited to transaction monitoring systems, customer profiling, and external data sources.

2.6. We will periodically review and update risk assessment procedures to ensure that they remain up-to-date with changing regulations and industry best practices.

2.7. We may conduct additional due diligence procedures for customers who engage in high-risk activities, such as large transactions or transactions involving high-risk countries.

2.8. We will ensure that all staff members are aware of our risk assessment procedures and are able to apply them effectively in their roles.

2.9. We may suspend or terminate a customer's account if we have reason to believe that the customer is engaged in suspicious or illegal activity, or if the customer's risk profile changes significantly.

3. Record-Keeping Procedures

3.1. We maintain accurate and up-to-date records of all customer transactions, including the date, time, amount, and nature of the transaction.

3.2. We maintain customer identification records for a minimum of 5 years after the customer's account is closed.

3.3. We ensure that all customer records are stored securely and confidentially using third-party service providers.

3.4. We have appropriate controls in place to ensure the accuracy and completeness of all customer records.

3.5. We ensure that customer records are easily retrievable and can be provided to relevant authorities upon request.

3.6. We retain all records related to the reporting of suspicious activity, including SARs, for a minimum of 5 years.

3.7. We will periodically review and update our record-keeping procedures to ensure that they remain up-to-date with changing regulations and industry best practices.

4. Politically Exposed Persons (PEP)

4.1. We acknowledge that Politically Exposed Persons (PEPs) present a higher risk for money laundering and terrorist financing. Therefore, we apply enhanced due diligence measures to PEPs as part of our Know Your Customer (KYC) and Anti-Money Laundering (AML) policies.

4.2. Definition of a PEP. A PEP is an individual who holds, or has held, a prominent public position or role, both nationally and internationally. This can include:

a) Heads of state, heads of government, ministers, and deputy or assistant ministers.
b) Members of parliament or of similar legislative bodies.

c) Members of supreme courts, constitutional courts, or other high-level judicial bodies.
d) Members of courts of auditors or of the boards of central banks.
e) Ambassadors, chargés d'affaires and high-ranking officers in the armed forces.
f) Members of the administrative, management, or supervisory boards of state-owned enterprises.
g) Directors, deputy directors, or members of the board or equivalent function of an international organization.

4.3. We will not establish any business relationship with PEPs from high-risk countries in accordance with the FATF recommendations and lists of high-risk jurisdictions, or those identified by reputable sources as posing a high risk of money laundering or terrorist financing.

5. Cooperation and Information Requests

5.1. We recognize the importance of cooperating with relevant authorities and regulators to combat money laundering and terrorist financing. We have therefore developed a Law Enforcement Request Policy.

5.2. We recognize the importance of protecting the confidentiality of our clients' personal and financial information. When requested by law enforcement agencies, we will only disclose non- public information if we have received an enforceable court order, subpoena, or search warrant that has been validated as legitimate.

5.3. If we believe that we are legally required to provide a client's personal or financial information to a law enforcement agency, we will notify the affected client, unless we are prohibited by law from doing so.

5.4. Only the information that is specifically requested and clearly outlined in an enforceable court order, subpoena, or search warrant will be disclosed. We will maintain appropriate records of all requests and responses, including the nature of the request, the identity of the requesting party, and the information provided.

5.5. This policy is intended for informational purposes only and does not constitute legal advice or a guarantee that we will respond to any requests for information in a specific manner or timeframe. All requests for information will be evaluated on a case-by-case basis, in accordance with applicable laws and regulations.

5.6. We reserve the right to modify this policy or these guidelines at any time, at our sole discretion.

5.7. When requesting confirmation of the existence of data on our platform, law enforcement agencies must provide specific details about the information they are seeking, as we may not be able to respond to vague, ambiguous, or blanket requests. Certain identifiers may be useful in determining whether we possess the requested information. We will make all reasonable efforts to provide the requested information in a timely manner, subject to applicable laws and regulations.