Back Home Page

AML AND KYC POLICY

INTRODUCTION

Victorum (VCC) decentralized Cryptocurrency, which is tradeable in markets worldwide, and further high-quality services to all clients with our Anti-Money Laundering (AML) and Know Your Customer (KYC) Policy (hereafter "AML/KYC Policy") identifying and eliminating potential risks of money laundering. The effectively implemented AML/KYC rules are aimed at improving efficiency and stability in the cryptocurrency for all parties.

For the purposes of this AML/KYC Policy, "us," "we," or "our" or "**Victorum"** refer to the website https://victorumcoin.com/ and related activities.

Both international and local regulations require us to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, the proliferation of weapons of mass destruction, corruption, and bribery and to take action in case of any form of suspicious activity of our customers.

1. AML/KYC Policy covers the following matters: Compliance Officer

- Compliance Officer;
- Money Laundering Reporting Officer (MLRO) [ONLY IF REGULATED BY THE FCA – DELETE OTHERWISE, OR I NEED TO ADD A NEW SECTION]
- Risk Assessment;
- Identity Verification Procedures;
- Monitoring Transactions.

2. Compliance Officer

The Compliance Officer is the person, duly authorized by us, whose duty is to ensure the effective implementation and enforcement of AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of our anti-money laundering and counter-terrorist financing requirements, 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; and
- Providing law enforcement authorities with information as required under the applicable laws and regulations.

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

3. Risk Assessment

We, in line with the international requirements, have adopted a risk-based approach to combating money laundering and terrorist financing. By establishing and maintaining risk-based systems and procedures, we are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

4. Identity verification

Our identity verification procedure requires the customer during the registration to provide us with such documents according to AML/KYC Policy:

a) Identity Document – this is a valid, reliable, and independent source document with the following information: First Name and Last Name; date of birth; customer's photo, identity document serial number. The customer is free to provide one of the following types of documents:

· National ID card (both sides) or national passport;
· International passport; and
· Driver's license (both sides).

b) Proof of address – this is a document confirming the customer's residence containing First Name and Last Name, address, and issued within the last 3 months.

The customer is free to provide one of the following types of documents:

· Certified tenancy agreement or a bank statement;
· Utility or electricity bill;
· Tax return or council tax;
· Other official documents with current residential address, First Name, and Last Name and issued within the last 3 months.

c) "Selfie" – a photo of yourself holding a sheet of paper with the inscription "Victorum (VCC)" and the current date.

We will take steps to confirm the authenticity of documents and information provided by the customer. 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.

We reserve the right to verify a customer's identity on an ongoing basis, especially when his identification information has been changed or his/her activity seemed to be suspicious (unusual for the particular customer). In addition, we reserve the right to request up-to-date documents from the customer, even though he/she has passed identity verification in the past.
Customer identification information will be collected, stored, shared, and protected strictly in accordance with our Privacy Policy and related regulations.
We reserve a right to reject any person on registering on https://victorumcoin.com/ and using related services if we are unable to verify any information due to non-cooperation of the customer, or if the customer's actions are likely to have a material adverse effect on us for being in violation of any applicable laws or industry best-practice guidelines.

We may from time to time temporarily reject customers from some countries/territories. The current list of such countries/territories can be reviewed here. This applies to both new customers at the registration stage and existing users of our services. In the latter case, we will notify the customer of the refusal to provide services in advance and provide a reasonable time for the termination of the use of our services.

5. Monitoring Transactions

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

a) A daily check of customers against recognized "blacklists" (e.g., OFAC), aggregating transfers by multiple data points, placing customers on watch and service denial lists, opening cases for investigation if it is essential, sending internal communications, and filling out statutory reports, if applicable;
b) Case and document management.

Victorum demonstrates a strong commitment to maintaining the integrity of its website services. The company constantly analyzes all provided customer data and monitors all transactions and it has the right to:

a) Monitor and control all transactions by means of automated screening by any Blockchain transaction monitoring tool and manual screening aimed at prompt identification of high-risk transactions. Transaction monitoring systems are reviewed regularly to ensure the system is operating appropriately and effectively;
b) Analyze customers' historical information and other contextual profile data (placing requests, offers, input and output data, website activity tracking, etc.); and
c) Monitor and control unnecessarily complex and unusual transactions to identify different suspicious actions.

In case of detection of any suspicious or toxic transactions, the company follows the algorithm:

- Request the customer to provide any additional information or documents in case of suspicious transactions;
- Temporarily suspend (lockout) or deactivate a user account if data provided by the user is fictitious (false, incomplete, or misleading) with regard to the origin of funds; and
- Terminate the user account and cancel all transactions engaged in suspicious (fraudulent) activities.
- Upon detection of any suspicious (fraudulent) transactions, the company reserves the right to employ corresponding prevention measures without prior notice or explanation to the user, which include but are not limited to:
    · blocking/closing of the existing/open client's transactions on the website;
    · restricting and/or blocking access to the website;
    · cancellation of all deposit/withdrawal transactions deemed as suspicious (fraudulent); and
    · reporting any suspicious user's transactions to the relevant enforcing authorities.

With regard to AML/KYC Policy, we will analyze all provided customer data and monitor all transactions and 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; and
- temporarily suspend (block) or terminate the customer's account when we have reasonable suspicion that such customer is 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 bonafide.
If you fail to provide the requested documentation within a reasonable time frame, your account will be blocked.
If you have any inquiries, please contact us via email: **verification@victorumcoin.com**