Access Control Policy

1. Overview

See Purpose.

2. Purpose

To ensure that access controls are implemented and in compliance with IT security policies, standards, and procedures.

3. Scope

This policy applies to all SproutLoud employees and systems.

4. Policy

4.1 Account Management

InfoSec team shall:

4.1.1 Identify and select the following types of information system accounts to support organizational missions and business functions: individuals, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

4.1.2 Assign account managers for information system accounts mentioned in point 4.1.1.

4.1.3 Establish conditions for group and role membership.

4.1.4 Specify authorized users of the information system, group and role membership, and access authorizations (i.e. privileges) and other attributes (as required) for each account.

4.1.5 Require approvals by system owners to create information system accounts.

4.1.6 Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.

4.1.7 Monitor the use of information system accounts.

4.1.8 Have a process in place that allows managers to review access setup on a bi-monthly cadence and confirm with the InfoSec team that it is accurate.

4.1.9 When feasible, enforce Multi Factor Authentication controls on connections from systems or users accounts to sensitive systems.

4.1.10 Authorize access to the information system based on a valid access authorization or intended system usage.

4.1.11 Review accounts for compliance with management requirements on a bi-monthly basis.

4.1.12 Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

4.1.13 Employ automated mechanisms to support the management of information system accounts.

4.1.14 Ensure that the information system automatically disables temporary and emergency accounts after usage.

4.1.15 Ensure that any inactive accounts are deleted after two months.

4.1.16 Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

4.2 Access Enforcement

InfoSec team Shall:

4.2.1 Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

4.3 Information Flow Enforcement

InfoSec team Shall:

4.3.1 Ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

4.4 Separation of Duties

InfoSec team Shall:

4.4.1 Separate duties of individuals as necessary, to prevent malevolent activity without collusion.

4.4.2 Document the separation of duties of individuals.

4.4.3 Define information system access authorizations to support separation of duties.

4.5 Least Privilege

4.5.1 Employ the principle of least privilege, allowing only authorized accesses for users (or processing acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

4.5.2 Authorize explicit access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.

4.5.3 Restrict accounts with elevated privilege in the information system (SproutLoud systems/services, Subprocesses, etc)

4.5.4 Ensure that the InfoSec team audits the execution of privileged functions with the relevant account manager.

4.5.5 Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

4.6 Unsuccessful Login Attempts

4.6.1 Locks the account automatically after 5 unsuccessful login attempts for 15 minutes on the endpoints or until the administrator unlock the account manually for company managed endpoints.

4.6.2 Locks the account automatically after 5 unnecessary attempts for 30 minutes or until the administrator unlock the account manually for SproutLoud managed applications (app.sproutloud.com, developer portal, etc)

4.7 Session Lock

4.7.1 Prevent access to the system by initiating a session lock after 7 minutes of inactivity on endpoints.

4.7.2 User logout is initiated after 30 minutes of inactivity on SproutLoud-developed applications.

4.7.3 Retain the session lock until the user reestablishes access using established identification and authentication procedures.

4.7.4 Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

4.8 Access Termination

4.8.1 Ensure that access is terminated for individuals no longer needing access (position change or termination) within 24 hours of being notified. If the account is privileged, access should be removed as soon as possible, but not exceeding 24 hours.

4.9 Remote Access

4.9.1 Establish and document usage restrictions, configuration/connection requirements, authentication methods and implementation guidance for each type of remote access allowed.

4.9.2 Ensure that the remote connections are being monitored and controlled.

4.9.3 Ensure that the cryptographic mechanisms are implemented per SproutLoud's encryption policy and protect the confidentiality and integrity of remote access sessions.

4.9.4 Ensure that all the remote access traffic is routed through a bastion host and proxy (where relevant) to reduce the risk of external attacks.

4.9.5 Authorize the execution of privileged commands and access to security-relevant information via remote access only for DevOps team members, ECS team members and/or Lead Architects.

4.10 Third-Party Access:

4.10.1 Ensure Third-Party Access to SproutLoud systems are reviewed and approved by the InfoSec team. Additionally, maintain monitoring and reviewing controls for Third-Party permissions.

4.11 Wireless Access

4.11.1 Establish usage restrictions, authentication methods, configuration/connection requirements, and implementation guidance for wireless access.

4.11.2 Ensure that wireless access protects users and devices by only allowing encrypted connections per SproutLoud's encryption policy.

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 and noted in the exception sheet 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

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;

NIST Federal Information Processing Standards (FIPS) 199

7 Revision History

Date of Change	Responsible	Summary of Change	Version ID
10/11/2022	Gustavo Malpica	Initial Release	1.0
12/16/2022	Anjan Upadhya	Edits	1.0
3/7/2024	Gustavo Malpica	Added 4.1.9 & 4.10	1.1