CMM INFRAPROJECTS LIMITED

RISK MANAGEMENT POLICY

1. PREAMBLE

This Risk Management Policy ("Policy") of CMM Infraprojects Limited ("the Company") is framed pursuant to the provisions of Section 134(3)(n) of the Companies Act, 2013, Regulation 17(9) and other applicable provisions of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI LODR Regulations"), together with applicable rules, circulars and amendments thereto.

The Company recognizes that risk is an integral and unavoidable component of business and that effective risk management is essential for sustainable growth, operational efficiency, protection of stakeholder interests and achievement of strategic objectives.

This Policy establishes a structured framework for identification, assessment, monitoring, mitigation and reporting of risks across the Company.

2. OBJECTIVES OF THE POLICY

The objectives of this Policy are:

1. To establish a systematic and consistent approach for identifying, assessing, monitoring and managing risks.
2. To integrate risk management into the Company's business planning and decision-making processes.
3. To safeguard the interests of shareholders, customers, employees, lenders and other stakeholders.
4. To ensure compliance with applicable laws, regulations and governance standards.
5. To strengthen internal controls and operational resilience.
6. To minimize adverse impact of risks on business performance and reputation.
7. To create and promote a risk-aware culture throughout the organization.
8. To ensure continuity of business operations during disruptions or crisis situations.

3. APPLICABILITY AND SCOPE

This Policy applies to all departments, business units, projects, locations and functions of the Company.

The scope of this Policy includes identification and management of risks relating to:

- strategic matters;
- operations and projects;
- finance and treasury;
- legal and regulatory compliance;
- environment, health and safety;
- information technology and cybersecurity;
- human resources;
- reputation and stakeholder relations;
- business continuity and disaster recovery;
- fraud and internal controls;
- any other material risk affecting the Company.

4. DEFINITIONS

(a) **"Board"** means the Board of Directors of the Company.

(b) **"Audit Committee"** means the Audit Committee constituted by the Board.

(c) **"Risk"** means the possibility of occurrence of an event which may have an adverse impact on the Company's objectives, operations, financial position, reputation or compliance obligations.

(d) **"Risk Management"** means the systematic process of identifying, assessing, mitigating, monitoring and reporting risks.

(e) **"Risk Register"** means a documented repository containing identified risks, assessment, mitigation plans, ownership and status.

Words and expressions used but not defined in this Policy shall have the meanings assigned under the Companies Act, 2013 and SEBI LODR Regulations.

5. RISK GOVERNANCE FRAMEWORK

A. Board of Directors

The Board shall:

1. Have overall responsibility for oversight of the Company's risk management framework.
2. Approve and periodically review the Risk Management Policy.
3. Ensure that appropriate systems for risk management and internal control are established.
4. Review major risks affecting the Company and adequacy of mitigation measures.
5. Monitor effectiveness of risk management systems.

B. Audit Committee

The Audit Committee shall:

1. Review the adequacy and effectiveness of risk management systems and internal controls.
2. Review significant risk exposures and mitigation plans.
3. Monitor implementation of corrective actions.
4. Review internal audit findings relating to risk management.
5. Report significant observations and recommendations to the Board.

C. Senior Management

Senior Management shall:

1. Identify risks within their respective functions and operations.
2. Develop and implement appropriate mitigation measures.
3. Ensure compliance with internal controls and regulatory requirements.
4. Report material risks and incidents to the Audit Committee and Board.
5. Promote risk awareness among employees.

D. Risk Management Officer / Team

Where designated, the Risk Management Officer or Team shall:

1. Coordinate risk identification and assessment activities.
2. Maintain and update the Risk Register.
3. Monitor implementation of mitigation measures.
4. Facilitate reporting and communication relating to risks.
5. Assist in development of risk management processes and training.

6. RISK IDENTIFICATION AND CLASSIFICATION

The Company shall identify and classify risks under broad categories including but not limited to:

Category	Description	Illustrative Risks
Strategic Risk	Risks affecting long-term business objectives and growth	Industry changes, competition, policy changes
Operational Risk	Risks arising from inadequate or failed processes, systems or human errors	Project delays, supply disruptions, manpower shortages
Financial Risk	Risks relating to liquidity, credit, interest rates and financial losses	Cash flow issues, debtor defaults
Compliance & Legal Risk	Risks due to non-compliance with laws or contractual obligations	Regulatory penalties, litigation
Reputational Risk	Risks affecting brand image and stakeholder confidence	Governance failures, negative publicity
IT & Cybersecurity Risk	Risks related to system failures, cyber attacks and data breaches	Ransomware, unauthorized access
Environmental & Safety Risk	Risks relating to environment, health and workplace safety	Accidents, pollution violations
Human Resource Risk	Risks relating to employee management and retention	Attrition, industrial disputes
Project Risk	Risks associated with execution of infrastructure and project activities	Cost overruns, execution delays

The above categories are indicative and may be modified depending upon business needs.

7. RISK ASSESSMENT

Each identified risk shall be evaluated based on:

1. Probability or likelihood of occurrence;
2. Magnitude of impact;
3. Financial and operational consequences;
4. Regulatory and reputational implications;
5. Existing controls and mitigation mechanisms.

The Company may adopt a Risk Matrix approach to classify risks into:

- High Risk
- Medium Risk
- Low Risk

High-risk areas shall receive priority attention and monitoring.

8. RISK MITIGATION STRATEGIES

Depending upon the nature and severity of risk, the Company may adopt one or more of the following strategies:

A. Risk Avoidance

Discontinuing or avoiding activities exposing the Company to unacceptable risks.

B. Risk Reduction

Implementing controls and safeguards to reduce probability or impact.

C. Risk Sharing / Transfer

Transferring risk through insurance, contractual arrangements or outsourcing.

D. Risk Acceptance

Accepting certain risks where mitigation cost exceeds potential impact.

The management shall develop Risk Mitigation Plans ("RMPs") for significant risks and review the status periodically.

9. INTERNAL CONTROLS

The Company shall maintain adequate internal control systems to:

- ensure operational efficiency;
- safeguard assets;
- prevent fraud and errors;
- ensure accuracy of financial reporting;
- ensure compliance with laws and internal policies.

The internal audit function shall periodically review effectiveness of internal controls.

10. CYBERSECURITY AND INFORMATION RISK

Recognizing the growing significance of information technology and cyber threats, the Company shall endeavor to:

- maintain adequate IT security systems and controls;
- implement access controls and data protection measures;
- ensure periodic backup of critical data;
- monitor cyber threats and vulnerabilities;
- establish incident response mechanisms;
- conduct employee awareness programs relating to cybersecurity.

11. BUSINESS CONTINUITY AND CRISIS MANAGEMENT

The Company shall maintain business continuity and crisis management mechanisms to minimize disruption arising from:

- natural disasters;
- cyber incidents;
- pandemics;
- fire and accidents;
- utility failures;
- political or economic disruptions;
- any other unforeseen events.

The Company may develop contingency and disaster recovery plans for critical operations.

12. MONITORING AND REPORTING

1. Key risks and mitigation measures shall be reviewed periodically by the Audit Committee and the Board.
2. Material changes in risk profile shall be promptly escalated.
3. The Risk Register shall be periodically updated.
4. Significant incidents and emerging risks shall be reported to management and the Board.

13. REVIEW OF POLICY

This Policy shall be reviewed periodically by the Audit Committee and the Board, at least once in three years or earlier if required due to:

- changes in laws or regulations;
- changes in business environment;
- operational or strategic developments;
- occurrence of significant risk events.

14. DISCLOSURE

This Policy shall be disclosed in the Board's Report and hosted on the website of the Company in accordance with applicable provisions of the Companies Act, 2013 and SEBI LODR Regulations.

15. AMENDMENT

The Board reserves the right to amend, modify or replace this Policy, in whole or in part, at any time in accordance with applicable laws.

In case of any inconsistency between this Policy and applicable law, the provisions of applicable law shall prevail.