Last updated:

AML / KYC POLICY

INTRODUCTION

CLOUDZONE PAYMENTS INC., a company incorporated and acting in British Columbia, Canada, (hereinafter – “Website”, “Service”, “CLOUDZONE”, “Company”, "we", "our" or "us") strives to protect our clients from any type of scams and fraudulent activities in the crypto world and complies to all rules and regulations present at the moment, and one of the ways that enables us to do so is the Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML/KYC Policy") procedure.

This AML/KYC Policy is designated to prevent and mitigate possible risks of the Company being involved in any kind of illegal activity.

This procedure confirms the full compliance carried out by you ("you", "your", "Customer") in front of the regulatory institutions. Therefore, you confirm that you are a law-abiding citizen and the state has no reason to address any claims towards you.

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

By accessing and using Company’s services and the Website, you acknowledge and declare that you are not located in, or are not a citizen or resident of USA and/or any country which is subject to the jurisdictions under increased monitoring according to FATF and/or any other country subject to Office of Foreign Assets Control and/or United Nations Security Council Sanctions List and its equivalent.

The Company 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: av@x-aura.com.

1. COMPLIANCE

1.1. Our company is committed to comply with all applicable anti-money laundering (AML) and counter-terrorist financing (CTF) regulations in Canada, including those set forth by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). We acknowledge that FINTRAC is Canada's financial intelligence unit and has been given

the mandate to enforce the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

1.2. To comply with FINTRAC regulations, we have established a comprehensive AML/KYC program that includes policies, procedures, and controls to prevent, detect, and report potential money laundering and terrorist financing activities. Our program includes:

- ***Customer identification procedures:*** We shall verify the identity of our customers using reliable and independent sources, in accordance with FINTRAC's requirements.
- ***Record-keeping:*** We shall maintain accurate and up-to-date records of our customers' identities and transactions, as required by FINTRAC.
- ***Reporting suspicious transactions:*** We shall promptly report any suspicious transactions to FINTRAC, as required by law.
- ***Training and awareness:*** We shall provide training and awareness to our employees and agents on AML/KYC matters, including FINTRAC regulations.

We understand that failure to comply with FINTRAC regulations may result in significant penalties and reputational harm. As such, we are committed to implementing effective AML/KYC controls and regularly review and updating our program to ensure ongoing compliance with all applicable regulations.

2. IDENTIFICATION AND VERIFICATION PROCEDURES

2.1. One of the important standards for preventing illegal activity is Customer due diligence (“CDD”). According to CDD, the Company establishes its own verification procedures within the standards of anti-money laundering and “Know Your Customer” frameworks, including enhanced due diligence for Customers presenting a higher risk, such as: (i) Politically Exposed Persons (PEPs); (ii) the Customers from a high-risk third country; or (iii) the Customers from the territory that is considered a low tax rate territory.

2.2. The Company's identity verification procedure requires the Customer to provide the Company with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, utility bill, source of funds, etc.) or in case of legal entities, in particular, the data and corporate documents showing the ultimate beneficial owner of such legal entity upon the Company's request.
For the AML/KYC purposes the Company reserves the right to collect Customer’s identification information.

2.3. The Company 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 the Company reserves the right to investigate certain Customers who have been determined to be risky or suspicious.

2.4. The Company reserves 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.

2.5. Customer's identification information will be collected, stored, shared and protected strictly in accordance with the Company's Privacy Policy and related regulations.

2.6. The Company is prohibited from transacting with individuals, companies and countries that are on prescribed sanctions lists. The Company will therefore screen against United Nations, European Union, UK Treasury and US Office of Foreign Assets Control (OFAC) sanctions lists in all jurisdictions in which we operate.

2.7. The Company 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.

2.8. The Company may refuse to provide the service to the Customers without receiving additional information from the Customer upon the respective request.

3. MONITORING TRANSACTIONS

3.1. Customers are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do). Therefore, the Company relies on data analysis as a risk-assessment and suspicion detection tool. The Company performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include:

(i) Daily check of Customers against recognized "black lists" (e.g. OFAC), 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 AML/KYC Policy, the Company will monitor all transactions and it reserves 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 the Company has 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.

4. RISK BASED APPROACH

4.1. The Company analyzing Customers and their behavior may undertake investigative efforts that are proportional to the risk and complexity of the case and collect evidence using observations gathered in the case.

4.2. If we identify any additional risks, we will need to conduct investigative research to understand these risks in the context of the case, and the additional documents may be required to support the review.

5. AUDITING AND REVIEW

We conduct regular audits of this AML/KYC program to ensure it is effective and up-to-date with the latest regulations. We also periodically review our policies and procedures to ensure they remain relevant and effective.

6. EMPLOYEE TRAINING

We provide regular training to our employees to ensure they are aware of our AML/KYC Policy and procedures and understand how to identify and report suspicious activities.

7. COMPLIANCE OFFICER

7.1. The Compliance Officer is the person, duly authorized by the Company, whose duty is to ensure the effective implementation and enforcement of the AML/KYC 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.

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

7.3. The Compliance Officer is: VENGLIUK ANDRII, whose registered office is located in 200 Old Carriege DR Kitchener On Canada N2P 1H1.