AML AND KYC COMPLIANCE POLICY

Last Updated Date: January 27, 2025

Aura551 Ltd., a company registered in accordance with the laws of the Republic of Seychelles (the "*Company*", "*Aura*", "*we*" or "*us*)" is committed to the highest standards of anti-money laundering ("*AML*") and counter-terrorist financing ("*CTF*"). It is the policy of the Company (the "*Policy*" or "*AML/KYC Compliance Policy*") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Our Know Your Customer ("*KYC*") compliance procedures are designed to ensure that we conduct business with reputable customers (the "Customer", "you" or "your" involved in legitimate business activities.

We adhere to all relevant laws and regulations and implement robust policies and procedures to identify, assess, manage, and mitigate risks associated with money laundering and terrorist financing. Our employees are trained to recognize and report suspicious activities to ensure full compliance with the AML/KYC obligations.

We are dedicated to maintaining a culture of integrity and compliance, fostering a safe and secure business environment for our Customers, employees, and stakeholders.

If you have any questions related to the terms of this Policy, please contact by using the following details - hello@aura5.cc

1. COMPLIANCE OFFICER

1.1. The Compliance Officer is the person, duly authorized by us, whose duty is to ensure the effective implementation and enforcement of thus AML/KYC Compliance Policy. It is the Compliance Officer's responsibility to supervise all aspects of the Company's anti-money laundering and counter-terrorist financing, including but not limited to:

- Collecting Customers' identification information;
- Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations;
- Monitoring transactions and investigating any significant deviations from normal activity;

- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;
- Updating risk assessment regularly;
- Providing law enforcement with information as required under the applicable laws and regulations.

1.2. The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity.

1.3. The Compliance Officer of the Company is: hello@aura5.cc

.

2. MONITORING

2.1. We perform a variety of compliance-related tasks, including capturing data filtering, record-keeping, investigation management, and reporting in order to identify who our Customers are. System functionalities include:

(i) Daily check of Customers against recognized “black lists” (e.g. OFAC, UN, HMT, EU), aggregating transfers by multiple data points, placing Customers on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;

(ii) Case and document management.

With regard to the terms of this AML/KYC Compliance Policy, we will monitor all transactions and we reserve the right to:

- Ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
- Request the Customer to provide any additional information and documents in case of suspicious transactions;
- Suspend or terminate Customer’s Account when we have reasonable suspicion that such Customer engaged in illegal activity.

The above list is not exhaustive and the Compliance Officer will monitor Customers' transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

3. IDENTIFICATION AND VERIFICATION

3.1. One of the international standards for preventing illegal activity is Customer due diligence ("CDD"). According to CDD, we establish our own verification procedures within the standards of the AML and the KYC frameworks, including enhanced due diligence for Customers presenting a higher risk, such as: (i) Politically Exposed Persons (PEPs); (ii) the Customer is from a high-risk third country; or (iii) the Customer is from the territory that is considered a low tax rate territory.

3.2. Our identity verification procedure requires the Customer to provide:

for individuals:

- national ID,
- international passport,
- bank statement, utility bill,
- source of funds, etc.).

for business:

- registry certificate and proof of legal existence.
- Identification of the ultimate beneficial owners (UBOs) holding 25% or more of shares or exercising control.
- proof of business activity (license, operation permit, or equivalent document).
- financial statements or proof of the source of funds where applicable.
- tax identification number and fiscal residence.

For the AML/KYC purposes we reserve the right to collect Customer's identification information.

3.3. We conduct verification and request for additional information from higher-risk Customers. This may include obtaining obtaining information on the source of funds, the purpose of the account, and the nature of the customer's business the "Enhanced Due Diligence" 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

3.4. We will take steps to confirm the authenticity of documents and information provided by the Customers. All legal methods for double-checking identification information will be used and we reserve the right to investigate certain Customers who have been determined to be risky or suspicious.

3.5. We reserve the right to verify Customer's identity on an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular Customer). In addition, we reserve the right to request up-to-date documents from the Customers, even though they have passed identity verification in the past.

3.6. Customer's identification information will be collected, stored, shared and protected strictly in accordance with the terms of our Privacy Policy and related regulations.

3.7. Once the Customer's identity has been verified, we are able to remove ourselves from potential legal liability in a situation where its services are used to conduct illegal activity.

3.8. We may always contact the Customer to clarify the information given or ask for additional information which is needed for the Customer identification, or to address the risks of the case.

3.9. We may refuse to provide the service to the Customers without receiving additional information from the Customer upon the respective request.

4. RISK BASED APPROACH

4.1. The Risk-Based Approach ("RBA") is a foundational element of our AML/KYC Compliance Policy. It enables us to efficiently allocate resources to

areas where they are most needed, focusing on identifying and mitigating the highest risks of money laundering, terrorist financing, and other financial crimes.

4.2. We utilize a structured risk assessment framework to evaluate the risk levels associated with our Customers:
- the profile of its Customers;
- the geographic area in which it conducts business;
- the product or products that it deals in;
- the service or services that it provides or receives;
- the means by which such products or services are delivered;
- the transactions that it conducts;
- customer due diligence carried out by third parties;
- the technological developments in identifying such risks.

Low Risk:

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

Medium Risk:

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

High Risk:

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

4.3. We implemented specific controls and measures based on the assessed risk level, as well as, clear procedures for escalating high-risk issues to senior management or the Compliance Officer.

4.4. We evaluate the risk associated with countries based on factors such as regulatory environment, prevalence of corruption, and known terrorist activity.

4.5. We do not provide services either to Customers from the following list of countries: 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, UK, countries of the European Union or any other country subject to United Nations Security Council Sanctions List and its equivalent or to the Customers from any of the high-risk and non-cooperative jurisdictions listed on the website of Financial Action Task Force (FATF).

5. KYC/KYT

5.1. Our service carries out Know Your Transaction (KYT) verification first and foremost. In case of high risk transactions, we reserve the right to freeze funds until successful identity verification - Know Your Customer (KYC).

5.2. 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.

5.3. Know Your Customer (the “KYC”) procedures are designed to verify customer identities and assess potential risks associated with their activities.

5.4. 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.

5.5 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 STR in accordance with applicable laws and regulations.

6. AUDITING AND RECORD KEEPING

6.1. Auditing and record keeping are critical components of our AML/KYC Compliance Policy. These processes ensure that we maintain transparency, accountability, and adherence to regulatory requirements while effectively managing and mitigating risks associated with money laundering and terrorist financing.

6.2. Internal audits are conducted to evaluate the effectiveness and efficiency of our AML/KYC Compliance Policy, procedures, and controls. The objectives include ensuring compliance with regulatory requirements, identifying areas for improvement, and verifying the integrity of our risk management framework.

6.3. Internal audits are performed regularly, with the frequency determined by the level of risk and regulatory requirements. High-risk areas may be audited more frequently.

6.4. The audit process includes a comprehensive review of customer records, transaction monitoring systems, and compliance with due diligence procedures. Auditors also assess the adequacy of employee training and the effectiveness of our risk-based approach.

6.5. We maintain records of all AML/KYC-related activities for a minimum period as required by law, typically seven years. This includes records of customer identification, due diligence, transaction monitoring, and any reports of suspicious activity.

6.6. We maintain records of all STRs filed with regulatory authorities, including the rationale for filing and any supporting documentation.

6.7. Periodic reports on our AML/KYC compliance activities are prepared for regulatory authorities, as required by law.

6.8. Our record-keeping and auditing processes are reviewed regularly to ensure they remain effective and compliant with evolving regulatory requirements. Updates are made as necessary to enhance efficiency and effectiveness.

7. TRAININGS

7.1. Training is essential to ensure that all our employees understand their roles and responsibilities in preventing money laundering and terrorist financing.

7.2. All our employees complete AML/KYC training upon hiring and annually thereafter. Employees in high-risk roles receive additional, targeted training relevant to their specific duties.

7.3. Employees are regularly tested to ensure understanding and retention of training materials. Training programs are continuously updated based on employee feedback, regulatory changes, and industry best practices.

7.4. Comprehensive records of all training sessions, materials, and employee participation are maintained and reviewed regularly.

8. REPORTING AND ESCALATION

8.1 SUSPICIOUS TRANSACTION REPORT (STR) shall submit to the Financial Intelligence Unit within two business days of ascertaining the reasonable grounds, forming the suspicion or receiving the information. The Financial Intelligence Unit shall acknowledge receipt of the suspicious transaction report within 24 hours of its receipt.