coinstash

4th February 2021

Coinstash Series A Information Memorandum

Security Strategy and Program

The safety of our customers' and treasury funds are a top priority. Our exchange has never had an incident where customers' funds have been compromised.

The following provides information about our security strategy. It describes the careful measures we have implemented to secure customer accounts and company assets.

Organisation controls

- All employees must pass a rigorous background check as part of the hiring process and are subject to ongoing screening throughout their employment (including the co-founders Ting Wang and Mena Theodorou).
- Employees are required to store files on protected-servers and not on local drives, change their passwords on a periodic basis, and lock their screen.
- Private keys are not stored in Coinstash offices.
- Employees must comply with all Information Security policies.

Platform

- Our website traffic runs entirely over encrypted using TLS (SSL/TLS 1.2).
- Our applications run on the latest stable version of .net core. We reduce the attack surface by isolating our processes via hardened containerization technology.
- Our security team sets architectural guidelines, conducts code reviews, and deploys every software system that can interface with customer data.
- Our developers are trained with specific attention toward security. Our code review processes look for any code that could potentially violate security policies.
- All customer data is stored in databases on Amazon, which are configured securely. Data is stored with at least dual redundancy, with backups, and is accessible only within the private cloud. We have also instituted per-service access protection and isolation of data.
- Internal testing and validation data in a production-stack equivalent internal stack populated with fictitious data.
- Coinstash continuously monitors application, infrastructure, network, data storage space and system performance.
- The application has been implemented with reference to the OWASP Security Guide.

Physical and Environmental Security

- We do not have in-house data centers. Amazon Web Services (AWS) manages the physical and environmental security of our data centers. For more details, please review AWS' control and security measures.

Accounts

- We check for strong passwords on account creation and password reset.
- We hash passwords stored in the database using the PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations.
- Application credentials are kept separate from the database and code base.
- Two-factor authentication is a feature on all accounts.
- We rate-limit a variety of actions on the site (login attempts, etc).
- Accounts are actively monitored for brute force attacks.

Assets

- Multiple digital signatures are required to transfer cryptocurrency out of our hot/cold wallet solutions.

Compliance

- We are subject to and comply with the AML/CTF rules and regulations in Australia.
- We are one of a few digital currency exchange providers who control an Australian Financial Services Licencee company.
- We hire independent third parties to perform regular penetration tests to proactively identify and resolve any security vulnerabilities.