BLOCK BEATS TOKEN ANTI MONEY LAUNDERING ("AML")
AND
KNOW YOUR CLIENT (KYC)

Block Beats Token is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Anti-Terrorist Financing and requires the management, and employees to follow the named standards.

Scope
This Policy outlines the minimum general unified standards of internal AML control which would be adhered to by the company in order to mitigate the legal, regulatory, reputational, operational, and as a consequence financial risk.

Objectives
The objective of the guidelines is to prevent the company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. The Policy also enables the company to know / understand status of its Investors / users and their financial dealings better, to manage risks including reputation.

Overview
Block Beats Token, like most companies providing services in the crypto market, adheres to the principles of Anti-Money Laundering and actively prevents any actions that aim or facilitate the process of legalizing of illegally gained funds. AML policy means preventing the use of the company's services by criminals, with the aim of money laundering, terrorist financing or other criminal activity.

For this purpose, a strict policy on the detection, prevention and warning of the corresponding bodies of any suspicious activities was introduced by the company. Moreover, Block Beats Token has no right to report users that the law enforcement bodies are informed on their activity. A complex electronic system for identifying every company's user and conducting a detailed history of all operations was introduced as well.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Terrorist financing is an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

The process of money laundering can be divided into three sequential stages:
Placement. At this stage funds are converted into financial instruments, such as checks, bank accounts, and money transfers, or can be used for purchasing high-value goods that can be resold. They can also be physically deposited into banks and non-bank institutions (e.g., currency

exchangers). To avoid suspicion by the company, the launderer may as well make several deposits instead of depositing the whole sum at once, this form of placement is called smurfing.
Layering. Funds are transferred or moved to other accounts and other financial instruments. It is performed to disguise the origin and disrupt the indication of the entity that made the multiple financial transactions. Moving funds around and changing in their form makes it complicated to trace the money being laundered.
Integration. Funds get back into circulation as legitimate to purchase goods and services.
In response to the scale and effect of money laundering, the United States of America and the European Union has passed Laws and Directives designed to combat money laundering and terrorism. These Acts, together with other regulations, rules and industry guidance, form the cornerstone of our AML/KYC obligations and outline the offenses and penalties for failing to comply.

Whilst Block Beats Token's business domain is currently relatively unregulated and does not fall within the scope of the AML/KYC obligations, our management has decided to implement systems and procedures that meet the standards set forth by the United States of America and the European Union. This decision reflects the management's desire to prevent money laundering and not be used by criminals to launder proceeds of crime.

ANTI-MONEY LAUNDERING POLICY

Block Beats Token has developed and will currently implement on a case-by-case basis a risk-based antimoney laundering program comprising of:

- Written Anti-Money Laundering Policies
- Customer Identification Procedures
- Anti-Fraud Procedures
- Record-Keeping Requirements
- Customer Risk Assessment Procedures
- Sanction Lists Procedures
- Block Beats Token Employees Training Procedures
- On-going Customers' activity procedures

The Block Beats Token AML Policy is designed to prevent money laundering by meeting the worldwide standards on combating money laundering and terrorism financing, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime. This AML Policy sets out the minimum standards which must be complied with and includes:

- Establishing and maintaining a Risk-Based Approach (RBA) to the assessment and management of money laundering and terrorist financing risks faced by the firm;
- Establishing and maintaining risk-based Customer Due Diligence (CDD), identification, verification and Know Your Customer procedures, including enhanced due diligence for customers presenting a higher risk, such as Politically Exposed Persons (PEPs);

- Establishing and maintaining risk-based systems and procedures for the monitoring of on-going customer activity;
- Establishing procedures for reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate;
- Maintaining appropriate records for the minimum prescribed periods; • Providing training for and raising awareness among all relevant employees.

Because of the company's commitment to the AML and KYC policies, each user has to finish a verification procedure. Before Block Beats Token starts a specific relationship with the user, the company may have to ensures that satisfactory evidence is produced or such other measures that will produce satisfactory evidence of the identity of any customer or counterparty are taken. The company as well may apply heightened scrutiny to users who are residents of other countries, identified by credible sources as countries, having inadequate AML standards or that may represent a high risk for crime and corruption and to beneficial owners who resides in and whose funds are sourced from named countries.

Individual users

Whenever necessary for the provision of any of the company's permanent or temporary services, during any required process of registration, each user may have to provide any or all of the following personal information: full name; date of birth; origin; complete address, including phone number and city code. For the avoidance of doubt: Block Beats Token does not require any or all of the documents hereinafter detailed for the provision of all the services, instead such requirements will be issued on a case-by-case basis, specifically whenever the law or the regulation applicable to any specifically provided service may require us to do so.

A user may have to send the following documents (in case the documents are written in nonLatin characters: to avoid any delays in the verification process, it is necessary to provide a notarized translation of the document in English) because of the requirements of KYC and to confirm the indicated information:

- a high-resolution copy of the first page of local or international ID or passport, where the photo and the signature are clearly seen, or a copy of driver's license with the same requirements. The indicated documents must be valid at least 6 months from the filing date.
- a high-resolution copy of a receipt of utility services payment or bank statement, containing the full user's name and the actual place of residence. These documents should not be older than 3 months from the date of filing.

<u>Required Information</u>

Upon registration, users go through an automated verification process where they submit:

- Full name;
- Date of birth;
- A unique photo of them holding their government-issued photo ID.

All submitted user information is manually reviewed. For users who cannot be verified through automated means (geolocation, algorithmic face detection, sanctions list check), enhanced due diligence is requested as described below.

Government-issued ID

Verification of identity is required by obtaining a high-resolution, non-expired copy of the user's government-issued ID (passport, national identity card, or a driver's license). The submitted imaged requirements include:

- Full color image. Black and white, watermarked, etc. are not accepted;
- Legible. All information on the ID must be completely clear and readable. Block Beats Token does not accept IDs that are torn or worn out; and
- Background. The edges of the ID document must be clearly visible on a contrasting background.

Proof of residence

Verification of residence is required by obtaining a copy of an acceptable address proof document issued in the 3 months prior to establishing an account. The document must carry the user's name and address.

A valid proof of residence document can be:

- bank statement;
- debit or credit card statement;
- utility bill (water, electricity, gas, internet, phone);
- payroll statement or official salary document from employer;
- insurance statement;
- tax document; or
- residence certificate.

Proof of residence documents must contain the user's name, address, and be dated less than 3 months ago.

Unique photo of user

Further verification is requested from users by submitting a unique photo of themselves holding their government-issued ID as well as a unique handwritten note. In the photo, the user must be visibly smiling. This allows Block Beats Token to easily prove that the user's picture was not stolen or photoshopped, and is being used exclusively for Block Beats Token.

The ID the user holds in their hand:

- must be the same government-issued ID the user submitted previously; and
- must be fully clear and readable.

The note the user holds in their hand:

- must be handwritten (not typed);
- must be in English;

- must contain today's date;
- must contain the sentence: For trading at wcex.com only; and
- must contain the user's signature.

Verification

Based on the risk, and to the extent reasonable and practicable, we ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about users. Our AML Compliance Officer analyzes 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. We may decide to use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;
- Checking references with other financial institutions;
- Analyzing whether there is logical consistency between the identifying information provided, such as the users' name, street address, postal code, and date of birth;
- Utilizing complex device identification (such as "digital fingerprints" or IP geolocation checks); and
- Obtaining a notarized or certified true copy of an individual's birth certificate or government-issued ID for valid identification.

Corporate users

In case the applicant company is listed on a recognized or approved stock exchange or when there is independent evidence to show that the applicant is a wholly owned subsidiary or a subsidiary under the control of such a company, no further steps to verify identity will normally be required. In case the company is unquoted and none of the principal directors or shareholders already has an account with Block Beats Token, the official provides the following documents:

- a high-resolution copy of the certificate of incorporation/certificate;
- an extract from the Commercial Register, or equivalent document, evidencing the registration of corporate acts and amendments;
- names and addresses of all officers, directors and beneficial owners of the corporate entity;
- a high-resolution copy of Memorandum and Articles of Association or equivalent documents duly recorded with the competent registry;
- evidence of the company's registered address and the list of shareholders and directors;
- description and nature of business (including the date of commencement of the business, products or services provided; and the location of principal business).

This procedure is performed to establish the identity of the user and to help Block Beats Token know / understand the users and their financial dealings to be able to provide the best services of online trading.

RISK-BASED APPROACH

Block Beats Token adopts and maintains a Risk-Based Approach (“RBA”) towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with users.
The guidelines are as follows:

- Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the users does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations;
- For the purpose of risk categorization of the users, the relevant information shall be obtained from the users at or before the time of entering into a transaction;
- The risk categorization process for different types of users may take into account the background of the users, country of origin, sources of funds, volume of turnover or deposits, as well as social and financial background;
- The outcome of the risk categorization process shall be decided based on the relevant information provided by the users at the time of commencement of business relationship;
- Enhanced due diligence would be required for higher-risk users, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by Block Beats Token at its sole and absolute discretion; and
- Block Beats Token must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the Block Beats Token in compliance with the relevant legislations in place.

MONITORING OF CLIENT ACTIVITY

In addition to gathering information from the users, Block Beats Token may have to continue to monitor the activity of every user to identify and prevent any suspicious transactions. A suspicious transaction is known as a transaction that is inconsistent with the user's legitimate business or the usual user's transaction history known from user activity monitoring. Block Beats Token has implemented the system of monitoring the named transactions (both automatic and, if needed, manual) to prevent using the company's services by criminals.
The company reserves the right to suspend any user's operation, which can be regarded as illegal or, may be related to money laundering in the opinion of the staff.

INTERNAL CONTROLS

Block Beats Token implements and maintains internal controls for the purpose of ensuring that all of its operations comply with AML legal requirements and that all required reports are made on a timely basis.

MONITORING AND REPORTING

Block Beats Token may have to diligently monitor transactions for suspicious activity. Transactions that are unusual are carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. When such suspicious activity is detected, the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and Block Beats Token may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

We will initially make the decision of whether a transaction is potentially suspicious. Once we have finished his review of the transaction details, we make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be made.

For the purpose of the Policies, a "Suspicious Transaction" means a transaction or attempted transaction, which to a person acting in good faith,

- gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- appears to be made in circumstances of unusual or unjustified complexity;
- appears to have no economic rationale or bona fide purpose; and
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

RECORD-KEEPING

We make sure that AML records are maintained properly.

We document our verification, including all identifying information provided by a user, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We keep records containing a description of any document that we relied on to verify a user's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we retain documents that describe the methods and the results of any measures we took to verify the identity of a user.

We also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We retain records of all identification information for seven years after the account has been closed, or as long as reasonably necessary to comply with applicable regulations; we retain records made about verification of the customer's identity for seven years after the record is made, or as long as reasonably necessary to comply with applicable regulations.

TRAINING

New employees may receive anti-money laundering training as part of the new-hire training program. All applicable employees are also required to complete AML training annually. Participation in additional targeted training programs is required for all employees with day-today AML and KYC responsibilities.

Our training includes, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags (3) what employees' roles are in Block Beats Token's compliance efforts and how to perform them; (4) Block Beats Token's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance.

Our operations are regularly reviewed to check whether certain employees require specialized additional training. Written procedures are updated to reflect any such changes.

SANCTIONS POLICY

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