Sesa Goa Iron Ore

Information Security Management System

(ISMS)

Procedure Documented information – Log file monitoring Procedure

Documented information Name: Policy Document Information – Log file monitoring Procedure

Version No: 3.0

Last Updated: 25-July-2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Procedure Documented information – Log file monitoring

Abstract: This Documented information is a procedure documented information highlighting the procedures for Log File Monitoring.

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 – Log File Monitoring
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_Log File Monitoring
Date of Release	05-Dec-2014
Documented information Revision	25-July-2023
Documented information Owner	IT Department
Documented information Author(s)	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 (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	11-Feb-2016	Company name logo update		19-Feb-2016
1.2	13-Oct-2016	Log review details	2.4	14-Oct-2016
1.3	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.4	01-Jul-2017	Retention period	2.5	05-Jul-2017
1.5	18-Aug-2017	SIEM process update		19-Aug-2017

1.6	22-Aug-2018	Review		29-Aug-2018
1.7	23-Aug-2019	Review		30-Aug-2019
1.8	09-Sep-2020	Review		16-Sep-2020
1.9	28-Sep-2021	Review and Update	1.1	21-Oct-2021
2.0	18 Mar 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

Table of Contents

1. Introduction

1.1 Scope of the Documented information

This procedure 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 , and VGCB , Visakhapatnam; referred as Sesa Group in this document.

These procedures apply to backup team and system administrators responsible for planning and performing backup as well as restoration activities.

- The following section provides detailed procedures for monitoring, reviewing and protecting log files across Sesa Group network.

1.2 Intended Use

The primary use of this documented information is to implement procedures for Log File Monitoring.

- Log files have been established to provide evidence of the conformity to requirements and of the effective operation of the ISMS. This procedure defines the method of monitoring, reviewing and protecting log files.

2. Procedures

ISMS log files shall be established and maintained to provide evidence of non-conformity to requirements and the effective operation of the ISMS. Log files shall be kept of the various critical systems and servers.

The following process should be considered in order to maintain the log files.

2.1 Identification

The systems are classified based on the criticality of each system and also based on regulatory and compliance needs.

Below are the broad classifications

Criticality	Systems
High	e.g. Firewall, Routers, AD, SAP Hanna
Medium	e.g. Sharepoint
Low	e.g. Teleconference, VC

2.2 Collection and Storage

- Log files shall be collected on Sesa internal network and would be adequately protected against unauthorized modifications and deletion
- Logging shall be enabled on security systems, network infrastructure devices and storage infrastructure, operating systems and applications
- Clock-synchronization shall be performed for all systems before enabling logging of events and activities
- Log Files information of systems and devices should be preserved based on the criticality of the system

- Storage availability of identified systems and log storages shall be reviewed weekly to avoid any failure of logging.
- It shall be ensured that secure disposal of logs takes place after retention period.

2.3 Access and Monitoring

- Managed SIEM (Security information and event management) services from Tata has been implemented for effective and 24*7*365 monitoring of critical systems of Sesa networks.
- Log files of identified systems in the network should be transfer to a sensor server located at Sesa HO and which further transfer the logs to Tata IDC Chennai for monitoring , analysis and alerting the concerned Sesa team for needful action .
- Access to log file should be only on need to know basis
- Activities of all the users including system administrator shall be logged
- Logs pertaining to activities of major changes shall be monitored
- Security related suspicious activities based on the log files review should be immediately reported as per incident management procedures
- Error logs shall be notified to the relevant team for appropriate action
- The logs should include the below when relevant

  a) user IDs;
  b) system activities;
  c) dates, times and details of key events, e.g. log-on and log-off;
  d) device identity or location if possible and system identifier;
  e) records of successful and rejected system access attempts;
  f) records of successful and rejected data and other resource access attempts;
  g) changes to system configuration;
  h) use of privileges;
  i) use of system utilities and applications;
  j) files accessed and the kind of access;
  k) network addresses and protocols;
  l) alarms raised by the access control system;
  m) activation and deactivation of protection systems, such as anti-virus systems and intrusion
  detection systems;
- An automated reporting system shall be established for generating reports for the captured logs.
- Alerts to be informed by email to the respective team with details for needful action

2.4 Review

- Security violations such as spoof attacks, packet dropping, IP address clashes, port scanning etc. should be reviewed.
- Warning messages and performance related parameters should be reviewed for highly critical and critical system
- Highly critical and critical system log files should be reviewed on a continuous basis
- Activities of all the users including system administrator shall be logged and reviewed
- Monthly review report to be reviewed by IT incharge , CISO and Head – IT.

The review timelines are as below

System	Monitoring and review timelines
Highly Critical	Real time monitoring and review
Critical	Real time monitoring and review
Low Criticality	Real time monitoring and review

2.5 Retention

The audit logs should be retained for at least 90 days in online storage and offline one year period.

3. Responsibility Matrix

Role	Responsibility
Tata Team	● Collection , monitoring and analysis of the Log files ● Alerting the Sesa team for needful action with details
Information security implementation team	● Responding the alerts send by Tata ● Weekly review of all incident ● Monthly report review and sign off from CISO and Head-IT
Users	● Adhering to this policy.
Tata Team	● Collection, monitoring and analysis of the Log files ● Alerting the Sesa team for needful action with details

4. References and Related Policies

- Network security policy
- Physical and environmental security policy

5. Enforcement

Any person, subject to this policy and procedures, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary or legal action in accordance with the Sesa Group Disciplinary Code and Procedures or rules of the organization.