Acceptable Use Policy

1. Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SproutLoud's established culture of openness, trust and integrity. Infosec is committed to protecting SproutLoud's employees, customers, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of SproutLoud. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review People and Organizational Development policies for further details.

Effective security is a team effort involving the participation and support of every SproutLoud employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at SproutLoud. These rules are in place to protect the employee and SproutLoud. Inappropriate use and/or data access exposes SproutLoud to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct SproutLoud business or interact with internal networks and business systems, whether owned or leased by SproutLoud, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at SproutLoud and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with SproutLoud policies and standards, and local laws and regulations. Exceptions to this policy are documented in section 5.2.

This policy applies to employees, contractors, consultants, temporaries, and other workers at SproutLoud, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by SproutLoud.

4. Policy

4.1 General Use and Ownership

4.1.1 SproutLoud proprietary information stored on electronic and computing devices whether owned or leased by SproutLoud, the employee or a third party, remains the sole property of SproutLoud. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

4.1.2 Client Confidential Information includes, but is not limited to, sales and marketing strategies, pricing data, sales data, buying habits or practices of Client or Client's Holders, marketing methods, marketing programs, marketing data, Client contact information, Sub-Account lists, usernames and passwords granting access to the Engine or any Licensed Software, information and data entrusted to SproutLoud by Client or Sub-Account, site launch kit materials, proprietary software applications including the Engine, source code, programming data, computer processes, email lists, research and development data, production workflows, costs, engineering processes, profit or margin information, finances, future business plans, programming techniques, terms of any contractual relationships, written and any other information and records used in SproutLoud's and Client's business, or any other information of, about or concerning SproutLoud's and Client's business, manner of operations, or any other data of any kind, nature or description which is not readily available and known to the public at large.

4.1.3 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of SproutLoud proprietary information and/or Client confidential information.

4.1.4 You may access, use or share SproutLoud proprietary information and/or Client confidential information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.5 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.6 An acceptable use of cloud services in a corporate setting includes securely accessing and utilizing cloud-based resources for work-related tasks while adhering to company policies on data privacy and security. This involves using cloud storage and applications for storing, sharing, and collaborating on documents, projects, and data that are relevant to job responsibilities. Employees should ensure data is encrypted, use strong passwords, and follow multi-factor authentication protocols. Sensitive company information must be handled according to data protection standards.

4.1.7 For security and network maintenance purposes, authorized individuals within SproutLoud may monitor equipment, systems and network traffic at any time, per Infosec's *Audit Policy*.

4.1.8 SproutLoud reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the principle of minimal access (zero trust model).

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 Network drive access is restricted to only drives and folders necessary to fulfill your assigned job duties.

4.2.4 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 7 minutes. You must lock the screen or log off when the device is unattended.

4.2.5 Postings by employees from a SproutLoud email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SproutLoud, unless posting is in the course of business duties.

4.2.6 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of SproutLoud authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SproutLoud-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SproutLoud.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SproutLoud or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting SproutLoud business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a SproutLoud computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any SproutLoud account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized

to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the SproutLoud network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, SproutLoud employees to parties outside SproutLoud.
18. Fulfilling requests for highly sensitive information, such as banking information, using channels outside of Google Workspace.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the ECS team.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within SproutLoud's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SproutLoud or connected via SproutLoud's network.

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using SproutLoud's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of SproutLoud's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate SproutLoud's policy, is not detrimental to SproutLoud's best interests, and does not interfere with an employee's regular work duties. Blogging from SproutLoud's systems is also subject to monitoring.

2. SproutLoud's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any SproutLoud confidential or proprietary information, trade secrets or any other material covered by SproutLoud's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of SproutLoud and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by SproutLoud's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to SproutLoud when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of SproutLoud. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, SproutLoud's trademarks, logos and any other SproutLoud intellectual property may also not be used in connection with any blogging activity

4.4 Phishing and Scams

Users must be vigilant in immediately deleting any messages, shared document requests, or other requests for information that seem suspicious or were not otherwise expected. Users receiving unexpected or suspicious requests should immediately contact the alleged sender by a trusted means of communication (i.e. Google Workspace channels) to confirm the legitimacy of the request. If a user succumbs to these types of requests, they must contact the ECS team immediately to have the potential security impact evaluated.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance per our Exception Policy

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. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy
- Exception Policy

7. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

8. Revision History

Date of Change	Responsible	Summary of Change	Version ID

12/2017	James Aggrey	Initial Release	1.0
04/2021	Dave Kinsella	Client Competitive Screen Additions	1.1
03/2023	James Aggrey	Added language regarding phishing and scams	1.2
03/2023	Gustavo Malpica	Changed Desktop Support for ECS Team	1.3
3/2024	Gustavo Malpica	4.1.6	1.4