Sesa Goa Iron Ore

Information Security Management System

(ISMS)

Policy Documented Information –Mobile Usage Policy

Documented Information Name: Policy Documented Information –Mobile Usage Policy

Version No: 3.0

Last Updated: 25-july-2023

Documented Information Owner: Sesa Group

Approval Authority: Sesa Group

Table of contents

Documented Information Management Information

Documented Information Title: Policy Documented Information –Mobile 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 – Mobile Usage
Documented Information Code	SESAIT/ISO27001/ISMS_Policy_Mobile Usage
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
1	Shobha Raikar (CDIO- IOB)	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	09-01-2015	Reviewed and updated as per Internal Audit	3.1	15-01-2015
1.2	10-Feb-2016	Company name logo update		18-Feb-2016
1.3	14-Feb-2017	Review and update	3.3	20-Feb-2017
1.4	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.5	21-Aug-2018	Policy review		28-Aug-2018
1.6	01-Nov-2018	Simple password settings	3.3	01-Nov-2018
1.7	22-Aug-2019	Pin length	3.3	30-Aug-2019

1.8	23-Sep-2020	Review and O365 mobile email update	3.4	30-Sep-2020
1.9	28-Sep-2021	Review and Update	1.1	05-April-2022
2.0	18 March-2022	Review and Update		25-Aug-2022
3.0	25 July 2023	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

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 handheld devices.

1.3 Audience

This policy is applicable to 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

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 Mobile Usage

No handsets will be purchased by the company. The employees shall buy handsets as per company mobile policy

Acceptable Usage:

- Employees requiring Information access on handheld devices shall obtain necessary authorization
- Employees shall report to IT helpdesk and change their AD password immediately on the loss of devices
- Employees shall store confidential business information in encrypted form.
- Employees shall keep the unused connectivity options such as Bluetooth, Wireless LAN in switched off mode and enable on need basis. Access to corporate wireless network should be done only after authorization
- In case of loss or misplacement of the Device, change or disposal of the Device, separation from Sesa Group for any reason, Employees will be solely responsible, or authorize Sesa Group, to immediately wipe the entire data contents (personal and official) off the Device
- Employees shall install applications on smart phones, tablets only from trusted and authorized source
- Employees shall install a trusted anti-virus and update them regularly

- Employee is solely responsible for protection of all forms of Sesa Group information including customer's (PII)Information that may be contained in the Device.

Unacceptable Usage:

- Employees shall not send business confidential information through short message service (SMS)
- Employees shall not use jail broken, rooted devices
- Employees shall not use camera or any other device embedded with camera, for taking photographs/shooting video clippings inside any of the identified sensitive areas.
- Employees shall not use camera, through remote access mechanisms, for taking photographs/shooting video clippings of information available
- Jail broken, rooted devices will not be connected to the EIS server

3.2 Mobile Approval and Configuration Process

- Step 1: User has to take approval from respective department head and IT head for mail facility in the handheld device
- Step 2: User needs to send the approval mail to sesa.itsupport@vedanta.co.in to do the configuration
- Step 3: User needs to submit the device to IT department for the configuration of device

3.3 Information to user regarding MDM (Intune)

- The device will have a pin and the pin should be changed every 45 days . The pin cannot be disabled nor can the time of locking be changed
- PIN length is 6 numbers only .
- Simple password to be disabled
- The device will lock automatically after 10 minutes of non-usage
- If the password is typed wrong 10 times the Corporate container will be erased completely
- The maximum pin history is 5 passwords

3.4 Information to user regarding O365 email on mobile

- All O365 Users have Microsoft outlook application to access email on mobile
- Mobile Application Management (MAM) Enabled: App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app, Mobile Application Management (MAM) app protection policies allows you to manage and protect your organization's data within an application
- App lock: Set 6-digit pin code to all MS mobile app with 10 min idle time.

4. ABBREVIATION

None

5. CONTROL CLAUSES COVERED

A.8.1.3, A.8.3.1, A.8.3.2, A.11.2.6, A.6.2.1, A.6.2.2