vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Policy Document Information – DLP Policy

Documented information Name: Policy Document Information – DLP Policy

Version No: 3.0

Last Updated: 18-September, 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Policy Documented information DLP Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for DLP Policy.

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 –DLP Policy
Documented information Code	SESAIT/ISO27001/ISMS_Policy_ DLP Policy
Date of Release	16.01.2012
Documented information Revision	3.0
Documented information Owner	IT Department
Documented information Author(s)	Sujay Maskara – Wipro Consulting Services Arjun N Rao – Wipro Consulting Services
Documented information Change Reviewer	Sandhya Khamesra, Pricoris LLP
Checked By	Dileep Singh – CISO
Security Classification	Internal
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature	Date Approved
1	Shobha Raikar (CDIO)	Shobha.raikar@vedanta.co.in	Electronically Approved	03-Oct 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	31-Aug-2017	DLP Process update		31-Aug-2017
1.5	21-Aug-2018	DLP Process update	3	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-Mar-2022	Policy update as per Data Governance review & recommendation, Removed Encryption from this policy.	1.1	01-April-2022
2.1	23-Sep-2022	Policy Review and Update	1.1	28-Sept-2022
3.0	18-Sep-2023	Review and Update		03-Oct 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, Orissa and Liberia, Pig Iron Division, Met Coke Division , Power Division in Goa , Sesa Coke – Vazare and Gujarat , FACOR – Orrisa , Nickel business and VGCB , Visakhapatnam referred as Sesa Group in this document.

The policy intends to protect information and information processing assets of Sesa Group used by its employees.

1.2 Purpose of the documented information

The purpose of this policy is to guide all users of Sesa Group about the protection of sensitive information both at rest and transit through suitable encryption.

1.3 Audience

This policy is applicable to employees who comprise of 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.
Also, it is necessary to ensure that no information residing in a computer resource is deleted, or its value diminished or its utility affected so as to cause wrongful loss or damage to the public or any person All employees must ensure the security of sensitive data by using encryption technology.

3. Policy Details

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

- DLP agent to be deployed for all the end user systems using Sesa IT services and AD group policy.
- DLP agent will monitor and provide control management the following – ○ Corporate email flow ○ USB data copied ○ Network data transfer ○ Printing usages
- IT Operation team will extract the one-month logs and provide to DLP review team during first week

.

- DLP review team to review the monthly incidents and observation from logs with analysis, the members of team are – ○ Fedora De Souza ○ Pradipta Boruah
  - ○ Prabhudatta Sahoo

- Suspected data transfer as per review and incident analysis on monthly basis will be send for user clarification with his HOD comments.
- Final report with details will be send to CISO for review and recommendation of action plan for noncompliance, in case of non-satisfactory response user system access id to be disabled for proper justification.
- CISO has to forward the final review report for CDIO (IOB) information & review comments.
- The review process need to be completed within one month timeframe.
- For ID enabling approved can be given by CISO (IOB) / CDIO (IOB)
- DLP can be disabled in case of Data transfer during system transfer with CISO (IOB) / unit HeadIT approval.

4. Abbreviation

- None

5. Control Clauses Covered

A.18.1.5