CODEX
INFORMATION SECURITY POLICY

Effective Date: January 2019

The "codex.one" platform is run by Cryptagio OÜ, the company registered under the laws of Estonia (the "Company", "Cryptagio", "we", "us" and "our"). We want you to know that Cryptagio is committed to ensuring the Confidentiality, Integrity, and Availability of your data and other information we possess. For this reason, we have developed this Information Security Policy (the "Policy"), so you can find out more about our approaches to information security management.

This Policy is an integral part of our Privacy Policy and Terms of Use. Please read them as well to have a holistic understanding of provisions that regulate your use of "codex.one" platform. In particular, we refer you to our Privacy Policy, where you may check the list of personal data we collect, process and store.

To ensure the highest level of protection, we may review and update this Policy. Please check this page sometimes to familiarize yourself with any such changes.

1. PRINCIPLES AND APPROACHES

We want you to know that Cryptagio has chosen to employ the following principles and approaches to ensure a level of security for the data:

(a) analysis of data processing activities, further identification, assessment and minimizing of the security risks;
(b) ability to ensure the ongoing confidentiality, integrity, availability, and resilience of information, as well as of processing systems and services;
(c) ability to restore the availability and access to the data in a timely manner in the event of a physical or technical incident;
(d) executing monitoring procedures and recording actions that might influence the confidentiality, integrity, availability, and resilience of the data;
(e) pseudonymization, anonymization, and encryption of personal data and other confidential information;
(f) providing access to the personal data and other confidential information on the "need to know" basis and in accordance with the principle of "least privilege";
(g) providing necessary training for Cryptagio's personnel;
(h) engaging only trustworthy sub-contractors;
(i) regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
(j) maintaining and improving the system of information security management;

The specific security measures that we have implemented are detailed below.

2. LEGAL & REGULATORY OBLIGATIONS

Cryptagio is responsible for adhering to all current Estonian and EU legislation as well as to a variety of regulatory and contractual requirements. This means that we undertake to comply with the provisions of GDPR as regards the personal data processing. Particularly, we employ the principles of lawfulness, fairness, and transparency of processing, purpose and storage limitation, data minimization, accuracy, integrity, and confidentiality of personal data. Please read our Privacy Policy to learn how these principles are implemented within Cryptagio.

3. TECHNICAL SECURITY

The following technical measures are present within the frames of Cryptagio's information security management:

- **Encrypted storage**

We store all personal data in an encrypted format within the protected cloud infrastructure. We also don't store your passwords as simple records. We use *bcrypt* hashing with salts to ensure the passwords' security.

- **Account Integrity & Withdrawals**

We use advanced verification instruments to monitor the integrity of each account. For instance, login data is saved and checked for any abnormal activity. The intelligent system detects any IP Address irregularities to prevent session hijacking. Email notifications report logins and contain a link to instantly freeze the account in case malicious activity is suspected. There is limited access to the account based on the IP address.

The security system also checks all withdrawals by IP address and other patterns of user behavior. If we indicate any odd withdrawals, our admin will manually examine this activity. The step of confirming a withdrawal is invulnerable to malware.

- **Two-factor authentication (2FA)**

We have implemented a two-factor authentication for sensitive operations within your account such as log in, generation of API keys, and withdrawals. You may configure the two-factor authentication with the help of Google Authenticator or SMS OTPs using Twilio.

- **EdDSA API keys**

You can enjoy the platform's full power through our REST and WebSockets APIs. Please note that unlike other exchanges, we don't store API secrets. By utilizing EdDSA, we store only the public key, which makes our platform as secure as it physically possible.

- **System Security**

Cryptagio daily checks all the infrastructure for security vulnerabilities with the help of Intrusion Detection System. We use the up-to-date software and the best technology practices to enable protection of our servers' network.

Offline, cold wallets are used to store practically all of the system funds. Only a tiny fraction of the funds that equals 0.5% is available in hot wallets for everyday operations. For the extra protection, the cold wallets cannot be accessed from the platform or the platform servers. The assets located in offline cold storage can only be accessed manually by several members of the management team.

- **Database Backup**

An automatic backup of the databases is launched in our Company. Such backup copies are encrypted and compressed in archives on a daily basis. We store our backup copies within an encrypted cloud file system which cannot be accessed from the outside.

- **Network Security and Data Transfers**

We protect the networks connections with firewalls. We also conduct monitoring to detect any abnormal activity. Data transfers are performed only through the secured channels.

- **Electronic Access Control**

To ensure that there is no unauthorized use of data processing and storage systems, we use secure passwords, implement automatic blocking/locking mechanisms and internal two-factor authentication. The data carriers and storage media containing personal data and other confidential information are secured with encryption.

- **Hardware Protection**

We install reliable software for antivirus and malware protection on all our devices. This software is automatically updated on a regular basis.

- **Other Security Features**

We also perform Penetration Tests and DDOS Sustainability Tests. Moreover, some of these tests are performed by external, independent specialists. Then we form the Security Reports that are further considered and used to improve our system of information security management.

4. ORGANIZATIONAL SECURITY

Alongside with technical measures, we have implemented the following organizational measures to secure the data:

- **Internal access control**

Access to all data bases is restricted to the minimum required level for all services as well as for personnel and third-party suppliers. Only explicitly authorized persons may read, copy, change or delete data within our systems. All actions with the data are recorded. Additionally, we have designated specific persons to manage the information security within Cryptagio.

- **Pseudonymization**

When it is possible, we process the personal data in such a way that the data cannot be associated with a specific data subject without the assistance of additional information. Such additional information is stored separately and is subject to appropriate technical and organizational measures.

- **Personnel Training**

We provide our personnel, including new employees, with instructions on how to securely deal with data and manage possible risks. For example, we require our staff to protect their unattended laptops and other devices with a screen locking mechanism controlled by a secure password. We also do not allow our employees to leave confidential material on the printer docks.

- **Third-Party Suppliers**

When we engage third-party suppliers, we stipulate each party's data protection and information security responsibilities in the contract. We also incorporate the non-disclosure provisions to such contract and may conclude a separate Non-Disclosure Agreement to establish a more specific control over confidentiality. We may provide the third-party suppliers with access only to strictly needed data according to the "need-to-know" and "least privilege" principles.

5. INCIDENT HANDLING

If you suspect that any information security incident has occurred, please contact us at: support@codex.one. We will do our best to identify the problem and mitigate the security risks quickly. In no case, you should attempt to resolve any security or privacy incident by yourself.

Our Security Incident Response Plan includes the following stages:

1) Detecting the vulnerabilities and possible risks;
2) Analyzing the identified problems;
3) Prioritizing and concluding action plan;
4) Handling security incidents.

If it needed, we will designate a dedicated team to deal with the security incident. This team will be formed of individuals responsible for IT and security, legal compliance, partnerships management, public relations, and human resources.

Lastly, when applicable data protection laws require it, we will provide you with a prompt notice on the data breach and all respective details.

6. REVIEW AND DEVELOPMENT

This Policy shall be reviewed and updated regularly to ensure that it remains appropriate in the light of any technical improvements in the field of information security, as well as of relevant changes to the law, organizational policies or contractual obligations.

If still you have any questions or concerns regarding the issues of information security within Cryptagio, contact us at info@codex.one.

Your "codex.one" team.