MANGALAM CEMENT LTD.
CIN: L26943RJ1976PLC001705
Regd. Office: P.O. Aditya Nagar - 326520, Morak, Distt. Kota (Raj.)
Phone: 07459-233127, Fax No.: 07459-232036
E-mail: shares@mangalamcement.com **Website:** www.mangalamcement.com

RISK MANAGEMENT POLICY

1.1. Preamble

This Risk Management policy ('the Policy') is governed by applicable regulations for risk management under SEBI (Listing Obligations and Disclosure Requirements), 2015 and Companies Act, 2013 (as amended from time to time). This policy shall be updated in line with the amendments brought in by the regulators from time to time in the aforesaid legislations.

1.2. Background

The business activities of the Company carry various internal and external risks.

"Risk" in literal terms can be defined as the effect of uncertainty on the objectives. Risk is measured in terms of consequences and likelihood. Risks can be internal and external and are inherent in all administrative and business activities. Every member of any organization continuously manages various types of risks. Formal and systematic approaches to managing risks have evolved and they are now regarded as good management practice also called as Risk Management.

"Risk Management" is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of uncertain events or to maximize the realization of opportunities. Risk management also provides a system for the setting of priorities when there are competing demands on limited resources.

Effective risk management requires:

a. A strategic focus,
b. Forward thinking and active approaches to management
c. Balance between the cost of managing risk and the anticipated benefits, and
d. Contingency planning in the event that critical threats are realized.

In today's challenging and competitive environment, strategies for mitigating inherent risks in accomplishing the growth plans of the Company are imperative. The common risks inter alia are: Regulations, competition, Business risk, Technology obsolescence, return on investments, business cycle, increase in price and costs, limited resources, retention of talent, etc.

1.3. Legal Framework

Section 134 (5) (e) of Companies Act, 2013 requires that, directors should provide a statement that, directors had laid down internal financial controls to be followed by the company and that such internal financial controls are adequate and were operating effectively. Further the Independent Directors shall satisfy themselves on the integrity of financial information, and that financial control and the systems of risk management are robust and defensible.

Also, as per section 134 (3) (n), Board Report should include a statement indicating development and implementation of a risk management policy.

1.4. Scope of Policy

Risk is an event, the occurrence or non-occurrence of it can adversely /favorably impact the achievement of an entity's objective. Risks can impact an organisation's objectives at two levels viz. operational/functional level objectives and strategic/enterprise level objectives. Operational /functional level risk management framework deals with operational/ day-to-day risks which are not significant in terms of their impact in terms of achievements of organisational objectives. These are generally inherently managed by operation level teams of the Company on day to day basis with support of internal control systems. On other hand, enterprise level risks impact the Company's strategic /enterprise level objectives and generally have material impact on Company's business, financial position and reputation.

1.5. Applicability

This Policy applies to all areas of the Company's Operations.

1.6. Enterprise Risk Management (ERM) framework

The Company shall prepare an Enterprise Risk Management Framework that is based on industry Standards and encompassing all enterprise level risks that the organisation is facing internally or externally under different categories such as financial, operational, sectoral, and information risks including ESG and cyber security risks.

1.7. Risk Category

The Risk identified shall be categorised under following 6 categories as provided under SEBI (Listing Obligations and Disclosures Responsibility) Regulations, 2015.

S.N.	Risk Category	Description	Risk areas
1	Financial Risks	Risk related to loss of money, capital to run/expand the business	• Liquidity & Credit Risk • Capital • Structure Risk • Forex Risk
2	Sectoral Risks	Risks related to industry /sector, non-achievement of business plans of the Company	• Market dynamics & competition risk • Business plan and execution risk • Lack of innovation/creativity and major initiative risk
3	Information and Technology Risk	Risk of inadequate reporting of financial /non-financial data and technological challenges	• Accounting and reporting risk • Investor relationship & communication risk • Cyber security risks

S.N.	Risk Category	Description	Risk areas
			• Technological and digitalization risks
4	Operational Risks	Risk of loss resulting from inadequate or failed processes people or information systems	• Sale & marketing risks • Supply Chain risk • Operating efficiency risk • Physical assets risk • Contracting risk • People Risk • Hazard Management
5	Sustainability Risks	Risks resulting from issues related to climate change, sustainability, legal & regulatory compliance	• Climate Change Risk • Social Responsibility Risk • Code of Conduct Risk • Corporate Governance Risk • Legal & Regulatory Compliance
6	Others	Residuary Category	Risk not falling in any of the above categories shall be covered in this category.

1.8. Process to Perform including review and revision

- **Identify Risks:** Risk identification is a process by which people identify major risks. This identification can be made in number of ways such as by tracking /list of leading events or key risk indicators, brainstorming, discussions with peers and internal analysis, comparison with other organisations, process flow analysis etc.

- **Assess Risk severity and Risk prioritization:** Once risks have been identified, they should be evaluated to determine which are of an unacceptable nature and should by targeted for mitigation. This can be done by evaluating them on potential impact on business objectives together with the likelihood of occurrence /non-occurrence.

- **Define mitigation plan:** Mitigation consists of risk responses and control objectives. Relevant Risk Owner shall be responsible to ensure that appropriate risk responses are in place. Risk response can be categorised of our four types i.e Treat/reduce(actions to reduce the impact and/or likelihood), Transfer/share (action to reduce the likelihood or impact by transfer full or portion of the risk such as buying insurance), take /accept as it is (with no further action to affect likelihood and impact) and terminate /avoid (actions to discontinue the activity that causes the risk)

1.9. Monitoring & Reporting:

Monitoring is the process assesses both the presence and functioning of Risk Management Process components and the quality of their performance over time. Ongoing monitoring of the framework is key to its effectiveness. While the relevant risk owners shall be primarily responsible for monitoring the risks and their mitigation plans/actions, internal audit will assist whatever required. Risk profiles and the effectiveness of the mitigation plan shall be reviewed / monitored and reported to the Board of Directors as and when required.

1.10. Internal Controls and their adequacy

Internal audit is used as an effective tool to check and enhance efficacy of systems, processes and controls of the Company. It is carried out by an independent agency. The review plan, drawn in consultation with the senior management, covers all the major areas. Standard operating procedure compliance and management-approved policies are reviewed and areas of improvement, if any, are identified. All the observations and suggestions for improvement form a part of the report. The report is discussed with Senior Management and Audit Committee of the Board. Wherever necessary, adequate corrective measures are initiated to ensure compliance.

1.11. Compliance and Control

All the Senior Executives under the guidance of the Chairman and Board of Directors has the responsibility for over viewing management's processes and results in identifying, assessing and monitoring risk associated with organization's business operations and the implementation and maintenance of policies and control procedures to give adequate protection against key risk. In doing so, the Senior Executive considers and assesses the appropriateness and effectiveness of management information and other systems of internal control, encompassing review of any external agency in this regards and action taken or proposed resulting from those reports.

1.12. Review

This Policy shall be reviewed at least once in two years to ensure it meets the requirements of legislation and the needs of organization.

AMENDMENT

This Policy can be modified at any time by the Board of Directors of the Company.

Note: This Policy modified and approved by the Board of Directors in its meeting held on 3rd November, 2023.