vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Policy Document Information – Human Resource Security Policy

Documented information Name: Policy Document Information – Human Resource 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 – Human Resource Security Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Human Resource Security.

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 – Human Resource Security
Documented information Code	SESAIT/ISO27001/ISMS_Policy_ Human Resource Security
Date of Release	16.01.2012
Documented information Revision	25-July 2023
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 (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	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		22-01-2014

1.4	04-11-2014	Aligned to ISO 27001:2013	1.1,3.1,6	
1.5	10-Feb-2016	Company name logo update		18-Feb-2016
1.6	13-Feb-2017	Policy Review		18-Feb-2017
1.7	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.8	21-Aug-2018	Policy review		28-Aug-2018
1.9	22-Aug-2019	Policy review		30-Aug-2019
1.10	28-Feb-2020	Policy review		28-Feb-2020
1.11	08-Sep-2020	Policy review		15-Sep-2020
1.12	28-Sep-2021	Policy reviews and update	1.1	21-Oct-2021
2.0	18 March 2022	Policy Review & Update – added aspects related to Privacy	2, 3.1.1,3.1.2,3.1.3,3.1 4, 3.2.3.2.1,3.3.1	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, Orissa and Liberia, Pig Iron Division, Met Coke Division , Power Division in Goa , Sesa Coke- Vazare & Gujarat, FACOR – Orrisa , Nickel Business and VGCB , Visakhapatnam; referred as Sesa Group in this document.

The policy is applicable to employees, third parties, contract employees and vendor employees who are utilizing, managing, and supporting the Information assets within Sesa Group, who are expected to be aware of this policy and comply with it.

1.2 Purpose of the documented information

People are one of the most valuable information assets and it is necessary to address the risks of human error, theft, fraud or misuse of facilities and assist all employees in creating a secure computing environment. Human Resource Security Policy identifies the measures adopted by Sesa Group to protect information assets from misuse, theft or fraud by its employees, third parties, contractors and vendors.

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

To reduce the risk of human error, theft, fraud, or misuse of electronic resources, information assets and facilities, security and privacy responsibilities for employees shall be defined and addressed at the employee recruitment stage, included in contracts, as applicable and monitored throughout an individual's employment within Sesa Group.

3. Policy Details

3.1 Security in Job description

- This aspect would be applicable at the time of commencement of employment and during the engagement of an employee with the objective of:
    - Ensuring that the employees and third-party staff understand their responsibilities and roles regarding information security
    - Reduce the risks due to human error, theft, fraud or misuse of information assets and facilities
    - Minimize the damage from the security incidents and malfunctions and learn from such incidents
- Failure to adhere to information security responsibilities may result in appropriate actions through the consequence management process.

3.1.1 Personal Screening

- Appropriate verification checks on permanent staff which deal with classified data or having access to secured information processing areas shall be carried out at the time of job application.

- All employees shall be subject to a formal pre-employment screening, which must include at minimum, the availability of at least 2 satisfactory professional references.
- The verification checks should take into consideration all relevant privacy, PII protection and employment-based legislation and shall include one or more options as mentioned below:
    - Availability of appropriate reference. (E.g., one business and one personal)
    - A check on completeness and accuracy of applicant's curriculum vitae
    - Confirmation of claimed academic and professional qualifications
    - Independent identity check (Passport or similar documented information)
    - Experience certificate issued by the previous employer
- The contract with the background verification agency, if any, shall clearly specify the agency's responsibilities for verification and its accountability in safeguarding the confidential records of employees.
- The third-party vendors are required to carry out background verification checks of their employees who have access to information assets of Sesa Group and provide a certificate to this effect to the HR function of Sesa Group.
- In situations where verification cannot be completed in a timely manner, following should be implemented, (if required, case-to-case basis) until the review has been finished:
    - Delayed On-boarding
    - Delayed deployment of corporate assets
    - Onboarding with reduced assets
    - Termination of employment

3.1.2 Information Security in Job Responsibilities

- Information Security roles and responsibilities must be included in job descriptions of employees wherever applicable.
- All employees shall sign their acceptance to Terms and Conditions of employment of Sesa Group at the time of joining. Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.
- Security roles and responsibilities shall include any general responsibilities required for implementing or maintaining the security policy, as well as any specific responsibilities for the protection of particular information assets or for the execution of particular security processes or activities.
- The Information security related roles and responsibilities shall be clearly communicated to every new employee during the induction process and also through sessions whenever there is any change in the policy.

3.1.3 Confidentiality Agreement

- All employees shall sign a non-disclosure agreement/confidentiality agreement before they are given access to the information processing facilities like the Intranet, Internet, Email or computing devices.
- All temporary workers / contractors not already covered by an existing contract (containing confidentiality agreement) shall be required to sign a confidentiality agreement prior to being given access to information processing facilities.
- The confidentiality agreement shall be reviewed when there are changes to terms of employment or contract.
- All users of information systems must sign the "Information Systems Acceptable Usage policy".
- There shall be processes and procedures defined for notification and reporting the violations of confidentiality agreements.

3.1.4 Termination or Change in Employment

- The HR function shall ensure that termination/ change of employment responsibilities including Information security responsibilities that remain valid after termination or change of employment of the employees and third parties are clearly defined, assigned, enforced and communicated to them.
- The termination process shall include the return of all issued assets such as laptops/computers, software, corporate documented information, equipment, mobile computing devices, access cards, manual and / or any other asset that is the property of Sesa Group.
- The HR department shall inform the respective Administration, Finance and IT Department about the transfer, resignation or termination of employee / trainee / contract personnel.
- The IT team shall ensure that all the relevant accounts are deactivated immediately on the departure of the employee.
- The IT team shall ensure that, in case of any change (including exit) in the responsibilities of an employee or third-party staff, the access rights are revoked or modified as required.

3.1.5 Management Responsibility

- The departmental heads of every business function shall ensure that every employee of his/her function attends information security training workshops, whenever these are conducted.
- Management shall ensure that employees, contractors and third-party users:
    - Are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems?
    - Are motivated to fulfill the security policies of the organization?
    - Achieve a level of awareness on security relevant to their roles and responsibilities within the organization.
    - Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.
    - Continue to have the appropriate skills and qualifications.

3.2 Information Security Awareness, Education and Training

This aspect aims to facilitate security awareness across the organization. There shall be an ongoing security awareness program that explains the need for information security and provides the user community with adequate security training. The purpose of implementing the awareness program is to ensure that the personnel are aware of and fulfill their information security responsibilities.

3.2.1 Information Security Awareness Training

- All Sesa Group employees and contractors shall get information security training prior to being given access to information systems.
- The training program is established in-line with the organization's information security policy and objectives, and includes the relevant sections with appropriate Do's and Don'ts that the employees need to practice in their day-to-day work.
- In the event of changes to the security policies and procedures, the same shall be communicated to all concerned employees and temporary workers / contractors.
- Security awareness programs shall be conducted on a regular basis.
- HR team in coordination with department heads should identify technical training requirements of employees based on specific job profiles regularly. Technical training should be aimed at acquisition of adequate skills and expertise that is required by the personnel to maintain the required level of information security as per their job responsibilities.

3.3 User responsibility/ Accountability

The protection of information system resources is a fundamental responsibility of all personnel. Users need to ensure that all activities carried out on information system resources are done in an authorized manner.

3.3.1 Disciplinary Process

The purpose of implementing a disciplinary process is to ensure that personnel understand the consequences of information security policy violation, to deter and appropriately deal with personnel who committed the violation.

- Certain categories of activities, which have the potential, or actually harm the information assets are defined as security violations and are strictly prohibited. Such security violations shall result in the invocation of the consequence management process.
- The HR function and functional heads dealing with third parties shall ensure that employees and third parties are made aware of the formal disciplinary process which may be initiated against them, if they violate the Sesa Group's information security policy or commit/ participate in any kind of security breach. The formal disciplinary process shall take into account factors such as nature and gravity of the breach, whether the offence was intentional or accidental, whether it was a repeated offence, whether or not the violator was properly trained and, its impact of the offence on relevant legal, statutory, regulatory contractual, and business requirements as well as other factors as required.
- The Information Security Manager shall forward the Post Incident Report (PIR) based on which, the disciplinary process shall be initiated by the HR Department.
- Deliberate information security violations shall require immediate actions and can result in strongest penalties including termination of employment.

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.7.1.1, A.7.1.2, A.7.2.2, A.7.2.3, A.13.2.4