vedanta | sesa goa iron ore

Information Security Management System (ISMS)

Policy Document Information – Change Management Policy

Documented information Name: Policy Document Information – Change Management Policy

Version No: 3.0

Last Updated: 03rd October, 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

Documented information Management Information

Documented information Title: Policy Documented information – Change Management Policy

Abstract: This Documented information is a procedure Documented information highlighting the policy for Change Management.

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 – Change Management
Documented information Code	SESAIT/ISO27001/ISMS_Policy_Change Management
Date of Release	16.01.2012
Documented information Revision	3.0
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 (CDIO)	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	28-03-2013	Sesa Goa Logo Change		28-03-2013
1.2	18-10-2013	Sesa Group Logo, file name changes for Sesa Sterlite Ltd – IOB Emergency Change regularization days limit, id unlock and password reset form	Section 3.3,3.4	18-10-2013
1.3	21-01-2014	Sesa Sterlite Logo incorporated		22-01-2014
1.4	01-12-2014	Aligned to ISO 27001:2013. Vedanta group policy	1.1, 3.1, 3.2, 5, 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	21-Aug-2018	Policy review		28-Aug-2018
1.9	22-Aug-2019	Policy review		30-Aug-2019

1.10	08-Sep-2020	Policy review		15-Sep-2020
1.11	28-Sep-2021	Policy reviews and Update	1.1	04-Oct-2021
2.0	18 Mar 2022	Policy reviews and Update		04-April-2022
2.1	23 Sept 2022	Policy review 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 Singh	dileep.singh@vedanta.co.in

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, Odisha and Liberia, Pig Iron Division, Met Coke Division, Power Division in Goa, Sesa Coke, FACOR – Odisha, MALCO Energy and Nickel Business, VGCB, Visakhapatnam and Sesa Cement referred as Sesa Group in this document.

The change management policy applies to all changes in the following areas:

- Changes to operating systems & database, which shall include application of patches and service packs, configuration changes, and version upgrades.
- Changes to applications which shall include application of patches, configuration changes, and version upgrades.
- Changes to networks and network devices like routers, switches, firewall, etc. This shall include changes to router and switch configurations, firewall policy changes, network layout / traffic changes and changes to intrusion detection systems.
- Changes to IT hardware such as any changes pertaining to servers, HDD, RAM, backup devices, SAN, NAS, etc.
- Changes in source code
- Additions of new location / new application / new hardware to the existing setup
- Changes in the access authorization

Exception: This policy shall not be applicable to applications or information systems or network devices which are not developed, maintained or managed within Sesa Group

1.2 Purpose of the documented information

The purpose of change management policy is to ensure that any changes, addition and removal of information processing facilities are controlled.

1.3 Audience

This policy is applicable to 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

Any changes and emergency changes to the systems, applications, and infrastructure of Sesa Group should be authorized, tested and documented

3. Policy Details

3.1 Change Management Process

- The change management process shall involve documenting and managing the change requests through Service Desk/FMS.

- The documentation description shall provide a brief description of the changes requested, the date on which the request was made, prioritizing of the request, tracking and controlling modifications
- All changes shall be scheduled and all the affected parties shall be informed in advance of the change
- Approval has to be obtained for each change request
- All changes have to be reviewed after the roll out
- Modifications to Vendor supplied products shall be discouraged. In case changes are warranted, vendors shall be contacted to obtain system patches or releases. The original software shall be retained and changes shall be clearly documented

3.2 Testing of Changes and Backup

- All changes shall be tested before being carried out in the live / production environment, wherever required.
- Testing Environment shall be separated from production environment to reduce the risk of unauthorized access and changes to production systems
- A quality assurance test of the changes to be implemented shall be performed in a test environment prior to implementation in the production environment, wherever required.
- A backup of the system impacted by the change shall be made prior to its being updated.
- For critical systems, Rollback and Recovery procedures, in case of unsuccessful changes shall be followed

3.3 Unscheduled/Emergency Changes

- Unscheduled / emergency changes shall be carried out only in case there are critical production issues, which require the change to be carried out
- Any unscheduled changes shall not be done without proper approval
- An audit trail of the emergency activity shall also be generated which logs all activity, including but not limited to:
  - The user-ID making the change
  - Time and date
  - The commands executed
  - The program and data files affected
- An audit trail of the emergency activity shall also be generated which logs all activity, including but not limited

3.4 User ID and Access Changes

- Any changes to user ID including changes to the authorization levels shall be done by following the procedure defined in Identity and Access Management policy.
- Active Directory ID unlocks and password request form to be used in case user require unlock / password reset.
- All changes shall be documented and a trail shall be maintained by means of preserving the change requests

3.5 Hardware Changes

- Any changes to hardware shall be done by following the change management process which includes the raising of change request, approval by the appropriate authorities and documentation of the same

- The custodian of the hardware shall conduct all the hardware changes after due approval of the change
- Changes done to the hardware shall be updated in the hardware / asset register after the change is done
- Changes done to the hardware shall be monitored after the change to ensure that there is no untoward impact due to the change

3.6 Operating System and Application Changes

- Any change to the operating system or application shall be strictly controlled by the use of the change management process, which shall include the raising of change request, testing, approval by the appropriate authorities and documentation of the same.
- Changes to the operating system or the application shall be done by following the steps mentioned in the documented operating procedures, wherever applicable.
- All changes shall be documented and a trail shall be maintained by means of preserving the change requests.
- Any change that involves downtime or disruption of services shall be done after giving an appropriate notification to the affected users by email

3.7 Patch and Service Management

- Application of patches shall be done in a controlled manner
- A patch or service pack shall be applied only when it is a critical patch or there is a requirement for the same
- Only tested and alpha versions of the patch or service pack shall be considered for applying, wherever needed
- The patch or service pack shall be obtained directly from the vendor or downloaded from the vendor site only.
- A test bed shall be prepared to simulate the actual production environment and the patch or service pack shall be installed in the testing environment. The environment shall be monitored for performance and other issues, wherever required.
- On successful testing by the team and the functional users, the patch shall be applied on the production systems or desktops

3.8 Addition of Hardware/Software and any other IT Resource

All hardware or any other resource addition or removal of it from the production environment shall be controlled and approved and a complete track of it shall be maintained to ensure non-disruption to the operating environment.

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

- Identity and Access Management
- Change Management Procedure

6. Control Clauses Covered

- A12.1.2, A12.1.4, A12.5.1, A14.2.2, A14.2.3, A14.2.4, A14.2.8, A15.2.2