Information Security Management System (ISMS)

Policy Document Information – Email Security Policy

Documented information Name: Policy Document Information – Email 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 – Email Security Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Email 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 – Email Security Policy
Documented information Code	SESAIT/ISO27001/ISMS_Policy_Email Security Policy
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	28-03-2013	External Email system & Sesa Goa Logo Change	3.2.2	28-03-2013
1.2	18-10-2013	Sesa Group Logo, file name changes for Sesa Sterlite Ltd - IOB		18-10-2013
1.3	21-01-2014	Sesa Sterlite Logo incorporated, Position Head IT replaced with GM-IT / Head-IT	3.2.2,3.2.5	22-01-2014
1.4	01 – 12 - 2014	Aligned to ISO 27001:2013, Vedanta Group Policy	1.1,3.2,6	05-12-2014

1.5	10-Feb-2016	Company name logo update		18-Feb-2016
1.6	13-Feb-2017	Policy Review		18-Feb-2017
1.7	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.8	28-Mar-2018	Email attachment size update	3.2.5	31-Mar-2018
1.9	22-Aug-2019	Policy review		30-Aug-2019
1.10	23-Sep-2020	Review and update O365	3.2.6	30-Sep-2020
1.11	28-Sep-2021	Review and Update	1.1	04-Oct-2021
2.0	18 Mar-2022	Review and Update		04-April-2022
2.1	23-Sept-2022	Review and Update	1.1	27-Sept-2022
3.0	25-July 2023	O365 access is given all users	3.2	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

vedanta | sesa goa iron ore

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 employees, vendors, contractors and third parties authorized to access Sesa Group E-mail System. The policy intends to protect information communicated within Sesa Group as well as with third parties and vendors.

1.2 Purpose of the documented information

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 Audience

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.

2. Policy Statement

Electronic mail is a business resource and it is important to use it responsibly and take adequate precautions to restrict its abuse.

3. Policy Details

3.1 Approval for E-mail

E-mail is an approved manner for communication in Sesa Group. The usage of E-mail must therefore be controlled to ensure that unauthorized persons do not get access to E-mail facilities. Approval by the appropriate authorities is required for the usage of E-mail by Sesa Group employees.

3.2 E-mail Usage

3.2.1 Authorized Use

- Unauthorized use of E-mail shall include, but is not limited to:
    - Transmitting or storing offensive material like political opinion, pornography and sexual harassment material
    - Soliciting for political, personal, religious or charitable causes or other commercial ventures outside the scope of the user's employment and the user's responsibilities to Sesa Group
    - "Spamming" unsolicited messages, promotions, sending or forwarding chain letters
    - 'Letter bombing' or `Chain letters' (re-sending the same E-mail repeatedly to one or more recipients for personal gain)
    - Creating, sending, receiving or storing materials that infringe the copyright or other intellectual property right of any third parties
    - Sending, transmitting or distributing proprietary information, data or other confidential Sesa Group information to unauthorized recipients

- The company provided e-mail access is intended to be for business use only. All e-mail messages shall be considered as company records and there must be no expectation of personal privacy.

3.2.2 Access to External (Public) E-mail Systems

- Access for all Internet E-mail Systems like Hotmail, Rediffmail, Yahoo Mail, Gmail etc. shall be prohibited for Sesa Group business use until and unless explicit approval is taken from HOD and CISO/CDIO/ Head-IT.

3.2.3 Access to Sesa Group's E-mail System

- Sesa Group shall reserve the right to inspect and review any data maintained in its E-mail system without prior consent of, or notification to, the employee.
- Sesa Group may disclose contents of E-mail either internally or to external parties, where necessary, for a legitimate business reason, without any permission of the employee.
- Sesa Group shall reserve the right to log use of e-mail systems and capture an adequate amount of information to assist with investigations and to detect misuse of e-mail.
- Mail Administrators shall not be permitted to access, copy, forward another individual's e-mail without approvals from CISO / Head-IT.

3.2.4 Transmission of Sensitive Information

- Users shall be prohibited from sending restricted information or data via E-mail, unless strong encryption (wherever possible) or secure methods are used.
- In absence of encryption, proper compensating controls (like password protection) shall be ensured by the end users prior to sending restricted information over public network.

3.2.5 Mailbox and E-mail Size Limitations (on Prim)

- Size of external (incoming/outgoing) E-mail attachments shall be restricted to 20 MB for internal and 8 MB for external network.
- E-mails for last 30 days of all users shall be retained on the server.
- Mailbox size for general users shall be 50 MB and for users with requirement of a larger mailbox size shall need to go through an authorization process, and shall require the approval of the HOD and CDIO/ Head-IT / CISO.
- Users shall be trained / reminded to periodically archive their mails on the local systems and the manner in which the personal folders need to be protected.
- E-mails sent outside Sesa Group must carry an automatic standard footer approved by authorized personnel.

3.2.6 O365 email solution process

- O365 email access has been given to all user as per management approval.
- Users who's having O365 Mailbox they get by default 100 GB storage space on for mailbox.
- SSO is configured for All O365 users to access O365 applications.
- Also, every mailbox having archival policy and Litigation policy enabled as per company standard
- Archival Policy 3 Years
- Litigation Hold Duration 3285 (9 years)
- Exchange Online Protection (EOP) - All O365 users can access their data from any device with conditional access. (No print, no download but user can save data on authorize app i.e. OneDrive for Business (OneDrive), SharePoint Online etc.)
- User can now schedule and join Video conference using Microsoft Teams also they can record meeting session and post meeting they can download Vides from Office 365 Videos / Stream
- Self-Service Password Change enabled for cloud users

- Azure information protection (AIP) - All O365 users are classified with Standard data classification labels
- Conditional Access enabled for all cloud users: Define policies that provide contextual controls at the user, location, device, and app levels to allow, block, or challenge user access.
- Conditional Access based on device state (Allow access from managed devices): Define policies that provide contextual controls at the user, location, device, and app levels to allow, block, or challenge user access.
- Azure Active Directory Join – Windows 10 only features - MDM auto-enrollment, Additional local administrators to Windows 10 devices via Azure AD Join, Enterprise State Roaming

4. Enforcement

All Sesa Group employees, third party employees and vendor employees shall follow the policy; violation of this can lead to termination of contract or financial penalties.

5. References and Related Policies

- None

6. Control Clauses Covered

A.8.1.3, A.11.2.6, A.13.2.1, A13.2.3, A.18.1.1, A.18.1.4