ANTI MONEY LAUNDERING POLICY.

Revised/Approved 26th February, 2025.

1.0. INTRODUCTION

1.1. We are a technology company that provides payments infrastructure through APIS solutions that enable businesses to receive and accept payments.

1.2. This AML/KYC policy is a procedural guideline on the following matters:

- Know Your Customer Verification Procedures
- Monitoring Transactions
- Compliance Officer
- Risk Assessment
- Transaction Reporting

- Cooperation with Regulators and Authorities
- Politically Exposed Persons(PEPs)
- Sanctions
- Record Keeping
- AML/FT Training
- AML/KYC Policy Audit and Review

1.3. This Policy provides safeguards to fight against all forms of financial crime, which includes money laundering, terrorism financing, bribery, and corruption. To this end, we created this Know Your Customer and Anti-Money Laundering Policy ("AML/KYC Policy") to articulate its stance to combat Money Laundering ("ML"), the Financing of Terrorism ("FT") and the Prevention of the Financing and Proliferation of Weapons of Mass Destruction.

2.0. APPLICATION

2.1. The AML/KYC Policy applies to us; our directors, officers, full-time, part-time, strategic partners, and anyone working on our behalf, e.g., consultants and representatives (collectively "Personnel", or the "Employees"). The AML/KYC Policy applies in all countries in which we operates or conducts business. Adherence to this AML/KYC Policy is a condition of employment and/or engagement with us, and therefore the Employees must acknowledge on an annual basis that they have understood the AML/KYC Policy and have disclosed any suspected and actual violations through appropriate channels.

2.2. The AML/KYC Policy will not give answers for every ethical or legal situation and the red flags annexed to this AML/KYC Policy is not exhaustive and the Compliance Officer will monitor customers' transactions on a day-to-day basis to define whether such transactions are to be reported and treated as suspicious. If Employees have any doubts about the right thing to do, they should seek advice from the Compliance Officer/the General Counsel, as appropriate.

2.3. This AML/KYC Policy sets out the key principles and obligations in relation to the AML/KYC Framework to identify and assess risk that we and our Employees become directly or indirectly involved in actual or potential money laundering activities, or terrorist financing activities to substantially prevent, manage, and mitigate these risks.

3.0. KNOW YOUR CUSTOMER ("KYC") PROCEDURES

3.1. We would conduct a Customer Due Diligence ("CDD") as a verification exercise on the information supplied before the registration of the customer is completed. We have partnered with Sumsub, a global identity verification service company that assists us to independently verify the data and documents supplied by a customer to mitigate fraud attempts and assist regulatory compliance. We will ensure that customers' information that is supplied, and or collected, is stored, shared, and protected in accordance with the companies Privacy Policy and related regulations.

3.2. Before the customer can be onboarded to use any of the companies' services, an individual customer shall provide the following Know Your Customer details:

a. Full name;

b. Date of birth;

c. Contact information such as phone number and email address;

d. Residential address;

e. Date of birth;

f. Occupation;

g. Valid means of identification (International Passport, National Identity Card, Driver's license);and

h. Other relevant information such as utility Bill, bank statement, selfie/video with or without the customer holding their ID Card.

3.3. Before the customer can be onboarded to use any of the companies' services, an institution, the customer shall provide the following Know Your Customer details:

a. Incorporation documents (certificate of incorporation, Memorandum and Articles of Association, certificate of good standing, proof of business, status report).The documents will disclose details of the ownership of the institution, its directors, trustees, and address;

b. Website(if any);

c. Contact details for the institution such as phone number and email address;

d. Object clause, principal business, description of sector of the institution; and

e. Identification of the beneficial owners of the institution; their name, date of birth (for an individual), address, social security number (for U.S customers) and Valid means of identification (passport, national identity card, Driver's license).

3.4. We reserve the right to request for further documentations such as video conference with beneficial owners in an institution may be requested for customers form high risk countries, customers deemed to be high risk or business operating in certain specialized, regulated, restricted high-risk sectors. A customer who does not meet the requirements would be denied access to the services provided by us during the creation of the business relationship or during its course.

3.5. We shall conduct a CDD exercise to investigate the information supplied by the customer to confirm the authenticity of the information and documents. KYC includes assessing the level of AML risk a customer could present. We will equally investigate the source of income and wealth of a customer before they are onboarded as well as while the

customer relationship exists based on documents, data or information obtained from reliable and independent sources. To this end, we shall use all legal methods to double check the identification information supplied by a customer and the employees shall take reasonable care to ensure that all documents supplied are original or true copies of the original.

3.6. Enhanced Due Diligence ("EDD") is applied prior to customer on boarding on high-risk customers who raise any of the red flags recognized by the company, Politically Exposed Persons ("PEPs"), and Cross border correspondent banking.

3.6. We on a non-going basis will monitor account activity for unusual size, volume, pattern, or type of transactions, considering risk factors and red flags that are appropriate to our business. Where a customer has been on boarded, we will apply its EDD in the following circumstances:

a. When the customer's trade volume increases or exceeds its assigned risk threshold;

b. Where there are unusual or suspicious patterns of activity on a customer account;

c. Where our verification exercise qualifies a customer as high risk;

d. Where a transaction request is not consistent with a customer's stated business activity; and

e. We would also apply EDD measures where the assessment of risk is assessed as higher, in accordance with our internal policies and procedures.

3.7. We reserve the right to investigate customers deemed high risk or suspicious. In addition, in any of the cases listed in clause 3.6 and 3.7 or where there shall be any doubt about the adequacy or veracity of previously obtained customers' identification data, further due diligence measures shall be undertaken to obtain additional documentation to prove a customer's identity, exact place of residence or business, education, occupation as well as source of funds the customer is using for the exchange.

3.8. The approval of the Managing Director and the Compliance Officer is required prior to establishing business relationships with persons and institutions in high-risk countries or PEPs. We reserve the right to verify customers identity on an ongoing basis and may request a customer to provide updated identification documents to verify the customers identification information particularly where the customers activity seemed suspicious (i.e., unusual for the customers risk profile).To keep a customer's information up to date, We reserve the right to request a renewed means of identification or utility bill (where necessary), even though the customer may have passed the identity verification exercise.

3.9. We take necessary and regulatory measures when creating a business relationship with Designated Non-Financial Businesses and Professionals ("DNFBP") and other prescribed businesses, in view of the perceived risk and in compliance with regulatory requirements. KYC includes requesting identification documents to identify who the (ultimate)

beneficial owner, Legal Representative, and Trustees as a reasonable measure to verify the ownership and control structure of such DNFBP.

3.10. When a customer's trade volume increases, the AML/FT risk increases as well. As a rule, the more money (or currency) a customer exchanges or intends to withdraw, the more information will be required about the customer and its source of funds.

3.11. The documents required as the AML/FT risks increase will be reviewed from time to time to reflect the changes in the legal requirements of countries and our improved knowledge and experiences on compliance requirements.

3.12. All assets derived from fraudulent transactions and/or suspicious activity maybe seized and forfeited with such transactions being referred to the appropriate authorities.

3.13. We ensure that due diligence measures/investigations performed are documented and kept on file.

4.0. TRANSACTION MONITORING

4.1 Customers are known by verifying their identity (information on who they are) and by analyzing their transactional patterns (information on what they do).Thus, we rely on data analysis as a risk assessment and suspicious detection tool. We perform transaction monitoring of AML/FT risks in accordance with our risk-based approach.

4.2 We conduct a variety of compliance related tasks, including capturing & updating customer data, filtering, transaction investigation reporting and management. Transaction monitoring includes:

a. Daily screening against recognized "Blacklists" (e.g., Office of Foreign Assets Control, US ("OFAC"), EU Sanctions amongst others) aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal reports, and filing statutory reports, if applicable.

b. Wallet related transactions screening.

c. Customer risk profile to ensure transactions/activities.

d. Investigation report management.

4.3. A daily ongoing screening and scrutiny of transactions is conducted as part of our transaction monitoring procedure to ensure that each transaction is consistent with the knowledge of the customer, their business, the nature of the transaction, red flags in our AML/KYC policy and source of funds where necessary.

4.4. All Employees endeavor to avoid carrying out a transaction which they know or suspect or have reasonable grounds to suspect to be related to money laundering.

All suspicious/unusual transactions, such as personal data changes, payments or withdrawals, or activities potentially linked to money laundering, which are identified by

employees are immediately escalated to the Compliance Officer for further investigation and filing of statutory reports to the appropriate authorities, if applicable.

4.5. Internal reports are done by an internal suspicious/unusual transaction report which includes full details of the person or institution involved, full details of transaction and nature of each person's involvement, suspected type of money laundering activity with exact basis for the suspicion, dates of the transaction, amount involved and any other information that may be useful for the investigation of the report.

4.6. The Compliance Officer shall maintain an internal log with information on unusual transactions, the investigations carried out for each report received and the outcome of such investigation, including whether the instance was reported to the Financial Transactions and Reports Analysis Center ("FINTRAC") or any other regulatory authority or not.

5.0. COMPLIANCE OFFICER

5.1. The Compliance Officer is duly authorized to monitor and enforce compliance with the AML/KYC Policy. It is the Compliance Officer's responsibility to develop and execute mitigation actions in respect of all AML/FT issues arising from a particular customer/transaction, including but not limited to:

a. Monitoring customers' identification and virtual currency wallet addresses against recognized virtual currency wallet associated with recognized sanctions.

b. Monitoring transactions and investigating unusual activities which significantly deviate from normal activity.

c. Ensure compliance with all relevant laws, regulations, rules, and professional standards set by Regulators with the support from the Board and Employees.

d. Advice the Board of emerging statutory and regulatory compliance issues to guide in the establishment of control to mitigate risks.

e. Develop, implement, and administer all aspects of our statutory and regulatory compliance program.

f. Ensure training of employees on AML/FT framework while ensuring compliance with all AML reporting requirements of varying Regulatory agencies.

g. Review and approve escalated suspicious transactions with a view to escalating to the appropriate authorities (if required).

h. Review of our AML/KYC Policy.

i. Regularly update the risk assessment framework.

6.0. RISK ASSESSMENT

6.1. We adopt a risk-based approach towards assessing and combating financial crime risks arising from any transaction it has with a customer. It uses all available data when reviewing customer activity. Thus, we proactively perform a risk based due diligence to identify and assess a customer's risk profile by collecting necessary information and documentation on each prospective customer before entering a customer relationship.

6.2. A risk assessment is to be conducted on customers to confirm that the identity of the customer does not match with a known blocked virtual currency asset address, criminal background, sanctioned institutions or banned entities such as terrorist organizations. Enhanced due diligence is required for customers who are determined to be high risk, particularly those for whom the nature (source of funds) is unclear, and for unusually large transactions with high frequency which can be determined by at its discretion.

6.3. As far as reasonably possible, all unusual patterns of transactions, which have no apparent economic or lawful purpose, are examined to determine whether those transactions or activities appear suspicious. For identification, assessment and examination of risks related to its activities, we have established a risk assessment, considering the customer risk profile, geographical risk, and delivery channel risk.

6.4. The risk profile of an existing customer is revised periodically upon acquiring more knowledge of the customer, its transactions, and its activities.

6.5. We reserve the right to refuse to onboard a customer where requested identification documents are not supplied, impose terms under which a customer may conduct transactions while we attempt to verify a customer's identity, close an account after attempts to verify a customer's identity fail and determine whether it is necessary to file a report to the appropriate authorities in accordance with applicable laws and regulations. We equally reserve the right to cease, suspend or block transactions made to exchange a virtual currency where it actively attempts to hide the nature of the transaction, the beneficiary, or the source of funds for the transaction.

7.0. TRANSACTION REPORTING

7.1. Regulatory and Statutory requirements provide that certain reports and returns are made to regulatory bodies. Under the Canadian Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime, the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") is charged with the responsibility of receiving the following core transaction-based reports:

- Suspicious Transaction Reports: Pursuant to subsection 9(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Suspicious Transaction Reporting Regulations, we shall as soon as practicable report any transaction where there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money laundering offence or a terrorist activity financing offence.

- Terrorist Property Reports.

- Large Cash Transaction Reports: when it includes the sum of $10,000 or more received from a person or entity in Canada. This requirement is subject to the 24-hour rule which prescribes that we consider multiple transactions within a 24-period as a single transaction.

- Large Virtual Currency Transaction Reports for transactions in an amount equivalent to $10,000 or more. This requirement is subject to the 24-hour rule which prescribes that we consider multiple transactions within a 24-period as a single transaction.

- Records of transactions of traveler's cheques, money orders or other similar negotiable instruments: This involves when we receive $3,000 or more in funds or an equivalent amount in VC for the issuance of traveler's cheques, money orders or other similar negotiable instruments from a person or entity.

- Electronic Funds Transfer Reports.

8.0. COOPERATION WITH REGULATORS AND AUTHORITIES 8.0. All Employees are obliged to cooperate fully with the appropriate governmental authorities responsible for combating AML if required. We shall promptly comply with all requests made, pursuant to the law, and provide information to regulators including FinCEN and other relevant agencies if needed.

9.0. POLITICALLY EXPOSED PERSONS ("PEPs")

9.1. PEPs are individuals who are or have been entrusted with prominent public functions in any country, their family members and those closely associated with them. Enhanced due diligence measures are employed for PEPs as with other high-risk customers to mitigate the AML/FT risk they pose to ensure that we are not unknowingly supporting ML/FT activities. We conduct a review of its existing customers to ensure that the transaction of any newly elected PEPs in its database is subject to EDD measures.

9.2. In accordance with The Financial Action Task Force ("FATF") recommendations, the approval of the Managing Director and the Compliance Officer is required prior to creating an account with PEPs or updating the account of those already in the system. An ongoing monitoring is conducted of the business relationship, source of wealth and source of funds.

10.SANCTIONS

10.1. Through our Compliance Officer we employ a daily screening process on new and existing customers to identify, and block known virtual assets addresses, associated with sanctions and numerous illegal and high-risk

activities. We would keep up to date with the Office of Foreign Assets Control, US ("OFAC") sanctions list, notice of other federal government agency list of known or suspected terrorists or other criminals. We conduct a CDD within a reasonable time before a customer is onboarded and during the customer relationship when the lists are updated to determine whether an existing customer appears on such lists.

10.2. In accordance with this AML/KYC policy, we do not open accounts or process transactions for citizens and residents of, as well as people staying in, countries where transactions are prohibited by international sanctions or their internal law regulations, or countries which based on various criteria selected by our Compliance Officer (for example Corruption Perceptions Index by Transparency International, FATF warnings, countries with weak anti-money laundering and terrorist financing regimes determined by European Commission) impose high AML / FT high risk.

10.3. All verified matches are automatically suspended, or blocked, and the account is escalated to the Compliance Officer for further investigation and report to the appropriate authorities where necessary.

11. AML/CFT TRAINING

11.1. We shall conduct training and workshops to ensure employees are well informed about the AML/CFT laws, KYC principles and red flags of money laundering or terrorism financing which may occur in the course of their duties. Training will be considered in person, virtually or by email.

12. RECORD KEEPING

12.1. In compliance with regulations, information is maintained about funds transfer (date cash is received), the parties to the funds transfer (name, address, date of birth, contact information, occupation, or in the case of an institution, the nature of their principal business), their account numbers or
its equivalent reference number, the entities involved in the payment chain, the type and amount of each fiat currency received, the method by which you received the cash, the exchange rate used and their source (if applicable), purpose of the transaction, and the method of remittance with the details of the parties involved.

12.2. In accordance with the FINTRAC guidelines, we are required to keep a record of the following:

- A copy of every report sent to FINTRAC
- Large cash transaction records.
- Large virtual currency ("VC") transaction records.
- Redemption of money orders for a total value of $3,000 or more in funds or in an equivalent amount of VC at the request of a person or entity.

- Records of transactions of $1,000 or more: remitting and transmitting funds by means other than an electronic funds transfer to a beneficiary at the request of a person or entity. Virtual currency transfers, electronic funds transfer sent as an intermediary, an international EFT or initiated by another reporting entity.

- Foreign currency exchange transaction tickets for every foreign exchange transaction we conduct regardless of amount.

- Virtual currency exchange transaction tickets for every VC exchange transaction we conduct regardless of amount.

- Created or received internal memorandums about MSB/FMSB services we provide to our customers.

- Service agreement records for an agreement entered with an entity to provide an MSB/FMSB service covered under section 5(h) (h.1) of Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).

12.3. Records are retained throughout the life of the account and for 5 years after the cessation of the relationship and for 5 years after the transaction date for transaction instruments. In litigation and/or regulatory investigations, the records will be kept for as long as they are required.

13. AML/KYC AUDITS

13.1. To adhere to evolving regulations and ensure a current compliance function, internal audit of the AML/KYC Policy is conducted on a quarterly basis. This is to test the adequacy of the existing AML/FT functions and ensure that the measures developed by us are effective. The report with highlighted recommendations is submitted to the Board to ensure the recommendations are implemented.

14. AML/KYC POLICY REVIEW

14.1. The policy shall be regularly reviewed to ensure that it remains current in view of the evolving regulatory requirement.

14.2. That revised policy shall prominently display the date of revision and approval on its cover page.