PREMIER INDUSTRIAL CORPORATION LIMITED

RISK ASSESSMENT AND MANAGEMENT POLICY

RISK ASSESSMENT AND MANAGEMENT POLICY

[Pursuant to Regulation 17(9) and 21 of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 and Section 134(3) of the Companies Act, 2013]

I. SCOPE

This Risk Assessment and Management Policy **("Policy")** establishes the philosophy of Premier Industrial Corporation Limited **("Company")**, towards risk identification, analysis and prioritization of risks, development of risk mitigation plans and reporting on the risk environment of the Company.
As per the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("Listing Regulations"), the Risk Management Policy shall include:

(a) A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the risk management committee;
(b) Measures for risk mitigation including systems and processes for internal control of identified risks;
(c) Business continuity plan

Accordingly, the board of directors of Company ("**Board**") has adopted this Policy at its meeting held on 9th September 2025, which can be amended from time to time.

II. OBJECTIVE

The objective of this Policy is to manage the risks involved in all activities of the Company to maximize opportunities and minimize adversity. This Policy is intended to assist in decision making processes that will minimize potential losses, improve the management of uncertainty and the approach to new opportunities, thereby helping the Company to achieve its objectives.

The key objectives of this Policy are:

(a) Safeguarding the Company's property and interest of all stakeholders.
(b) Managing risks with an institutionalized framework and consistently achieving desired outcomes;
(c) Laying down of a framework for identification, measurement, evaluation, mitigation and reporting of various risks.
(d) Evolving the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects, which the business and operations of the Company are exposed to.
(e) Balancing between the cost of managing risk and the anticipated benefits.
(f) To create awareness among the employees to assess risks on a continuous basis and develop risk mitigation plans in the interest of the Company.
(g) Provide a system for setting priorities when there are competing demands on limited resources.

III. RISK GOVERNANCE

An organization's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities. Risk governance signifies the way the business and affairs of an entity are directed and managed by its Board and executive management.

The Risk Management Committee ("**RMC**") is applicable to the top 1000 listed entities, determined based on market capitalization as at the end of the immediately preceding financial year. [Since the Company does not fall into the said category, currently, the RMC is not applicable. However, when the Company meets the criteria where the RMC becomes applicable, it will comply with the regulations governing its formation and operation.

The RMC as and when formed shall have a minimum of three members with majority of them being members of the board of directors, including at least one independent director. The chairperson of the RMC shall be a member of the board of directors and senior executives of the listed entity may be members of the committee. The RMC shall meet at least twice a year. The quorum for a meeting of the RMC shall be either two members or one third of the members of the committee, whichever is higher, including at least one member of the board of directors in attendance. The meetings of the risk management committee shall be conducted in such a manner that on a continuous basis not more than two hundred and ten days shall elapse between any two consecutive meetings. RMC shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure the attendance of outsiders with relevant expertise, if it considers necessary. The board of directors shall define the role and responsibility of the RMC and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit such functions shall specifically cover cyber security.

The role of the committee shall, inter alia, include the following:

1. To formulate a detailed Risk Assessment and Management Policy which shall include:
   (a) framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the RMC;
   (b) measures for risk mitigation including systems and processes for internal control of identified risks; and
   (c) business continuity plan.
2. To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
3. To monitor and oversee implementation of the Risk Assessment and Management Policy, including evaluating the adequacy of risk management systems.
4. To periodically review the Policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
5. To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;
6. The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.
7. The Risk Management Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.

IV. RISK MANAGEMENT FRAMEWORK

The Board's role is to ensure framing, implementing and monitoring risk management plan and systems for risk management as part of internal controls. The Board or the RMC, as the case may be, shall periodically review the Policy of the Company and evaluate the risk management systems so that management controls the risk through a properly defined network.

Heads of departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning.

V. RISK MANAGEMENT PROCESS

Conscious that no entrepreneurial activity can be undertaken without assumption of risks and associated profit opportunities, the Company operates on a Risk Management Process /Framework aimed at minimization of identifiable risks after evaluation so as to enable management to take informed decision. Broad outline of the framework is as follows:

a) Risk Identification:

Management identifies potential events that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. Potentially, negative events and represent risks are assigned a unique identifier. The identification process is carried out in such a way that an expansive risk identification covering operations and support functions are put together and dealt with.

Risks can be identified under the following broad categories. This is an illustrative list and not necessarily an exhaustive classification.

(i) Internal risks including:

- Strategic Risk: Competition, inadequate capacity, high dependence on a single customer/vendor.
- Business Risk: Project viability, process risk, technology obsolescence/ changes, development of alternative products.
- Finance Risk: Liquidity, credit, currency fluctuation.
- Environment Risk: Non-compliances to environmental regulations, risk of health to people at large.
- Personnel Risk: Health & safety, high attrition rate, incompetence.
- Operational Risk: Process bottlenecks, non-adherence to process parameters/ pre-defined rules.
- Reputation Risk: Brand impairment, product liabilities.
- Regulatory Risk: Non-compliance to statutes, change of regulations.
- Technology Risk: Innovation and obsolescence.
- Information and Cyber Security Risk: Cyber security related threats and attacks.

(ii) External risks including:

- Sectoral Risk: Unfavorable consumer behavior in relation to the relevant sector etc.
- Sustainability Risk: Environmental, social and governance (ESG) related risks including climate change, energy efficiency, waste management, water usage, and other sustainability factors that may impact the Company's long-term business continuity and reputation.
- Political Risk: Changes in the political environment, regulation/ deregulation due to changes in political environment.

b) Root Cause Analysis:

Undertaken on a consultative basis, Root Cause Analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.

c) Risk Scoring:

Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on cost, revenue, profit etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion and the table is known as Risk Register (RR). The Company has assigned quantifiable values to each Risk Element based on the 'Impact' and 'Likelihood' of the occurrence of the Risk on a scale of 1 to 3 as follows.

The resultant 'Action Required' is derived based on the combined effect of Impact & Likelihood and is quantified as per the summary below.

Impact	Score	Likelihood
Minor	1	Low
Moderate	2	Medium
Significant	3	High

d) Risk Categorization:

The identified risks are further grouped in to (i) Preventable (ii) Strategic and (iii) External categories to homogenize risks

(i) Preventable Risks are largely internal to organization and are operational in nature. The endeavor is to reduce /eliminate the events in this category as they are controllable. Standard operating procedures (SOP) and Audit Plans are relied upon to monitor and control such internal operational risks that are preventable.

(ii) Strategic Risks are voluntarily assumed risks by the Senior Management in order to generate superior returns / market share from its strategy. Approaches to strategy risk is 'Accept'/'Share', backed by a risk-management system designed to reduce the probability that the assumed risks actually materialize and to improve the Company's ability to manage or contain the risk events should they occur.

(iii) External risks arise from events beyond organization's influence or control. They generally arise from natural and political disasters and major macroeconomic shifts. Management regularly endeavors to focus on their identification and impact mitigation through 'avoid'/'reduce' approach that includes measures like Business Continuity Plan / Disaster Recovery Management Plan / Specific Loss Insurance / Policy Advocacy etc.

e) Risk Prioritization:

Based on the composite scores, risks are prioritized for mitigation actions and reporting

f) Risk Mitigation Plan:

Management develops appropriate responsive action on review of various alternatives, costs and benefits, with a view to managing identified risks and limiting the impact to tolerance level. Risk Mitigation Plan drives policy development as regards risk ownership, control environment timelines, standard operating procedure (SOP) etc.

Risk Mitigation Plan is the core of effective risk management. The mitigation plan covers:

1. Required Action
2. Required Resources
3. Responsibilities
4. Timing
5. Performance Measures and
6. Reporting and Monitoring requirements

The mitigation plan also covers (i) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (ii) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken; (iii) corrective controls - responses to reduce the consequences or damage arising from crystallization of a significant incident.

Hence it is drawn up in adequate precision and specificity to manage identified risks in terms of documented approach (accept, avoid, reduce, share) towards the risks with specific responsibility assigned for management of the risks.

g) Risk Monitoring:

It is designed to assess on an ongoing basis, the functioning of risk management components and the quality of performance over time. Staff members are encouraged to carry out assessments throughout the year.

h) Options for dealing with risk:

There are various options for dealing with risk.

Tolerate – If we cannot reduce the risk in a specific area (or if doing so is out of proportion to the risk) we can decide to tolerate the risk; i.e., do nothing further to reduce the risk. Tolerated risks are simply listed in the corporate risk register.

Transfer – Here risks might be transferred to other organizations, for example by use of insurance or transferring out an area of work.

Terminate – This applies to risks we cannot mitigate other than by not doing work in that specific area. So if a particular project is of very high risk and these risks cannot be mitigated we might decide to cancel the project.

i) Risk Reporting:

Periodically key risks are reported to Board or empowered committee with causes and mitigations undertaken / proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carries out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial control system was maintained and whether such internal financial controls system operated effectively in the Company in all material respects with respect to financial reporting.

On a regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the chief executive officer and the chief financial officer, on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

The Board shall include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

j) Risk Management Measures adopted in general by the Company:

The Company has adopted various measures to mitigate the risk arising out of various areas described above, including but not limited to the following:
(i) A well-defined organization structure;
(ii) Defined flow of information to avoid any conflict or communication gap;
(iii) Hierarchical support personnel to avoid work interruption in absence/ non-availability of functional heads;
(iv) Discussion and implementation on financial planning with detailed business plans;
(v) Detailed discussion and analysis of periodic budgets;
(vi) Employees training and development programs;
(vii) Internal control systems to detect, resolve and avoid any frauds;
(viii) Systems for assessment of creditworthiness of existing and potential contractors/subcontractors/ dealers/vendors/ end-users;
(ix) Redressal of grievances by negotiations, conciliation and arbitration; and
(x) Defined recruitment policy.

VI. BUSINESS CONTINUITY PLAN

Business Continuity Plans (BCP) are required to be defined for High Impact & High Velocity risk, to enable rapid response to address the consequence of such risks when they materialize. Business Continuity Planning shall be embedded in the internal controls and risk management framework for products, systems and processes etc.

VII. COMMUNICATION AND CONSULTATION

Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process as well as on the process as a whole.

VIII. PERIODICAL REVIEW OF EFFECTIVENESS

Effectiveness of Risk Management Framework is ensured through periodical Internal Audits. These play an important validation role to provide assurance to the Audit committee that the critical processes continue to perform effectively, key measures and reports are reliable and established policies are in compliance.

As the risk exposure of any business may undergo change from time to time due to continuously changing environments, the updation of this Policy will be done as and when required.

IX. APPROVAL OF THE POLICY

The Board will be the approving authority for the Company's overall Risk Management System. The Board will, therefore, approve the Risk Management Policy and any amendments thereto from time to time.

X. SUMMATION

The above framework is proposed as a broad risk management policy of the Company.

XI. AMENDMENTS/ LIMITATION

This Policy is framed based on the provisions of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and the Companies Act, 2013, as amended from time to time. In case of any subsequent changes in the provisions of the applicable laws which make the provisions in the Policy inconsistent with the applicable laws, the provisions of such law shall prevail over the Policy and the provisions in the Policy shall be modified in due course to make it consistent with the applicable laws. Any omission shall not be construed as non-compliance with any relevant regulations or provisions thereof