Information Security Management System (ISMS)

Procedure Document Information – Physical & Environmental Security

Documented information Name: Procedure Document Information – Physical & Environmental Security Procedure

Version No: 3.0

Last Updated: 18-Sep-2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

This Documented information is a confidential documented information of Sesa Group

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 Management Information

Documented information Title: Procedure Documented information – Physical & Environmental Security

Abstract: This Documented information is a procedure Documented information highlighting the procedure for Physical & Environmental 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 – Physical & Environmental Security Procedure
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_ Physical & Environmental Security Procedure
Date of Release	16.01.2012
Documented information Revision	3.0
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 (CITOI)	Shobha.raikar@vedanta.co.in	Electronically Approved	03-Oct-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 Sesa Group		18-10-2013
1.3	25-01-2014	Sesa Sterlite Logo incorporated, Position Head IT replaced with GM-IT / Head-IT	4.1	27-01-2014
1.4	01 – 12 – 2014	Aligned with ISO 27001:2013, Vedanta Group Policy	1.1,1.2,3.1,3.2,7	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- Mar-2022	Review and Update of Data Privacy requirements		05-April-2022
2.1	14-Jun-2022	Procedure review and update to incorporate privacy related changes.	2.1, 4.1, 4.3, 6.1	25-August-2022
3.0	18-Sep-2023	Review and Update		03-October 2023

Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep 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, Odisha and Liberia, Pig Iron Division, Met Coke Division, Power Division in Goa, Sesa Coke- Vazare and Gujarat, FACOR – Odisha, MALCO Energy and Nickel Business, VGCB, and Visakhapatnam referred as Sesa Group in this document.

The following section provides detailed procedures and templates for implementation of Physical and Environmental Security policy.

The Physical and Environment Controls Policy contains:

- Physical Security
- Environmental Security
- Equipment Security
- Physical Security of Laptops
- Clear desk and Clear screen

1.2 Intended Use

The primary use of this documented information is to implement the Physical and Environmental security related controls as specified in the policy documented information. The documented information serves:

- As the process documented information for implementing Physical and Environmental Security controls
- To define various templates and procedures in this area for use by the implementation and sustenance teams.

2. Procedure

2.1 Securing Physical Perimeter and Sensitive Areas

- Security team will ensure all doors / gates and windows are capable of being locked.
- 24/7 manned security guards will be employed at all the entry / exit gates and at emergency entries. Security guards will be well trained and have a clean background before getting employed for the service.
- If any third-party vendor provides the necessary amount of security guards, then that third party must ensure that background verification of their employees is done and must provide the details of background verification to Sesa Group.
- Areas where critical resources or assets (including sensitive information, PII) are located will be classified as sensitive areas.
- Access to sensitive areas / secured areas will be provided on a need to have basis and after proper authorization and approval process. Whenever the employee terminates from the service or access to any sensitive area is no longer required, the administration team or team responsible for access creation / revocation would revoke the facility access.
- The procedure for providing access to facility is as follow:
    - User would send an email to his immediate supervisor or Department Head requesting access to facility areas where access is required.
    - Immediate supervisor or Department Head would approve the request and forward the same to the administration team or the team responsible for authorizing the facility access. ○ For new joiners, the HR department would send the email to the administration department.
    - On approval from immediate supervisor or Department Head or HR, designated personnel in the admin team or team responsible for providing facility access would action the request. ○ The designated personnel would maintain the record of access requests and would present the same during the internal audits conducted by the Internal Audit team of Sesa Group or during the external audits. ○ For third party users or vendor access requests; the respective department Head for which the vendor is working for must raise the access request at the HR / Admin Helpdesk.
- The procedure for revocation of facility access is as follows:
    - Whenever an employee terminates from the company services, he /she would need to get a sign off from the Administration Department Head on the exit or clearance form (No Dues form).
    - During the sign off from the Administration Department Head, designated personnel from the administration team would note the relieving date of the employee and after that the Administration Department Head would sign off on the exit form. ○ The designated administration department personnel will revoke the facility access on the last day of the employee as noted. ○ Immediate supervisor or Department Head will inform the administration team whenever access to employee is required to be removed on the basis of following grounds:
    - Employee is found to be absconding ○ Employee is transferred to some other location ○ Employee doesn't require access to certain areas of the facility, due to change in the functional role or interdepartmental transfers in the same facility
    - Employee on leave for more than 2 months

- The HR Department will send an email to the Administration Department Head and team every month mentioning the list of employees who have been transferred to other locations or terminated from the services of the company. ○ Designated Admin Personnel managing the facility access would verify the no. of facility access IDs revoked or deleted from the access control system with reference to the no. of employees transferred / terminated within a month. ○ Administration Head or designated personnel would review the access rights provided to the employees on a periodic basis. ○ Temporary access to the facility will be removed or revoked immediately after the expiry of the temporary time frame.

2.2 Visitor Management

- All visitors, third party users, vendors will be required to fill details in the visitor register / third party register or provide the details to be filled in the system at the reception (entry gate).
- Security personnel at the reception will issue a visitor badge / slip to authorized visitors and inform the concerned employee about the visitor.
- Visitor badge / slip will be of different color than that of employee badges to easily distinguish between visitors and employees.
- Employees must be aware about this difference established in visitor badges and also, they must be encouraged to report if they observe any suspicious visitor inside the company premises, especially near the sensitive areas.
- Security guard will record the visitor’s badge number in the register / system and direct the visitor to wear the badge.
- Security guard will ensure that he collects the visitor badge/ slip and logs the exit time of the visitor when the visitor leaves the Sesa Group premise. The visitor slip collected must be duly signed by the Sesa Group employee visited.
- Security guards must maintain a record of any personal information processing equipment or media like Tape Drives, laptops etc. brought in the office premise. The serial number, make, and model of the same would be noted in the visitor register. Security guard will match the serial number of the laptop when the visitor leaves Sesa Group premises.
- Permanent Gate pass will be provided to those employees to whom laptops are issued by the company. Temporary gate passes could be issued to third party vendor employees or contract employees who visit Sesa Group on a daily basis and carry laptops. Laptop gate pass must include details like
    - Employee ID number ○ Employee Name ○ Laptop serial number
    - Make and model of the laptop issued
- For temporary gate pass along with the above-mentioned details, the expiry date and vendor organization name will be clearly mentioned.
- At random, the laptop gate pass will be checked at the gate. The gate pass will be checked along with the employee ID badge to ensure photo identity check to support the laptop check.
- Personal belongings of employees like laptops, CDs, Hard Disk Drives, pen drives, etc. are not allowed to be taken inside without getting them authorized by the Supervisor of the employee or Department Head of the employee or Head of Administration Department.
- Reconciliation of badges issued to visitors would be done at the end of each day.

2.3 Banners for Physical Security

Banners need to be posted at the reception, all sensitive areas and the server room area, so that Sesa Group employees and visitors are aware of the implemented security measures in the organization. The banners will prominently display:

- Restricted entry area notification.

- The requirements that the visitors need to comply with, such as “Visitors need to report to reception”, “Visitors shall declare their IT belongings like laptops, CDs, Hard disk Drives, Pen drives, etc. at the security gate” etc.
- The requirements that the employees need to comply with, such as “Please wear your identification badges when inside the premises”, “Don’t let company confidential and valuable materials unattended”, etc.
- Notification of any security measure that is employed, like CCTV, Fire safety procedures and equipment, etc.

2.4 Roles and Responsibilities Matrix

Role	Responsibility	Forms templates
Gate Security	● Issue visitor badge and note details in the visitor register / visitor management system ● Collect visitor badge ● Reconcile badges ● Check laptops and other information processing equipment ● Record details of any information processing equipment ● Employee Random checks for laptops against the details provided in the laptop’s gate pass	● Visitor entry / exit Register format. ● Personal IT Asset Declaration Register Format.
IT Infrastructure Manager	● ● Review access rights to Server Room ● Approve requests for permanent and temporary gate passes for laptops. ● Display list of authorized users on the entry gate of server room	● Permanent and Temporary laptop Gate pass.
IT Team	● Circulate details of laptops issued to employees to the administration team, so that permanent gate passes can be created. ● Escort the visitors only if access to sensitive areas is authorized by the Infrastructure Manager ● Ensure visitors make entries during the entry and exit in the sensitive areas/server room.	● List of Employee laptop details

3. Environmental Security

3.1 Fire Prevention Steps

- The Health, Safety and Environment Team will ensure that all information-processing facilities are housed in an environment equipped with fire detection and prevention measures.
- Adequate fire protection methods and systems will be implemented which includes provision of fire extinguishers, hydrants, fire alarms and sensors, instruction manuals and displays for protection from fire.

- Fire Extinguishers shall be located in easily accessible areas like near IT equipment, prominent places like common areas, secured areas etc. The locations of fire extinguishers must be clearly marked.
- Clear instruction on usage will be available near the extinguishers.
- Fire emergency and evacuation procedures should be posted in common areas or on notice boards. The procedures for the emergency evacuation plan for the organization shall be prepared and displayed by the HSE Team.
- Smoke detectors and Fire alarms must be appropriately tested periodically (quarterly). The vendor who does this should ensure all smoke detectors are tested and the fire panel circuitry is functioning properly and reports shall be maintained.
- Fire panel system must raise the auto alarm in case of any malfunctions.
- Fire extinguishers must be checked periodically and reports shall be maintained. The sticker indicating the fire extinguishers are functioning properly and the next date for checking the fire extinguishers must be properly displayed on that sticker.
- Emergency phone numbers or contact details such as fire brigade, key security personnel, doctors, and hospitals should be posted in prominent places.
- All offices should have distinct space and pathways, marked as emergency exits as per the recommendations of statutory or external Fire safety agencies. The routes for exit shall be clearly displayed at such entrances. Fluorescent banners indicating the directions towards the fire exit should be placed at prominent places.
- Access to emergency exit doors should not be restricted in any way i.e., boxes; furniture, etc. should never be stored in corridors or near emergency exit doors.
- Combustible materials and any other materials that may provide fuel to a fire should be kept to an absolute minimum and at designated places. It must be ensured that such material is never stored in server rooms.
- All employees and temporary staff should be trained in the fire safety precautions and must be imparted basic knowledge of escape and safety during fire accidents.
- Mock-drills should be conducted every 6 months. The emergency evacuation procedures must be practiced during these mock drills. An appropriate report of the drill must be prepared indicating the gaps if any are observed. Any identified gaps during these drills must be noted and appropriate corrective actions must be taken to eliminate these gaps.
- Mock Drill report must contain details on following:

  ○ List of people who lead other users during the Emergency evacuation
  process. ○ Observing the time required to completely evacuate the
  building. ○ Audibility of alarms in all areas of the organization. ○ Any
  congestion occurred near the exit path ways during the evacuation process.
  ○ Co-operation provided by users in the mock drill exercise. ○
  Learnings from the exercise/experience shall be used for
  improvement.

3.2 Maintenance and Monitoring

- The HSE Team must ensure that all personnel including temporary staff must receive adequate training in an emergency.
- This training must be documented and must cover fire safety, evacuation procedures, access rules and incident management.
- Environmental conditions should be monitored for conditions such as extreme temperatures, dust, water leakage/seepage, humidity, etc. that could adversely affect the operation of information processing facilities.
- All telecommunication lines, network cables and internal power lines must be monitored and kept secured against any kind of tampering or damage.

- Cabling of network racks must be done neatly. Proper labels must be provided at both the ends of the cables. The cabling structure must be properly documented to maintain the track of connections. This Documented information must be updated on a periodic basis and as and when changes occur. Changes in the cabling must be controlled by applying strong change management procedures.
- A maintenance schedule should be drawn up for preventive maintenance of equipment used to control environmental threats including air-conditioning, power and fire control systems.
- Periodic testing should be carried out for the following to ensure that such equipment function when needed: - ○ Fire control systems including hydrants, water pipes etc. ○ Fire Detection system like Fire alarm system, Smoke detectors, etc. ○ Backup power supplies like Generator, UPS ○ Alarm systems like fire alarms etc.

3.3 Power Supplies

- Power systems should be designed to provide power, at appropriate levels and of desired quality, without interruption. There should be adequate redundancy for power sources and a single point of failure should be avoided.
- Arrangements should also be made for supply of power from a back-up generator.
- Backup power should also be provided for access control systems and other physical security systems such as alarms, fire detection and suppression systems, emergency lights, etc.
- The backup electrical power supply to the Server Room should be isolated from other circuits of the building.
- Power cables must be separated from telecommunication cables to prevent interference, wherever possible.

3.4 Air-conditioning and Humidity Control System

- Air conditioning mechanisms should be implemented to ensure that the operational environment conforms to the equipment manufacturer's specifications. The air conditioning mechanism deployed should have the capability to: ○ Monitor and control temperature and humidity ○ Circulate and filter air to remove dust & contaminants.
- Ensure that the HVAC (Heating, Ventilation, and Air-conditioning) system provides appropriate airflow, temperature and humidity for continuous availability of the Server Room and wherever applicable on switch locations.

3.5 Additional Control for Server Room

- False ceiling is recommended for flexibility in electric wiring, lighting, concealing AC ducts and protection against water seepage.

4. Equipment Security

4.1 Taking Equipment's Off-Premises / Outgoing Material

- If any information processing equipment is required to be taken out, IT Team/department shall ensure that; ○ Backup of the data containing sensitive information and PII taken.
    - ○ appropriate data security control implemented before material is moved outside the Sesa Goa premise
    - ○ gate pass (returnable / non-returnable) prepared
    - ○ The gate pass given to the security team at the entry / exit, and a copy will be maintained in the IT department
- The gate pass shall be given to the security team at the entry / exit, and a copy will be maintained

The gate pass shall be given to the security team at the entry / exit, and a copy will be maintained

- The gate pass shall be given to the security team at the entry / exit, and a copy will be maintained in the IT department.
- All equipment movement within and outside Sesa Group should be tracked and continuously monitored to mitigate the

risks of unauthorized removal of equipment.

- Approvals from authorized signatory and respective Head of Department must also be obtained on the gate pass. The IT team (CISO/CDIO / Head-IT) must sign the gate pass only after the approvals have been obtained.
- The equipment movement must be recorded in an asset movement register maintained for the same purpose. Separate registers must be maintained for returnable and non-returnable materials.
- Security Guard should check whether gate pass is signed by head of concerned department and authorized signatory: ○ Security personnel should inform head of concerned function and administration function in case material is without valid gate pass;

○

- It is the responsibility of the person taking the equipment off-premises to ensure that it is returned in the same condition and within the expected return date.
- The CDIO/ Head IT must ensure that if the equipment is being taken off-premises for any repairs, the entire data stored must be appropriately backed up and appropriate security controls are taken before it leaves Sesa Group premises.
- Any material sent out through couriers must be sent through trusted courier services; to which it is easy to track.
- Before handing the material to the courier person, his identity must be verified by checking his ID badge provided by the courier company.

Formatted: Font: (Default) Cambria, 11 pt, Font color: Auto

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.63 cm + Indent at: 1.27 cm

4.2 Receiving Equipment/ Incoming Material

- Delivery person brings the materials to the unloading area.
- The security personnel/IT Team should carry out the following activities while receiving the materials:

  ○ Check whether the material is new or old (returnable) by cross verifying with the pass (returnable pass).

  ○ If it is a returned item, then check whether it has returned in time. ○ If the IT material is returned in time, hand it over to the IT Department. ○ If the IT material is not returned in time, IT Team shall escalate the matter to respective team/Function.

  ○ If the material is new, check the validity of order from the user.

  ○ If the order is not valid, return it to the delivery person.

  ○ If the order is valid, check whether it contains any hazardous item.

  ○ If the material contains any suspicious/ hazardous item, inform the user and administration function and take the approval from them for accepting it. ○ After getting the approval, allow the material to be unloaded.

4.3 Equipment Siting and Protection

- Access to tape, disk, and documentation libraries would be restricted exclusively to those employees who are responsible for their maintenance.
- Location of equipment will be sited appropriately and noted in the asset register maintained by the asset owners.

Formatted: Font: (Default) Cambria, 11 pt, Font color: Auto

The organization also ensures that, whenever storage space is re-assigned, any PII previously residing on that storage space is not accessible to unauthorized personnel.

- Electric panel rooms must be protected from unauthorized access.
- The siting of equipment must comply with health/safety requirements provided by the manufacturer. The health and safety requirements must be displayed on the equipment and the operators must be made aware of the procedures to be followed while operating these equipment.

4.4 Roles and Responsibilities Matrix

Role	Responsibility
Admin Team	• Raise Incident report if any material is being taken out without gate pass or an invalid gate pass is used; • Ensure all critical equipment are covered under annual maintenance contracts and proper service is provided by the vendors;
Employee	• Obtain required approvals for taking equipment off-premises; Submit request with approvals to administration department;
Gate Security	• Check for authorized Gate pass and verify the signature on the Gate pass with the available specimens in authorized signatory list; • Record details of returnable / non-returnable materials in the respective register; • Track the return of material and inform Administration department and concerned user about the delay in return of material if any observed; • Inform administration department if any material is taken out without authorized gate pass or invalid signature is observed on the gate pass.

	• Submit equipmen • Ensure proper pa
IT Team/FMS	• Issue returnable/ • Adequate equipm • Escalate if returna • Ensure data back • Ensure appropria is moved outside • • Ensure returnable the expected retu • Take backup of da • Update asset regi

5. Physical Security of Laptops/Desktops

5.1 Laptops

- Laptops should be kept in locked cabinets when not in use.
- Laptops must be properly insured against any theft.
- The owner of the laptop should be clearly identified.
- Identified owners should sign ‘Acceptable Usage Policy’.
- It is the responsibility of laptop owners to ensure physical safety of laptops in public places (like airports, hotels, conferences, etc.). Laptops should never be left unattended.

- All laptops should have a unique serial number. All add on hardware components connected to the laptops should be identified and linked to the serial number of the laptop. The IT Service Engineer / Helpdesk must record the entire details in Asset Register / Inventory.
- Any loss or theft of laptop must be immediately reported to the concerned IT department and a FIR must be logged with the concerned Police Station.
- Users having sensitive data on their Laptops shall ensure the use of encryption technology for protecting unauthorized disclosure of data.

5.2 Desktops

- All desktops/laptops should have a unique serial number. IT Service Engineer / Helpdesk must record the desktop details in Asset Register.
- The owner of the device should be clearly identified.
- Hard disks should be secured against unauthorized access, tampering, or removal.

6. Clear Desk & Clear Screen Procedures

6.1 Securing Information Assets

- All the employees, vendors' employees and contract employees should apply key locks, screen saver and password features on their computer terminals, laptops, or servers while moving away from their cubicles.
- The organization should restrict the creation of hardcopy material including PII to the minimum needed to fulfill the identified processing purpose.
  Users should store all the confidential and restricted documented information in appropriate folder arrangements. 'Confidential' and 'Restricted' documented information should be stored with a password to open.
- Computer media like CDs, pen drives, Hard disk drives, etc. must not be left unattended when not in use.
- If faxes are received that contain sensitive information and/or PII like customer personal details, financial statements, etc., then the sender must ensure that the recipient is aware about the fax.
- Paper media containing sensitive information and/or PII must be securely destroyed once the information is no longer needed.

7. Templates

- Returnable and Non-Returnable Gate Pass Format as per Security / stores dept.

Sr. No.	Documented Information Name	Documented Information Version	Documented Information Attachment

8. References and Related Policies

- Acceptable Usage Policy
- Physical and Environmental Security Policy

-