Last updated: *December, 2024*

AML AND CUSTOMER IDENTIFICATION POLICY

Ensuring the safety and security of our customers (hereinafter the "**Customers**", "**you**" or "**your**") and our business operations is a top priority at Spika Ltd, a company registered in accordance with the laws of the Republic of Seychelles (hereinafter the "**Spika**", "**Company**", "**we**", "**us**", "**our**", "**Services**" or "**Site**"). Our Anti-Money Laundering (hereinafter the "AML") and Customer Identification (hereinafter the "**CI**") Policy (hereinafter the "**AML/CI Policy**" or "**Policy**") is integral to this commitment.
By implementing rigorous identification and verification processes, we aim to create a secure environment that protects both our clients and our Company from the risks associated with money laundering and terrorist financing.

The Company reserves the right to change or modify this Policy at any time and at its sole discretion, and the Company will provide the notice of the changes by posting the revised Policy on the Site and changing the "Last updated" date at the top of the Policy, and the updated Policy will be effective at such time.

1. COMPLIANCE STANDARD

1.1. The Company is committed to complying with all applicable AML laws and regulations. This Policy outlines the procedures and controls in place to detect, prevent, and report potential money laundering activities. It also sets forth the requirements for the CI and verification to ensure the legitimacy of its Customer base.

1.2. The Customer acknowledges that the Company does not provide its Services on the Site to customers from the following list of countries: North Korea, Central African Republic, Cuba, Crimea and Sevastopol, Afghanistan, Democratic Republic of Congo, Eritrea, Libya, Somalia, South Sudan, Sudan, Yemen, Iran, Iraq, Syria, Mali, Guinea-Bissau, Lebanon, USA, UK, countries of the European Union or any other country subject to United Nations Security Council Sanctions List and its equivalent (hereinafter the "Prohibited Jurisdictions").

1.3. Customers from any of the high-risk and non-cooperative jurisdictions provided on the website of Financial Action Task Force (hereinafter the "FATF") are prohibited from registering as the Customer of the Site and/or use any Services provided by the Company.

2. POLICY STATEMENT

2.1. The Company maintains a rigorous AML program designed to protect the organization from being used to facilitate money laundering and terrorist financing. This program includes, but is not limited to, the following key elements:

- Customer Identification Program ("CIP");
- Ongoing Monitoring of Transactions;

- Risk Assessment Procedures;
- Record Keeping;
- Reporting Suspicious Activities;
- Training and Awareness.

3. TRANSACTIONS MONITORING

3.1. The Company has implemented a comprehensive and multi-layered approach to transaction monitoring and reporting, ensuring the detection, investigation, and reporting of suspicious activities that may indicate money laundering, terrorist financing, or other illicit activities. This section outlines detailed procedures.

3.2. The Company utilizes automated monitoring systems designed to provide real-time surveillance of customer transactions.

3.3. In addition to automated systems, the Company conducts periodic manual reviews to ensure comprehensive oversight. Manual review procedures may include: (i) random sampling, (ii) targeted investigations, and (iii) exception handling.

3.4. The Company has established clear protocols for the prompt reporting of suspicious activities to the relevant regulatory authorities. Company's reporting procedures may include: (i) suspicious activity reports ("SARs"), (ii) internal escalations, and (iii) timely reporting.

3.5. The Company maintains the confidentiality of reports and protects customer information. Company's employees are strictly prohibited from informing Customers or any third parties about the filing of SARs or ongoing investigations. The Company ensures that all Customer data and transaction records are stored securely, with access limited to authorized personnel only.

4. CUSTOMER IDENTIFICATION

4.1. Company's CI is a critical component of its AML compliance. The program ensures that we know our customers and understand their financial activities. The key components of our CIP include:

- **Customer Identification and Verification*:*** The Company requires all customers to provide valid identification documents prior to the establishment of a business relationship. Acceptable documents include government-issued photo IDs, passports, and other legally recognized forms of identification;

- **Enhanced Due Diligence (EDD):** For higher-risk customers, additional information and verification steps are required. This may include obtaining information on the source of funds, the purpose of the account, and the nature of the customer's business;

- **Ongoing Due Diligence:** The Company continuously monitors and updates customer information to ensure its accuracy and relevance.

5. RISK ASSESSMENT AND MANAGEMENT

5.1. The Company conducts regular risk assessments to identify and mitigate potential money laundering risks. Our risk management framework includes:

- **Customer Risk Profiling:** the Company classifies Customers based on risk factors such as geography, industry, transaction patterns, and account types;

- **Periodic Reviews:** the Company regularly reviewing and updating risk profiles and controls to address emerging threats and vulnerabilities;

- **Employee Training:** the Company ensures all employees are trained on AML regulations, recognizing suspicious activities, and the procedures for reporting them.

6. RECORD KEEPING

The Company maintains comprehensive records of Customer information, transactions, and AML activities in accordance with regulatory requirements. This may include:

- **Customer Records:** the Company retains identification and verification documents for a minimum of five years after the termination of the customer relationship;

- **Transaction Records:** the Company keeps detailed records of all transactions for at least five years from the date of the transaction;

- **AML Documentation:** the Company maintains documentation related to risk assessments, training programs, and suspicious activity reports for at least five years.

7. TRAINING AND AWARENESS

7.1. A well-informed and vigilant workforce is essential for the effective implementation of this Policy. The Company is committed to providing comprehensive training and fostering awareness among all employees to ensure compliance with AML regulations and to detect and prevent potential money laundering activities.

7.2. Company's training program is structured to provide employees with the necessary knowledge and skills to recognize and report suspicious activities. The key components of our training program include:

- **Initial Training:** All new employees, regardless of their role, receive mandatory AML training as part of their onboarding process. This training covers the basics of money laundering, regulatory requirements, and the Company’s policies and procedures;

- **Role-Specific Training:** Employees in higher-risk roles, such as those in customer-facing positions, compliance, finance, and auditing, receive additional, more detailed training tailored to their specific responsibilities;
- **Ongoing Training:** All employees are required to participate in annual refresher training sessions to stay current with evolving AML regulations, emerging risks, and changes to internal policies and procedures.

7.3. The Company continuously monitors and evaluates the effectiveness of our training program to ensure it meets regulatory requirements and addresses emerging risks.

7.4. In addition to formal trainings the Company actively promotes AML awareness throughout the organization via: (i) internal communications, (ii) awareness campaigns and (iii) management support.

8. COMPLIANCE SUPERVISOR

8.1. The Compliance Supervisor holds a vital position within our Company, responsible for ensuring the effective implementation and oversight of this Policy. This section outlines the responsibilities, authority, and expectations for the Compliance Supervisor to maintain the highest standards of regulatory compliance and organizational integrity.

8.2. The Compliance Supervisor is appointed by the Company's management and possesses: (i) expertise in AML Regulations, (ii) applicable experience, (iii) professional certifications.

8.3. Primary responsibilities of the Company's Compliance Supervisor include the following:

8.3.1. Oversee the implementation of CI and verification procedures, ensuring thorough and accurate Customer due diligence;

8.3.2. Develop, implement, and regularly update the Company's AML/CI Policy to ensure compliance with current regulations and best practices;

8.3.3. Oversee the implementation of the CI and verification procedures, ensuring thorough and accurate Customer due diligence;

8.3.4. Coordinate the internal reporting of suspicious activities and ensure timely filing of the SARs with the appropriate regulatory authorities;

8.3.5. Conduct regular risk assessments to identify and mitigate potential AML risks, including periodic reviews of high-risk Customers and transactions;

8.3.6. Develop and deliver AML training programs for all employees, ensuring they are well-informed about their roles and responsibilities in detecting and preventing money laundering;

8.3.7. Ensure that all required AML records are maintained accurately and retained for the appropriate periods as mandated by regulations;

8.3.8. Coordinate internal audits and reviews of the AML program, addressing any deficiencies and implementing corrective actions as necessary;

8.3.9. Serve as the primary point of contact with regulatory authorities for all AML-related inquiries, examinations, and reporting obligations;

8.3.10. Regularly report to senior management and the board of directors on the status of the AML program, including significant issues, compliance risks, and areas for improvement.

8.4. The Compliance Supervisor has an authority to: (i) access the information collected by the Company during the CI and verification procedures, (ii) make applicable decisions related to this Policy and AML compliance, and (iii) implement respective controls.

8.5. The Company's Compliance Supervisor is: exchange@spika.io.

9. INTERNAL CONTROLS AND AUDIT

9.1. The Company has established internal controls to ensure compliance with AML policies and procedures. Such controls include:

Internal Reviews: Periodic internal reviews and assessments to identify areas for improvement and ensure adherence to Company's Policies.

Independent Audits: Conducting regular independent audits of our AML program to assess its effectiveness and compliance with regulatory standards.

10. CONTACT

10.1. If you have any questions related to this Policy, your rights and obligations arising from this Policy, please contact us via exchange@spika.io.