Information Security Management System (ISMS)

Policy Document Information – Password Management Policy

Documented information Name: Policy Document Information – Password Management Policy

Version No: 3.0

Last Updated: 25th July, 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Policy Documented information – Password Management Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Password Management.

Documented information Publication History

(All revisions made to this documented information must be listed in chronological order, with the most recent revision at the top)

Type of Information	Documented information Data
Documented information Title	Policy Documented information – Password Management
Documented information Code	SESAIT/ISO27001/ISMS_Policy_Password Management
Date of Release	05-12-2014
Documented information Revision	25-July-2023
Documented information Owner	IT Department
Documented information Author(s)	Arjun N Rao – Wipro Consulting Services
Documented information Change Reviewer	Sandhya Khamesra - Pricoris LLP
Checked By	Dileep Singh - CISO
Security Classification	Internal Use
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature	Date Approved
1	Shobha Raikar (CITO-I&S)	Shobha.raikar@vedanta.co.in	Electronically Approved	10-Aug 2023

Documented information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.1	10-Feb-2016	Company name logo update		18-Feb-2016
1.2	13-Feb-2017	Policy Review		18-Feb-2017
1.3	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.4	01-Jul-2017	Split password controls	4	05-Jul-2017
1.5	21-Aug-2018	Policy review		28-Aug-2018
1.6	22-Aug-2019	Policy review		30-Aug-2019
1.7	08-Sep-2020	Policy review		15-Sep-2020
1.8	28-Sep-2021	Policy Review and Update	1.1	21-Oct-2021
2.0	18 March-2022	Policy Review		04-April-2022
2.1	23 Sept 2022	Policy review and update	1.1	27-Sept-2022
2.2	21-June-2023	Updated Policy Details	3.0	30-Jun-2023
3.0	25-July-2023	Reviewed and Updated	3.0	10-Aug 2023

Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep Singh	dileep.singh@vedanta.co.in

Table of Contents

1. Introduction

1.1 Scope

This Policy document is applicable for Vedanta Limited – Sesa Goa Iron Ore Division including SRL and SMCL in Goa, Karnataka, Odisha and Liberia, Pig Iron Division, Met Coke Division, Power Division in Goa, Sesa Coke- Vazare & Gujarat, FACOR – Odisha, MALCO Energy and Nickel Business, VGCB, Visakhapatnam and Sesa Cement referred as Sesa Group in this document.

The policy covers all equipment's within the organization. It intends to establish adequate controls for password management of systems within the organization

1.2 Purpose of the documented information

This policy defines the controls that need to be implemented and maintained to protect information assets against unauthorized access through vulnerable Password Management that would pose as a substantial risk to the organization.

1.3 Audience

This policy is applicable to employees, contract employees and vendor employees who are utilizing, consuming, managing, and supporting the Information assets within Sesa Group.

2. Policy Statement

Any logical access to Sesa Group's 'Information Processing Systems' shall be controlled on the basis of business and security requirements. Access to information assets and rules governing such access shall be defined and documented.

3. Policy Details

- The password policy must be defined and made applicable for all users and information systems.
- The password policy must be enforced through appropriate configuration of the operating systems, applications, network devices, and access management systems.
- Passwords shall be distributed to user(s) in a secure manner.
- Passwords shall be selected carefully and following security controls shall be ensured.
    - Users shall be forced to change their passwords upon its first use
    - Systems shall be configured to accept case sensitive passwords.
    - The passwords must be at least twelve characters in length
    - Passwords must be complex as mentioned below
        1. Password must contain at least five characters.
        2. Password must contain five numerals.
        3. Password must contain two special characters.
        4. Password must contain one capital letter.

  Above all four conditions must be meeting in order to achieve password complexity.
    - Passwords for all user and privilege accounts shall expire in 45 days.
    - Administrator account password is changed once in 6 months and hardcopy of the same is kept in Safe.

- Systems must not accept last ten passwords or passwords entered during the last 12 months
- A maximum of five successive login failures shall result in a user's account being locked out.
- A record of ten previous passwords shall be maintained to prevent re-use of these passwords
- Any account locked out due to invalid logon attempts must be reset by the respective System Administrator. Account resetting must be done only on written request from the concerned employee
- Account lockout duration and Reset account lockout duration for rest of the users shall be set to minimum 10 minutes.
- If any tool is deployed for password reset and generation then password shall be reset by the tool.
- Passwords shall not be displayed in clear text when they are being keyed in.

- In-house and custom developed application must have provision to implement the password policy.
- Passwords are mandatory for all user accounts on all network and standalone information systems.
- System must force the user to change the password (assigned by the system administrator or Help Desk) at time of first logon
- Passwords shall be encrypted during transmission and storage on all system components.
- Support procedures shall be in place to deal with forgotten passwords and account lockouts.
- User password reset requests shall be acted upon only after validating the identity of the requestor. Passwords shall be communicated to the owner of the ID.
- Users shall be forced to change their password matching password complexity requirements on the first use after passwords are reset.
- A secure 'Password List' shall be maintained for all critical accounts in sealed envelopes. This list shall be maintained by the nominated person from the IT department. Only authorized individuals shall have access to these envelopes.
- Passwords shall not be coded into logon scripts, batch programs, databases or any other executable files when user authentication or authorization is required to complete a function.
- Users must input all passwords themselves, when receiving technical assistance instead of sharing the passwords with the helpdesk.
- Due to system limitations or business necessity, if any of the password and account policy parameters cannot be followed, specific mechanisms must be put in place to obtain approvals and implement countermeasures to mitigate the risk of not following the password policy
- The password for privileged users (e.g. Administrator, User IDs with special Privileges etc.) on information systems including network and security devices must be stored in two separate sealed envelopes and placed under custody of CITO / CISO. Only authorized employee(s) must be granted access to this password, in the event that the administrator cannot be reached during an emergency. The event must be recorded and the password must be changed immediately after use.
- IT operation team need to ensure password policy implementation
- Any exception to this shall require formal approval from the Chief Information Security Officer (CISO / CDIO).

4. Split Password Controls

- Split password authentication must be implemented for critical applications.
- Each authentication server for split password implementation must be deployed on a physically separate machine.

- An inventory list of applications shall be maintained containing list of applications on which split password authentication has been implemented.
- Annual review of the inventory list shall be carried out to verify whether any new applications need split password authentication to be implemented

5. Enforcement

All employees, vendors and third parties shall follow the policy; violation of this can lead to disciplinary action, termination of contract, civil action or financial penalties.

6. References and Related Policies

- Identity and Access Management

7. Control Clauses Covered

- A9.1.1, A9.2.1, A9.2.2