RISK MANAGEMENT POLICY

1. Preface:

Title	**RISK MANAGEMENT POLICY**
Version Number	**1.1**
Effective Date	**28.03.2023**
Authorised by	**Board of Directors**
Date of Previous version	**30.03.2015**

2. Objective:

The policy aims to ensure resilience for sustainable growth and sound corporate governance by having an identified process of risk identification and management (in compliance with the provisions of the Companies Act, 2013 and Regulation 17 (9) of the Securities & Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations,2015.

3. Applicability and Effective Date:

The policy applies to all units and functions of the company. The revised policy will come into force w.e.f 01.01.2023. This policy documents the present practices and will continue to capture practices which evolve

4. Policy:

JSW Infrastructure Ltd follows the Committee of Sponsoring Organisations (COSO) framework of Enterprise Risk Management (ERM) to classify, communicate, respond to risks and opportunities based on probability, frequency, impact, exposure and resultant vulnerability and ensure Resilience such that:

a) Intended risks, like for growth, are taken prudently so as to plan for the best and be prepared for the worst through de-risking strategies clearly defined priorities across strategic purposes, consistent rationale for resource allocation, stress testing on what if kind of scenarios on critical factors even if source is indirect, probability is uncertain and impact is immeasurable, better anticipation, flexibility and due diligence

b) Execution of decided plans is handled with action focus

c) Unintended risks like related to performance, operations, compliance, systems, incident, process and transaction are avoided, mitigated, transferred (like in insurance), shared (like through sub contracting) or probability, or impact thereof is reduced through tactical and executive management, code of conduct, competency building, policies, processes, inbuilt

systems controls, MIS, internal audit reviews etc. No threshold limits are defined as objective will be to do the best possible

d) Knowable unknown risks in fast changing Volatile, Uncertain, Complex and Ambiguous (VUCA) conditions are managed through timely sensitisation of markets trends, shifts and stakeholders sentiments.

e) Overall risk exposure of present and future risks remains within Risk capacity.

5. Process:

a. The Risk owners identify risks, opportunities & make risk response plans.

b. High risks affecting unit are discussed at respective locations.

c. Risks affecting the entire company are discussed at corporate meeting.

d. The Risk committee of directors consisting of executive & nominated directors reviews the framework & high risks & opportunities which are emerging or where impact is substantially changing.

e. Board of Directors takes note of proceedings at Risk committee of Directors.

f. Risk Management cell facilitates discussion on business risks.

g. Internal audit reviews process risks & controls.

6. Roles & Responsibility:

a. The Board of Directors (the Board) is responsible for implementing and monitoring the risk management plan of the Company. The Board shall constitute a Risk Management Committee (RMC). The Board shall define the roles and responsibilities of the RMC and may delegate monitoring and reviewing of the risk management plan to the RMC including cyber security and such other functions as it may deem fit.

b. The RMC shall –

- Ensure that appropriate methodology, processes, and systems are in place to monitor and evaluate risks associated with business of the company.

- Monitor and oversee implementation of the risk management policy, including evaluation of the adequacy of risk management systems.

- Periodically review the policy, at least once in two years, considering the changing

industry dynamics and evolving complexity.

- Keep the board of directors informed about the nature and content of RMC discussions and recommendations, as well as the actions to be taken.

c. RMC shall assist the board of directors with the identification and management of risks to which the Company's group is exposed.

Constitution of RMC - The majority of RMC shall consist of members of the Board. The Risk committee of directors consisting of mix of some executive directors & atleast one nominated Independent Director. Senior executives of the company may be members of the said Committee. The Chairman of the Committee shall be a member of the Board. RMC members shall have a working familiarity with the fundamentals of finance, accounting and risk management and represent a range of backgrounds, skills and experiences due to the strategic, business, operational, financial and non-financial risk profiles of the Company.

The Board shall take note of proceedings of Risk Management Committee meeting of Directors

d. CEO – CEO shall be responsible for all the company risks and determine its risk capacity under the guidance of the Chairman to ensure that risk exposures are within the limit.

e. Unit/ Functional Risk Owners – Unit incharge shall be responsible for all risks related to the unit. Functional head shall be responsible for the risks related to the specific function.

7. Business Continuity Plan (BCP):

All Site Units of the Company shall have Business Continuity Plan (BCP).

The main objective of BCP is to maintain business continuity in case of unplanned events & potential disruptive incidents with an aim to minimize impact on -

- Human life and other living beings
- Environment and related eco systems
- Economic losses
- All stakeholders (such as investors, employees, local communities)

8. Environmental, Social & Governance (ESG) risks:

The Company is engaged in port operations and cargo handling which involves various environmental, safety, operational & governance risks. The Company's aim has always been for an all-inclusive & sustainable growth while addressing these risks.

The key risks identified have been tagged with Environmental / Social / Governance category for a holistic review from Sustainability point of view.

9. Risks, Impact and response strategies:

Type of Risk	Impact	Risk response strategies	Risk Owner
Macro and Strategic risks	1) Macro-Economic: Macro factors such as global GDP growth, shipping industry cyclicality etc can impact business and future plans of the company. 2) Government Policies: Changes in government policies like following can affect business: a) Development of new ports and Hinterland connectivity b) Eco system around the ports c) Export/imports policies affecting the volume of business. 3) Business Dynamics: Competition from upcoming new private sector ports can affect the revenue and profitability of the company. 4) Strategy: Not identifying right opportunities at the right time and imprudent investment can affect growth and profitability. Concentration of business with JSW group can cause dependency risk.	In-house research, reports of specialized agencies and interactions with all concerned help track macro environment, government policies, competition etc. so as to take prudent and timely decision.	CEO
Projects	Time and cost overruns due to: - Gap in co-ordination and monitoring of the project. - Delay in government/ other regulatory clearances like for land acquisition, CRZ Approval, environment, state maritime board and for	Company de-risks by - Strong co-ordination team and use of projects software. Timely financial closure. Selection of capable vendors and continuous follow up.	Head – Projects.

Type of Risk	Impact	Risk response strategies	Risk Owner
	hinterland connectivity - Fund availability. - Delay from vendor end	Liaising with government for timely clearance.	
Operations and maintenance	Non-fulfillment of obligations by JSW infrastructure in relation to operations and incidental activities and maintenance of earthmoving and material handling equipments and obligations of operating companies on minimum qty, maintenance of major equipments etc can affect performance	Review of the risks affecting each other	Unit Heads
Reputation, governance and values	Reputation of the company may be affected by- 1) Poor corporate governance- inadequate/ ineffective controls which may give rise to fraud, negligence etc 2) Violation of law affecting reputation.	Company de-risks by- 1) Robust corporate governance practice, code of conduct 2) Effective systems for compliance	CEO

Type of Risk	Impact	Risk response strategies	Risk Owner
Finance- a) Funding, b) Liquidity, c) Credit and d) Volatility	Finance can be affected by- 1) Market sentiments and norms setting limits on funding 2) Business risks affecting volume, margins and working capital 3) Increased operational cost, interest, unplanned expenditure or bunching of payments 4) Customer financials affecting collection 5) Systemic weakness in commodity and financial markets causing volatility in prices, interest and exchange rates	Company de-risks by – 1) Effective stakeholder management and tracking of external events 2) Regularly reviewing financing, hedging, pricing policy and exposure limits 3) Managing third party risks through due diligence, performance tracking and business scenario tracking 4) Effective monitoring of internal performance and cash flows through internal meetings and information and communication systems 5) Standby finance sources.	CFO

Type of Risk	Impact	Risk response strategies	Risk Owner
Human Resource	Organisational Competency, culture and Performance are affected by: 1) Non availability or obsolescence of talent 2) Extent of institutionalisation of organisational learning, succession planning, leadership development and competency building 3) Manpower planning, placement, role definition or performance management.	Company de-risks by 1) Effective talent search process 2) Competitive compensation 3) Robust performance mgt. system to reward potential and initiative 4) Adequate training for leadership and specific competency	Head - HR
Systems – a) Business alignment, b) Controls, c) Reporting and d) compliance	Judicious balance is necessary between business enabling and control systems to ensure – 1) Business enablement to ensure organisational learning with timely and right sensitisation and insight which is available to right person at right time to facilitate strategy, plans, prudent decisions, actions and monitoring 2) Controls to minimise frauds, leakage of confidential information and attack on systems 3) Correct financial reporting in compliance with regulations, standards, disclosure requirements and prudent basis of valuation and estimates like that for contingent liabilities	Company de-risks by – 1) Aligning IT strategy with business strategy to take care of future needs and leverage new technologies. 2) Inbuilt systems controls IT security and internal audit 3) Standards to ensure high standards of governance supported by effective systems, clearly laid down roles. Estimates for contingencies are based on sound judgment considering circumstances and available guidance	Unit Head/Head-IT

Type of Risk	Impact	Risk response strategies	Risk Owner
Cyber security	Cyber security risk could result in substantial reputation and financial loss arising from: 1. Theft of corporate information 2. Theft of financial information (e.g. Financial results, bank details etc.) 3. Ransom ware – cyber extortion. 4. Disruption to business (e.g. inability to carry out SAP transactions, online payments) Loss of business or contract.	Company de-risk by: 1. Periodically assessing the current state and prioritize the foundational components of cyber security. 2. Conducting periodic audits of security systems and procedures. 3. Developing a new capability, technologies and processes to combat cyber-threats. 4. Incorporating cybersecurity and privacy into everyday business decisions and processes. (like Information Security Awareness Program) 5. Assessing readiness to adapt advanced technologies in IS domain. Monitor threats and respond, investigate and remediate cybersecurity related incidents and data breaches.	Head - IT

Type of Risk	Impact	Risk response strategies	Risk Owner
Environment, Health and Safety	The following can affect the life, property, operations, environment and regulatory compliances for the same: i) excess emissions ii) discharge of pollutants, waste iii) natural calamity iv) occupational disease v) accidents vi) fire / leakages vii) security;	Company de-risks by 1) Selecting right equipment, processes and inputs and tracking emissions vis a vis norms 2) Proper treatment and discharge of waste like de-dusting, RO plant, slime pond 3) Safety training, structures audit, 4) Fire prevention processes 5) Medical facilities 6) Security arrangements like access monitoring system, vigilance, mock drills 7) Disaster management practices review by external agencies at regular intervals 8) Incident systems to ensure timely communication, analyse root cause and capture learning to prevent recurrence	Head – ESG & Unit Heads

Type of Risk	Impact	Risk response strategies	Risk Owner
Technology and operational disruptions	The following can have impact on competitive edge and operations 1) Timely decision/ action on technology up gradation, innovation, product development and patenting thereof to meet unarticulated product needs of consumers 2) Non availability of spares for obsolete technology and sub optimal performance of outdated or unproven technology 3) Inadequacy of vendor support, automation systems, redundancies, operational training and maintenance which can disrupt operations	Company de-risks by 1) Full-fledged R and D infrastructure at Ports 2) Understanding customer needs for new products by Application engineering and customer service dept 3) Effective management of vendors, automation systems, operating procedures, maintenance scheduling, spares maintenance management, operator training, equipment life cycle tracking and condition monitoring	Head – IT & Unit Heads