Encryption Policy

Version 2 - Approved by Madhav Bhagat

Contents

1. Objective

Encryption is a process in which data is encoded so that it remains hidden from or inaccessible to unauthorized users. It helps securely protect data that you do not want anyone to access. By encrypting our data at rest and in transit, we can better protect private, proprietary, or critical data and enhance communication security between client applications and servers. This policy provides the guidelines to follow for the encryption of data.

2. Scope

This policy is applicable to all systems and networks that store and transfer critical data. This includes cloud-hosted vendor services, endpoints, production networks, cloud assets, etc., used in delivering SpotDraft's services. This may also include third-party systems that support the business of SpotDraft.

3. Policy Statement

The purpose of this policy is to ensure the security of data at rest and data in transit for SpotDraft. Data at rest refers to physically stored data, which is encrypted using various tools and managed by the infrastructure provider. Data in transit, actively moving between locations, also needs to be encrypted using TLS and trusted security certificates. Passwords and cryptographic keys need to be encrypted and stored securely. Rolling one's own cryptography is strongly discouraged.

4. Encryption Guidelines

4.1 Encryption at Rest

- Data at rest is defined as data that is physically stored and not actively moving from one location to another (i.e., device to device or network to network). This includes data stored on laptops, flash drives, and hard drives.
- SpotDraft encrypts data at rest using a variety of tools, including but not limited to
    - Utilizing managed databases by infrastructure providers that have options to encrypt data at rest. In these cases, encryption keys are managed by the infrastructure provider.
    - Utilizing the infrastructure provider's option to encrypt the underlying storage of the assets that persist data. Again, encryption keys are managed by the infrastructure provider.
    - Company laptops are encrypted as outlined in the Endpoint Security Policy.

4.2 Encryption in Transit

- Data in transit is defined as data that is actively moving from one location to another (i.e., device to device or network to network). This includes data transferred over public networks such as the Internet. SpotDraft encrypts data in transit using a variety of tools, including:
    - TLS: Always use HTTPS, SSL enabled (minimum standard is TLS v1.2).
    - Use security certificates provided by a known, trusted provider for all of SpotDraft's public-facing properties on the Internet.

4.3 Rolling your own Crypto

Please don't roll your own crypto. If you really think you have a situation where it makes sense to do this, please don't. If you're absolutely sure you have an edge case where this makes sense, please contact the Information security officer so they can work with you on finding an alternative.

4.4 Password Encryption

All passwords of end-users and customers should be encrypted in transit and when stored at rest within the application or database.

4.5 Cryptographic Keys

Cryptographic keys should be generated and stored in a secure manner that prevents collision, loss, theft, or compromise.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Encryption Policy. For version history, please see the next page.

Version history

Version	Log	Date
2 Current	Policy version approved by Madhav Bhagat	29 Jul, 2024
2	New Policy version Created	29 Jul, 2024
1	Policy version approved by Madhav Bhagat	02 Aug, 2022
1	New Policy version Created	02 Aug, 2022