sproutloud

Risk Assessment Policy

1. Overview

SproutLoud is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When SproutLoud addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Sproutloud will take every measure to ensure the safety of its clients data and address any issues proactively that compromise it.

2. Purpose

The purpose of this policy is to ensure that security risks are assessed on a periodic basis and whenever possible, on a real-time basis.

3. Scope

This policy applies to employees, contractors, consultants, temporary employees, and other workers at SproutLoud, including all personnel affiliated with third parties.

4. Policy

Network Operations and Security personnel will periodically assess internal and external security risks and document any irregularities or vulnerabilities. Risks must be assessed and documented a minimum of once per quarter.

Security risks are assessed using the following methods:

- Documents potential threats and vulnerabilities
- Rates the likelihood a vulnerability could be exploited
- Rates the impact a vulnerability would have on an organization if it is exploited
- Provides an overall risk rating for the vulnerability
- Provides mitigation techniques

All data throughout the enterprise should be encrypted at rest and in transit (on-premise storage, laptops, Google Drives) and behind 2-factor authentication. This specifically is mandatory for data classified as Restricted and High Impact per SproutLoud's Data Classification Policy.

All Stakeholders will be engaged early in the risk assessment process, ensuring their input and insights inform risk identification, prioritization, and mitigation strategies. Regular communication channels will be established to keep stakeholders informed and involved in ongoing risk management activities.

5. Policy Compliance

5.1 Compliance Measurement

Networking and security personnel will verify compliance to this policy every quarter through various methods, including but not limited to, business tool reports, internal and external audits.

5.2 Exceptions

None.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Revision History

Date of Change	Responsible	Summary of Change	Version ID
07/2018	Anjan Upadhya	Initial Release	1.0
4/2022	Gustavo Malpica	No changes	1.0
4/2023	Gustavo Malpica	No changes	1.0
4/2024	Gustavo Malpica	Added Stakeholders	1.1