Information Security Management System

(ISMS)

Policy Document Information –

Information System Acquisition, Development & Maintenance Policy

Documented information Name: Policy Document Information – Information System Acquisition, Development & Maintenance

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: Policy Documented information – Information System Acquisition, Development & Maintenance

vedanta | sesa goa iron ore

Abstract: This Documented information is a procedure Documented information highlighting the policy for Information System Acquisition, Development & Maintenance of information assets.

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 – Information System Acquisition, Development & Maintenance
Documented information Code	SESAIT/ISO27001/ISMS_Policy_ Information System Acquisition, Development & Maintenance
Date of Release	05-12-2014
Documented information Revision	Rev. No. 3.0
Documented information Owner	IT Department
Documented information Author(s)	Arjun N Rao – Wipro Consulting
Documented information Change Reviewer	Sandhya Khamesra, Pricoris LLP
Checked By	Dileep Singh – CISO
Security Classification	Internal Use
Documented information Status	Final

Documented information Approver List

S. No	Approver	Approver Contact	Signature	Date Approved
1	Shobha Raikar (CITO - IOB)	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	09-01-2015	Reviewed and updated as per Internal audit	3.9	15-01-2015
1.2	10-Feb-2016	Company name logo update		18-Feb-2016
1.3	22-Aug-2016	Information security for Project	3.30	29-Aug-2016

Sensitivity: Internal (C3)

		Management as per Group IS Policy		
1.4	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.5	21-Aug-2018	Policy review		28-Aug-2018
1.6	22-Aug-2019	Policy review		30-Aug-2019
1.7	08-Sep-2020	Policy review		15-Sep-2020
1.8	28-Sep-2021	Policy review and update	1.1	04-Oct-2021
2.0	18-Mar-2022	Policy review and update	4	05-April-2022
2.1	16-Jul-2022	PIMS Update		25-Aug-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

Sensitivity: Internal (C3)

vedanta | sesa goa iron ore

Table of Contents

Sensitivity: Internal (C3)

Sensitivity: Internal (C3)

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 policy addresses the protection requirements associated with the following activities.

- Software development by in-house team of Sesa Group
- Procurement of information systems from third party vendor
- System integration performed by Sesa Group or performed by third parties under contract to Sesa Group

1.2 Purpose of the documented information

The purpose of this policy is to ensure that security is built into information systems; prevent loss, modification or misuse of user data in application systems and to maintain the security of applications, system software and information.

1.3 Audience

This policy is applicable to 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

This policy provides the directions to ensure that the information systems security requirements are identified before procuring a new information system or enhancing an existing information system and maintaining the security ensuring confidentiality, integrity and availability of the information system.

3. Policy Details

3.1 Information security requirements analysis and specification

- It shall be ensured Information security and compliance requirements are addressed early at the start of any business project.
- Identification and management of information security requirement and associated process shall be mandatorily integrated in every business project.
- Wherever development projects are involved, it must be ensured that security requirements are addressed in the designing phase only.
- While identifying information security requirement, the following points shall be considered:

Sensitivity: Internal (C3)

- User authentication requirements ○ Access provisioning and authorization process for all users. ○ Awareness of user roles and responsibilities
- Requirements of achieving and maintaining confidentiality, availability and integrity of assets.
- Requirement derived from business processes, such as transaction logging and monitoring, non-repudiation requirements
- Requirements mandated by other security controls eg; interfaces to logging and monitoring or data leakage detection systems.

3.2 Securing application services on public network

- Applications which are passing over public networks shall be secured in order to prevent any loss of business information.
- Security controls shall be implemented to ensure the protection of data, including PII flowing through public networks.
- It shall be ensured that:
  - Authentication mechanism is established
  - Authorization responsibility of signing and approving key documented information is defined.
  - Key Documented information is protected with approved and appropriate methods like password protection etc.
  - When application is passing over a public network, both communication partners shall be fully informed of their authorization for provision or use of service.
- Secure method of payment shall be enforced to guard against any fraud.
- Sesa Group shall clearly define the liability of fraudulent transactions, if any.

3.3 Protecting application services transactions

- It shall be ensured that electronic signatures, of both parties, are included in transactions.
- It shall be ensured that authentication shall be performed before performing any transactions.
- All transactions from applications passing over public networks shall be encrypted.
- Secure network protocols like IPSec, SSL etc. shall be used.
- Transaction details shall be stored in a separate storage server segregated from the local network and not accessible from the internet directly.
- CISO shall ensure that digital certificates, for applications, shall be issued by some recognized issuing authority.
- Sesa Group shall not use self-signed certificates.
- Certificates shall be renewed with-in time, before expiration.
- CISO along with the legal Department shall ensure that Sesa Group is compliant to all applicable legal and regulatory requirements pertaining to generation, processing, completion and storage of transaction.

3.4 Secure development policy

- Sesa Group shall establish guidelines to be followed for all software, application and system developments within the organization.
- During the design stage of software, along with the functional requirements specification (FRS) a security requirements specification must be developed.
- Process owners and developers shall adhere to the guidelines while performing development of software and systems.
- Secure coding practices shall be followed.
- Wherever mandated, secure coding standards shall be used.

Sensitivity: Internal (C3)

- Wherever required, developers shall be trained on the use of secure coding practices and testing. Sesa Group shall perform secure code review to ensure that secure code practices are being followed.
- Vendor/third-party shall follow the security guidelines established by Sesa Group
- It should be ensured that Sesa Group has the right to audit/verify the code developed by vendor/third party.

3.5 System Change control procedure

- All changes shall follow a change control procedure.
- Any change shall be carried out in accordance with change control policy of Sesa Group ● Change control procedure shall be followed through all stages of development life cycle.
- Changes to systems, applications etc. during any stage of development life cycle shall include a risk assessment, impact analysis and specification of security controls needed.

3.6 Technical review of applications after operating platform changes

- Whenever operating platform changes, every application shall undergo a technical review process.
- This process shall include:
    - Review of application control and integrity procedures to ensure that they have not been compromised by operating system changes. ○ Ensuring that notification of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation
    - Changes to business continuity plans as per changes to operating platform.

3.7 Restrictions on changes to software packages

- Wherever possible, changes to software packages shall be discouraged.
- As far as possible, vendor supplied software packages should be used without modification.
- Wherever possible, required updates shall be obtained from the vendor as standard program updates. ○ Where modification is required to be performed, the following points shall be taken into consideration:
    - Consent of the vendor is obtained.
    - Built-in controls and security processes are not compromised. ○ Compatibility with other software in use. ○ Impact if the organization becomes responsible for the future maintenance of the software as a result of changes
- Any change to software packages shall be carried out with reference to Change Management policy.

3.8 Secure system engineering principle

- Sesa Group shall establish and implement principles for engineering secure systems.
- Principles shall ensure security designed to all architectural layers including business, data, application and technology. Corresponding procedures shall be established as applicable
- Wherever applicable, procedures shall also be applied to outsourced information systems through contracts and other binding agreements between the organization and supplier.

3.9 Secure development environment

- Only authorized persons shall have access to development area ● Development systems shall comply with security policies of Sesa Group. ● Development area shall remain separated from the test and production environment ● Test area shall remain separated from production environment.

Sensitivity: Internal (C3)

- It must be ensured that development systems are provided with controlled access to authorized persons only.
- Backup shall be taken and kept off-site. Backup & restoration policy shall be referred for enforcing backup & restoration controls.
- Background verification shall be performed for SESA employees involved in system, software and application development activities.
- Security awareness training shall be conducted as per the training and awareness program of Sesa Group
- Wherever required, other specialized trainings shall be provided to ensure secure system development.
- Outsourced/ third party/ supplier movement shall be controlled in the development area.

3.10 Outsourced development

- Appropriate security measures shall be put in place wherever system, software and application development is outsourced.
- SLA/Contracts shall be obtained from all outsourced vendors.
- SLA/Contracts shall cover all the licensing, copyright and trademark requirements of Sesa Group ● SLA/Contracts shall ensure secure coding technique implementation by vendor.
- SLA/Contracts with outsourced development vendor shall cover the requirements of provisioning of evidence to ensure that security thresholds were established to implement security and privacy requirements of Sesa Group
- SLA/Contracts with outsourced development vendor shall cover the requirements of provisioning of evidence to ensure that sufficient testing has been done to prevent any intentional or unintentional malicious content in the software or application.
- Wherever required, escrow agreement shall be obtained from the outsourced development vendor.

3.11 System security testing

- Security review and testing shall be performed for all in-house and outsourced system development.
- Testing shall be established as a part of development process.
- Testing schedule shall be developed along with testing process, test inputs and expected output results.
- For in-house development, testing shall be initially conducted by development team.
- An independent acceptance testing shall be carried out for all systems, in-house or outsourced.

3.12 Acceptance Testing

- The use of operational data for testing shall not be allowed.
- If a deviation is sought to the restriction, the data shall be sanitized before it is copied to the test environment.
- Measures shall be implemented to ensure that the sanitized operational data cannot be distributed outside the test environment or returned to production.
- Use of operational information must comply with any legislation related to privacy of personal information.

3.13 Protection of test data

- Appropriate test data shall be used for testing purposes.
- Personal information or personal identifiable information shall not be used for any testing purposes.

Sensitivity: Internal (C3)

3.14 Acceptance Criteria

- Acceptance criteria for software and integrated systems shall be established to address security requirements and ensure that proper tests are performed.
- The Asset Owner shall formally accept systems and changes to existing systems prior to deployment of the system or change.

3.15 System/Application Risk Assessment

- A risk assessment shall be performed for systems/applications before development/acquisition.
- Risk assessments shall be performed for integrated systems at least every one year or whenever the scope of the system is expanded to include new information assets.
- When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security

3.16 System Specifications

- All systems developed by Sesa Group shall have a written specification that addresses all security requirements.
- System specifications shall be documented addressing security requirements.
- Design reviews shall address the security requirements of the system/application

3.17 Vendor Security Requirements

- When commercial information systems are purchased from a vendor or manufacturer as part of a development or integration effort, all Sesa Group security requirements shall be identified prior to the selection process and shall be documented in the purchase agreement and provided upon delivery of the product.
- Evaluation of a third-party product shall include verification that the security attributes of the product satisfy the stated security requirements associated with the component.

3.18 Third Party Software Source Code

- Commercial software used in development or integration efforts shall only be obtained from reputable sources.
- Bespoke systems (made-to-order) and applications shall require the delivery of source code to Sesa Group.
- Requirements for the escrow of vendor source code shall be addressed before purchasing commercial software where required

3.19 Data Integrity

- Whenever Sesa Group develops new applications or modify existing applications, development team shall be instructed to incorporate controls to ensure data integrity such as Input/output validation, Message authentication and Control of internal processes.
- Access to source code would be made available only to authorized personnel

3.20 Separation of Development, Test and Production environments

- Development environment shall be separated from Test and Production environments
- Test environments shall be kept separate from production environments.

Sensitivity: Internal (C3)

- The separations could be preferably by using physically separate computer systems or by employing adequate logical separation with proper access controls.

3.21 System Change Control

- System change control procedures and documented information shall comply with the requirements of Sesa Group's Change Management Policy.

3.22 System Deployment

- Assigned system and/or security administrators shall perform all new system deployments following initial system/application acceptance.
- Deployment document and procedures shall comply with the requirements of Sesa Group's Change Management Policy

3.23 Pre-deployment Planning

- The Asset Owner shall develop a plan for the deployment of the system or release.
- The plan shall identify resource requirements; suggest a sequence of events and estimate timing, and documented information responsibilities.
- Any training necessary prior to software implementation shall be addressed by the plan as well as a roll-back scenario.

3.24 System Maintenance

- To maintain the integrity and availability of IT services, system maintenance and backup procedures shall be developed.
- Such procedures shall specify appropriate periodic maintenance activities associated with each system depending on classification.
- Patches and releases shall be tested based on security requirements prior to deployment.
- All patches and releases shall be applied using proper change control procedures.

3.25 Developer Restrictions

- Systems developers shall be prohibited from the following tasks, unless the development team is so small that the required separation is impossible to achieve: ○ Performing acceptance testing of software they developed. ○ Performing the duties of a software librarian. ○ Migration of systems and/or modification to existing systems from staging environments to production.

3.26 System Access Control

- Access controls shall be employed in production and test environments to implement the general principle that only authorized personnel shall be allowed access to any information asset based on legitimate, documented business need and with the prior approval of the Asset Owner.
- Procedures for the use of access controls shall comply with the requirements of Sesa Group's Access Control Policy.

3.27 Training

- Complete training and training manuals shall be provided to the designated administrators by the developers to insure proper operation and maintenance of the systems.

Sensitivity: Internal (C3)

3.28 Procedural Requirements

- Standard Operating Procedures (SOP) and guidelines defining detailed security processes, component configurations, and reporting shall be implemented in all business units.

3.29 Control of technical vulnerabilities

- For effective technical vulnerability management, the business units/departments will prepare a complete inventory of technology assets, along with the list of software vendors and software version number.
- The CISO shall ensure that an annual technical risk assessment is undertaken for all critical information systems.
- A detailed report of identified vulnerabilities and the action taken.
- A periodic patch management activity shall be undertaken
- The patch management activity will be undertaken according to the Patch Management Policy.

3.30 Information security in Project Management

IT department shall ensure an effective coordination of information security in project executed. The purpose of these activities is to ensure that:

a) information security policy is compiled to;
b) all non-compliances to information security policy are addressed.
c) significant changes in threats and exposure to information and information processing facilities are identified and mitigated.
d) Information security incidents are identified, reported and addressed appropriately; and
e) Any application/systems going to be installed in company shall go through the approval of Head-IT.

4. Reference

This Policy should be read in conjunction with other security policies of Sesa Group including the following policies.

- Information Security Policy.
- Application Security Policy
- Secure System Engineering Principles • Patch Management Policy.
- Asset Management Policy.
- Network Security Policy.
- Access control policy.
- Server Security Policy.
- Change Management Policy.

Commented [1]: Added references

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, as per the rules of organization. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Sesa Group.

6. ISO 27001:2013 Controls

- A 14.1.1 – Information security requirements analysis and specification.

Sensitivity: Internal (C3)

- A.14.1.2– Securing application services on public network. ● A.14.1.3– Protecting application services transactions ● A.14.2.1– Secure development policy.
- A.14.2.2– System change control procedures
- A.14.2.3– Technical review of application after operating system changes ● A.14.2.4– Restrictions on changes to software packages ● A.14.2.5– Secure system engineering principles.
- A.14.2.6 –Secure development environment.
- A 14.2.7 – Outsourced development.
- A.14.2.8 – System security testing.
- A.14.2.9 – System acceptance testing.
- A.14.3.1– Protection of system test data.
- A 12.6.1 – Control of technical vulnerabilities.

7. Abbreviation

- CISO- Chief Information security officer

Commented [2]: Removed PDA From abbreviations

Sensitivity: Internal (C3)