




Identity and Access Management Policy


Doc. Control Number	Version
SNL-18	0.3



Document Reference

Item	Description
Title	Identity and Access Management Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	25 March 2024
Revision-Date	25 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	25/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	25/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	25/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	12 June 2022	Muhaned Ali	First Release
0.2	31 May 2023	Muhaned Ali	The policy has been updated
0.3	25 March 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Overview	4
2. Policy Guidelines	4
3. Compliance and Enforcement.....	6
4. Policy Review	6

1. Overview

This policy establishes the principles and guidelines for effective Identity and Access Management (IAM) within SNLC. It aims to ensure the secure and efficient management of user identities, access rights, and authentication processes. The policy covers user account creation, privilege accounts, access rights granting and revoking, authentication and authorization requirements, and password management. The implementation of this policy is crucial to safeguard sensitive information, protect against unauthorized access, and maintain the integrity of SNLC's digital assets.

2. Policy Guidelines

2.1 User Accounts and Privilege Accounts

- a) User accounts shall be created for individuals who require access to SNLC's information systems, applications, and data to perform their job duties.
- b) Privilege accounts with elevated access rights shall be granted only to authorized personnel and in accordance with the principle of least privilege.
- c) All user and privilege accounts shall be reviewed and approved by the respective data owners or system administrators.
- d) All privileged accounts must be limited, justified, and reviewed on a regular basis.

2.2 Granting and Revoking Access Rights

- a) Access rights shall be granted based on Role-Based Access Control (RBAC), ensuring users have access only to the minimum information necessary for their job roles.
- b) Access requests shall be submitted through an established process and be documented for audit and accountability purposes.
- c) Access rights shall be promptly revoked or modified when no longer required due to job changes, transfers, or termination of employment.

2.3 Authentication and Authorization Requirements

- a) Remote access to SNLC's systems and data shall require strong authentication methods, such as two-factor authentication (2FA) or multi-factor authentication (MFA).
- b) User authentication and authorization shall be managed based on the access control principles of need-to-know, need-to-use, principle of least privilege, and segregation of duties.
- c) An up-to-date Access Control List (ACL) shall be maintained to track user access rights and privileges.

2.4 Password Management Requirements

- a) Password complexity rules shall be enforced to ensure strong and secure passwords that are resistant to unauthorized access.
- b) Passwords shall be stored using industry-standard encryption mechanisms to protect against unauthorized access.
- c) Passwords shall be changed at regular intervals, and users shall not reuse previous passwords.

2.5 Process for Allocating/Revoking User Right

- a) Access Rights Allocation
 - User access rights shall be granted based on their roles and responsibilities, as defined in the RBAC framework.

- Changes in job functions or departments shall trigger a review and reallocation of user access rights to ensure continued appropriate access.
- b) User Authentication and Authorization
 - Access rights shall be granted based on the principle of least privilege, allowing users only the access they require to perform their job duties effectively.
 - The Access Control List (ACL) shall be regularly updated to reflect any changes in user roles and privileges.
- c) Access Rights Revocation
 - Upon the termination of employment or contractual agreements, all access rights to the SNLC's information systems shall be promptly revoked to prevent unauthorized access.

2.6 Regularly Review

- a) Determine the review frequency based on the criticality of information assets and the sensitivity of data accessible through user accounts.
- b) User identities and access rights for critical systems should be reviewed monthly.
- c) Consider the risk associated with different account types (e.g., regular user accounts, privileged accounts, administrative accounts) when determining the review cycle.

2.7 Identify Responsible Roles

- a) Designate responsible roles for conducting the reviews, such as data owners, system administrators.
- b) Clearly define the responsibilities of these roles in the review process and ensure they understand the importance of maintaining access control principles.

2.8 Conduct Regular Access Reviews

- a) Regularly perform access reviews for all user accounts, ensuring they are aligned with the principle of least privilege.
- b) Review the permissions granted to each user and validate that they are necessary for their job roles and responsibilities.

2.9 Review & Revoke Access Policy

- a) Review & Revoke Access form should be used mandatorily whenever any SNLC company employee is going on Annual leave, Transferred, resigned, or no longer associated with SNLC company.
- b) SNLC company must inform Saudi Aramco when employees provided with Saudi Aramco user credentials no longer need their access, or are transferred, re-assigned, retired, resigned, or no longer associated with SNLC company.
- c) All the assets related to SNLC company or Saudi Aramco must be retrieved or revoked whenever any employee is resigning, retired & terminated.
- d) Review & Revoke Access form must be maintained mandatorily for all assets used to process or store Saudi Aramco data and information to sanitize the end of the Data Life Cycle, or by the of the retention period as stated in the contract, if defined.

This includes all data copies such as backup copies created at any sites of SNLC company. SNLC shall certify in writing to Saudi Aramco that the data sanitization has been completed.

2.10 Document Review Findings

- a) Document the results of access reviews, including any identified discrepancies or outdated access rights.
- b) Keep track of the actions taken to address any issues found during the review.

2.11 Review High-Risk Accounts More Frequently

- a) Identify high-risk accounts, such as privileged accounts and accounts with access to highly sensitive data.
- b) Conduct more frequent reviews for high-risk accounts to minimize potential security risks.

3. Compliance and Enforcement

- 3.1 Compliance with this policy is mandatory for all employees, contractors, and individuals with access to SNLC's systems and data.
- 3.2 Non-compliance with this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.

4. Policy Review

- 4.1 This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.