STABLY DATA SECURITY POLICY

stably

PRIME TRUST DATA SECURITY POLICY

Stably’s regulated trust company partner, Prime Trust, LLC (“Prime Trust”), maintains its own Data Security Policy which can be viewed here. Prime Trust’s GLBA Notice can also be viewed here. Prime Trust’s policies are separate from Stably’s policies and Prime Trust neither endorses nor enforces Stably’s Data Security Policy.

STABLY DATA SECURITY POLICY

Last Edited: 10/14/2019

Table of Contents

Policy Overview

The security of our data and platform are core to our business and operations. In the world of cryptocurrency, security is key. We treat all our data and processes with an eye towards least privilege and best practices.

Our policies and procedures are grounded in fundamental logic and practicality. Where possible and practical, we employ best-practices, generally enforced by technology, corporate policy and management oversight.

We review our policies and procedures regularly. We may from time to time change our security policies and practices by enhancing them or by simplify them.

Change Management

All code that enters production is thoroughly tested and peer reviewed. No code enters production without a human signoff.

- All production code must be unit and integration tested
- All production code must have at least 1 other review sign off
- Production deployment is reviewed before being rolled out

We do not notify customers of platform updates or feature changes since there is generally no disruption or downtime.

Data Transmission and Storage

Classification

Data is classified into 4 tiers based on risk:

T0 - Private keys and cryptographic secrets. These are mission critical secrets that can never be lost or stolen. The utmost diligence, redundancy measures, and protection should be applied to the storage and security of this tier of data.
T1 - Personally identifiable information (PII) and other sensitive data that could cause significant risk or harm to the company. This tier of data should be maintained in a way that puts top priority on security and controls.
T2 - Private data that could cause some risk or harm to the company. This tier of data should be maintained in a way that reduces the likelihood of loss or theft. Reasonable measures should be in place to protect and secure this data.
T3 - Public data that has no meaningful risk and cannot cause measurable harm to the company. This tier of data can be kept in a way that optimizes for usage rather than security.

Transmission

T0 - Data should never be transmitted in plaintext over any network. We should always know the recipient of the data. When possible transmission should be over a physical medium instead of over the wire. Transmission should be kept to a minimum.
T1 - Data should never be transmitted in plaintext over any public network. We should always know the recipient of the data. Transmission should only occur when necessary.
T2 - Data should not be transmitted in plaintext over any public network when possible. We should aim to only expose the data to the intended recipient.
T3 - Data can be transmitted in a way that optimizes usability.

Access

All Stably employees, including our engineers, are required to comply with information security protocols, including the use of strong passwords on all devices used to conduct firm business. Access to production systems, including databases, is restricted to our Chief Technology Officer.

Stably employees are strictly prohibited by policy from downloading and transmitting by email or other unsecured mechanism any T0 or T1 data for any reason. Any collateral containing proprietary or personally identifiable information ("PII") must be transmitted using a secure mechanism only. As a condition of interacting with Stably’s systems, all employees are trained in PII handling and data security.

Storage

T0 - Data should be stored in a way that minimizes systematic, geopolitical, technical, and human risk. An example could be offline storage of secrets using an M of N approach where at least M of the N secrets are needed to be useful. Multiple copies of these different pieces could be held in different geopolitically distributed secured institutions such as banks with long track records of security. No single person should have enough access to recreate the full secret and processes should be in place to ensure that no single person is a point of failure in this system (bus count > 1).
T1 - Data should be encrypted and stored with access controls such that only mission critical access is permitted, and only with sufficient access logging and human redundancy.
T2 - Data should be stored with access controls such that only those who need the data should have access. Encryption is strongly recommended in case access controls fail.
T3 - Storage should be dependent on the use of the data.

Incident Response

In the event of a catastrophe (private keys compromised, data center data loss, loss of key personnel, acts of god, etc...) we will first enact damage controls where possible and then assess the situation. In the case where it makes sense to bring down our services and products we can do a combination of the following based on the situation:

- Pause token transfers on mainnet
- Shut down inbound traffic into our VPC
- Spin down our services

Once damage control is in place, the executive team will convene remotely or in-person to assess the situation and determine appropriate next steps and any public communications. If the situation is under control we will bring the system back up as soon as we are confident that it will not exacerbate the issue.

Customer Data

We collect customer data to meet the compliance requirements of the financial institutions that we partner with (“FI partners”). Our data is given to our FI partners so they can process “Know Your Customer” checks, run anti-money laundering (“AML”) controls including OFAC sanctions screening, and otherwise comply with federal and state laws.

The data we collect includes but is not limited to:

- Name
- Address
- Email
- Tax ID
- Date of birth
- Company identification information

This data when together is considered **T1** and must be treated as such.

Transaction Data

To enable usage of our platform, we store user bank account information so that we can push funds to their account when they request it. We use the data by sending it to our financial partners for funds processing.

The data we collect includes but is not limited to:

- Bank name
- Bank routing number
- Bank account number
- Account holder’s name

This data when together is considered **T1** and must be treated as such.