vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Procedure Documented information – Firewall Configuration Guidelines

Documented information Name: Procedure Document Information – Firewall configuration Guidelines

Version No: 3.0

Last Updated: 18-Sep-2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Procedure Documented information -Firewall configuration Guidelines

Abstract: This Documented information is a guideline Documented information for Firewall configuration

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 – Firewall configuration Guidelines
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_Firewall configuration Guidelines
Date of Release	05-Dec-2014
Documented information Revision	3.0
Documented information Owner	Sesa Group – 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 (CITO)	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	11-Feb-2016	Company name logo update		19-Feb-2016
1.2	13-Feb-2017	Procedure review		18-Feb-2017
1.3	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.4	22-Aug-2018	Review		29-Aug-2018
1.5	23-Aug-2019	Review		30-Aug-2019
1.6	09-Sep-2020	Review		16-Sep-2020

1.7	28-Sep-2021	Review and Update	1.1	21-Oct-2021
2.0	18-Mar-2022	Review and Update		05-April-2022
2.1	23-sept-2022	Reivew and Update	1.1	27-Sept-2022
3.0	18-Sep-2023	Review and Update		03-Oct 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 4
1.1 Scope 4
1.2 Introduction 4
1.3 Objectives 4
2. Firewall 4
2.1 Configuration 4
2.2 Administration and Monitoring 4
2.3 Firewall Application 5
3. References and Related Policies 5

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 Firewall configuration Guidelines is applicable to the Sesa Group IT firewall devices

1.2 Introduction

This Documented information defines secure configuration parameters to be used when deploying firewall devices in the Sesa Group IT network.

1.3 Objectives

The objective of this documented information is to introduce the security requirements for Configuration, Administration and Monitoring of firewalls

2. Firewall

2.1 Configuration

- Firewalls shall be deployed in locations where Internet connections and data transfer connections are provided.
- Firewalls shall be deployed as per business requirements • Firewalls shall be configured for the below:
  - Anti-spoofing malware ○ Botnet Prevention
  - Deny all services by default and allow services only on need basis ○ Allow only 'established' connections ○ Deny all unauthorized access from internet, DMZ and the internal networks ○ Block incoming packets having Internal IP address range.
  - Deny all inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic ○ Deny all inbound or outbound traffic containing directed broadcast addresses
- Configuration changes to the firewall shall follow Change Management process
- Care shall be taken while applying changes on the firewall to ensure minimal disruption to production environment
- The firewall application must always have the latest vendor issued patches installed.

2.2 Administration and Monitoring

- Administrative and User access to firewalls shall be provided only on need basis

- There must be at least two firewall administrators with unique login IDs ● Access through firewalls should be duly authorized by the concerned person ● Encryption technologies shall be used for Remote Administration on firewalls.
- Access to most used services from Internal network to Internet/ data connections and vice-versa through firewall shall be provided through suitable Gateway systems deployed in the Demilitarized Zone ● Firewall configuration backup shall be taken on a monthly basis
- Firewall configuration backup media shall be stored in a secure place
- Firewall facilities shall have back up power supply
- Firewall facility shall be protected from natural disasters such as fire and flood.
- Only approved Third party software shall be installed on firewalls
- Firewall logs for failure/deny operation shall be monitored on a daily basis and reviewed for specific actions if any.
- Firewall rules shall be reviewed quarterly
- CISO / Head-IT to ensure the firewall controls

2.3 Firewall Application

- The firewall application must always have the latest vendor issued patches installed.
- Roll back plans must be established prior to any changes including configuration changes, upgrades and updates.
- After any upgrade, the firewall must be tested to verify proper functioning prior to going operational.

3. References and Related Policies

- Change Management
- Access Control