Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of SproutLoud Media Network, LLC (SproutLoud)'s resources. All users, including contractors and vendors with access to SproutLoud systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any SL facility, has access to the SproutLoud network, or stores any non-public SproutLoud information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must not use the same password for SproutLoud accounts as for other non-SproutLoud access (for example, personal ISP account, option trading, benefits, and so on).

4.1.3 Where possible, users must not use the same password for various SproutLoud access needs.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every three months. Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential SproutLoud information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. We implement Keeper Security as a solution when single authentication needs to be shared across multiple users. This ensures that username/passwords are not being shared and known to multiple people.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share SproutLoud passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members. Credentials should only be shared as described in section 4.3.1.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, 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.

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

- Password Construction Guidelines

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/

- Simple Network Management Protocol (SNMP)

8 Revision History

Date of Change	Responsible	Summary of Change	Version ID
12/2017	James Aggrey	Initial Release	1.0
06/2020	James Aggrey	Updated program used for password sharing, clarified sharing usage terms	1.1