vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Procedure Document Information – Wireless Security Guideline

Documented information Name: Procedure Document Information – Wireless Security Guideline

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 – Wireless Security Guideline

Abstract: This Documented information is a procedure Documented information highlighting the procedure for Wireless Security Guideline.

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 – Wireless Security Guideline
Documented information Code	SESAIT/ISO27001/ISMS_Procedure_Wireless Security Guideline
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 Services 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-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	Sesa Goa logo Change		28-03-2013

1.3	18-10-2013	Sesa Group Logo, file name changes 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	2.2,3	27-01-2014
1.5	01 – 12 - 2014	Aligned to ISO 27001:2013	1.1	05-12-2014
1.6	11-Feb-2016	Company name logo update		19-Feb-2016
1.7	18-Nov-2016	Wireless audit - frequency	3	24-Nov-2016
1.8	24-May-2017	VGCB inclusion in scope	1	30-May-2017
1.9	22-Aug-2018	Review		29-Aug-2018
1.10	23-Aug-2019	Review		30-Aug-2019
1.11	09-Sep-2020	Review		16-Sep-2020
1.12	28-Sep-2021	Review and Update	1.1	21-Oct-2021
2.0	18 Mar-2022	Review		05-April-2022
2.1	23 Sept 2022	Review and update	1.1	27-Sept-2022
3.0	25 July ,2023	Review and update		10-Aug 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 of the documented Information

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.

This policy applies to all wireless LAN (WLAN) infrastructure used by Sesa Group and employees, contractors, third parties using wireless LAN resources within Sesa Group.
This documented information narrates the steps for securing the WLAN of Sesa Group from malicious users or intruders, who may cause denial of service attacks, steal identities, violate the privacy of legitimate users, insert viruses or malicious code and disable operations.

1.2 Responsibility

The E-mail Security Policy defines security measures adopted by Sesa Group for proper and productive use of organization's electronic mail facility.

1.3 Type of Users

This policy is applicable to employees who comprise of internal employees, contract employees and vendor employees who are utilizing the Internet Services assets within Sesa Group.

1.3.1 Sesa Group Employees

Sesa Group employees using the wireless LAN would be authenticated by the native Windows Domain Controller.

1.3.2 Third Party Employees

Third party employees will be treated as guests and allowed to access Internet only.

2. Security Considerations

- This section specifies security parameters that need to be considered by IT while designing, deploying, operating and maintaining the Wireless LAN infrastructure at Sesa Group.
- Following should be practiced by IT team to ensure adequate WLAN security:
  - Periodic review of wireless signal strength at all Sesa Group companies' locations and HO where the WLAN is deployed. This can be done by using various sniffer tools such as AirMagnet or AiroPeek.
  - Walk through the Sesa Group companies' facilities to detect rouge access point in the network using sniffer tools.
  - Finding unregistered wireless devices that are connected to Sesa Group WLAN.
- IT team should be trained for secure deployment and operation of wireless infrastructure.
- Sesa group employees or external users, contractors who are using WLAN infrastructure should not attempt to either identify or exploit the weakness in the wireless infrastructure.
- If any users observe any weakness or security incident related to wireless infrastructure, should report it to the IT Helpdesk.
- Following additional sections shall be referred as per "Network Security Policy and Procedures":
  - Network Access Points
  - Network Traffic types and limits
  - Network Monitoring

- Baseline Security Configuration
- Vulnerability analysis
- Network Abuse
- Network Authoritative Services like DHCP, DNS etc.
- Malicious Software use
- Incident Response

2.1 Physical Security

- IT should ensure that security guards are placed at the perimeter area of Sesa Group's locations to avoid any unauthorized access into the premises.
- IT should restrict physical access only to administrators of the access points.

2.2 Configuration Security

IT should ensure that the following counter measures are undertaken before deploying wireless access points within the premises of Sesa Group companies':

- The access points, which control access to WLAN and bridge a client connection to internal LAN, should be securely configured.
- The access point should not broadcast the Service Set Identifier (SSID) of the wireless network. Also, SSID of the access point should be unique and must not contain or indicate any information about Sesa Group's personnel, business or product identifiers. It is recommended that multiple SSIDs be used to avoid any compromise.
- Routing protocols should be filtered to the Access Points so as to eliminate network injection attack.
- Enable MAC address filtering.
- Access points should be configured to reasonably control wireless radiation. After configuring it, it should be checked to ensure that wireless radiation is not detected beyond the permissible distance.
- The wireless access point and its configuration should be approved by the CISO/CDIO / Head-IT. Vendor default configuration of the access points should be disabled.
- Client devices (Laptop/Desktop) and access points should be securely configured and basic hygiene check should be conducted for these at regular intervals.
- The SSID of the wireless network should be manually configured by the IT in the user's laptop/desktop that is used to access wireless network.
- IT should configure the wireless card, installed in the client device, to ensure that its SSID is not broadcast. The default SSID of the wireless card should be changed to a difficult-to-guess SSID and should be configured not to participate in any 'ad-hoc' wireless network connection.
    - The users of wireless client device should be educated on the secure use of wireless networking so that they do not unknowingly connect to any unknown or unauthorized access point or wireless network.

2.3 Network Security

2.3.1 Network Authentication and Authorization

- The IT should use WPA - 2 (Wi-Fi Protected Access) Enterprise modes for providing authentication and authorization service.
- Virtual Private Networks (VPN) with VPN gateways should be configured to supplement encryption and authentication provided by WPA.

2.3.2 Network Management Security

If wireless access points are running the SNMP agents, SNMP read/write community strings should be securely configured (if not required then it can be disabled). Default community string should be changed by the administrator.

2.3.3 Wireless Network for Guest Users

- The use of Guest Wireless Networks should be limited to those persons visiting Sesa group companies' premises and have a business need to communicate over the Internet.
- The wireless network segment for guests must be logically segregated from the enterprise wireless network of Sesa group. A separate VPN should be defined for WLAN users.
- Guests who need to use the Sesa Group-controlled and operated Guest Wireless Network would need to raise a request to the IT, which it will verify.
- Only authorized personnel from IT at respective Wi-Fi-enabled locations of Sesa group should configure the necessary setting in the guest's laptop to connect to the Internet through Guest Wireless Network.
- Only Internet access should be allowed through Guest Wireless Network.
- IT should ensure that the guest users wireless device have adequate security software installed like antivirus.
- IT should ensure the same level of security for the Guest Wireless Network as the Enterprise Wireless Networks.

2.4 WLAN Traffic Monitoring

- IT should ensure that audit logging is enabled on the Wireless LAN and its associated devices.
- Log administrator should monitor these logs on a weekly basis. Weekly report for log monitoring should be submitted to Security Team. IT should scan the Wireless network on a weekly basis to detect any 'ad-hoc' or 'unauthorized' access points. In case any such access point exists, a root cause analysis should be carried out to ascertain the same.

3. Wireless LAN Security Audit

Vulnerability Assessment or Penetration Testing should be conducted for Wireless Infrastructure once in year. The report of the VA/PT should be submitted to the CIDO/CISO/ Head-IT for review. The VA/PT exercise should, at a minimum, include the following:

- Review of wireless network architecture that is deployed in Sesa Group.
- Run a scan on the wired-network on a weekly basis to detect the presence of any unauthorized access point.
- Conduct a configuration test of wireless access points and client devices.
- Conduct a test to ascertain that insecure SNMP community strings exist.
- Conduct a test to find out the extent of wireless radiation by war driving (War-driving is the most common form of passive attack. The RF signal of 802.11 networks may extend beyond the confines of a building. With a wireless laptop or terminal, a hacker simply drives through business districts passively listening for a strong RF signal. Without good security, very little effort is then required to penetrate the network).
- Conduct a test to find out if MAC-address spoofing is possible in the deployed wireless network.

4. Templates

- None

5. References and Related Policies

- Network Security Policy

6. Abbreviations

- LAN – Local Area Network
- WAN – Wide Area Network
- VLAN – Virtual Local Area Network
- SSID – Service Set Identifier
- VPN – Virtual Private Network
- SNPM – Simple Network Management Protocol
- VA/PT – Vulnerability Assessment / Penetration Testing