Sesa Goa Iron Ore

Information Security Management System

(ISMS)

Procedure Documented information – Human Resources

Security Procedure

Documented information Name: Procedure Documented information – Human Resources Security Procedure

Version No: 3**.0**

Last Updated: 25th July 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Table of contents

Documented information Management Information

Documented information Title: Procedure Documented information – Human Resources Security

Abstract: This Documented information is a procedure Documented information highlighting the procedures for human resources 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	Procedure Documented information – Human Resources Security
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_Human Resources 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 Consultancy Services Arjun N Rao – Wipro Consultancy 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
1.	Praveen George (Head-HR)	praveen.george@vedanta.co.in	Electronically Approved
2.	Shobha Raikar (CDIO-IOB)	shobha.raikar@vedanta.co.in	Electronically Approved

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 change for Sesa Sterlite Ltd - IOB		18-10-2013
1.3	25-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT	2.1.5	27-01-2014

1.4	05 – 11 - 2014	Aligned with ISO 27001:2013	1.1,1.2,3	05-12-2014
1.5	11-Feb-2016	Company name logo update		19-Feb-2016
1.6	13-Feb-2017	Procedure review		18-Feb-2017
1.7	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.8	22-Aug-2018	Review		29-Aug-2018
1.9	23-Aug-2019	Review		30-Aug-2019
1.10	09-Sep-2020	Review		16-Sep-2020
1.11	28-Sep-2021	Review and Update	1.1	21-Oct-2021
2.0	18 March 2022	Review and Update		27-Aug-2023
3.0	25th July 2023	Review and Updated		10-Aug 2023

Documented information Contact Point

S. No	Documented information Author	Email
1.	Sujay Maskara	sujay.maskara@wipro.com
2.	Vivek Kumar Rai	Vivek.rai@wipro.com
3.	Arjun N Rao	arjun.rao1@wipro.com

1. INTRODUCTION

1.1 Scope of the documented information

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 - Gujarat & Vazare , FACOR – Odisha , Nickel Business and VGCB , Visakhapatnam; referred as Sesa Group in this document.

The following section provides detailed procedures for implementation of Human Resource Security Policy of Sesa Group. The Human Resource Security Policy contains the following:

- Security in Job Definition
- Security Awareness and Training Sessions
- User Responsibilities / Accountability

1.2 Purpose of the documented information

The primary use of this documented information is to implement the human resource security controls as specified within Human Resource Security Policy Documented information.

1.3 Definition

- **Induction** refers to the process of introducing employees to various aspects / dimensions of the organization/employer and terms of employment.
- **Background Verification** refers to the process of verifying academic qualification, professional experience and criminal background (wherever applicable) details provided by the candidate while applying for a job with Sesa Group.

2. PROCEDURES

2.1 Human Resource Security

2.1.1 Recruitment Process

- The HR Department should ensure preparation of job descriptions based on the profile described by departmental heads.
- The profiles matching the job descriptions must be short-listed and interviewed. At least two professional references should be sought from the candidate.
- The relevant information security roles and responsibilities e.g. maintenance of confidentiality and integrity of information of Sesa Group should be clearly defined in the offer letter.
- Conduct 2 reference checks and documented information the information in reference check as part of joining formalities.
- For all designations performing critical activities and/or dealing with sensitive information, a background verification must be done considering the below points:
    - A check on completeness and accuracy of applicant's curriculum vitae
    - Availability of satisfactory character reference through personal and business references
    - Background check on the duties or responsibilities performed in previous organization
    - Check for security clearance from nearest police station (should be applicable for Security Guard roles)
    - More detailed verification, such as credit review or review of criminal records in case the candidate takes on a critical role.
- In case background verification is being conducted by a third party then the following points should be considered:
    - Receive and acknowledge the receipt of documented information to HR function.
    - Process verification checks as per agreement.
    - Prepare and send the verification report to HR function in the format agreed.
    - Insufficiency in the verification shall be highlighted in the report sent to SESA within the agreed compliance timelines as stated in the contract
    - Ensure confidentiality and privacy of information throughout the verification lifecycle.
- In case of favorable medical report and satisfactory reference checks, the HR must confirm Date of Joining with the employee.
- All employees must sign the following at the time of joining:
    - Employment Offer letter
    - Acceptance to Information Security Policy

    - All employees must sign a non-disclosure agreement before they are given access to the information processing facilities like Intranet, Internet, Email or computing devices.
    - Acceptance to Terms and conditions of employment of Sesa Group.
    - Acceptance on Acceptable Usage Policy
- All employee Documented information should be protected properly in a secured location with access to few people.
- All the Documented information should be archived for future references.

2.1.2 Induction Process for New Joinees – Information Security

- The Induction training for all new joinees must cover a session on introduction to Information Security and Security practices at Sesa Group which includes :
    - Security Policies and procedures.
    - Care to be taken while handling Sesa Group information.
    - Information classification, handling and disposal.
    - Incident response and reporting.
    - Access restrictions in secure areas (like Server room, Data Center etc.)
    - Emergency plans during fire or other disasters.
- Sesa Group's identification badge should be issued to a new employee at the time of joining
- HR should send communication to the IT Helpdesk-Service/FMS about issuing login ID and creation of email account for the new joinees.
- Once the employee e-mail ID is generated, Helpdesk should mail new joinee with copy of Sesa Group's Acceptable Usage Policy to the employee email ID.
- Employee should read the policy and send the acceptance of policy.

2.1.3 Information Security Awareness Training

- A Training Calendar should be prepared by the HR department with help from Information Security Manager (ISM) and the same should be communicated to respective department heads well in advance to check for suitable resource availability.
- Training attendance form and feedback form should be circulated during all training sessions to track actual attendance.
- Awareness Training materials should cover information on the following:

    Management's commitment to information security throughout the organization;
- An assessment should be conducted to test the effectiveness of the training imparted and reported to the respective heads.

- Records must be maintained and archived for the training sessions conducted.
- Feedback must be sought after every training session.

2.1.4 Exit / Transfer Procedure

- The respective HOD/Supervisor should forward the employee resignation letter or termination / transfer intimation to the HR.
- HR should conclude the relieving process once an employee submits a formal acceptance from individual departmental heads (like Admin, IT, Finance).
- HR should communicate to the designated authority from IT & Admin department to initiate the process for revocation of access rights of the relevant employee.
- For transfer cases, the transfer of employee should be completed only after submission of transfer letter from HR.

2.1.5 Handling of Information Security Breaches

Disciplinary Process

- Every incident or security breach by the employee should get recorded in the PIR (Post Investigation Report).
- In case of breaches of Information Security Policy, Information Security Manager must mail the PIR to CDIO / Head-IT and Head HR of Sesa Group, who will then take up the case with the Compliance Committee.
- Any incident must be reported to the designated Chief Information Security Manager or CDIO / Head-IT.
- Information Security Manager must take up the case with HR immediately and may request an explanation from the employee on the same with concurrence of HR and the Compliance Committee.
- If the explanations are not found satisfactory and the person is found to have intentionally breached the information Security policies of the organization, appropriate punitive action should be initiated against him by HR.
- Disciplinary proceedings must be done through the Compliance Committee as per normal disciplinary process. Any disciplinary action against the employee should be done through the HR function.
- The Compliance Committee should classify the severity of the incident and take appropriate actions.
- For high severity cases, the final decision on the punitive part should vest with the Compliance Committee.
- Annexure 1 depicts the severity matrix for various categories of violations. Repetitive breach of a lower severity category can upgrade the punitive action from a lower severity category to a higher severity category.

- The matrix mentioned below should be used as a guideline for classifying the severity of violations and taking an appropriate punitive action.

Sr.	Severity Category	Possible Punitive Action
1	**High**	Dismissal / Suspension / Cancellation of Contract
2	**Medium**	Severe Reprimand / Warning Letter
3	**Low**	Reprimand/ Verbal Warning

3. Roles and Responsibility Matrix

Role	Responsibility
Human Resource (HR)	Pre-Employment - Personnel Screening for employment & educational verification - Arrange Induction training. - Maintain NDAs of new as well as existing employees - Issue employee number and Identification badge. - Forward mail to IT for creation of Login ID. Post-Employment - Arrange continuous training for employees - Forward Exit form/Transfer Form - Exit interview - Issue show cause notice to employee - Take disciplinary actions Arrange and conduct trainings
New Recruits	- Provide required Documented information - Provide references - Sign required Documented information - Attend Induction training - Formal Acceptance of Information Security Policy - Conform to the security policies and procedures of the organization
System Administrator/Network Administrator/Application Administrator-IT	- Issue Login ID for each employee - Create Email Account - Disabling/Deletion of accounts from all systems based on Exit form on account of separation/termination/transfer
Administration	- Issue ID cards to employees - Revoke access after employee separation/termination/transfer

4. Templates

- None

5. References and Related Policies

- Human Resources Security Policy

6. Annexure

Suggested Categorization of Various Violations

Type of violation		Severity		
		High	Medium	Low
1	Making or allowing an unauthorized entry into restricted areas		**M**	
2	Unauthorized removal of IT equipment from the office premises	**Medium to High**		
3	Unauthorized relocation of IT equipment inside the premises with a malicious intent.			**L**
4	Leaving laptops in insecure areas (i.e., unlocked cabinets)		**M**	
5	Unauthorized use of another person's e-mail knowingly with an intent of getting unauthorized information	**H**		
6	Using e-mail in a manner that: ○ Interferes with normal business activities or hampers employee productivity, ○ Embarrasses the company or the recipient ○ Involves solicitation of business damage to Sesa Group interests. ○ Reflects Sesa Group, its management/staff and staff in a bad light. ○ Mails sent inside or outside "for-profit" solicitation contrary to appointment clause.	**Can range from medium to high depending on the content**		
7	Transmitting **Confidential, Restricted or Secret Company Information** to other parties not in line with Sesa Group business interests or as a breach of Information Security	**H**		
8	Sending profane, obscene or derogatory e-mails or mails with sexually explicit content with a view to harass or share contents.		**Low to Medium**	
9	Wilful non-adherence to Information Security policies and processes.		**Low to Medium**	
10	Requesting / making unauthorized password resets of other users in their absence		**M**	

Type of violation		Severity		
		High	Medium	Low
11	Wilful non-usage of screen saver / power-on passwords		**Low to Medium**	
12	Not following the Information Security Acceptable Policy		**Low to Medium**	
13	Surfing sites with obscene or porn content		**M**	
14	Storing / Sharing of obscene content on Sesa Group Computing environment		**M**	
15	Using personal computing resource inside office premises for sustained access to Corporate Information without explicit permission on the same from IT		**M**	

Security Breaches are not limited to the violations mentioned above and covers Information security policies and procedures laid down by IT in Sesa Group.