Last updated: 13 January, 2020

# Crypterium Anti-Fraud Policy

## 1. Introduction

The Anti-Fraud Policy (the "AF Policy") of Crypterium AS of Harju maakond, Tallinn, Kesklinna linnaosa, A. Lauteri tn 5, 10114, Estonia, registration number 14352837 ("we", "our", "us" or "Crypterium") is established to prevent and mitigate possible risks of Crypterium being involved in illegal or illicit activities and to enable Crypterium to meet its legal and regulatory obligations in this area (if any, where applicable). This AF Policy is subject to changes and updates by Crypterium from time to time to ensure compliance with any applicable legislation and global AF practices.

## 2. Policy Statement

2.1. Crypterium will comply with applicable laws of Republic of Estonia. In line with applicable laws Crypterium has a 'zero tolerance' policy towards fraud, collusion, money laundering, financing of terrorism and other criminal conduct and will thoroughly investigate and seek to take legal action against those who perpetrate, are involved in, or assist with fraudulent or other improper actions in all Crypterium activity and related transactions.

2.2. Crypterium will provide adequate and appropriate resources to implement the Anti-Fraud Policy and will ensure it is communicated and understood.

## 3. Purpose&Scope

3.1. The purpose of this document is to outline the responsibilities of all the involved parties with respect to fraud prevention, the actions to be taken if fraud is suspected and the mechanism of verifying suspicion of fraud, the reporting process and the recovery action plan.

## 4. Legislation Compliance

4.1. The Anti-Fraud Policy has been drafted to comply with the current applicable law, including, but not limited to applicable laws of Republic of Estonia.

4.2. Adherence to the Anti-Fraud Policy Crypterium will ensure compliance with all relevant legislation and internal policies.

## 5. The User verification

5.1. The User undertakes to provide Crypterium with correct and relevant personal information and documents contained therein. In case the User provides counterfeit documents and false personal information, such behavior will be interpreted as a fraudulent activity.

5.2. The User hereby authorizes Crypterium, directly or indirectly (through third parties), make any inquiries as we consider it necessary to check the relevance and accuracy of the information provided for verification purposes. Personal Data transferred will be limited to strictly the necessary and with security measures in use to protect the data and is specifies in our Privacy Policy.

## 6. Account security

6.1. The User is responsible for maintaining the confidentiality of their Account's credentials, including, but not limited to a password, email, wallet address, balance and of all activity including transactions made through the Account.

6.2. If the User has any security concerns about his/her Account, login details, password or other security feature being lost, stolen, misappropriated, used without authorization or otherwise compromised, the

User is advised to change the password. The User must contact us via support@crypterium.com without undue delay on becoming aware of any loss, theft, misappropriation or unauthorized use of the Account, login details, password or other security features. Any undue delay in notifying Crypterium may not only affect the security of the Account but may result in the User being liable for any losses as a result.

6.3. Any loss or compromise of User's electronic device or User's security details may result in unauthorized access to User's Account by third parties and the loss or theft of any digital currency held in User's Account. User must always keep his/her security details safe. For example, User should not write them down or otherwise make them visible to others.

6.4. User should never allow remote access or share his/her computer screen with someone else when User is logged on to Account. Crypterium will never under any circumstances ask User for IDs, passwords, or 2-factor authentication codes or to screen share or otherwise seek to access to computer or Account. User should not provide details to any third party for the purposes of remotely accessing User's Account unless specifically authorized.

6.5. Crypterium assume no responsibility for any loss that User may sustain due to compromise of Account login credentials due to no fault of Crypterium.

## 7. Key Responsibilities

7.1. In view of the Anti-Fraud Policy Crypterium is responsible for:

- Undertaking a regular review of the fraud risks associated with each of the key organizational objectives;
- Establishing an effective anti-fraud response plan, in proportion to the level of fraud risk identified;
- The design of an effective control environment to prevent fraud;
- Establishing appropriate mechanisms for:
    - reporting fraud risk issues.
- Making sure that all staff are aware of Crypterium Anti-Fraud Policy and know what their responsibilities are in relation to combating fraud; and
- Ensuring that appropriate action is taken to minimize the risk of previous frauds occurring in future.

## 8. Fraud detection and investigation

8.1. Crypterium's Operational Anti-Fraud Department, in particular, the Head of Anti-Fraud Services, is the first line of detection, investigation and protection in preventing Prohibited Activities through the Users and transactions appraisal process. The Head of Anti-Fraud Services will be responsible for the proper fulfillment of the Anti-Fraud Policy.

## 9. Miscellaneous

9.1. Crypterium will review the Anti-Fraud Policy to reflect new legal and regulatory developments and ensure good practice.