

# **Sesa Goa Iron Ore**

## **Information Security Management System**

### **(ISMS)**

## **Procedure Documented information – Asset Management and Classification Procedure**

**This documented information is a confidential documented information of Sesa Group**

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the written permission of Sesa Group. This documented information includes confidential information related to Sesa Group and shall not be distributed to any persons other than those mentioned in the distribution list without the consent of Sesa Group. All product name(s) referenced herein are trademarks of their respective companies.

**Documented information Name: Procedure Documented information – Asset Management and Classification Procedure**

**Version No: 3.0**

**Last Updated: 25<sup>th</sup> July, 2023**

**Documented information Owner: Sesa Group**

**Approval Authority: Sesa Group**

**Table of contents**

<b>1.</b>	5	
1.1	5	
1.2	5	
1.3	5	
<b>2.</b>	6	
2.1	6	
2.1.1	6	
2.1.2	6	
2.1.3	6	
2.2	8	
2.2.1	8	
2.2.2	8	
2.3	11	
2.4	11	
2.5	11	
2.6	11	
REVIEWING	:	13
.13		
<b>3.</b>	17	
<b>4.</b>	18	
<b>5.</b>	18	
<b>6.</b>	18	

## Documented information Management Information

**Documented information Title:** Procedure Documented information – Asset Management and Classification

**Abstract:** This documented information is a procedure documented information highlighting the procedures for asset management and classification.

### 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 – Asset Management & Classification
Documented information Code	SESAT/ISO27001/ISMS_Procedure_Asset Management
Date of Release	16.01.2012
Documented information Revision	<b>25<sup>th</sup> July,2023</b>
Documented information Owner	Sesa Group – 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
1.	Shobha Raikar (CIDO- IOB)	<a href="mailto:shobha.raikar@vedanta.co.in">shobha.raikar@vedanta.co.in</a>	

### Documented information Change Approver List

Version No	Revision Date	Nature of Change	Affected Sections	Date Approved
1.1	20.03.2012	Added abbreviation	Section 6.0	20.03.2012
1.2	18.12.2012	Form Updated	Form	18.12.2012
1.3	28-03-2013	Sesa Goa Logo Change		28-03-2013
1.4	18-10-2013	Sesa Group Logo , file name change for Sesa Sterlite Ltd - IOB		18-10-2013
1.5	25-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT	3 and Form	27-01-2014

1.6	01-12-2014	Aligned to ISO 27001:2013, Vedanta Group policy	1.1,2.5,2.6, 4	05-12-2014
1.7	09-01-2015	Reviewed and updated as per internal audit	2.6	15-01-2015
1.8	11-Feb-2016	Company name logo update		15-Feb-2016
1.9	13-Feb-2017	Procedure review		18-Feb-2017
1.10	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.11	22-Aug-2018	Review		29-Aug-2018
1.12	23-Aug-2019	Review		30-Aug-2019
1.13	23-Sep-2020	Review and update	2.2.2	30-Sep-2020
2.0	18 March 2022	Review and update	2.13,	05-Apr-2021
2.1	23-Sept-2022	Review and update		27-Sept-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 . I N T R O D U C T I O N**

### **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.

This 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 Sesa Group's Asset Management procedure is to:

- Maintain information assets purchased and owned by Sesa Group and classify the same based on its sensitivity.
- Allow audit verification of addition to and deletions from the information asset register.

### **1.3 Intended Use**

The primary use of this documented information is to provide guidance for implementation of Classification of Information and Asset Management within Sesa Group. The documented information serves:

- As guideline documented information for the Process Owners
- To define various templates in this area for use by Information Security Committee

## 2 . P R O C E D U R E S

### 2.1 Defining Information

#### 2.1.1 Need to Know

One of the fundamental principles of information security is the "need to know basis". This principle holds that information should be disclosed only to those people who have a legitimate business requirement for the information. The data classification scheme has been designed to support the “need to know basis” principle so that information will be protected from unauthorized disclosure, use, modification, and deletion.

#### 2.1.2 Consistent Protection

The information of Sesa Group must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity; no matter where it resides, what form it takes, what technology was used to handle it, and what purpose it serves. Although this data classification scheme provides overall guidance to achieve consistent information protection, employees of Sesa Group need to apply and extend these concepts to fit the needs of day-to-day operations.

#### 2.1.3 Asset Type

- **Digital Data/Information Asset:** This would include all soft copy files in word, excel, power point, requirements, test cases documents, invoices, records, standard operating procedures, network diagram, system documentation, user manuals, training material, scanned copies of non-digital information such as agreements, etc.
- **Non digital Assets:** This would include all hard copy documents such as hard copy documents such as contract documents, agreements, service level agreements (SLAs), customer contracts, visitor register, training material etc.
- **Software Asset** - This would include Application software, System software, Development tools & Utilities etc.
- **Physical Asset** - This would include Computer equipment (servers, desktops, laptops, modems, printers etc.), Communication equipment (Network devices, Fax machines etc.), Unused magnetic media (Tapes, Disks, CDs) etc. Define asset labeling method and put it on all physical assets to enable identification as property of Sesa Group.
- **Services Asset** - This would include general utility services such as Power, Lighting, and Air Conditioning etc.
- **Personnel** - This would include personnel required to support and run other assets.



## 2.2 Asset Classification Steps and Labeling

The steps that are involved in the information asset identification and classification process would be as follows:

- Identification of business processes in the organization
- Identification of information assets involved in the business process
- Identify information owners
- Assign classifications to the information asset
- Build asset register capturing details of the asset and the classification of the same

### 2.2.1 Rules for Data Classification

- All information possessed by or used by a particular business process / department of Sesa Group will have a designated information owner.
- The information owners must be responsible for assigning / maintaining appropriate data classifications. All information stored in several media formats (either hard copy or electronic) will be classified as defined in the asset register.
- Files / e-mails created by individuals will be owned and classified by them on need basis.
- One person for each business process is nominated for the asset register maintenance across the process.

### 2.2.2 Information Classification Matrix

Information owners of Sesa Group will use the classification matrix as defined by the organization to classify information assets in a manner that balances the risk of compromise with the needs of normal business operations.



Classification Level	Definition	Examples
<b>SECRET (C1)</b>	This classification applies to possible 20-30% of Sesa Group information which is intended for access and viewing of only a particular group or persons designated by the Information Owner. Its unauthorized disclosure/destruction would cause damage to Sesa Group: loss of customers, embarrassment to the Company, and violation of federal and/or state regulatory requirements resulting in fines or litigation against the Company.	Information that falls under privacy-related statutes, nonpublic personal customer information; sensitive customer-identifying information; certain customer documents.
<b>CONFIDENTIAL (C2)</b>	This classification applies to highly sensitive business information, which is intended for use within Sesa Group and its other business units. Its unauthorized disclosure could adversely impact Sesa Group, its stockholders, its business partners, its employees, and/or its customers. Information that some people would consider to be private is included in this classification.	Employee performance evaluations, internal audit reports, critical project documented informations, source code, Proposals, designs and network architecture
<b>INTERNAL (C3)</b>	This classification applies to all other information, which does not clearly fit into any of the other four classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact Sesa Group, its employees / customers, stockholders & business partners.	Sesa Group training materials, and manuals, information posted on intranet portals for employee's usage, project tracking reports etc.
<b>PUBLIC (C4)</b>	This classification applies to information, which has been explicitly approved by Sesa Group management for release to the public. By definition, there is no such thing as	Information posted on internet portals, Service brochures, advertisements, job opening

Classification Level	Definition	Examples
	unauthorised disclosure of this information and it may be freely disseminated without potential harm.	announcements, and published press releases.

## 2.3 Cumulative Classification

The data classification levels represent cumulative information sensitivity. As the levels of sensitivity increase, the access and modification controls become more rigorous and comprehensive.

## 2.4 Consistent Classification Labels

All information with confidential classification will be labeled accordingly; from the time it is created until the time it is destroyed or re-labeled. Such markings will appear on all manifestations of the information (hard copies, floppy disks, CD-ROMs, etc.).

## 2.5 Declassification / Downgrading

Following guidelines will be considered for reclassification of Information Assets:

- Classification of information assets will be reviewed periodically (at least once a year) to ensure appropriateness of classification as per the business requirements.
- Whenever there is a need to reclassify the information, asset owner will inform process owner and asset user/ users. Asset owner will receive an approval from process owner, prior to changing the information classification.
- The asset owner will also inform the person responsible for maintaining the asset register about the change in the level of classification.
- Reclassification date will be mentioned on the documented information statistics section of each documented information.

## 2.6 Storing and Handling Classified Information

- All information will be processed and stored strictly according to the classification assigned to that information.
- Formal distribution lists will be used to ensure accurate distribution of restricted information. The Data Owner will be responsible for reviewing the distribution lists and lists of authorized recipients at regular intervals.
- All information classified, as 'Proprietary'(confidential and restricted) will specify destruction date and recipients will destroy the documented information according to distribution instructions. The following handling requirement will be followed:

Handling Requirements:

Usage	Secret (C1)	Confidential (C2)	Internal (C3)	Public (C4)
<b>Labeling</b>	<ul style="list-style-type: none"> <li>Marked as “Secret (C1)” on every page.</li> <li>Labeling Position: At the top/bottom of each page</li> <li>All pages should be numbered (e.g., 1 of 5,2 of 5) to ensure that no page is missing</li> <li>Documented information should carry name of owner on cover page</li> <li>Date of creation and/ or last update</li> <li>Expiry date</li> </ul>	<ul style="list-style-type: none"> <li>Marked as “Confidential(C2)” on every page.</li> <li>Labeling Position: At the top/bottom of each page</li> <li>All pages should be numbered (e.g., 1 of 5,2 of 5) to ensure that no page is missing</li> <li>Document Documented information should carry name of owner on cover page</li> <li>Date of creation and/ or last update</li> <li>Expiry date</li> </ul>	<ul style="list-style-type: none"> <li>Marked as “Internal (C3)” on at least the Cover page.</li> <li>Labeling Position: At the top/bottom of at least the cover page</li> <li>All pages should be numbered (e.g., 1 of 5,2 of 5) to ensure that no page is missing</li> <li>Date of creation and/ or last update</li> <li>Expiry date (Optional)</li> </ul>	<ul style="list-style-type: none"> <li>Marked as “General Business” on at least the Cover page.</li> <li>Labeling Position: At the top/bottom of at least the cover page</li> <li>All pages should be numbered (e.g., 1 of 5,2 of 5) to ensure that no page is missing</li> <li>Documented information should carry name of Sesa Group on cover page</li> <li>Date of creation and/ or last update</li> <li>Expiry date</li> </ul>
<b>Duplication</b>	<ul style="list-style-type: none"> <li>Mandatory to have a distribution list for sharing in Softcopy/Hardcopy</li> <li>Printing/Copying processes must be physically controlled by the user, to ensure that no information remains left in the printers or copying machines.</li> <li>Copies must contain the same classification mark as the original</li> </ul>	<ul style="list-style-type: none"> <li>Mandatory to have a distribution list for sharing in Softcopy/Hardcopy</li> <li>Additional protection should be applied to prevent unauthorized production of copies or onward distribution.</li> <li>Printing/Copying processes must be physically controlled by the user, to ensure that no information remains left in the printers or copying machines.</li> </ul>	<ul style="list-style-type: none"> <li>Duplication for business purposes only.</li> </ul>	<ul style="list-style-type: none"> <li>No special requirements.</li> </ul>

Usage	Secret (C1)	Confidential (C2)	Internal (C3)	Public (C4)
<b>Mailing of Information</b>	<ul style="list-style-type: none"> <li>• Mailing allowed with permission of owner using secure email channel</li> <li>• No classification marking on external envelope; Restricted marking on cover sheet;</li> <li>• Confirmation of receipt at discretion of information owner</li> </ul>	<ul style="list-style-type: none"> <li>• Mailing allowed with permission of owner using secure email channel</li> <li>• No classification marking on external envelope; CONFIDENTIAL marking on cover sheet;</li> <li>• Confirmation of receipt at discretion of information owner</li> </ul>	Mailing requirements determined by information owner	No special requirements
<b>Disposal</b>	Owner must observe physical destruction beyond ability to recover	Owner must observe physical destruction beyond ability to recover	Controlled physical destruction	No special requirements
<b>Storage</b>	<ul style="list-style-type: none"> <li>• Locked up when not in use.</li> <li>• Master Copy secured against destruction</li> <li>• Encryption must be used</li> </ul>	<ul style="list-style-type: none"> <li>• Locked up when not in use.</li> <li>• Master Copy secured against destruction</li> <li>Encryption must be used</li> </ul>	Master copy secured against destruction	No special requirements
<b>Distribution / Read Access</b>	Owner establishes user access rules; generally highly restricted	Owner establishes user access rules; generally highly restricted	Owner establishes user access rules; generally widely available within Sesa Group	No special requirements; generally available within and outside company
<b>Reclassification Review</b>	Information owner to establish specific review date	Information owner to establish specific review date	Information owner to review at least annually	No special requirements

Special Handling Requirements for Information in Electronic Formats:

Usage	Secret (C1)	Confidential (C2)	Internal (C3)	Public (C4)
<b>Storage on fixed media</b>	Encryption desirable, Password protection, Access control required All reusable media used for the storage of Restricted information must be overwritten three times with randomized data prior to disposal or re-use. CD-ROMs and other „write-once“ media must be	Encryption desirable, Password protection, Access control required All reusable media used for the storage of confidential information must be securely wiped. CD-ROMs and other „write-once“ media must be rendered unreadable by physical destruction prior to disposal.	Access control required	Access control not required

	rendered unreadable by physical destruction prior to disposal.			
<b>Storage on removable media</b>	Encryption needs to be used, Password protection	Encryption Desirable needs to be used, Password protection	No specific requirement	No encryption required
<b>Read/Update/delete access to information</b>	Information owner to authorize individual users	Information owner to authorize individual users	Information owner to authorize a user, group or function	No particular requirements
<b>Disposal of electronic media (tapes, hard disks, etc.)</b>	Completely destroy all magnetic media. Format hard disks. Owner to observe and verify the same.	Completely destroy all magnetic media. Format hard disks. Owner to observe and verify the same.	Completely destroy all magnetic media. Format hard disks	No special requirements

#### Transmission of Electronic Data:

Usage	Secret (C1)	Confidential (C2)	Internal (C3)	Public (C4)
<b>By Fax</b>	Fax to be attended to by recipient	Fax to be attended to by recipient	To be defined by information owner	No special requirement
<b>By Internet</b>	Receipt confirmation required. Encryption needs to be used	Receipt confirmation required. Encryption Recommended needs to be used	Receipt confirmation required. Encryption optional	No special requirement
<b>By LAN/WAN</b>	Receipt confirmation required. Encryption needs to be used	Receipt confirmation required. Encryption needs to be used optional	Information owner to define requirements	No special requirement
<b>By Voice Mail</b>	Not to be sent by voice mail	Not to be sent by voice mail	Receipt call required	No special requirement
<b>Cellular phone/normal phone</b>	Do not transmit	Do not transmit	No special requirements	No special requirements

- **Reviewing :**
- After the process of identifying and classifying information assets has been performed, it is essential that the information residing in the information asset register remains relevant to the organization over time. The asset register will be reviewed by the information owner for the sanctity of all the fields pertaining to an asset. A review can be initiated by one of the events documented in the following table. This list is not exhaustive and so, any other business or technical reason should also use as triggering event for reviewing of information classification.

Event	Description
Corporate acquisition or merger/ Strategic change or rationalization	Introduction of new organization capability, another organization's data assets, or multiple business units may be consolidated —this may introduce a new information asset type and therefore the need to profile the assets.
New Project	Introduces new, or replaces existing information assets—this requires changes in the profile, or introducing new data assets that need to be profiled.
Time period	An asset may need reclassification—this requires the change to the asset's profile. For example, annually or once in two years.

Event	Description
Legislative or regulatory change	Legislature requires that additional controls be applied and an alteration to the information asset definition.
Addition of new services or products	Addition of new services or products may result in new information assets being recognized in the system.
Addition/ change in business processes	Addition or change in business processes may result in new data assets being created or old ones becoming redundant.




### 3. ROLES AND RESPONSIBILITY MATRIX

Role	Responsibility
Department / Process Owners	Maintain and update Asset Register for their department / process. Send Approved Asset Registers to Security Manager every 3 months.
CISO/CDIO / Head-IT	Approve and validate Asset Registers every quarter.
IT Manager	Maintain Asset Register provided by Department/process. Update CISO of modifications. Based on modifications to the register, recommend and implement controls for updated assets.

## 4. TEMPLATES

- Media Disposal Form

Sr. No.	Documented information Name	Documented information Version	Documented information Attachment
1	Media Disposal Form	V 1.4	 Sesa Group_Form_Media D

## 5. REFERENCES AND RELATED POLICIES

- Asset Management and Classification Policy

## 6. ABBREVIATION

**LAN** – Local Area Network

**WAN** – Wide Area Network