Business Continuity Management System

(BCMS)

Business Continuity Policy

Documented information Name: Business Continuity Policy

Version No: 2.0

Last Updated: 25th July 2023

Documented information Owner: Sesa Group

Approval Authority: Sesa Group

This Documented information is a confidential documented information of Sesa Group

Documented information Management Information

Documented information Title: Business Continuity Policy

Abstract: This Documented information is a policy documented information of the Business Continuity

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	Business Continuity Policy
Documented information Code	SESAIT/ISO22301/ Business Continuity Policy
Date of Release	25 Aug 2022
Documented information Revision	1.0
Documented information Owner	IT Department
Documented information Author(s)	Pricoris LLP
Documented information Change Reviewer	Jyoti Singh
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 - IOB)	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
1.0	20-Jun-2022	Initial Release		25-Aug 2022
1.1	31-Aug 2022	Inclusion of Risk Appetite for Business continuity and IT aspects of business continuity as suggested in Stage 1 Audit	Section 5	3-Sept 2022
2.0	25-Jul 2023	Change in the BCMS Organization Structure Chart		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

1. Introduction

The aim of business continuity management system is to prevent, identify and eliminate the risks of business interruption, as well as to create conditions for business recovery if such interruption occurs.

Business continuity system is one of the most important components of the organization, which makes it possible to avoid and prevent the risks of business interruptions, maintain and enhance Sesa Group's image among its consumers, Business Partners, and public regulators ("Interested Parties"), strengthen confidence in Sesa Group and improve loyalty.

The purpose of the Business Continuity Policy is to provide an effective documented framework and a process to manage critical IT services and activities & their dependencies in case of an emergency or crisis.

2. Scope

This policy applies to all Information processing systems or information assets owned/operated by Sesa Group or owned/operated by a third-party service provider on behalf of Sesa Group.

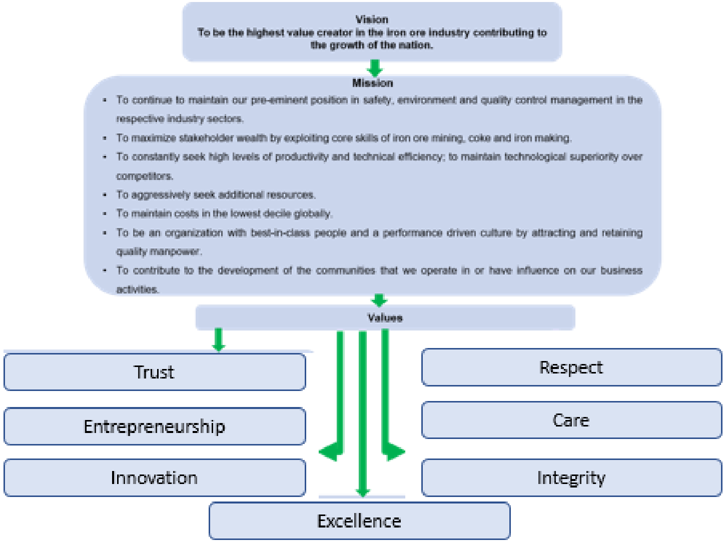
This policy applies to all the employees, contracted staff, business partners & anyone associated with Sesa Group IT Infrastructure and applications.

*Note: 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 - Vazare and Gujarat, FACOR – Odisha, Nickel Business, VGCB, Visakhapatnam referred as Sesa Group in this document.

Purpose of the documented information

The purpose of the Business Continuity Policy is to provide an effective documented framework and a process to manage critical IT services and activities & their dependencies in case of an emergency or crisis.

3. Mission, Vision and Values



Vision
To be the highest value creator in the iron ore industry contributing to the growth of the nation.

Mission

- To continue to maintain our pre-eminent position in safety, environment and quality control management in the respective industry sectors.
- To maximize stakeholder wealth by exploiting core skills of iron ore mining, coke and iron making.
- To constantly seek high levels of productivity and technical efficiency; to maintain technological superiority over competitors.
- To aggressively seek additional resources.
- To maintain costs in the lowest decile globally.
- To be an organization with best-in-class people and a performance driven culture by attracting and retaining quality manpower.
- To contribute to the development of the communities that we operate in or have influence on our business activities.

Values

Trust
Respect
Entrepreneurship
Care
Innovation
Integrity
Excellence

Aligned to the organizational mission, vision and values IT has defined the following objective "Transform Iron and steel sector into technology and data driven organization enabling improved recovery from a production optimization, enhance safety & maximized productivity.

4. Risk Appetite:

Risks to the values defined for Vedanta are considered in defining the Acceptable Risk.
At Sesa Goa Risk Appetite is defined based on the following principles:

- Entrepreneurship and Innovation involve undertaking risks and the organization will accept risks which are low. Medium risks may be accepted based on factors such as exploiting the risk to create an opportunity, cost benefit analysis etc. All high risks will be treated.
- The organization has zero tolerance for risks to the following values:
- Trust, Integrity, Care, Sustainability and Excellence.
- Risk appetite for IT processes is as follows:
    - We accept risks to confidentiality, integrity, availability, privacy and continuity which have a value lower than 5 i.e., low risks (function of impact and probability)
    - We have low appetite for risks which are medium risks to confidentiality, integrity, availability, privacy and continuity which are greater than 5 and less than 15 for which treatment plan **may** be prepared and shall be monitored closely.
    - We have no appetite for risks which are high risks to confidentiality, integrity, availability, privacy and continuity which are greater than 15 for which treatment plan **must** be prepared and which shall be monitored closely.
    - For Business Continuity purposes the risk appetite determines the RTO wherein the impact becomes medium.
    - For Business Continuity purposes all IT applications which have an RTO within 8 hours are considered as critical and for which Sesa Goa does not have a risk appetite and hence risks, strategy and BCP for each such application covering the underlying infrastructure and network

This is reflected in following key areas and corresponding initiatives:

Key Areas	Initiatives
1 Cloud Transformation	1 Cloud Migration On-prem to Cloud Migration of DC- Phase 1 Set-up Cloud Platform for Digital Enterprise (IOTHUB/AI/ML) 2 Data Management & smart analytics
2 One Vedanta, One experience	1 One Vedanta O365 Platform adoption & establish Common Centralized Services and Solution e.g. - AV & EDR, Wifi, sharepoint 2 Unified Communication & collaboration Platform 3 Infra Augmentation 4 RPA deployment for Ariba, logistics etc.
3 Drive SAP Adoption	1 Drive SAP Util & Harmonising best practice (Limble / SAP) 2 Drive Ariba Utilization and Standardization 3 SAP Rollout – Liberia, Desai Cement, Nicoment, IOO 4 Rise with SAP for I&S 5 Sox Control Automation – 70% & GRC No High risk
4 Non- SAP Applications Rationalization	1 Rationalization & Consolidation of Non- SAP Applications & Mobile Apps
5 Managed IT Operations	1 Fully Operationalize Accenture TOS 2 Extend ITOS to Liberia
6 Cyber Security & Data Governance	1 Managed Security Operations IT & OT Env 2 Strengthen PTS Security posture 3 Integrated ISO Process Framework Implementation 4 Data Privacy Tool Implementation

5. Responsibilities

Following are the responsibilities of roles involved in the implementation of Business Continuity Management System policy and/or those responsible for overseeing the implementation of this process.

- Responsibility of the Top Management, represented by the IT Steering Committee (IT SC), is to ensure that the business continuity management system and business continuity objectives established are compatible with the strategic direction of the organization; BCMS requirements are integrated into the Sesa Group's business processes and adequately managed in all IT support services efficiently and continuously improved.

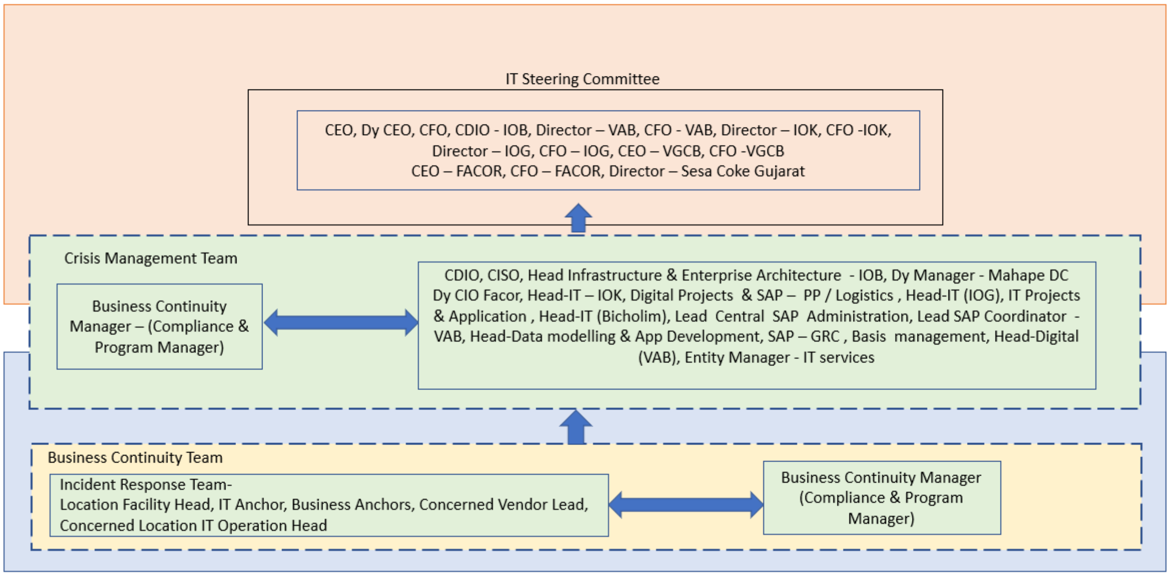
- All Employees: It is the responsibility of all employees and third-party employees to read, understand and abide by this policy and related procedures.
- Individual business stakeholders and/or business units shall mandate controls as described in this policy and ensure its enforcement.
- IT Steering Committee, BCP Team and Crisis Management Team are responsible for complying and monitoring of this policy based on inputs of individual businesses.

The CITO (BC Head) in conjunction with BC manager is responsible for ensuring that business continuity policies are maintained, implemented, operated and reflect the requirements of SESA GROUP. Specific guidance to this policy may be provided by individual business stakeholders and/or business units as appropriate.

6. BCMS Organization Structure

BCMS Organization structure will be govern by BCMS policy and executed based on IMS organization structure.

BCMS Governance Structure



IT Steering Committee

CEO, Dy CEO, CFO, CDIO - IOB, Director – VAB, CFO - VAB, Director – IOK, CFO -IOK, Director – IOG, CFO – IOG, CEO – VGCB, CFO -VGCB
CEO – FACOR, CFO – FACOR, Director – Sesa Coke Gujarat

Crisis Management Team

Business Continuity Manager – (Compliance & Program Manager)

CDIO, CISO, Head Infrastructure & Enterprise Architecture - IOB, Dy Manager - Mahape DC Dy CIO Facor, Head-IT – IOK, Digital Projects & SAP – PP / Logistics , Head-IT (IOG), IT Projects & Application , Head-IT (Bicholim), Lead Central SAP Administration, Lead SAP Coordinator - VAB, Head-Data modelling & App Development, SAP – GRC , Basis management, Head-Digital (VAB), Entity Manager - IT services

Business Continuity Team

Incident Response Team-
Location Facility Head, IT Anchor, Business Anchors, Concerned Vendor Lead, Concerned Location IT Operation Head

Business Continuity Manager (Compliance & Program Manager)

7. Policy Statement

BCMS Policy Statement

The company shall establish, implement, maintain and continually improve holistic and robust business continuity management system (BCMS), putting in place adequate and appropriate arrangements which shall enable it to effectively respond and recover from disruptive incidents when they arise. While planning the BCMS, the company shall take into account its internal and external issues along with the requirements of the interested parties including its outsourced partners and supply chain to determine risks and opportunities which could affect the critical activities supporting the provision of its products and services. The top management shall provide the required resources and sufficiently contribute towards the BCMS ensuring it achieves its intended outcome(s).

7.1 Business Continuity Management

To identify security controls for business continuity of Sesa Goa IT in the event of an incident or a disaster. This policy establishes the basic principles and framework necessary to ensure emergency response, resumption and permanent recovery of Sesa Goa businesses operations during and after a business interruption due to either man-made or natural disasters.

7.2 Business Impact Analysis

The business impact to be established considering unavailability of the identified IT-applications. The impact to be measured on the scale of low, medium and high.

Refer to Business Impact Analysis Methodology.

7.3 Business Continuity strategy and solution

The Business Continuity strategy and solution is limited to defining recovery and resumption procedures for threats resulting in unavailability of people, facility and technology required for ensuring continuity of IT services required by the business to continue its operations and service the customers.

7.4 Crisis Management Plan

This plan Incident crisis management structure, by defining responsibilities and response procedures to be followed, preventing an Incident from escalating into a crisis.

Refer Crisis Management Plan.

7.5 Exercising and testing

Periodically testing, exercising and maintaining the BCP to ensure that it can be implemented in emergency situations.

Refer Exercising and Testing Procedure.

7.6 Crisis communication

It is to define an effective communication procedure on what to communicate, when to communicate, for the exchange of information with interested parties to prevent the Crisis ASAP.

Refer Crisis Communication Plan.

8. BCMS Objectives and Approach

Taking input from Business Continuity requirements, the internal issues, external issues, interested parties' requirements, risk assessment, risk treatment and applicable requirements of business continuity objectives are determined at relevant functions and levels.

Business Continuity Management System Objectives are aligned to the organizational mission and vision under below given categories:

- Conduct Business impact analysis for all the IT applications in accordance with the requirements of ISO 22301:2019.
- Proactively Identify & Mitigate Risks which could lead to unavailability of the facilities hosting IT Infrastructure
- Identify & implement Business Continuity Options for processes supporting Information Technology (for example, in the absence of the Data Center(s))
- Define Recovery & Restoration Procedures for processes supporting Information Technology.
- Train the personnel identified for roles related to BCMS.
- Communicate the importance of effective business continuity and of conforming to the BCMS requirements.
- Test the arrangements to achieve Recovery Time Objective (RTO), Recovery Point Objective (RPO) and to assess the relevance and effectiveness of the BC plans and crisis management plans.
- Continuously monitor and improve the BCMS to ensure alignment with the overall objective.
- Ensure that the BCMS achieves its intended outcome(s).

Considering the organizations' vision and business continuity the objectives can be achieved by following below approach:

- Establish, implement, document and maintain a formal BCMS process based on "Plan-Do-Check-Act" model.
- Identify and prioritize critical IT-Applications which support business operations
- Performing risk assessment which includes identification, analysis and assessment of risk impact on Sesa Goa's business.
- Thorough analysis of impact of incident on business which includes the analysis and assessment of possible repercussion of incidents on Sesa Goa's business processes
- Strategic crisis management planning to ensure Sesa Goa's business continuity, which includes the pre-developed principles of crisis management in case of the following scenarios: lack of personnel availability, lack of premise availability, lack of technology availability, lack of data availability, and lack of vendors availability.
- Formulation of Business continuity plans which is documented procedure to be applied/invoked in the event of business interruption.
- Formulation of Recovery strategy containing the action and task list to be applied to recover and protect the IT applications and supporting infrastructure.

- Crisis management planning and documenting plan of actions to minimize impact of incidents on personnel and business processes.
- Formulation of pre-established Crisis communications planning containing documented priorities in communications and ways to alert of the incidents to the internal and external stakeholders.
- Protection of Human Resources and all assets during a disruptive incident.
- Consider legal, regulatory and statutory requirements in Business Continuity
- Periodically testing, exercising and maintaining the BCP to ensure that it can be implemented in emergency situations
- Embed BCM culture and promote BCM awareness in the organization by means of effective communication, education and training.
- Establish methods for monitoring, measurement, analysis and evaluation of the BCMS.

Key Outcomes of Policy Implementation

- Reduction of the risk of business interruption.
- Preservation of customer and supplier loyalty through demonstration of business sustainability verified by the business continuity system.

9. Assumptions

The following assumptions are made in the Business Continuity Policy:

- Key personnel and/or their backups identified in the plan are available
- Recovery location(s) and facilities, as required, are available that can handle the specified recovery activities
- Vital resources including backup media and other immediate requirements, identified in the strategy, required for BCP are available at the respective recovery location
- BCP shall not apply to non-recoverable situations such as global disaster
- BCP shall not be invoked for addressing day-today failures like link or system failure

10. Enforcement

Violation to Sesa Goa Policy, Procedures, standards are subject to disciplinary action, which could be jointly decided by CITO and HR Head/IT Steering Committee.

11. Exceptions to the Policy

By default, there are no exceptions to this policy. However, any exception on matters relating to BCMS shall be approved by the CITO and recorded.

Business Continuity objective Exclusions

- Business Continuity Planning for Business Processes & Support Processes (Head Office / Regional Offices / Units)
- Business Continuity Planning for Manufacturing and related processes (Plant / Supply Chain)

The exception request, validation and management shall be performed as prescribed in Sesa Goa BCMS Policy.

12. Policy Review

To incorporate the impact of changes in the organizational strategy, this policy would be reviewed annually as part of, or at least to coincide with, the business operational and strategic planning processes. A more frequent review of this policy may be triggered by any of the following factors:

- Any change in the scope of the business continuity management system
- Any change in the Objective of the business continuity management system
- Significant expansion / contraction of volumes, space or headcounts.
- Changes in process / service attaining the status of key process / service.
- An incident invoking the Business Continuity Plan and the associated recovery.

The IT Steering Committee shall review and update this policy annually or if major changes occur in the operations or systems or policy directives by the regulatory authorities.

The CITO is responsible for the independent review of the implementation of this policy annually or when significant changes to the business occur.

13. Regulatory Obligations

Sesa Group is required to comply with certain Regulatory requirements. The company also operates under the various provisions of acts or guidelines issued by Legal authorities from time to time. The applicable Legal requirements and Regulatory directives have been identified and assessed by the Company and complied with, from time to time. There is a separate document which provides procedure for identifying various applicable Legal, Regulatory and Contractual obligations from time to time to ensure their compliance.

13.1 Associated Legislations/Regulations/Standards

- ISO 22301:2019
- ISO 22313:2020
- Information Technology Act, 2000 (as amended in 2008)
- Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011

14. Definition

Critical Activities	IT – Applications/ systems, which are crucial for attaining the business objectives for an organization or a specific unit. These processes support the key products and services being delivered by an organization.
Recovery Time Objective (RTO)	Target time set for resumption of product, service or activity delivery after an incident.

Recovery Point Objective (RPO)	The recovery point objective (RPO) is the age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.
Maximum Acceptable Outage/ Maximum Tolerable period of disruption (MAO/MTPD)	Duration after which an organization's viability will be irrevocably threatened if the application cannot be resumed.

------------------------------------End of the document------------------------------------