ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

***Last Updated**: January 27, 2025*

Softchet Inc., a service provider registered under the laws of the of the Republic of Panama (the "**Company**", "**we**" or "**us**"), is committed to upholding the highest standards of anti-money laundering (the "**AML**") and counter-terrorist financing (the "**CTF**") practices. This AML and CTF policy (the "**AML/CTF Policy**" or "**Policy**") outlines our dedication to preventing financial crimes and ensuring compliance with «Ley 23 de 27 de abril de 2015 Que adopta medidas para prevenir el Blanqueo de Capitales, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva», and other applicable regulations.

1. Risk Assessment and Management Framework

1.1. We implement a comprehensive risk-based approach to identify, assess, and mitigate AML/CTF risks associated with our customers, products, services, and geographical locations.
1.2. Our risk assessment framework evaluates:

- Customer profiles and behavior;
- Product and service offerings;
- Transaction types and patterns;
- Geographical factors and jurisdictional risks.

1.3. Risk assessments are conducted annually in response to significant changes in our business or regulatory environment.

1.4. We apply enhanced due diligence measures for high-risk customers, including:

- Politically Exposed Persons (PEPs);
- Customers from high-risk jurisdictions;
- Customers engaged in high-risk industries or activities.

2. Customer Verification and Due Diligence

2.1. Our Know Your Customer (the "**KYC**") procedures are designed to verify customer identities and assess potential risks associated with their activities.
This KYC applies to transactions that are spotted by our scoring system as suspicious. We will collect certain customer identification information from each customer who passes KYC; utilize risk-based measures to verify the identity of each customer who passes KYC; record customer identification information and the verification methods and results; provide adequate KYC notice to customers that we will seek identification

information from to verify their identities. Based on the risk, and to the extent reasonable and practicable, we will proceed with the verification to the extent that we have collected all information needed in order to know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers.

2.1.1. Sum & Substance Ltd, being our third-party service provider, which entirely complies with our Privacy Policy in respect to processing the personal information of our customers will analyze the information we obtain to determine:

- whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies);
- whether the documents provided by the customers are valid and do not appear in the Specially Designated Nationals and Blocked Persons List or any other lists of sanctioned individuals.

2.1.2. We will verify the information within a reasonable time, depending on the nature of the account and risk level of transactions. We may refuse to complete a transaction before we have verified the information, or in some instances, when we need more time, we may, pend verification, restrict transactions and the associated account under suspicion. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Officer, freeze the funds and file a SAR in accordance with applicable laws and regulations.

2.2. We collect and verify customer information using reliable, independent sources, including:

- Government-issued identification documents;
- Proof of address (e.g., utility bills, bank statements);
- Source of funds documentation.

2.3. Enhanced Due Diligence (the "EDD") is applied to high-risk customers, including Politically Exposed Persons (the "PEP"), which includes:

- Obtaining additional identification documents;
- Verifying source of wealth and source of funds through:
    - Bank statements;
    - Tax returns;
    - Property ownership records;
    - Business financial statements;
- Conducting adverse media searches;
- Obtaining senior management approval for the business relationship;
- Implementing enhanced ongoing monitoring, including:
    - More frequent transaction reviews;
    - Regular updates of customer information;
    - Annual risk reassessment

PEPs are tracked through:

- Initial identification during onboarding using PEP databases and screening tools;
- Ongoing screening of the customer base against updated PEP lists;
- Monitoring of transactions and activities for patterns consistent with PEP status.

2.4. Customer information is updated and re-verified on a regular basis to ensure ongoing compliance with the AML/CTF requirements.

3. Compliance Oversight and Management

3.1. Our Compliance Officer is responsible for overseeing the implementation and enforcement of this policy. Their duties include:

- Supervising all aspects of AML/CTF activities;
- Collecting and verifying customer identification information;
- Establishing and updating internal policies and procedures;
- Monitoring transactions and investigating significant deviations;
- Implementing a robust records management system;
- Updating risk assessments regularly;
- Liaising with law enforcement and regulatory authorities.

3.2. The Compliance Officer is authorized to interact with law enforcement agencies involved in preventing money laundering, terrorist financing, and other illegal activities.

3.3. Regular internal audits are conducted to evaluate the effectiveness of our AML/CTF measures and identify areas for improvement.

4. Transaction Monitoring and Reporting

4.1. Transaction monitoring is an essential element of effective KYC procedures. We have an understanding of the normal and reasonable activity of the customer, ensuring that we have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. High-risk accounts have to be subjected to intensified monitoring. In case of sudden swaps of big amounts, these accounts can be flagged by the risk scoring system as low, medium, or high risk as stipulated in Section 8 of this Policy.

4.1.1. Know-Your-Transaction service is the real-time anti-money-laundering compliance solution for monitoring cryptocurrency transactions. As a result of its targeted approach, it empowered our compliance team to significantly speed up the detection of transactions with fraudulent funds involved.

4.2. We employ advanced systems to monitor transactions for suspicious activities, including:

- Unusual transaction patterns;
- Deviations from expected customer behavior;
- Customers requesting an exchange of untraceable cryptocurrencies;
- An ongoing investigation in regards to customers;
- The trading activity appears to be from higher-risk countries;
- Virtual asset transfers above the threshold set by the FATF guidelines;
- PEPs.

4.3. Our transaction monitoring system utilizes risk-based rules and machine learning algorithms to identify potentially suspicious activities.
4.4. The Compliance Officer promptly investigates suspicious transactions within 24 (twenty-four) hours of detection, and files Suspicious Activity Reports (the "SARs") with the relevant authorities within 3 business days.
4.4.1. The SAR filing process includes:

- Gathering all relevant transaction data and customer information;
- Documenting the reasons for suspicion;
- Completing the SAR form as required by local regulations;
- Submitting the SAR through the designated reporting channel

4.4.2. All the SAR-related documents, including internal reports, investigation notes, and copies of filed SARs, are securely stored for a minimum of 5 (five) years from the date of filing.
4.4.3. The company maintains strict confidentiality regarding SARs and prohibits tipping off customers about filed reports.
4.4. We maintain comprehensive records of all transactions, customer interactions, and compliance activities for a minimum of five years, as required by law.

5. Employee Training and Awareness

5.1. All employees undergo comprehensive AML/CTF training upon hiring and annually thereafter, with additional specialized training for high-risk roles.
5.2. Training programs cover:

- Regulatory requirements and obligations;
- Identification of suspicious activities;
- Internal reporting procedures;
- Customer due diligence processes;
- Record-keeping requirements.

5.3. Training materials are regularly updated to reflect regulatory changes, emerging risks, and industry best practices.

5.4. Employee understanding is assessed through regular testing and performance evaluations.

6. Prohibited Activities and Jurisdictions

6.1. We do not provide services to customers from high-risk jurisdictions as identified by the Financial Action Task Force (FATF) or countries subject to United Nations Security Council sanctions.

6.2. We maintain a list of prohibited countries, which currently includes: Afghanistan, Central African Republic, Cuba, Crimea and Sevastopol, Democratic Republic of Congo, Eritrea, Libya, Lebanon, North Korea, Somalia, South Sudan, Sudan, Yemen, Iran, Iraq, Syria, Mali, Guinea-Bissau, USA, countries of the European Union, United Kingdom and any other country subject to UN Security Council Sanctions.

6.3. We reserve the right to refuse or terminate services to customers engaged in suspicious or illegal activities.

7. Record Keeping and Audit Trail

7.1. We maintain detailed records of all AML/CTF activities, including:

- Customer identification and verification documents;
- Transaction records and monitoring alerts;
- Suspicious activity reports and investigations;
- Training records and employee assessments;
- Risk assessments and audit reports.

7.2. Our record-keeping practices ensure compliance with regulatory requirements and facilitate efficient auditing and reporting.

7.3. All records are securely stored and easily retrievable for a minimum of five years or as required by applicable laws.

8. Risk-Based Approach and Customer Risk Rating

9.1. The Company employs a risk-based approach to classify clients into low, medium, or high-risk categories.

8.2. Client risk rating is determined based on the following factors:

- Geographic location;
- Nature of business or occupation;
- Transaction patterns and volumes;
- Products and services used;

8.3. Risk Classification Criteria:

Low Risk:

- Individuals from low-risk jurisdictions;
- Predictable transaction patterns;
- Low-value transactions

Medium Risk:
an exchange of untraceable cryptocurrencies

- Customers from countries with average AML/CTF controls;
- Occasional high-value transactions;
- Use of higher-risk products or services

High Risk:

- ***an exchange of untraceable cryptocurrencies with high-value***
- PEPs or their close associates;
- Customers from high-risk jurisdictions;
- Customers from sanction country
- Complex corporate structures or trusts;
- Frequent high-value transactions;
- Involvement in high-risk industries (e.g., gambling, precious metals)

8.4. Risk assessment is conducted at onboarding and reviewed periodically or when significant changes occur in the customer's profile or activities.

9. Policy Review and Updates

9.1. This Policy is reviewed and updated annually or more frequently in response to regulatory changes or emerging risks.

9.2. All updates are communicated to employees and relevant stakeholders in a timely manner.

9.3. We may implement amendments without prior notification to the customers. Any changes to this Usage Policy will be reflected in an updated version on the Company's website, with a revised "Last Updated" date.

9.4. The Company conducts a comprehensive review of its AML/CTF policies, procedures, and controls:

- Annually, as part of the regular policy review process;

- Within three months of any major regulatory changes affecting AML/CTF obligations;
- Immediately following any significant AML/CTF incidents or identified weaknesses in the company's controls

These amendments strengthen our AML/CTF Policy by providing more detailed procedures for handling high-risk customers, improving our risk-based approach, enhancing corporate due diligence, and ensuring regular policy reviews. The updated policy demonstrates our commitment to maintaining robust AML/CTF practices in the rapidly evolving cryptocurrency industry.

For any questions regarding this Policy, please contact: info@softchet.com

By implementing this comprehensive AML/CTF policy, **Softchet Inc**., demonstrates its commitment to maintaining the integrity of the virtual asset ecosystem and combating financial crimes in accordance with the latest regulatory requirements.