Information Security Management System

(ISMS)

Policy Document Information –

Secure System Engineering Principles

Documented information Name: Policy Document Information – Secure System Engineering Principles

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 – Secure System Engineering Principles

Abstract: This Documented information is a procedure Documented information highlighting the policy for Secure System Engineering Principles.

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	Secure System Engineering Principles
Documented information Code	SESAIT/ISO27001/ISMS_Policy_ Information System Acquisition, Development & Maintenance
Date of Release	05-12-2014
Documented information Revision	3.0
Documented information Owner	IT Department
Documented information Author(s)	Arjun N Rao
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 (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	10-Feb-2016	Company name logo update		18-Feb-2016
1.2	13-Feb-2017	Policy Review		18-Feb-2017
1.3	23-May-2017	VGCB inclusion in scope	1	30-May-2017
1.4	21-Aug-2018	Policy review		28-Aug-2018
1.5	22-Aug-2019	Policy review		30-Aug-2019
1.6	08-Sep-2020	Policy review		15-Sep-2020
1.7	28-Sep-2021	Policy review and Update	1.1	21-Oct-2021
2.0	18 Mar-2022	Policy review and Update	4	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 K 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 policy is applicable to all IT systems, including general support systems and major applications within Sesa Group.

1.2 Purpose of the documented information

The purpose of this policy is to give a list of system-level security principles to be considered in the design, development, and operation of an information system.

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 a structured approach to the design, development, and implementation of IT security capabilities is being followed and help in maintaining information security ensuring confidentiality, integrity and availability of the information system.

3. Policy Details

The principles mentioned below should be considered in all phases of system life cycle i.e. initiation, development/ acquisition, implementation, operation and disposal of information system. The principles are those prescribed by NIST

3.1 Principles

Sl. No	Principle	Explanation
	Security Foundation	
1	Establish a sound security policy	A security policy is an important document to develop while designing an information system. The security policy emphasizes organization's basic commitment to information security formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution.
2	Treat security as an integral part of the overall system design	Security must be considered in information system design. This includes establishing security policies,

		understanding the security requirements at all phases, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system
3	Clearly delineate the physical and logical security boundaries	Security boundaries must be considered and communicated in relevant system documentation and security policies
4	Ensure that developers are trained in how to develop secure software	Developers need to be trained in the development of secure software before developing the system. This includes application of engineering disciplines to design, development, configuration control, and integration and testing
	Risk Based	
1	Reduce risk to an acceptable level	Risk mitigation should be the foremost objective of the organization when a risk is identified. However, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. The goal is to enhance mission/business capabilities by mitigating mission/business risk to an acceptable level.
2	Assume that external systems are insecure	An external domain is one that is not under your control. In general, external systems should be considered insecure until an external domain has been deemed “trusted”. The design of the system security features should be done accordingly

3	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness	To meet stated security requirements, a systems designer, architect, or security practitioner will need to identify and address all competing operational needs. It may be necessary to modify or adjust (i.e., trade-off) security goals due to other operational requirements. By identifying and addressing these trade-offs as early as possible, decision makers will have greater latitude and be able to achieve more effective systems
4	Implement tailored system security measures to meet organizational security goals.	IT security measures are tailored according to an organization’s unique needs. Recognizing the uniqueness of each system allows a layered security strategy to be used
5	Protect information while being processed, in transit, and in storage	System engineers, architects, and IT specialists should implement security measures to preserve, as needed, the integrity, confidentiality, and availability of data, including application software, while the information is being processed, in transit, and in storage.
6	Consider custom products to achieve adequate security	Designers should recognize that in some instances it will not be possible to meet security goals with off the shelf products. In such instances, it will be necessary to design a custom product
7	Protect against all likely classes of threats and vulnerabilities	In designing the security controls, multiple classes of “attacks” need to be considered. Those classes that result in unacceptable risk need to be mitigated
	Ease of Use	

1	Use common language in developing security requirements	The use of a common language when developing security requirements permits organizations to evaluate and compare security products and features evaluated in a common test environment. It will lead to easier comprehension as well
2	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process	As mission and business processes and the threat environment change, security requirements and technical protection methods must be updated. ITrelated risks to the mission/business vary over time and undergo periodic assessment. Periodic assessment should be performed to enable system designers and managers to make informed risk management decisions on whether to accept or mitigate identified risks with changes or updates to the security capability.
3	Strive for operational ease of use	Security controls should be designed to be consistent with the concept of operations and with ease-of-use as an important consideration. The experience and expertise of administrators and users should be appropriate and proportional to the operation of the security control. An organization must invest the resources necessary to ensure system administrators and users are properly trained
	Increase Resilience	
1	Implement layered security	Security designs should consider a layered approach to address or protect against a specific threat or to reduce vulnerability.

2	Design and operate an IT system to limit damage and to be resilient in response	Information systems should be resistant to attack, should limit damage, and should recover rapidly when attacks do occur. The principle suggested here recognizes the need for adequate protection technologies at all levels to ensure that any potential cyber-attack will be countered effectively. In addition to achieving a secure initial state, secure systems should have a well-defined status after failure, either to a secure failure state or via a recovery procedure to a known secure state.
3	Provide assurance that the system is, and continues to be, resilient in the face of expected threats	Assurance is the grounds for confidence that a system meets its security expectations. These expectations can typically be summarized as providing sufficient resistance to both direct penetration and attempts to circumvent security controls. Good understanding of the threat environment, evaluation of requirement sets, hardware and software engineering disciplines, and product and system evaluations are primary measures used to achieve assurance
4	Limit or contain vulnerabilities	Design systems to limit or contain vulnerabilities. If vulnerability does exist, damage can be limited or contained, allowing other information system elements to function properly. Limiting and containing insecurities also helps to focus response and reconstitution efforts to information system areas most in need
5	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).	In cases where the sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data is stored and isolate them, either physically or logically

6	Use boundary mechanisms to separate computing systems and network infrastructures	To control the flow of information and access across network boundaries in computing and communications infrastructures, and to enforce the proper separation of user groups, a suite of access control devices and accompanying access control policies should be used
7	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations	Organizations should monitor, record, and periodically review audit logs to identify unauthorized use and to ensure system resources are functioning properly.
8	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability	Continuity of operations plans or disaster recovery procedures address continuance of an organization's operation in the event of a disaster or prolonged service interruption that affects the organization's mission.
	Reduce Vulnerabilities	
1	Strive for simplicity	The more complex the mechanism, the more likely it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance.
2	Minimize the system elements to be trusted	Hardware, firmware, and software should be designed and implemented so that a minimum number of system elements need to be trusted in order to maintain protection. Further, to ensure cost-effective and timely certification of system security features, it is important to minimize the amount of software and hardware expected to provide the most secure functions for the system
3	Implement least privilege	The concept of limiting access, or "least privilege," is simply to provide no more authorizations than
		necessary to perform required functions. Its goal is to reduce risk by limiting the number of people with access to critical system security controls.

4	Do not implement unnecessary security mechanisms	Every security mechanism should support a security service or set of services, and every security service should support one or more security goals. Extra measures should not be implemented if they do not support a recognized service or security goal. Such mechanisms could add unneeded complexity to the system and are potential sources of additional vulnerabilities
5	Ensure proper security in the shutdown or disposal of a system	Although a system may be powered down, critical information still resides on the system and could be retrieved by an unauthorized user or organization. Access to critical information systems must be controlled at all times
6	Identify and prevent common errors and vulnerabilities	Many errors reoccur with disturbing regularity - errors such as buffer overflows, race conditions, format string errors, failing to check input for validity, and programs being given excessive privileges. Learning from the past will improve future results
	Design with Network in Mind	
1	Implement security through a combination of measures distributed physically and logically	It is important to associate all elements with the security service they provide. These components are likely to be shared across systems to achieve security as infrastructure resources come under more senior budget and operational control
2	Authenticate users and processes to ensure appropriate access control decisions both within and across domains	It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with crossdomain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required

3	Use unique identities to ensure accountability	Unique identities are a required element in order to be able to: ● Maintain accountability and traceability of a user or process ● Assign specific rights to an individual user or process ● Provide for non-repudiation ● Enforce access control decisions ● Establish the identity of a peer in a secure communications path ● Prevent unauthorized users from masquerading as an authorized user

4. Reference

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

- Information Security Policy.
- System Acquisition Development and Maintenance policy ● Patch Management Policy.
- Asset Management Policy.
- Network Security Policy.
- Access control policy.
- Server Security Policy.
- Change Management Policy.
- Application Security Policy
- Remote access policy
- Audit management
- Risk assessment methodology

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.14.2.5

7. Abbreviation

None