Data Safeguard Policy

1. Overview

This policy addresses the expectations of all SproutLoud employees as they are accessing SproutLoud Intellectual Property and client data.

2. Purpose

The company must restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

3. Scope

3.1 Scope

This data security policy applies to all customer data, personal data, or other company data defined as sensitive by the company's data classification policy. Therefore, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Every user who interacts with company IT services is also subject to this policy.

Regardless of the origin or sensitivity of the data, all data in our possession is handled with the same level of security, confidentiality, and encryption in order to guarantee data integrity.

4. Policy

4.1 Appropriate Use

We must take great care of the data that we're entrusted with to do our jobs, including SproutLoud Intellectual Property and our clients' data. Avoid using this data with inappropriate/free/freemium websites that claim to provide a service. This includes websites used for screenshot sharing, converting file formats, etc.

4.2 Appropriate Action

In the event that you are in need of a tool to assist with your job, especially in the manners demonstrated above, please contact the InfoSec team. A solution will be provided for you that has been previously vetted, otherwise a new solution will be vetted and made available. If you currently use an unapproved method/solution as a part of your workflow, please discontinue use immediately and contact Infosec so a solution can be provided.

5. Security

5.1 Encryption

All data as specified in our Data Classification Policy is encrypted at rest using AES-256 across our company's infrastructure and employee devices. Employee devices are encrypted using BitLocker or FileVault depending on the operating system. Data in transit (via email, FTP, etc.) is encrypted using TLS 1.2+, SSH.

5.2 Authentication

Access to all company resources are behind multifactor authentication (MFA). The two main methods in use for enforcing MFA are via JumpCloud and Google, which utilize push notifications, rotating secure tokens, biometrics, SMS verification and one time use backup codes.

5.3 Mobile Device Access

Access to employee email, data stored in online shared folders, and other Google apps are allowed as long as a screen lock is enabled for the mobile device. Screen lock authentication via a passcode, password, or a form of biometric authentication (fingerprint, facial recognition, etc.) must be enforced, otherwise access will not be permitted.

5.4 Physical Access

Access to SproutLoud offices are secured by biometric authentication or key card authentication. All sensitive information that is non-digital, is secured behind locked doors and locked cabinets with key holders clearly identified by the People and Organizational Development department.

5.5 Encryption Keys

a. SproutLoud's infrastructure is hosted in the Google Cloud for Collaboration and its Enterprise SaaS offering. Encryption keys for data at rest for the entire infrastructure are managed by Google

(https://cloud.google.com/docs/security/encryption/default-encryption). Client specific encryption keys are not supported for this purpose.

b. Client encryption keys can be generated and provided to encrypt data exchanged with clients (SFTP transfers, Email file exchanges etc). If keys are exchanged with customers for data transfer, they should be rotated at a maximum of every twelve months.

5.6 Software/Application Management

In order to ensure the security and compliance of SproutLoud's assets the installation and usage of software and SaaS applications are reviewed by the InfoSec team after an official request is submitted. The InfoSec team shall:

a. Analyze the usage and the scope of the application.
b. Review the privacy statements of the application mentioned on the request.
c. Depending on the data managed by the application, it might be categorized based on SproutLoud Data Classification Policy.
d. If the application handles data categorized as private or restricted, the InfoSec team will require that the application provides a SOC 2 Type II Report or any other equivalent document.
e. The InfoSec team will provide a recommendation to approve or reject the software based on the security assessment.
f. Periodic audits will be conducted to ensure compliance with this policy.
g. Non-compliance or security incidents related to software usage must be reported to the IT department and InfoSec team immediately.

6. Traveling Employees

6.1 Working Outside of the Country

Safeguards have been put in place to protect our data across our company's infrastructure in the locations that we operate. This includes the data located on employees' personal laptops. In the event that an employee travels outside of their home country, they must notify the Enterprise Collaboration and Security Team a minimum of 5 days before traveling. This is to ensure that the destination would not put company data at greater risk of being compromised. The ECS Team reserves the right to deny the request if deemed that company

data would be at a greater risk of being compromised. Please review the "Employees Working Outside their Normal Location" document for more details.

7. Policy Compliance

Violation of this policy may be grounds for disciplinary action.

6 Revision History

Date of Change	Responsible	Summary of Change	Version ID
2/2022	James Aggrey	Initial Release	1.0
4/2022	Anjan Upadhya	Tweaked language.	1.1
5/2022	James Aggrey	Added Section 5.3 - Mobile Device Access	1.2
6/2022	Anjan Upadhya	Added Section 5.4 - Physical Access	1.3
10/2022	James Aggrey	Added Section 6 - Traveling Employees	1.4
2/2023	James Aggrey	Added Section 5.5 - Encryption Keys	1.5
9/2023	Gustavo Malpica	Added Section 5.6 - Software/Application Management	1.6