Information Security Management System (ISMS)

Policy Document Information – Vulnerability Assessment Policy

Documented information Name: Policy Document Information – Vulnerability Assessment Policy

Version No: 3.1

Last Updated: 18 Sep, 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Policy Documented information – Vulnerability Assessment Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Vulnerability Assessment 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 – Vulnerability Assessment
Documented information Code	SESAIT/ISO27001/ISMS_Policy_ Vulnerability Assessment
Date of Release	30-Mar-2022
Documented information Revision	18-Sep-2203
Documented information Owner	IT Department
Documented information Author(s)	Sandhya Khamesra, Pricoris LLP
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	Date Approved
1	Shobha Raikar (CITO-I&S)	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
2.0	18 Mar 2022	Policy review and update		30-Mar-2022
2.1	23 Sept 2022	Policy review and update	1.1	27-Sept-2022
3.0	25-july-2023	Policy review and update		10-Aug 2023
3.1	18-Sep-2023	Policy review and update		03-Oct-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 & Gujarat, FACOR – Odisha, MALCO Energy and Nickel Business, VGCB, Visakhapatnam and Sesa Cement referred as Sesa Group in this document.

The policy is applicable to all employees, vendors, contractors and third parties authorized to access Sesa Group vulnerability management..

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

1.2 Policy Objectives

This document details the vulnerability management policies and controls required to maintain high levels of system and application security in a diverse IT environment. It outlines the technology and procedures necessary for implementing a comprehensive, integrated program to detect and remediate vulnerabilities in operating systems, applications, mobile devices, cloud resources, and network devices to maintain maximum levels of security.

2. Responsibilities

2.1 CDIO/CISO

- Responsible for approving and reviewing the policy.
- Providing and maintaining an enterprise class vulnerability scanner to conduct scans.
- Conduct annual compliance reviews of organization.
- Assist organization with risk assessment processes and to remediate or mitigate vulnerabilities in cases where such vulnerabilities cannot be eliminated through conventional means.
- Review quarterly and annual vulnerability reports.
- Provide approval for internal and external VAPT.
- Review and approve the controls to be implemented for vulnerability management.
- Approve vulnerability assessment system and tools.
- Approve the remediation plan.

2.2 IT Service Team/Admin Team

- Supporting and complying with this policy.
- Performing remediation as directed.
- Perform remediation as per the approved remediation plan Security Operations function.
- Development, implementation and execution of the vulnerability assessment process.
- Submit vulnerability assessment reports for review.

2.3 Employee

- Responsible for adhering to the policy.

3. Policy Statements

- The development, implementation and execution of the vulnerability assessment process is the responsibility of the CISO & it's team.
- Periodic or continuous vulnerability assessment scans shall be performed on all network assets deployed on Sesa Goa Iron Ore IP address space.

- A centrally managed vulnerability assessment system will be deployed. Use of any other network-based tools to scan or verify vulnerabilities must be approved, in writing, by the CISO.
- Sesa Goa Iron Ore personnel are expected to cooperate fully with any vulnerability assessment being conducted on systems for which they are held accountable.
- Sesa Goa Iron Ore personnel are further expected to cooperate with the IT team in the development of a remediation plan.
- Any vulnerability scans or follow-up activities, performed outside of the centrally managed vulnerability assessment tool, required to assess vulnerabilities must be approved, in writing, by the CISO
- The CISO is permitted, with approval of CDIO, to hire third party security companies to run external vulnerability scans against Sesa Goa Iron Ore assets, products or services.
- Sesa Goa Iron Ore shall request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. Sesa Goa Iron Ore shall identify the technical vulnerabilities it will be responsible to manage, and clearly define a process for managing them.
- Outcomes for findings can include:
  - Unacceptable Risk - ACTIONS: track with ticket; hold the release; remediate finding before release.
  - Acceptable Risk - ACTIONS: track with ticket; remediate finding in subsequent sprint (accept short-term risk). Low Risk,
  - Non Risk, or False Positive - ACTION: add to baseline. Vulnerability findings reports will be retained.

4. Vulnerability Management Lifecycle

The threat and vulnerability management lifecycle consist of the following three steps:

- Vulnerability Research - This describes the active research for newly discovered vulnerabilities in the systems used by the organization. This includes proactive research conducted by IT, monitoring of relevant news feeds, podcasts, mailings and the usage of dedicated provider services.
- Vulnerability Scanning -This describes the active testing of the information systems of the organization for vulnerabilities. This includes penetration tests, network scans, the utilization of intrusion detection systems and other measures.
- Vulnerability Treatment -This describes a set of activities to handle identified vulnerabilities. The activities range from risk evaluation and management, the proactive installation of patches, to the deactivation of ports or vulnerable services on servers, endpoints and network equipment.

4.1 Vulnerability Research

Vulnerability research focuses on identifying vulnerabilities relevant to Sesa Goa Iron Ore information systems before they are actively used. To achieve this, available information sources are actively monitored by IT to stay up to date with current developments. Examples for such sources are the following:

- Vendor bulletins, newsletters, announcements
- Newsfeeds, podcasts
- Exploit and vulnerability databases
- CERTs of public organizations or larger companies Whenever vulnerabilities applicable to information systems are identified through research, their impact must be determined through the standard risk management processes and according measures must be defined and undertaken.
- Base lining: Vulnerability scanning tools are known to produce many findings that are not useful to act on. A baseline of findings that we will not be acting on will be maintained in wiki. This baseline represents the set of findings we expect to find in subsequent assessments and expect to also choose not to act on them. The baseline will be reassessed at least annually.

4.2 Vulnerability Scanning

- Internal security scanning, including network scans (e.g., utilizing NESSUS) must be conducted at least annual once for all productive environments.
- External penetration tests must be conducted at least annually once for all productive systems, preferably by independent specialists.
- Additionally, security tests must be conducted when deemed necessary, e.g., when a security breach is suspected or in the aftermath of such a breach.
- Approved Scanning tools: There are numerous tools that can provide insight into the vulnerabilities on a system. Not all scanning tools have the same set of features. The Information Security Officer and Privacy Officer shall be the sole entity to implement an enterprise scanning tool. Use of any other vulnerability scanner must have documented justification for use and requires approval by the CISO.
- Periodic Vulnerability Assessment: Vulnerability assessment of all information Assets must be conducted on a periodic basis (At least annually once). The assessment will scan information assets from inside the perimeter of the Sesa Goa Iron Ore .
- An enterprise-class vulnerability scanning, and assessment tool must be used to conduct the scans. This tool must be capable of scanning information systems from a central location and be able to provide remediation suggestions. The scans must cover all information assets of the organization.
- Sesa Goa Iron Ore may contract external staff to complete the work however the contractors must use an enterprise-class assessment tool that provides similar capabilities as mentioned above.
- If contractors are engaged to conduct scans using the XXX scanning tool, approval must be obtained from the CISO.
- Scans shall be performed during hours appropriate to the business needs of the organization and to minimize disruption to normal business functions.
- Data from scans must be treated as Confidential.
- The vulnerability scanning tool must have the ability to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the organization.
- IT staff shall not make any temporary changes to information systems, for the sole purpose of "passing" an assessment. Any attempts to tamper with results will be referred to the organization’s IT management for disciplinary action.
- Vulnerabilities on information systems shall be mitigated and eliminated through proper analysis and repair methodologies.
- No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.
- At a minimum, an organization shall run authenticated scans from the enterprise class scanning tools on a quarterly basis against all information assets within its control.
- New Information System Vulnerability Assessment: Sesa Goa Iron Ore shall conduct several vulnerability assessments of all information systems during installation and testing and prior to production operations. No new major information system shall be considered in production until a vulnerability assessment has been conducted and vulnerabilities addressed.
- A vulnerability assessment shall be conducted at the completion of the installation of any vendor provided or in-house developed major application.
- A vulnerability assessment shall be conducted just prior to moving the major information system into production.
- If an information system is provided by a vendor prior to user acceptance testing and again before moving into production, vulnerability assessments must be conducted.
- All new major network infrastructure equipment must have a vulnerability assessment conducted during the "burn in" phase and prior to moving to production.
- At the completion of each of the above vulnerability assessments, all discovered vulnerabilities must be addressed with a mitigation plan developed, submitted to and approved by the Information Security Officer .

4.3 Vulnerability Treatment

- At the conclusion of each assessment a Mitigation and Compliance Report shall be produced. This report shall summarize the following:
- List of Vulnerabilities -All discovered vulnerabilities, the severity, and the affected information systems.
- Remediation Steps - Each vulnerability listed shall have detailed information on how the vulnerability will be remediated or eliminated.
- The report shall be submitted to the CISO with a timeline for completion of remediation steps.
- The treatment of vulnerabilities consists of the definition and implementation of controls and measures to eliminate vulnerabilities (e.g., applying a patch to the affected system) or to prevent the vulnerabilities from being exploited (e.g., deactivating a service or disallowing a firewall connection).
- Vulnerability treatment as a process has direct interfaces to the change management, the incident management and the patch management processes, as well as to several others. The treatment of vulnerabilities normally directly results in changes, incidents or patching activities; hence, all these processes must be followed as defined and documented.
- Vulnerabilities shall be categorized as Critical, High, Medium, Low and Information.
- Open vulnerability needs to be included / get covered in next cycle VAPT assessment as part of continuous cyber threat management .
- Remediation timeline is based on feasibility and budget availability. Howsoever, the below are the timelines for the common vulnerabilities as mentioned in the table below:

Sr. No	Vulnerability Category Remediation	Timeline (days)
1	Critical	2 Weeks
2	High	4 Weeks
3	Medium	60 days
4	Low	90 days

- Tracking of vulnerability scanning activity is in case of outsourced, then Sesa Goa Iron Ore shall ensure the following considerations:
  - NDA shall have signed with vendor
  - SLA adherence o Periodic review
  - Updated report should be submitted to Sesa Goa Iron Ore
  - All incidents shall be notified by vendor

5. Abbreviations and Definitions

- CAPA - Corrective and Preventive Action
- CDIO – Chief Digital Information Officer
- CISO – Chief Information Security Officer

Term	Definition
Framework	Sets an overall approach to managing certain areas of the business. They help outline guiding principles and key standards to influence decision making in line with the organization’s strategy and objectives.

Guidelines	Guidelines are recommendations to enable employees to perform their general responsibilities or specific tasks effectively. Conformance is expected unless, when applying professional judgement, circumstances justify Deviation
Regulations	Regulations, legislations and standards that govern the conduct and management of company. References to regulations should be reviewed regularly to ensure they are correct and accurately reflect company regulatory obligations.
IT Risk	IT business risk associated with the use, ownership, operation, involvement, influence and adoption of IT Within Sesa Goa Iron Ore.
Employee	Employees/customers/vendors/business partners/consultant in individual as well as official capacity.
Individual	Ultimate responsible person