SECURITY POLICY

1. Introduction

We, at Greedex.org, highly prioritize your security. We undertake measures to guarantee your data, materials, communication, and other information (“Data”), which are exchanged, disclosed, shared, stored or used in our system, is safe and secure.

In the world of cryptocurrencies, blockchain and digital assets understanding and providing security is our main priority. Thus, endless efforts are given to and for the security in the privacy, confidentiality and integrity of Data. We will proactively and perpetually combat any cyber threats and we will provide updated defense techniques for the protection of Data.

We are glad to be able to provide you our Security policies and guidelines.

2. Our Security Measures

To ensure the privacy, confidentiality and integrity of Data which are exchanged, disclosed, shared, stored or used in our system, we employ these security measures, but not limited to:

Encryption

We use AES 192-bit encryption in encrypting all private data of all our users. Any user data, whether both encrypted and/or not encrypted, shall not be given back to the client.

We use transport layer security protocol 1.2 and 1.3 version in every request on Greedex.org.

Password and Authentication

We support any password from 8 to 2000 characters.

We further support Two Factor Authentication by using TOTP Authentication. This Two Factor Authentication (TOTP) is necessary to log in to your account.

API

API Accounts which we store are very well encrypted and are not returned in the same to our client.

We use proxy servers for all API requests in order to secure the primary servers.

We will store and/or display API Keys in encrypted format. User’s browser will not make requests to the exchange API directly from your computer.

TLS

All requests to Greedex.org are done across TLS. In this case all data transmitted to or from any of our servers are completely encrypted. That applies to browser and mobile app. SSL encrypts user’s key only once when the user submits it to the servers first time.

User Request Filter

We filter and check all requests on the front-end and the back-end to prevent any possible XSS, CSRF, Click jacking and Session Impersonation attacks.

In the database only parameterized queries are used. It helps to the to avoid any injection attacks.

We do not allow external access to DBMS servers.

Fund Storage

Greedex.org never handles your funds directly. All funds remain stored in the exchange's wallets.

3. Best Practices

We regularly audit the systems and exert utmost efforts to keep the systems updated with the latest in security fixes.

Only authorized team members can access to our servers, which are protected with a strong firewall.

We use DNS level DDOS protection.

We restrict and compartmentalize employee accounts.

4. User Responsibilities and Guidelines

It is your responsibility to audit your Greedex.org account and change your password regularly.

Use a long, unique and complex password with a mix of alphanumeric characters and symbols.

Maintain the confidentiality of your password by not sharing it or making it accessible to any other person and by signing off before visiting any other websites.

Use only the API functions that you intend to use.

It is your responsibility to keep both Greedex.org account and exchange account secure.

You are required to independently ensure the security and anti-virus protection of your device/s.

To protect your exchange’s wallet from computer failures and/or to recover your wallet after your mobile or computer is stolen, you need to back up and encrypt your wallet.

You may secure offline wallet for savings.

Keep your software up to date to receive security fixes.

5. Contact

For inquiries on Security Policy of Greedex.org, you may contact us via Greedex Support. We're happy to hear from you!