vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Policy Document Information – Remote Access Policy

Documented information Name: Policy Document Information – Remote Access Policy

Version No: 3.0

Last Updated:25-July-2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Policy Documented information – Remote Access Policy

Abstract: This Documented information is a procedure Documented information highlighting the policies for acceptable usage of information assets.

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 – Acceptable Usage
Documented information Code	SESAIT/ISO27001/ISMS_Policy_Remote Access
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
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	21-Aug-2018	Policy review		28-Aug-2018
1.5	22-Aug-2019	Policy review		30-Aug-2019
1.6	08-Sep-2020	Policy review		15-Sep-2020
1.7	04-Nov-2020	Policy update as per Group policy update	3.1	11-Nov-2020
1.8	28-Sep-2021	Policy Review and Update	1.1	21-Oct-2021

2.0	18-March-2022	Policy Review and Update		04-April-2022
2.1	23 Sept 2022	Policy review and update	1.1	27-Sept-2022
3.0	25-July-2023	Policy review and update		10-Aug 2023

Documented information Contact Point

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

Table of Contents

vedanta | sesa goa iron ore

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 intends to provide controlled remote access to Sesa Group Internal network. This helps safeguard unauthorized access into Sesa Group Systems and unauthorized use of Sesa resources

1.2 Purpose of the documented information

The purpose of this policy is to guide all users of Sesa Group about appropriate handling of remote access

1.3 Audience

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

2. Policy Statement

The security policy of Sesa Group is as follows:

“Sesa Group is committed to delivering customer excellence by ensuring Availability of Information while adhering to the most stringent standards of Integrity and Confidentiality.”

The assured business continuity of Sesa Group is therefore dependent upon the fact that the security of Information Assets in the form of data, and information processing systems is not compromised at any point in time.
All employees must ensure the security of these information assets by protecting them from unauthorized use, modification, disclosure or destruction, whether accidental or intentional.
It is mandatory that employees shall make themselves aware of the Information Security Policies and Procedures which are available at the portal: http://sgl-panj-sp-01/sites/sesaportal. It is expected and required that users must abide by Sesa Group’s Information Security Policies and Procedures. Any employee found violating the Information Security Policies and Procedures would be liable for Disciplinary action.

3. Policy Details

All employees of Sesa Group shall abide by the guidelines mentioned below to comply with Sesa Group’s Information Security Policy.

3.1 Remote access to Sesa group resources

- Identification and authentication of users should be done before giving remote access to Sesa group resources
- Secured communication channels such as SSL or IPSEC should be used to provide remote access to intranet-based applications
- VPN access to Sesa's resources shall be authenticated by the Active Directory.
- User Authentication for establishing VPN session shall be encrypted.
- All remote access/teleworking access must be logged and an adequate amount of information must be captured to assist with investigations and to detect misuse of the remote access service.
- Remote access logs and access denial logs shall be maintained
- Remote access to systems by vendors & system administrators shall be as per defined agreements with the vendor
- Employees shall not extend remote access to Sesa Group Intranet resources to unauthorized personnel including family and friends.
- Users shall not connect the desktop/laptop to Intranet & Internet network (includes datacards) simultaneously
- Remote access to systems using Mobile devices shall be protected as per Acceptable Mobile Phone Policy
- Users shall exercise caution while using mobile devices and connecting to Sesa Group network remotely from public places, meeting rooms and other unprotected areas
- Dial-out and Dial-in connectivity from/to the Sesa backbone as well as restricted network shall only be allowed after authorization
- Employees within the company network are not permitted to access external systems through dialup-up modems connected to a landline voice phone.
- External modems must not be installed with any PC until authorized by the authorized personnel.
- The Data Cards / mobile phones / modems for accessing Internet/VPN must be used only under the following conditions.
    - The provision of data card to the user is approved by the user's manager
    - The data card service provider is approved by the company
    - Antivirus is updated with latest definitions
    - The Operating System is updated with the latest patches
    - The personal firewall is enabled
    - File sharing is disabled
    - The user computer is disconnected from Local network (wired/ Wireless)
- For all users accessing the organization's network must minimally have the below requirements:
    - Antivirus must be installed and must have the latest signatures updated.
    - Latest patch updates for the OS and Security should be preferably installed on the system.

4. Abbreviation

- None

5. Control Clauses Covered

A6.2.1, A6.2.2