Sesa Goa Iron Ore

Information Security Management System

(ISMS)

Policy Documented Information – Acceptable Usage Policy

This documented information is a confidential documented information of Sesa Group

Documented Information Name: Policy Documented Information – Acceptable Usage Policy

Version No: 3.1

Last Updated: 2nd September, 2023

Documented Information Owner: Sesa Group

Approval Authority: Sesa Group

Table of contents

Documented Information Management Information

Documented Information Title: Policy Documented Information – Acceptable Usage

Abstract: This documented information is a policy documented information highlighting the policies for acceptable usage 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 – Acceptable Usage
Documented Information Code	SESAIT/ISO27001/ISMS_Policy_Acceptable Usage
Date of Release	26.12.2011
Documented Information Revision	02-September-2023
Documented Information Owner	IT Department
Documented Information Author(s)	Sujay Maskara – Wipro Consulting, 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
1.	Shobha Raikar (CDIO - IOB)	shobha.raikar@vedanta.co.in	

Documented Information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.1	20-Mar-12	Added abbreviation	5.0	20-Mar-12
1.2	28-Mar-13	Sesa Group Logo Change		28-Mar-13
1.3	18-Oct-13	Sesa Group Logo , file name change for Sesa Sterlite Ltd - IOB		18-Oct-13
1.4	21-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT	3.2,3.5,3.6,3.7,3.8,4	22-01-2014
1.5	01-12-2014	Alignment to ISO 27001:2013.	3.4, 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	01-Jul-2017	Social Media acceptable use	3.9	05-Jul-2017
1.10	21-Aug-2018	User data backup	3.4	28-Aug-2018
1.11	22-Aug-2019	Policy review		30-Aug-2019
1.12	08-Sep-2020	Policy review		15-Sep-2020
1.13	28-Sep-2021	Policy review and Update	1.1	05-April-2022
2.0	18 Mar-2022	Policy review and Update		25-August-2022
3.0	25 July-2023	Updated the end user backup process on one-drive	3.4	10-Aug-2023
3.1	02-Sep-2023	Added Sections : Section 3.10, Section 3.11, Section 3.12,	3.10, 3.11, 3.12,	06-Sep-2023

Documented Information Contact Point

S. No	Documented Information Author	Email
1.	Dileep K Singh	dileep.singh@vedanta.co.in

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 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 Information Systems on appropriate use of its assets & facilities.

1.3 Audience

This policy is applicable to employees who comprise 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. All employees must ensure the security of these information assets by protecting them from unauthorized use, modification, disclosure or destruction, whether accidental or intentional.

It is mandatory that employees shall make themselves aware of the Information Security Policies and Procedures which are available at the portal: http://sgl-panj-sp-01/sites/sesaportal. It is expected and required that users must abide by Sesa Group’s Information Security Policies and Procedures. Any employee found violating the Information Security Policies and Procedures would be liable for Disciplinary action.

3. Policy Details

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

3.1 Physical and Environmental Security

Acceptable Usage:

- Sesa Group’s ID Badges shall be displayed all times within Sesa Group premises
- ID Badge should be carried in such a manner that it is visible at all times
- Employees shall participate in safety drills organized by Sesa Group
- Employees should ensure that visitors are always escorted while visiting the sensitive areas (server room, UPS room, room containing confidential information, etc.).

Unacceptable Usage:

- Employees shall not tailgate or allow tailgating in secured areas like server rooms
- Employees shall not lend or borrow Access Cards
- Employees shall not disregard safety instructions

3.2 Desktop / Laptop Usage

Acceptable Usage:

- Desktops / laptops or any other IT resources provided to employees shall be used only for official purpose
- Employees shall only use Sesa Group's approved software. Refer acceptable Usage of Software Policy
- Employees shall always keep their desktop / laptop suitably fastened/locked when they are not at their desk and laptops shall not be left on the desk or in the work area overnight.
- Adequate precautions should also be taken to ensure safe carriage of laptops during travel. Laptops shall always be carried as hand luggage whilst traveling.
- In the event of a laptop being stolen, the concerned personnel shall file a police report and subsequently inform the administration department
- Employees shall declare personal computing equipment (like CDs, pen drives, laptops etc.) to the security guard before carrying them inside Sesa Group's premises
- Employees using external Internet connections on laptops shall ensure that:
    - Anti-virus signatures are updated
    - Personal firewalls are enabled on laptops
    - Latest security patches are installed
- Classified data shall not be copied to external portable media like USB's, CDs, etc. without the permission of HOD and Chief Information Security Officer (CISO / CDIO / Head-IT)

Unacceptable Usage:

- Employees shall not connect their personal laptops or mobile devices to the Sesa Group Network
- Employees shall not install freeware or shareware which are not provided by Sesa Group
- Employees shall not use external devices unless it is approved by the HOD and CISO/CDIO / Head-IT

3.3 Access Control

Acceptable Usage:

- All Employees shall use their unique ID assigned to them for accessing Sesa Group information assets
- All employees shall adhere to the password policies of Sesa Group as mentioned in "Sesa Group_Policy_Identity and Access Management".

Unacceptable Usage:

- Employees shall not use shared accounts for accessing Sesa Group's information assets
- Employees shall not share their passwords with anyone
- Employees shall not write or paste passwords in public spaces or at the workplace

3.4 Data / Privacy Protection

Acceptable Usage:

- Employees shall understand business/contractual requirements of data protection from their respective Managers or HOD
- Employees shall classify information assets according to their level of sensitivity and handle the same accordingly
- Employees shall protect vital physical records which contain business related information
- Employees are responsible for backup of the data on their own systems. Employees shall take the backup of their data on a regular basis and the backup of the official folders shall be taken on One-Drive by the employees.

Unacceptable Usage:

- Employees shall not send business data related to the department to any third party without approval of their respective HOD
- Employees shall not use camera mobile phones in secured areas like server rooms/data center
- Employees shall not leave confidential documented information on the desk; instead it should be kept in a locked cabinet
- Employees shall not leave printouts unattended at the printer machine
- Employees shall not reveal information about Sesa Group's business details in white papers or presentations

- Employees shall not discuss official matters in public places
- Employees shall ensure that no material which is obscene is published or transmitted

3.5 Internet Access

Acceptable Usage:

- Employees shall exercise caution while accessing official internet connections provided by Sesa Group
- Employees shall adhere to Sesa Group's internet usage policies such as:
    - Do not send/receive/view racial, sexually threatening, defamatory or harassing messages
    - Do not upload and download large files not related to business
    - Do not release computer viruses, worms, or Trojan horses, etc.
- Internet / Email traffic logs may be maintained by the company without prior notice. This information can be used by the company to take disciplinary action against employees who have misused Sesa Group internet services, which may result in termination of services

Unacceptable Usage:

- Employees shall not use Sesa Group resources for non-business purposes like downloading songs, pictures, objectionable site contents
- Employees shall not connect to internet via data card while using Sesa Group network
- Usage of any kind of Internet chat services like MSN messenger, Yahoo chat, Rediff chat and social networking sites like Orkut, Face book etc. is strictly prohibited
- Employees shall not participate in public chat session for official purpose. An explicit written permission from the HOD and CISO/CIDO / Head-IT should be obtained for a user to use the Internet chat facility for official purposes. Appropriate disciplinary action shall be initiated if any user is found to be using such service without permission
- Employees shall be strictly prohibited from using any automated tools or any other means for gaining unauthorized entry into any third party systems or Sesa Group systems or any resource over the Internet to which they do not have access rights
- Employees are further prohibited from engaging in any activity that may result in disruption in operations of either Sesa Group or any third party computer systems

Refer Internet Usage policy for details

3.6 Email Access / Usage

Acceptable Usage:

- Employees shall use Sesa Group e-mail only for official purposes
- Employees shall exercise caution in disclosing Sesa Group e-mail address to strangers
- Employees shall be cautious in opening attachments from suspicious e-mail addresses
- Employees shall report suspicious e-mails to the CISO / CDIO / Head-IT
- Employees shall archive mails and take regular backups
- Employees shall follow the controls specified by Sesa Group while accessing emails from mobiles / PDAs
- Employees shall report about spam to the CISO / CDIO / Head-IT

Unacceptable Usage:

- Employees shall not use e-mails within the organization to harass other employees
- Employees shall not send unwanted e-mails to the outside world that project a wrong image of Sesa Group
- Employees shall not communicate with any third party which may potentially invite involvement of law enforcement agencies
- Employees shall not participate in chain e-mails
- Employees shall not forward sensitive e-mails containing Sesa Group's information to the external world, even inadvertently
- Employees shall not register Sesa Group e-mail addresses on external websites

3.7 Virus Protection

Acceptable Usage:

- Employees shall ensure that the antivirus on his / her workstation is updated
- Employees shall promptly communicate to their immediate supervisor/senior/HOD, if they discover any security incident (like virus infection, unusual activity, passwords shared etc.)

Unacceptable Usage:

- Employees shall not open attachments from unknown sources
- Employees shall not use any external source such as CDs, USB drives etc. on Sesa Group technology infrastructure unless scanned for viruses, and approved by the HOD and CISO / CDIO / Head-IT

3.8 Reporting Security Incidents / Weaknesses

- It is the responsibility of each employee to report any observed or suspected information security incidents and/or weaknesses to the CISO / CDIO / Head-IT telephonically and by email to sesa.isms@vedanta.co.in
- Employees shall be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Any action in testing the weakness shall be interpreted as a potential misuse of the system
- Employees shall not discuss with colleagues about the suspected weakness once it is reported to higher authority for investigation

3.9 Social Media acceptable use

Employees shall adhere to the controls for Social Media Acceptable Use while using social media websites.

- All employees shall adhere to Vedanta Information Security Policy and Standards while accessing social media platforms.
- Adequate care should be taken to ensure that the information being shared on social media platforms does not affect the reputation of Vedanta, its constituent entities, business associates or affiliates.
- While sharing information of social media platforms, dignity and privacy of colleagues, customers, competitors and third parties must be considered. Social media platforms must not be used for the purpose of harassment, abuse, threat, intimidation and / or offence against any person, group or community. Links to external websites containing offensive or unlawful content must not be posted
- All applicable laws and regulations, and their corresponding amendments must be adhered to as and when they are released, while using social media platforms
- Users shall not post / share information / comment on social media platforms on behalf of Vedanta Limited or any of its entities, unless approved by relevant authority.
- Users shall not disclose any information (including confidential information) on social media platforms which the users are in knowledge of as a result of their role / responsibilities in Vedanta Limited or its entities.
- Social media platforms shall not be used for sharing references of Vedanta customers or partners.
- Use of Vedanta Logo, Trademarks (Vedanta Intellectual Property Rights) on social media platforms is prohibited unless prior approval has been acquired by relevant authority.

3.10 Generative AI Tools/Services Usage

Acceptable Usage:

- While using any Generative AI tools, services, platforms user must ensure the software licences compliance, confidentiality and privacy protection of the company data and information .
- Generated content should be reviewed and validated for accuracy and appropriateness before use.
- Ensure that generated content complies with the organization's confidentiality and privacy policies.
- Keep backups of generated content, especially if it is crucial for business operations.
- Regularly update and maintain security measures on systems where generative AI tools are used.
- Report any unusual or suspicious behaviour of generative AI tools to the IT department.

Unacceptable Usage:

- Use of generative AI tools to create false or misleading information is strictly prohibited.
- Do not use generative AI tools to generate content that infringes on copyright, trademark, or intellectual property rights.
- Avoid using generative AI tools for malicious activities, such as generating harmful code or content.
- Do not share generated content that could potentially harm the organization's reputation, privacy, or security.

3.11 Phishing email protection:

Acceptable Usage:

- Follow the organization's email security policy to prevent falling victim to phishing attacks.
- Ensure that email attachments and links are from trusted sources before opening or clicking on them.
- Employees should promptly report any suspected phishing emails through the "Report Phishing" button provided in O365 and IT dept .
- Regularly update and maintain strong and unique passwords for email accounts.
- Encourage colleagues to be vigilant and cautious when receiving emails with suspicious content or requests.

Unacceptable Usage:

- Do not share sensitive information, such as passwords or financial details, in response to email requests.
- Avoid clicking on links or downloading attachments from unknown or suspicious sources.
- Employees should not engage with or respond to phishing emails, even to report their suspicions
- Do not forward phishing emails to colleagues, as this may inadvertently spread the threat.
- Do not ignore or dismiss suspicions of phishing; timely reporting is crucial to mitigating potential risks.

System Action:

- If the employee opens the phishing email and clicks on the suspicious links inside phishing email, then his system access will be disabled, and for access enablement he must provide signed confirmation for “Acceptance usages Policy” and attend again Mandatory - Cybersecurity Awareness Training Module.
- If the employee submits their confidential/critical data in the forms/links in the phishing email, then his access will be disabled, and for access enablement he must provide signed confirmation for “Acceptance usages Policy” with his HOD approval and attend again Mandatory - Cybersecurity Awareness Training Module.
- If employee do this multiple times their case will be presented in the IT steering committee meeting and accordingly their access can be restricted or revoked.

3.12 Voice Phishing/Vishing protection

Acceptable Usage:

- Employees shall undergo regular training and awareness programs to recognize and respond to voice phishing (vishing) attempts.
- Employees shall always verify the identity of the caller, especially if they request sensitive information or actions.
- If in doubt, employees shall ask for a call-back number, name, and extension to independently verify the caller's identity.
- Employees shall never share sensitive personal or company information over the phone unless they are certain of the caller's identity and the necessity of the request.
- Employees shall immediately report any suspected vishing attempts or suspicious phone calls to the IT department .

Unacceptable Usage:

- Employees shall never share personal or confidential information, such as login id , passwords, PIN, account numbers etc, over the phone without proper verification.
- Employees shall never provide any sensitive company information or access credentials to unknown callers.
- Employees shall not ignore or underestimate suspected vishing calls, even if they appear harmless initially.
- Employees shall not succumb to pressure tactics, threats, or urgent demands made by unknown callers.

System Action:

- If the employee reveals any personal or sensitive information on the vishing call, then his system access will be disabled, and for access enablement he must provide signed confirmation for “Acceptance usages Policy” and attend again Mandatory - Cybersecurity Awareness Training Module .

- If employee do this multiple times and their case will be presented in the IT steering committee meeting and accordingly their access can be restricted or revoked.

3.13 Accountability Controls

- All communications, hardware, software, files and records transmitted through Vedanta systems remain a property of Vedanta Limited. Vedanta Limited reserved the right to monitor / view /audit the same at its sole discretion, any time and without consent from or notice to users.

- All users shall be personally responsible for complying with Terms and Conditions of the respective social media platforms. Vedanta Limited shall not be held responsible for any violations thereof.

- User alone shall be personally held responsible for all claims, proceedings, damages, losses, costs and expenses (including third party claims) arising for any wrongful, negligent or unauthorized usage of social media. Vedanta Limited reserves the right to recover any monetary amount paid / being payable by Vedanta Limited to any third party due to negligence / misconduct of users while handling social media.

4. ACCEPTANCE OF POLICY

ACCEPTANCE OF POLICY

I have read and understood the Acceptable Usage Policy, applicable to me as an employee of Sesa Group, working with _________________ Department as ________________.

I understand Sesa Group's Information Security Policy and the associated Security Policies available on Intranet Portal. I further agree to comply with the Information Security Policy and understand that any violation of this policy will subject me to disciplinary action, up to and including possible termination.

Employee Name:

Signature:

Date:

(Received and forwarded a copy to Chief Information Security Officer (CISO / CDIO / Head-IT.)

5. ABBREVIATION

HOD – Head of Department

CISO – Chief Information Security Officer

PDA – Personal Digital Assistant

6. CONTROL CLAUSES COVERED

A.8.1.3, A11.2.6, A13.2.1, A13.2.3, A18.1.1, A18.1.4