vedanta | sesa goa iron ore

Information Security Management System (ISMS) Policy Document Information – Vendor Security Policy

Documented information Name: Policy Document Information – Vendor Security 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 – Vendor Security Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Vendor Security 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 – Vendor Security
Documented information Code	SESAIT/ISO27001/ISMS_Policy_ Vendor Security
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	19-Mar-12	Scope; NDA Clauses, Vendor clauses as per vetted comments from Legal Advisor	1.3; 2.0; 3.1.2; 3.12; 3.1.3	19-Mar-12
1.2	28-03-2013	Sesa Goa Logo change		28-03-2013
1.3	18-10-2013	Sesa Group Logo , file name change for Sesa Sterlite Ltd - IOB		18-10-2013
1.4	25-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT	3.3.1	27-01-2014
1.5	01 – 12 -2014	Aligned with ISO 27001:2013	1.1,3.1,3.2,3.3,5,6	05-12-2014
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	17-Jan-2020	NDA format removed, need to be taken from legal	7	17-Jan-2020
1.12	08-Sep-2020	Policy review		15-Sep-2020
1.13	28-Sep-2021	Policy Review and Update	1.1	21-Oct-2021
2.0	18-Mar-2022	Policy review		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

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.

This policy is applicable to all third parties' vendors and third parties' employees associated with the management of the information systems of Sesa Group.

1.2 Purpose of the documented information

For the purposes of this documented information, a 'vendor' is a service provider who associates with Sesa Group and is involved in handling, managing, storing, processing and transmitting information of Sesa Group.

1.3 Audience

The policy covers all vendors and vendor's employees working with Sesa Group. The vendors could be a service provider as mentioned below but not limited to:

- Product Third parties
- Service Engineers

1.4 Service Providers

- Facilities maintenance agencies for data center/server rooms
- Consultants
- Technology Partners
- Auditors

2. Policy Statement

Sesa Group's information assets and information processing facilities that are accessed, processed, communicated to, or managed by external vendor shall be adequately protected.

3. Policy Details

3.1 Identification and Mitigation of Risks

3.1.1 Vendor Security

- All vendors are required to adhere to Sesa Group Vendor Security Policy. If the vendor sub-contracts any service/work pertaining to Sesa Group, the sub-contracted parties and their employees are also required to adhere to the vendor security policy.
- In accordance with the vendor security policy, all vendors shall be required to submit specified documented information such as the Vendor security agreement, Non-disclosure agreement, Legal Agreement, etc. pertaining to information security prior to any engagement.
- In accordance with the vendor security policy, vendors shall be subjected to independent reviews of their compliance with the policy.

3.1.2 Identification of Risks related to Vendors

- Access by vendors to information assets and IT facilities shall be formally assessed and documented for associated risks. The risk assessment shall take the following into account:
  - the type of access required
  - the value and sensitivity of the information involved
  - duration of access required

- controls implemented by the external party when storing, processing, communicating, sharing and exchanging information
- controls implemented by Sesa Group to limit/restrict access
- legal, regulatory and any other contractual obligation
- the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information
- practices and procedures followed by external party to deal with information security incidents and potential damages

- Security team shall review the risk assessment carried out and the results shall be presented to Information Security Management Committee for documentation of Acceptable Risk. Further, a Risk Assessment of the same shall be carried out once every year or before renewal of the contract; whichever is applicable.
- Security requirements identified from risk assessment must be reflected as security conditions in third party contract.
- Access to all classified information shall be documented and carried out in a controlled fashion. A list of personnel is to be maintained to ensure that only the listed personnel have legitimate access to the Information System areas. Any change in personnel shall go through a Change Control process.
- All third-party personnel shall be given the Access Cards/Identification badges based on need. The Access Cards/Identification badges given to the personnel shall be marked as Non-Transferable and Returnable on termination of contract. 'Physical& Environmental Security Policy' and 'Identity & Access Management Policy' shall be referred for detailed clauses to be followed while dealing with vendors.

3.1.3 Addressing Security in Third Party Contracts

- Arrangements involving external party access to Sesa Group's information assets shall be based on a formal contract that defines the terms and conditions of access. All critical contractual agreements shall be reviewed by the Company legal department
- The well-defined security provisions shall be included in all contracts governing vendor access to Sesa Group's information. Sample provisions to be included in contract have been defined in "vendor security procedures".
- Vendors shall be made aware of and shall accept their obligations, responsibilities and liabilities involved in accessing, processing, communicating, or managing Sesa Group's information and IT facilities before commencement of the Vendors/third parties association with Sesa Group in providing services to Sesa Group.

3.1.4 Addressing Security in Outsourcing Contracts

- The risks posed by outsourcing the management of all or part of the facilities or information systems, networks and/or desktop environments must be evaluated.
- Risk mitigation measures where possible must be addressed in a contract agreed between the parties.
- The contract must include the following:
  - Availability of services in event of a disaster.
  - Security responsibilities of the vendor
  - Responsibilities and liabilities in the event of information security incident such as loss of data.
- The terms given under Standard Security Conditions in Third Party Contracts must also be considered as part of the contract.
- The vendor must, during the stage of specification, design, development, testing, implementation, configuration, management, maintenance, support use security controls within or associated with IT systems. The supplier must also use source code escrow wherever applicable
- The vendor must return or destroy all of Sesa Group's information assets after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity

- All outsourcing contracts must anticipate the eventual termination or ending of the contract and plan for an orderly in-house transition or a transition to another service provider. On completion/termination of a contract, the supplier must:
    - Provide Sesa group with access to its facilities to remove and destroy Sesa Group owned assets and data.
    - takes all necessary actions to ensure a smooth transition of service with minimal disruption
    - provides a fully documented service description.
    - Provides a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation

3.2 Information Exchange

3.2.1 Securing Information Exchange

- Appropriate security controls shall be implemented to exchange the business information or software assets with the vendors. The security controls shall include technical controls and contract/agreements signed with the vendors.
- Employees and vendor staff shall exchange classified information as authorized by the appropriate information asset Owner.

3.3 Service Delivery Management

3.3.1 Third Parties' Service Delivery Management

- For services involving vendor, the respective manager dealing with the third party shall ensure that:
    - All the security controls, service definitions and delivery levels included in the third parties' contracts are implemented, operated, and maintained by the third parties
    - The service performance levels are regularly monitored and service reports provided by the third parties are reviewed to ensure if any identified problems are resolved
    - Third Parties' access to Sesa Group information shall be tracked and audited on periodic basis
- The CISO/ CDIO / Head-IT shall do the regular review of the third party service delivery reports in compliance to the policy.
- Any changes to provisioning of services, both initiated by Sesa Group and/or by the external party shall be managed by:
    - taking account of the criticality of information systems and processes involved
    - undertaking a re-assessment of risks
- Depending on the scope and upon Sesa Groups request, the vendor must provide:
    - Effectively deployed and administered firewalls
    - Intrusion Detection with 24x7 alerting capability
    - An individual or group responsible for Incident Response, available 24x7
    - Access controls to enforce restrictions on a need-to-know basis
    - Established and tested policies and procedures
    - Contingency Plans and Disaster Recovery Plans
    - Security testing and evaluation process for security controls, to include regularly scheduled, at least annually, vulnerability assessments.
    - Configuration settings required to maintain the system's security on the system itself and other State systems that interface with it.

4. Enforcement

All third parties should follow the policy; violation of this policy could lead to termination of contract, civil action or financial penalties.

5. References and Related Policies/Procedures

- Identity and Access Management Policy
- Vendor Security Procedure
- Information Transfer

6. Control Clauses Covered

A.15.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

7. NDA- document

NDA latest document to be taken from Sesa legal dept at the time of signing.