vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Policy Document Information – Incident Management Policy

Documented information Name: Policy Document Information – Incident Management Policy

Version No: 3.0

Last Updated: 18-Sep-2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Policy Documented information – Incident Management Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Incident 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 – Incident Management Policy
Documented information Code	SESAIT/ISO27001/ISMS_Policy_Incident Management 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	28-03-2013	Sesa Goa Logo Change		28-03-2013

1.2	18-10-2013	Sesa Group Logo, file name changes for Sesa Sterlite Ltd - IOB		18-10-2013
1.3	21-01-2014	Sesa Sterlite Logo incorporated,	3.1.2	22-01-2014
		Position Head IT replaced with GMIT / Head-IT		
1.4	01-12-2014	Aligned to ISO 27001:2013, Vedanta group policy	1.1,3.1,3.2,6	05-12-2014
1.5	09-01-2015	Reviewed and updated as per Internal audit	3.1	15-01-2015
1.6	10-Feb-2016	Company name logo update		18-Feb-2016
1.7	13-Feb-2017	Policy Review		18-Feb-2017
1.8	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.9	21-Aug-2018	Policy review		28-Aug-2018
1.10	22-Aug-2019	Policy review		30-Aug-2019
1.11	08-Sep-2020	Policy review		15-Sep-2020
1.12	28-Sep-2021	Policy Review and Update	1.1	04-Oct-2021
2.0	18 Mar -2022	Policy Review and Update		04- April-2022
2.1	23-Sept-2022	Policy review and update	1.1	27-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, Odisha and Liberia, Pig Iron Division, Met Coke Division, Power Division in Goa, Sesa Coke, FACOR – Odisha, MALCO Energy and Nickel Business, VGCB, Visakhapatnam and Sesa Cement referred as Sesa Group in this document.

The policy is applicable to those incidents which have a significant probability of disrupting business operations and threatening the information security of the organization. The policy also states the requirements for creating awareness about the procedures for reporting information security incidents and about the contact points to whom the incidents must be reported.

1.2 Purpose of the documented information

Incident management policy aims at ensuring that Sesa Group establishes a strategy for managing information security incidents resulting in a coordinated and orderly response for incidents.

1.3 Audience

This policy is applicable to all 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

Information security incident reporting and management procedures and responsibilities shall be established to ensure quick, effective and orderly response to security incidents.

3. Policy Details

3.1 Information Security Incident

Information security incident is any event that has the potential to affect the confidentiality, integrity or availability of information in any format and/or indicates at a possible breach of ISMS framework and/or indicates a failure of information security controls affecting business operations.

3.2 Reporting of Information Security Events and Weaknesses

3.2.1 Reporting Information Security Events

- A formal information security reporting procedure shall be defined and implemented to ensure that information security events are reported as quickly as possible through appropriate management channels

- Appropriate training shall be provided to all the users to create awareness on information security incident reporting procedures along with the responsibilities for addressing security breaches.
- The user shall not attempt to perform any investigations, which could unintentionally compromise the investigation or contaminate evidence. The user shall not attempt to 'clean- up' until directed to do so by the Chief Information Security Officer. A key aspect of incident investigation is preservation of evidence.

3.2.2 Reporting Security Weaknesses

- All users of Sesa Group and administrators of IT systems shall note and report any observed or suspected security weaknesses in systems and services on to the service desk/ FMS or to their HOD or to the Chief Information Security Officer/ CDIO / Head-IT as quickly as possible in order to prevent any possibility of information security incidents.

3.3 Management of Information Security Incidents and Improvements

3.3.1 Responsibilities and Procedures

- All information security incidents shall be promptly, effectively and orderly investigated.
- Procedures and responsibilities shall be defined and documented to handle different types of information security incidents.
    - Along with the application of normal contingency plans, the procedures shall be set for the following: ○ Appropriate analysis of information security incidents and identification of root cause of the incidents
    - Immediate actions to be taken for suppressing the impact of the incident ○ Implementation of corrective actions to prevent recurrence of the incident
    - Proper communication with the affected parties and people involved in the recovery process after the occurrence of the incident
    - Reporting of impact faced and actions taken by the appropriate authorities
- Action to recover from security incidents and correct system failures shall be carefully and formally controlled and recorded; in particular the procedures shall ensure that:
    - Information security incidents are recorded. ○ Only authorized personnel with adequate knowledge/skills are allowed to access affected systems and data. ○ Actions are taken to limit the impact of a security incident by isolating the problem as narrowly as possible.
    - All emergency actions taken are documented in detail. ○ The integrity of information systems and controls is confirmed with minimal delay. ○ Suitable feedback is provided to the person/s who reported the information security incident after the incident has been dealt with and closed.
- A logbook shall be maintained for all security incidents. The information to be logged must include the following:
    - Date and Time of Incident ○ Description of Incident
    - List of all information system equipment/ components that have been affected ○ List of all the people that have been contacted during recovery ○ Resolution of the detected vulnerability

3.3.2 Learning from Information Security Incidents

- All information security incidents shall be analyzed to identify:
    - recurring information security incidents ○ high impact incidents

- enhancements to existing controls or additional controls to be deployed to limit the frequency and impact of future occurrences ○ any gaps in the current security policy and initiate review of the same.

3.3.3 Collection of Evidence

- In information security incidents involving follow-up or legal action against a person or organization, evidence shall be collected, retained and presented to conform to the rules for evidence laid down in relevant jurisdiction(s).
- Evidence collected must be kept secured from any kind of destruction either accidental or intentional. In case of documented information evidence, a complete care shall be taken to ensure that the original of the documented information cannot be tampered by any means. In case of information or computer media-based evidence, at least one mirror image or copy of the original shall be taken and kept securely.

4. 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.

5. References and Related Policies

- None

6. Control Clauses Covered

A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7