RISK MANAGEMENT POLICY

1. PURPOSE

This Policy is adopted by **Kanohar Electricals Limited** ("Company") pursuant to Regulation 17 and other applicable provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 to provide a framework for identification, assessment and management of risks in accordance with applicable law.

Accordingly, the Board has adopted the Policy vide Board Resolution dated January 10, 2026 which can be further amended from time to time.

2. SCOPE

This Policy applies to risks that may have a material impact on the Company's business, operations, financial performance or reputation.

3. RISK MANAGEMENT FRAMEWORK

The Company's risk management framework is intended to enable identification, assessment and management of risks relevant to its business and operations.

3.1 RISK IDENTIFICATION

Risk identification may be carried out, inter alia, through:

- strategic planning and budgeting processes;
- operational reviews;
- internal and external audits;
- regulatory and compliance assessments;
- sustainability and ESG-related considerations;
- incident reporting; and
- stakeholder feedback.

3.2 CATEGORIES OF RISKS

For the purpose of this Policy, risks may include, inter alia:

a) Financial Risks

- liquidity risk;
- credit risk;
- interest rate risk;

- foreign exchange risk; and
- capital structure and funding risks.

b) Operational Risks

- process inefficiencies;
- supply chain disruptions;
- human resource risks;
- health, safety and environmental risks; and
- dependence on key personnel.

c) Sectoral / Industry Risks

- demand-supply fluctuations;
- competitive pressures;
- technological changes; and
- regulatory or policy developments affecting the industry.

d) Sustainability and ESG Risks

- environmental risks;
- social risks; and
- governance-related risks.

e) Information and Data Risks

- data integrity and confidentiality risks;
- information accuracy and reporting risks; and
- intellectual property risks.

f) Cyber Security Risks

- cyber-attacks and data breaches;
- system outages;
- unauthorised access; and
- technology infrastructure vulnerabilities.

g) Other Risks

- legal and compliance risks;
- reputational risks; and
- force majeure or geopolitical risks.

3.3 RISK MITIGATION MEASURES

The Company may consider adopting appropriate risk mitigation measures, including, inter alia:

- risk avoidance;
- risk reduction;
- risk transfer (including insurance or contractual arrangements); and
- risk acceptance with appropriate monitoring.

4. GOVERNANCE AND OVERSIGHT

- The **Board of Directors** shall have overall responsibility for risk oversight.

- The **Risk Management Committee** shall monitor the risk management framework and report to the Board at such intervals as it considers appropriate.

- **Senior management** shall be responsible for addressing risks within their respective areas of responsibility.

5. BUSINESS CONTINUITY FRAMEWORK

The Company has a business continuity framework intended to support continuity of critical business operations in the event of disruptions arising from natural disasters, pandemics, cyber incidents, system failures or other unforeseen events.

The framework may, inter alia, consider:

- identification of critical business processes;
- disaster recovery and information technology backup arrangements;
- alternate working arrangements;
- crisis management and communication mechanisms; and
- roles and responsibilities during disruption events.

6. REVIEW

The Risk Management Committee may review this Policy from time to time and recommend changes to the Board, as considered appropriate.

7. AMENDMENT

The Board of Directors may amend this Policy from time to time in accordance with applicable law.

8. PUBLICATION

This Policy shall be disclosed on the website of the Company.