vedanta | sesa goa iron ore

Sesa Goa Iron Ore

Information Security Management System

(ISMS)

Policy Documented information SCADA– Physical & Environmental Security

Documented information Name: Policy Documented information SCADA– Physical & Environmental Security

Version No: 1.9

Last Updated: 7th August 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Table of contents

Documented information Management Information

Documented information Title: Policy Documented information SCADA– Physical & Environmental Security

---

Abstract: This Documented information is a policy Documented information highlighting the policies 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	Policy Documented information SCADA– Physical & Environmental Security
Documented information Code	SESAIT/ISO27001/ISMS_Policy_P&E Security SCADA
Date of Release	12.12.2014
Documented information Revision	7-August-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	DK Singh – CISO
Security Classification	Internal
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature
1.	Shobha Raikar	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	22-Mar-2016	Company name and logo update		30-Mar-2016
1.2	22-Mar-2017	Document review		31-Mar-2017
1.3	25-May-2017	VGCB inclusion in scope	1	30-May-2017
1.4	23-Aug-2018	Review		30-Aug-2018
1.5	26-Aug-2019	Review		30-Aug-2019
1.6	10-Sep-2020	Review		16-Sep-2020
1.7	27-Sep-2021	Review and Update	1.1	21-Oct-2021

1.8	20-Sep-2022	Review and Update	1.1	21-Sep-2022
1.9	7-August-2023	Review and Update	1.1, 3.1.2, 3.1.6, 3.3.2	10-Aug 2023

Documented information Contact Point

S. No	Documented information Author	Email
1	Arjun N Rao	arjun.rao1@wipro.com

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

The policy intends to protect information and information processing assets related to SCADA/ PTS of Sesa Group used by its employees.

The policy intends to establish adequate controls for unauthorized physical access, environmental threats, both natural and man-made (for e.g. fire, floods, cyclones, landslides, earthquake, power disruption, water seepage etc.); factors threatening the availability and integrity of Sesa Group's information and information systems.

1.2 Purpose of the documented information

The Physical and Environmental Security Policy identifies the measures adopted by Sesa Group to protect the information assets from physical security and environmental threats.

1.3 Audience

This policy is applicable to all employees who comprise of internal employees, third parties contract employees and vendor employees who are utilizing, consuming, managing, and supporting the Information assets related to SCADA/PTS operations within Sesa Group.

2. POLICY STATEMENT

All information assets of Sesa Group shall be appropriately located, maintained and physically and environmentally protected in a manner that adequately reduces the risk of loss, damage and unauthorized access to these assets.

3. POLICY DETAILS

3.1 Physical Security

3.1.1 Securing Physical Perimeter and Secure Areas

- Sesa Group premises shall have a well-defined and physical strong perimeter.
- Adequate measures, including receptions manned with security guards, shall be implemented at all entrances to Sesa Group premises in order to prevent unauthorized access.
- All doors and windows shall be locked, when unattended and beyond working hours.
- All secure areas shall have a well-defined perimeter and location of these secure areas and the strength of its perimeter shall be determined by the criticality of the information assets protected by it.
- Adequate measures shall be adopted to prevent the disclosure of secure areas (like Server room or UPS room) to the visitors/public.
- Cameras, video and audio recording equipments shall not be allowed inside secure areas without appropriate authorization.
- Fire-Exit should be used only in case of emergency.
- Cameras shall be used to monitor sensitive areas and proper records shall be maintained for further investigation.

3.1.2 Physical Access Control

- Access to secure areas shall be strictly restricted only to authorized individuals.
- Biometric access control to be provided to the PLC/SCADA control rooms.
- Only authorised person to be allowed to enter.
- Use of adequate authentication mechanisms (e.g. proximity card, biometric access) shall be considered for controlling access to secure areas.
- Signs indicating "No Unauthorized Access" shall be prominently displayed at all entrances of all secure areas.
- Secure areas shall be locked when vacant and physically checked beyond working hours.
- All authorized users, visitors and third party shall always wear appropriate identification badges/passes within Sesa Group premises.
- Users shall inform security if they encounter individuals without appropriate identification badges/passes.

- Access privileges to secure areas shall be reviewed every 6 months
- All electronic access control systems must have provision for emergency release. The emergency feature must be tested at least every six months.
- Electromagnetic door locks must not be deactivated without prior permission from the Administration Department unless needed for emergency evacuation in case of events like fire/ earthquake.
- The system on which the access control software is installed must be adequately secured.
- The access to OT systems must include physical security measures, such as surveillance cameras and access control systems to prevent unauthorized access and tampering.

3.1.3 Visitor Access Control

- The date and time of entry and departure of visitors to Sesa Group premises shall be recorded in the 'Visitor's Log' maintained and the visitor access to secure areas like server room, control room and UPS rooms should be recorded in the log books of the secure areas.
- The visitor pass shall capture the visitor details like name, organization, person to whom they have come to meet and the respective department. Also, details of equipments such as laptops, mobile phones, portable media, etc. shall be captured and recorded.
- At the time of exit, the visitor can be asked for random checks.
- All visitors shall be given a temporary ID (daily / weekly / monthly pass) for identification inside the premises which should be returned before leaving the premises.
- All visitors shall always be escorted at the time of entry and exit from the Sesa Group premises and shall always be accompanied in secure areas.
- Visitors shall not be allowed to access user workstations without prior authorization.
- Access cards/visitor passes of individuals no longer requiring access to Sesa Group premises shall be collected prior to their departure. Passes issued to visitors and/or contractors shall be reconciled on a day to day basis.

3.1.4 Secure Delivery and Loading Areas

- Delivery and loading areas shall be designed so that supplies can be unloaded and loaded without getting access to other parts of Sesa Group premise.
- Access to the delivery and loading areas from outside Sesa Group premises shall be restricted to authorized personnel.
- Incoming materials shall be inspected for potential threats and registered before being moved to other parts of Sesa Group premises.
- Any outgoing material shall be accompanied by the proof of authorization from a designated official.

3.1.5 Video Surveillance

- Video surveillance cameras must be located at all entrances and exits and other strategic points at Data Centers, Corporate Headquarters and other such locations with high risk.
- CCTV used shall be monitored and, the system should be recorded for incident review and playback as required.
- The video surveillance recording must be retained securely for a minimum of 4 weeks, for possible future playback
- The CCTV Media (post recording) must be stored in a secure location.

3.1.6 Alarms

- Proper procedures should be established for monitoring and alarming when physical and environmental security is compromised.
- Personnel should be required to respond to all alarms with the appropriate response measures.
- All facilities, commensurate with their security level, should be alarmed for both physical and environmental intrusions. These may include motion detectors or cameras for physical intrusions and fire alarms for environmental concerns.

3.2 Environmental Security

3.2.1 Suitable Environmental Conditions

- Manufacturer's specifications for environmental control equipment shall be observed for temperature, humidity and electrical power requirements.
- The temperature and humidity levels within secure areas shall be monitored to identify conditions that might adversely affect the operations of the equipments and to take corrective measures.
- Use of cooking appliances (such as microwave), eating, drinking shall be prohibited within secure areas.

3.2.2 Electrical Protection

- Equipments shall be protected from electrical disruptions (e.g. power outages, surges, spikes etc.) that could cause the equipment to malfunction by using backup power arrangements.
- Electrical distribution control panels shall be clearly labeled and located in secure areas.
- The electrical central main switch shall be located in designated electrical room. The authorized personnel shall have access over this electrical room.
- The quality of power to equipments shall be monitored to enable taking corrective action.

- Back-up generators or provision for appropriate quantity of fuel shall be arranged to ensure uninterrupted operations of Critical Information Systems hosted in Data Centre/ Server Rooms/ NOC operations, in case of power failure for a prolonged period.
- A preventive maintenance of the UPS shall be carried out at least once in 6 months in accordance with the manufacturer‟s recommendations. The records of the same must be maintained.
- Diesel Generator (DG) sets must be subject to preventive maintenance every 6 months.

3.2.3 Fire Protection

- All secure areas shall be supported by a working fire detection system that provides early warning that smoke and/or fire has been discovered and a response action needs to be taken immediately.
- For secure areas not provided with automatic fire detection and prevention system, hand-held fire extinguisher shall be used. Fire extinguishers shall be kept for protection of IT equipments, in easily accessible areas and their locations shall be clearly marked.
- Fire detection / prevention systems shall be periodically (6 months) tested and reports shall be maintained.
- Fire safety equipments shall be checked periodically for their functionality in accordance with manufacturer's instructions and reports shall be maintained.
- Hazardous and combustible materials (e.g. packaging material) shall be stored at a safe distance from secure areas in identified areas. Computer supplies such as stationery shall not be stored within secure areas.
- Personnel shall be trained for the use of fire detection/suppression systems, the use of portable fire extinguishers and proper responses to fire alarms.
- All fire exits shall be marked clearly.
- Comprehensive fire and emergency instructions shall be displayed in prominent locations.
- Mock drills shall be conducted every six months to practice emergency evacuation procedures and procedures shall be refined using the lessons learnt during these mock drills.

3.2.4 Water Protection

- Secure areas shall have elevated floors and shall be located away from water pipes and overflow mechanisms.
- Floors above secure areas shall be provided with protection to prevent accidental water spillage or other possibilities of water leakages.
- Adequate drainage provision shall be provided to prevent damage from water logging.
- Data centres must be equipped with water / moisture sensors to detect water leakage and seepage.

3.3 Equipment Security

3.3.1 Equipment Siting and Protection

- Equipment shall be sited appropriately and controls implemented to reduce the risk of potential threats (e.g. theft, fire, explosive, smoke, flooding, dust, vibrations, chemical effects, electrical supply interference) to continued operations of the equipment.
- Unattended equipment such as network switches, servers etc. shall be placed in secure enclosures.
- The siting of the equipment shall comply with health and safety regulations/requirements.
- Equipment requiring special protection shall be isolated to reduce the extent of general protection required.

3.3.2 Equipment Maintenance

- All equipment shall be maintained in accordance with the suppliers' recommended service intervals and specification.
- Only authorized maintenance personnel shall carry out repairs and service the equipment's.
- A half-yearly return in form I containing details of the sales and buy-back of lead acid batteries to the State Pollution Control Board shall be filed before the 30th of June and 31st of December every year
- A half-yearly return in Form VIII shall be filed with the State Pollution Control Board.
- Maintenance schedules should be established, and preventive maintenance performed. Equipment maintenance should be tracked, and trends noted to determine if maintenance schedules should be adjusted.

3.3.3 Supporting Utilities

- Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
- All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning shall be adequate for the systems they are supporting.
- UPS systems and generators shall be installed to support controlled shutdown or continued functioning of equipments supporting critical business operations.
- Water supply shall be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (when used).
- Adequate contacts shall be in place with authorities including utilities, emergency services and health and safety departments such as, fire department, Police department, Telecommunication provides etc.

3.3.4 Cabling Security

- Internal power, telecommunications and network cables carrying data shall be protected from unauthorized interception and physical damage.
- Power cables shall be separated from communication cables to prevent interference.
- Cables shall be clearly labeled at both ends.

3.3.5 Secure Disposal or Re-use of Equipment

- SCADA/ PTS equipment shall be disposed or re-used as per the secure disposal procedure.
- The asset register shall be updated to reflect the disposal of SCADA/ PTS equipment.
- Used batteries shall be sent only to registered recyclers

3.3.6 Removal of Property

- Equipment, information or software shall not be taken out of Sesa Group premises without prior authorization.
- Appropriate records shall be maintained to trackS CADA/ PTS related equipment taken out of Sesa Group premises.
- It shall be ensured that no damage to the environment occurs during transportation
- It shall be ensured that used batteries will be deposited with the dealer, manufacturer, importer, assembler, registered recycler, reconditioned or at the designated collection centre

3.3.7 Securing Information Storage Media

- All information storage media (e.g. hard disks, pen drives, magnetic tapes and CD-ROMs) containing sensitive or confidential data shall be physically secured, when not in use.
- Physical access to magnetic tape, disk and documentation libraries shall be restricted to authorized personnel based on job responsibilities.
- Media containing Sesa Group sensitive information shall be accounted.

4. Enforcement

All employees, vendors and third parties shall follow the policy; violation of this can lead to disciplinary action, termination of contract, civil action or financial penalties.

5. References and Related Policies

None

6. Control Clauses Covered

A11.1.1, A11.1.2, A11.1.3, A11.1.4, A11.1.5, A11.1.6, A11.2.2, A11.2.3, A11.2.4, A11.2.9