vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Policy Document Information – Network Security Policy

Documented information Name: Policy Document Information – Network Security Policy

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: Policy Documented information – Network Security Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Network 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 – Network Security Policy
Documented information Code	SESAIT/ISO27001/ISMS_Policy_Network Security
Date of Release	16.01.2012
Documented information Revision	25 July ,2023
Documented information Owner	IT Department
Documented information Author(s)	Sujay Maskara – Wipro Consulting Arjun N Rao – Wipro Consulting
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-I&S)	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	20.03.2012	Added abbreviation	Section 6.0	20.03.2012
1.2	28-03-2013	Patch Management & Sesa Goa Logo Change	3.2.7	28-03-2013
1.3	18-10-2013	Sesa Group Logo , file name change for Sesa Sterlite Ltd - IOB		18-10-2013
1.4	25-01-2014	Sesa Sterlite Logo incorporated , Position Head IT replaced with GM-IT / Head-IT	3.1.7 , 3.1.9	27-01-2014
1.5	01-12-2014	Aligned to ISO 27001:2013, Vedanta Group Policy	1.1,3.1,3.2,5,6	05-12-2014
1.6	09-01-0215	Updated as per Internal audit report	3.1,3.2	19-01-2015
1.7	10-Feb-2016	Company name logo update		18-Feb-2016
1.8	13-Feb-2017	Policy Review		18-Feb-2017
1.9	29-Apr-2017	VPN access	3.2.3	12-May-2017
1.10	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.11	21-Aug-2018	VAPT frequency correction	3.2.9	28-Aug-2018
1.12	08-Nov-2018	Patching timeline and priority	3.2.8	08-Nov-2018
1.13	22-Aug-2019	Policy review	3.2.8	30-Aug-2019
1.14	08-Sep-2020	Policy review		15-Sep-2020

1.15	04-Nov-2020	Policy update as per Group policy update	3.2.2	11-Nov-2020
1.16	28-Sep-2021	Policy Review and Update	1.1	21-Oct-2021
2.0	18-Mar-2022	Policy Review and Update		04-April-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

Documented information Contact Point

S. No	Documented information Author	Email
1.	Dileep K Singh	dileep.singh@vedanta.co.in

‘

vedanta | sesa goa iron ore

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, Orissa and Liberia, Pig Iron Division, Met Coke Division , Power Division in Goa , Sesa Coke- Vazare & Gujarat, FACOR – Orrisa , Nickel Business and VGCB , Visakhapatnam; referred as Sesa Group in this document.

The policy is applicable to all IT assets within Sesa Group. Network components like routers, firewalls, switches, servers, desktops, laptops and the VPN should be configured to meet Sesa Group security requirements.

1.2 Purpose of the documented information

The Network Security Policy intends to establish adequate controls for protecting information transmitted to and from the Sesa Group environment. It also establishes proper security controls to safeguard the equipment belonging to Sesa Group.

1.3 Audience

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

2. Policy Statement

Adequate network security controls shall be implemented to:

- Protect Sesa Group's information transmitted, stored and processed on the network from unauthorized disclosure, modification or destruction;
- Protect the supporting network infrastructure of Sesa Group.

Explanatory Notes

Networks play an important role in Sesa Group's business operations. Computer networks of Sesa Group shall be segregated from external networks and all connections to external networks including the Internet, outsourced vendors and partners shall be authorized and provided in a secure manner. All remote access to the Sesa Group's network must be authenticated and provided based on business requirements. Networks should be designed and maintained for high availability and to meet the requirements of the users

3. Policy Details

3.1 Network Management

3.1.1 Network Design

The design of the network shall adopt the following guidelines:

- The hardware and software configuration of the network/servers shall be documented.
- Network shall be divided into logical segments, based on sensitivity / physical zones / functional zones / internet exposure and business requirements.
- Incorporate coherent technical standards, support consistent naming conventions and comply with statutory and industry regulations.

- If there are any internet exposed servers, DMZ shall be implemented to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.
- Network design shall be supported by formal documentation of the network details and users' service requirements.
- Firewall or filtering devices shall be used to protect internal network from Internet.
- Single points of failure and the number of entry points into the network shall be minimized by having redundant network equipment and links.
- Network management reports shall be enabled and audit trails shall be maintained.
- Hardware redundancy mechanisms (i.e. duplicating certain or all hardware elements) shall be adopted for all critical application and network components.
- Mechanisms for high availability shall be considered and implemented, if possible and if necessary.
- An updated network diagram shall be maintained which depicts the current architecture and the technologies used. Appropriate documented information control shall be ensured for the same.
- Network diagrams of LAN / WAN must be held current and confidential.
- Strong cryptography and protocols like SSL or IPSec shall be used when sensitive data is transmitted over public or internet networks.
- If there is a loss of connection or unexpected fault in the network, administrators must be able to manage the network elements via the management network

3.1.2 Network Services

The following guidelines shall be followed for network services:

- The servers shall be implemented for single primary function, wherever possible. This shall simplify configuration, thereby reducing the risk of configuration errors. In some cases, however, it may be appropriate to offer more than one service on a single host computer (e.g., database, DNS, VPN, ftp and http services).
- The appropriate authority shall assess the security risks associated with enabling a network service to arrive at the security requirements as per the change management policy.
- Any unused or unwanted network services shall be removed or disabled as per the respective hardening documented information.
- A documented list of services and ports required for business purpose shall be maintained and updated regularly.
- If the business requires any services or ports to be enabled, they shall be enabled only after proper authorization and testing and putting in proper controls to avoid misuse.
- On a regular basis, vulnerability assessment shall be carried out to check for unused services or missing patches or vulnerable services which could be misused for malicious activities.
- Services known to be vulnerable (such as NetBIOS, Rlogin, RPC etc) shall not be permitted over WAN, unless for a group wide service provisioning.

3.1.3 Network Connectivity and Interconnection of Business Information Systems

- Modems and wireless devices shall be used as per the Acceptable Usage Policy.
- For non-public information, all equipment that provides access to the network shall positively identify the user through a login sequence for providing access as per "Identity & Access Management Policy".
- All access to the network shall be controlled using measures as per the "Identity & Access Management Policy".
- A Risk Assessment shall be done prior to allowing information flow between different business information systems or granting access to third parties. Controls shall be implemented to mitigate any risk associated with interconnection of Business Information System.

3.1.4 Network Component Security

- Identification of Network Components shall be done and access shall be restricted to authorized personnel.
- Inventory of all network components shall be maintained along with details like device name, owner, version details, etc.
- All premises hosting communication equipment like cables, network devices shall be secured from unauthorized physical access. The access control may be in the form of:
- Manned by Security Guards
- Access control systems like Card readers, Biometric scanners, Keypad locks
- Controls for physically securing network components shall be guided by “Physical and Environmental Security Policy”.

3.1.5 WAN (Wide Area Network) Access

- Proper Access control mechanism shall be defined to prevent unauthorized access to Sesa Group equipment.

3.1.6 Network Segregation

- Proper segregation shall be defined to limit access to Sesa Group equipment. Any application servers storing confidential data shall be separated from the user segments by applying proper access controls through the VLANs.
- IPS and Firewall shall be configured by Sesa Group to monitor all traffic flowing from external networks.

3.1.7 External Access

- Users shall get prior approval from Sesa CISO / CDIO / Head-IT before connecting with external networks that are outside the security management of the Sesa Group.
- External networks shall be separated from Sesa Group network through access control devices.

3.1.8 Remote Access

- There shall be proper authorization procedure for determining who are allowed to access the networks and networked services remotely. Proper protection shall be ensured before providing such connectivity.
- Secured communication channels such as SSL or IPSEC should be used to provide remote access to intranet-based applications
- VPN access to Sesa’s resources shall be authenticated by the Active Directory.
- User Authentication for establishing VPN session shall be encrypted.
- Remote access logs and access denial logs shall be maintained
- Remote access to systems by vendors & system administrators shall be as per defined agreements with the vendor
- Employees shall not extend remote access to Sesa Group Intranet resources to unauthorized personnel including family and friends.
- Users shall not connect the desktop/laptop to datacard, external modem etc and Internal network simultaneously
- Remote access to systems using Mobile devices shall be protected as per Acceptable Mobile Phone Policy
- Employees within the company network are not permitted to access external systems through dialup-up modems connected to a landline voice phone.
- External modems must not be installed with any PC until authorized by the authorized personnel.

- The Data Cards / mobile phones / modems for accessing Internet/VPN must be used only under the following conditions.
  - The provision of data card to the user is approved by the user‟s manager
  - The data card service provider is approved by the company
  - Antivirus is updated with latest definitions
  - The Operating System is updated with the latest patches
  - File sharing is disabled
  - The user computer is disconnected from Local network (wired/ Wireless)

3.1.9 Third Party Access

- All new connection requests for granting connectivity between third parties and Sesa Group shall require third party and Sesa Group representatives' signoff on the Third-Party Agreement / NDA.
- All connectivity established shall be based on the least-access principle, in accordance with the approved business requirements and the security review.
- Third party or vendor shall follow Sesa Group security policies.
- All changes in the third-party connections shall be approved and authorized by CISO / CDIO / Head-IT.
- Third party access privileges should be reviewed at regular intervals.
- When a connection with a third party is not required proper procedure shall be followed for deactivating the access.

3.1.10 Encryption

- Encryption shall be used when information of "confidential" and "restricted" classification is passed over the network.
- CISO team shall evaluate the different protocols and implement strong cryptographic controls to safeguard information
-

3.1.11 Wireless Access

- Wireless LAN Access across Sesa Group shall be used over encrypted channel using stronger encryption methods
- All wireless LAN access points must require an authentication, encryption and MAC registration.
- The authentication for wireless access points must adhere to WEP -128, or WPA or EAP / 802.1x standards. The encryption must adhere to minimum WEP-128 or WPA standards.
- It shall be ensured that wireless access points are secured properly. A formal process to detect and disable rogue access points on a periodic basis must be established
- SSID (Service Set Identifier) of the wireless network shall be unique and shall not be broadcasted.
- All wireless devices shall be configured as per "Wireless LAN Security Guidelines" before being deployed in the Sesa Group network.

3.1.12 Change Control

- Any change in the internal network architecture or network connectivity shall follow change control policy.
- Modifications to access control lists on the network devices shall follow proper change control policy.

3.1.13 Documentation

- Network Documented information shall be considered as sensitive information. It shall only be made available to authorized individuals strictly on a need-to-know basis.
- There should be detailed documentation of the network architecture and the IP addressing schema maintained.

- All network related documented information shall always be kept updated. Some examples are as listed below:
  - LAN-WAN Network Diagram
  - Network Configuration Standards

3.1.14 Enforced Path

- Specific ports for specific applications and systems shall be allocated.
- Access restrictions at perimeter devices like routers shall be placed.
- Separate logical domains or Virtual LANs based on the need for segregation in the network shall be created.
- The segregation shall be based on the access control policy and business and access requirements.
- Command line access to systems shall be limited to the authorized people only.

3.1.15 Redundancy

- Adequate redundancy shall be built-in to the network links.
- Redundant links shall have the same level of security as the primary links.

3.1.16 Clock Synchronization

- Time synchronization through NTP shall be implemented across the organization's various processing platforms thereby enabling generation of time-based audit trails.

3.1.17 Node Authentication

- Node authentication shall be established for external network connections coming from identified networks through secured channels established prior to authentication. This may include VPN as an alternative for authenticating of remote users where they are connected to secure, shared computing facility.

3.2 Network Devices

Explanatory Notes
This section aims at measures to build up a secure network by adopting best practices in managing network devices.

3.2.1 General

- All default passwords used on network devices and various IT components for administrative or otherwise authorization shall be changed.
- All network components shall be configured with strong authentication and password settings as per the "Identity & Access Management Security Policy".
- All network devices which transmit the information on the network shall be configured properly so as to protect the information from being leaked, hacked or intercepted.
- A warning banner shall be displayed at login to any system, This shall constitute a special notice, which shall include:
  - The system shall be used only by authorized users.
  - The user represents that he/she in an authorized user by continuing to use the system.
  - Use of this system constitutes consent to monitoring.
- The banner shall not include any system or application identifiers, which may provide valuable information to a would-be intruder e.g. hardware and operating system present on the host, information about the organization or other internal matters.
- All devices shall be configured as per the Sesa Group Hardening Guidelines.

- All system components and software shall have the latest vendor-supplied patches and updates installed. Patch Management Procedure shall be followed for ensuring compliance with stated clause.
- It shall be ensured that anti-virus mechanisms are current, actively running, and capable of generating audit logs.
- All network devices shall be set to a time out for inactivity.
- A process shall be implemented to identify newly discovered vulnerabilities.

3.2.2 Routers and Switches

- Routers and switches must be housed in a physically secure location
- The configuration information of routers and managed switches must be properly documented and securely stored.
- Any user who gains access to the command prompt must not have administrator privileges by default.
- All routers and managed switches must be hardened
- Central repository of logs from all network devices should be maintained such that logs could always be made available, to fetch point in time events, whenever required.
- The implicit deny all ACL should not be changed in routers or L2(wherever applicable)/L3 switches

3.2.3 Virtual Private Networks (VPNs)

- All the company employees' grade M3 and above VPN access will be given as default at the time of creating AD id.
- For all other internal employees, contract employees and vendor employees VPN access can be given as per for business requirement and access request approval process.
- It shall be the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Sesa Group internal networks.
- VPN use shall be controlled by using strong password authentication.
- When actively connected to the corporate network, VPNs shall force all traffic to and from the PC over the VPN tunnel: all other traffic shall be dropped.
- VPN gateways shall be set up and managed by Sesa Group network operations.
- All computers connected to Sesa Group internal networks via VPN or any other technology shall use the Sesa Group authorized antivirus software and shall ensure that it is up-to-date.
- Users of computers that are not Sesa Group owned equipment shall configure the equipment to comply with Sesa Group's VPN and Network policies.

3.2.4 Desktop/Laptop

Basic Security

Measures

- Operating systems shall be secured as per the Sesa Group Information Security Policy.
- Labeling of the Laptops with proper asset tag shall be ensured.

Physical Security

- For physical security of laptops and desktops "Physical and Environmental Security Policy" shall be referred

3.2.5 Servers

Ownership and Responsibility

- All Internal servers deployed at Sesa Group must be owned by an operational that is responsible for system administration**.**
- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
  - Information in the corporate enterprise management system must be kept up-to-date.
  - Configuration changes for production servers must follow the appropriate change management procedures.

Configuration Guidelines

  - Operating System configuration should be in accordance with approved Information Security guidelines.
- Services and applications that shall not be used shall be disabled where practical.
- The most recent security patches shall be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Secure channel connection shall be used when confidential data is passed through the channel (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.

Monitoring

- All security-related events on critical or sensitive systems shall be logged and audit trails saved.
- Security-related events shall be reported to Management Representative, who shall review logs and report incidents to IT management. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:
  - Port-scan attacks.
  - Evidence of unauthorized access to privileged accounts.
  - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits shall be performed on a regular basis by authorized organizations within Sesa Group.
- Audits shall be managed by the internal audit, in accordance with the Audit Policy. Internal Audit shall filter findings not related to a specific operation and then present the findings to the appropriate support staff for remediation or justification.
- Every effort shall be made to prevent audits from causing operational failures or disruptions.

3.2.6 Audit Logging and Monitoring

- The following minimum information shall be logged for servers, applications and network devices
  - Login Successes and failures
  - Addition/deletion/ modification of users
  - Changes to security settings
  - Changes to logging and auditing settings
- All unsuccessful login attempts shall be recorded. The System Administrator shall review a log of such attempts on a periodic basis.
- Only authorized users shall have access to utilities that reconfigure logging mechanisms.
- The log files shall be protected from being accessed, modified or deleted by unauthorized users.
- Audit trails should be backed up on a regular basis and should be stored on a centralized location which has limited access.
- Audit trails should be retained minimum for one year with at least three months online availability.

3.2.7 Network/Remote Diagnostics

- Physical and logical access to diagnostic and configuration ports of network devices should be controlled.
- Ports, services, and similar facilities installed on a computer or network facilities, which are not specifically required for business functionality, should be disabled or removed.

3.2.8 Patch Management

- Sesa IT Team will be responsible to handle the patch management process.
- Patch deployment / firmware upgrade need to be done within 30 days from date of release of patch for critical update within 2-3 days.
- Firmware upgrade need to be done, if any bugs are available in current version or else any new features are made available which is as per requirement of business / security controls.
- Patching of IT system need to be done as per classification priority defined in Application business impact analysis document.
- Both OS level and application level patched must be constantly be tracked so that critical patch released are not missed out.
- Following methods can be employed for keeping a track on the patches:
  - *Tracking through Web sites*
  - *Automatic patch alerts*
- Verification of the installation of the patch must be done on a periodic basis.
- Patches must be categorized based upon the criticality ratings given by the vendor.
- Applicability of patch to Sesa Group network must be verified before applying it.
- Patch must be first tested in a test environment before deploying in Production servers.
- Test setup will be periodically replicated with the current status of the production setup.

3.2.9 Vulnerability Management and Penetration Testing

- No application security, vulnerability assessment or penetration testing should be performed against Vedanta's assets without authorized approval.
- Vulnerability assessment and Penetration testing on Critical Systems and Applications shall be carried out once in 1 year.
- Penetration testing when required must be done in a controlled manner by the third party.
- Prior to carrying out penetration testing, approvals from respective Application Owners must be obtained.
- The type of attack like denial of service must not be carried out as part of the penetration testing exercise unless authorized by authorized personnel.
- CISO / Head-IT can decide the Penetration testing as required for any specific system.

3.2.10 Network Diagnostic tools

- A list of security and penetration testing tools shall be approved every year. Such tools will be used by designated personnel, with prior approval from authorized personnel.
- All information systems equipped with diagnostic software / penetration testing / vulnerability assessment tools shall be secured

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

- Acceptable Usage Policy
- Identity & Access Management Security Policy
- Physical and Environmental Security Policy
- Network Security Procedure

6. Control Clauses Covered

- A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.13.1.1, A.13.1.2, A.13.1.3