



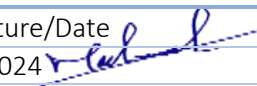
Password Protection Policy

| Doc. Control Number | Version |
|---------------------|---------|
| SNL-56 | 1.1 |



Document Reference

| Item | Description |
|---------------|----------------------------|
| Title | Password Protection Policy |
| Department | Cybersecurity department |
| Version No | 1.1 |
| Status | Draft |
| Type | DOCX |
| Publish-Date | 8 August 2024 |
| Revision-Date | 8 August 2025 |

| Authors | | |
|-------------------|---------------------------------|--|
| Name | Department | Signature/Date |
| Muhaned Kamal Ali | Cybersecurity - I. S Specialist | 8/8/2024  |

| Reviewed by | | |
|-------------|-----------------------------------|---|
| Name | Department | Signature/Date |
| Yasir Awad | Head of Cyber Security Department | 8/8/2024  |

| Approved by | | |
|---------------------|------------|--|
| Name | Department | Signature/Date |
| Abdullah Al Shuhail | V.P | 8/8/2024  |

Control-Page

| Document Amendment Record | | | |
|---------------------------|----------------|-------------|--|
| Version-No | Date | Prepared-by | Explanation |
| 0.1 | June 2018 | Muhaned Ali | First Release |
| 0.2 | July 2021 | Muhaned Ali | Updated and converted to a new format |
| 0.3 | September 2021 | Muhaned Ali | Password protection has been updated. |
| 1.0 | August 8, 2023 | Muhaned Ali | The policy has been updated and reviewed |
| 1.1 | August 8, 2024 | Muhaned Ali | The policy has been reviewed |



Contents

| | |
|----------------------------|---|
| 1. Overview | 4 |
| 2. Purpose | 4 |
| 3. Scope..... | 4 |
| 4. Policy | 4 |
| 5. Policy Compliance | 5 |

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of our resources. All staff, including contractors and vendors with access to SNLC 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 and the protection of those passwords.

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 SNLC facility, has access to the SNLC network, or stores any non-public SNLC information.

4. Policy

4.1 Password Creation

- a) All user-level and system-level passwords must conform to the Password Construction Guidelines.
- b) Users accessing applications and information systems must be issued unique user logins and passwords. Generic accounts must not be allowed.
- c) Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own personal accounts.
- d) 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. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.2 Password Change

- a) Passwords should be changed only when there is reason to believe a password has been compromised.
- b) Passwords should be changed every 90 days.
- c) Minimum length: 8 alphanumeric characters and special characters.
- d) History: last 12 passwords.
- e) Account lockout threshold: 10 invalid login attempts.
- f) Screen saver settings: automatically locked within 15 minutes of inactivity.
- g) 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 follow the Password Construction Guidelines.

4.3 Password Protection

- a) Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential SNLC information.
- b) Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.
- c) Must not write down, electronically store, or disclose any password or authentication code that is used to access Assets or Critical Facilities.
- d) Passwords may be stored only in "password managers" authorized by the organization.
- e) Do not use the "Remember Password" feature of applications (e, g. Google Chrome, Microsoft Edge, Firefox, and Internet Explorer).
- f) Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.
- g) HR will inform the ARAMCO's team by email when credentials are no longer required.

4.4 Multi-Factor Authentication

- a) Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.
- b) Multi-factor authentication must be enforced on all remote access, including access from the Internet to Company resources.
- c) Multi-factor authentication must be enforced on all privileged accounts access, including remote access to information systems and applications.

4.5 Cloud Application

- a) Multi-factor authentication must be enforced on all Cloud services access, including access to cloud-based email.
- b) Google workplace is used by SNLC for email services.
- c) FortiClient is used for remote access.
- d) Dafater ERP system.

4.6 Cloud Application Access Control Procedures (Email)

- a) The HR department will send an email to the IT department to create an email account for the new employee and add them to the members group.
- b) The IT department will generate and send email details.
- c) The HR department will inform the employees of all details and enable MFA.
- d) The HR department will inform the new employee of all the details of the new email and send him how to activate the multi-factor authentication (MFA).

4.7 Remote Access Control Procedures (FortiClient)

- a) The engineer will request remote access from his manager.
- b) After the line manager agrees to this, an email will be sent to the Information Security Manager.
- c) The information security department will establish remote access on time.
- d) The SNLC employee will follow the rules and procedures for remote access.
- e) After completion, the Information Security department will delete the account.

5. Policy Compliance

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

5.1 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.2 Non-Compliance

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