ASTRAL LIMITED

RISK MANAGEMENT POLICY

Preamble:

Astral Limited (hereinafter referred to as 'Astral or Company" is in the business of manufacturing Pipes used for various applications like plumbing, drainage, agricultural, infrastructure, industrial, fire protection etc. and in manufacturing of Adhesives products with a diversified range of adhesives, sealants, putties and construction aids. With our vision to be a leading manufacturer in the industry, we aim to expand our legacy of trust and innovation in other category such as Bathware & Faucets. This business carries various internal and external risks.

The nature of Astral's business exposes it to a wide range of internal and external risks, including but not limited to financial, operational, technological, regulatory, environmental, social, governance (ESG), cyber security and strategic risks.

In today's challenging and competitive environment, strategies for mitigating inherent risks in accomplishing the growth plans of the Company are imperative. This Risk Management Policy provides a structured framework for identification, assessment, monitoring and mitigation of risks, with the objective of ensuring sustainable growth, resilience and long-term stakeholder value.

Objective:

Key objective of this Policy are identify, assess and prioritise risks that may impact the achievement of Astral's business objectives, establish appropriate risk mitigation and control mechanisms, ensure business continuity and operational resilience, protect the interests of stakeholders under adverse conditions and support sustainable growth with long-term stability.

Regulatory Framework:

Corporate Governance norms of SEBI and the Companies Act 2013 have incorporated various provisions in relation to Risk Management. Brief of some provisions are as under:

Section 134(3) of the Companies Act 2013 necessitates that the Board's Report should contain a statement indicating development and implementation of Risk Management Policy including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

Section 177(4)(vii) of the Companies Act 2013 require that every Audit Committee shall act in accordance with the terms of reference in writing by the Board which shall *inter alia* include evaluation of Risk Management System.

Regulation 21 of SEBI (LODR) Regulations 2015 as amended from time to time provides for constitution of Risk Management Committee and delegation of review and monitoring of risk management systems to the said committee. Further, 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 Committee.

(b) Measures for risk mitigation including systems and processes for internal control of identified risks.

(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 management policy, including evaluating the adequacy of risk management systems;

(4) To periodically review the risk management 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.

Area of Application:

This Policy shall apply to **all operations, functions, projects, subsidiaries, plants and locations** of the Company.

Risk management Framework:

Risk Management typically includes three steps. (i) Risk Identification (ii) Risk Assessment and (iii) Risk Mitigation.

Risk Identification:

The Company is exposed to various kinds of internal and external risk. Major Risk Categories are listed as under:

Internal Risks Factors
Financial Reporting
Quality & Project Management
Dependency on key distributors
Human Resources Management
Compliance with Laws

External Risk Factors:
Exchange Rate fluctuations
Crude oil and raw material price volatility
Real Estate and infrastructure market conditions
Changes in technology (PVC / CPVC and allied products)
Environment, Social, Governance Risk (ESG)
Cyber security and information technology risks
Economic and Political environment

Risk assessment:
Having identified the risk factors, the next important step is to assess the risk. At Astral, risk factors are rated on the scale of High-Medium-Low. Based on the likelihood of occurrence of event and potential impact on the Company, the risks are assessed as under

Risk Factor	**Rating**
Internal Risk Factors:	
Financial Reporting	High
Quality & Project Management	Medium
Dependency on key distributors	Medium
Human Resources Management	Medium
Compliance with Laws	Medium
External Risk Factors	
Exchange Rate fluctuations	High
Crude oil and raw material price volatility	Medium
Real Estate and infrastructure market conditions	Medium
Changes in technology (PVC / CPVC and allied products)	High
Environment, Social & Governance Risk (ESG)	High
Cyber security and information technology risks	High
Economic and Political environment	Low

Risk mitigation:

Once the risks have been assessed and prioritized, comprehensive mitigation strategies are defined for each risk. Each employee and process owner of the Company is responsible for implementation of the risk management system as may be applicable to respective area of functioning. Each employee is duty bound to report the risk based on the defined parameters for each process to respective departmental head. Each Departmental Head shall take immediate action to review the risk and implement mitigation strategy. The Company shall have separate Hedging Policy under direct control and supervision of the Chief Financial Officer to effectively manage inherent forex risks.
For any cyber-security breach/attacks, the company has multiple listening, tracking, tracing systems and capabilities including a SOC which on a continuous basis identifies, priorities and remediates vulnerabilities in order to control/minimize the likelihood or impact of any event. Our IT Security team maintains clear and actionable

Security Policies, regularly updates software patches, limits access and controls to critical software/data and servers, installs firewalls and antivirus software, does segregation of networks, has a comprehensive system recovery plan, recovery ready data and redundant systems, manages access controls by monitoring internal and third-party access and continuously scans for network intrusions to eliminate chances of cyber-attack.

Risk Management Governance Structure:

In order to effectively review and monitor risk management across the organization, following governance structure is followed.

Risk Officers	Each departmental/plant head shall act as Risk Officer for his/her department. It is the duty of the Risk Officer to immediately implement the risk management system in its department and immediately escalate the risk going beyond normal conditions to the Risk Management Committee through e-mail to the Managing Director and/or Chief Financial Officer. Risk register shall be maintained identifying risk and mitigation strategy for each process.
Risk Management Committee constituted in accordance with Regulation 21 of SEBI (LODR)	It shall comprise of Chairman of Audit Committee, Managing Director and the Chief Financial Officer and other Members. The Committee shall: • oversee implementation of the risk management framework; • review adequacy and effectiveness of risk management systems; • review ESG and cyber security risks; • review appointment / removal / remuneration of the **Chief Risk Officer (if any)**; • meet **at least twice a year**; and • report periodically to the Board of Directors.
Audit Committee / Board of Directors	The Audit Committee shall evaluate the risk management system as part of its statutory duties. The Board shall: • review risk management framework periodically; • ensure that material risks are adequately addressed; and • include appropriate disclosures in the Annual Report.

Business Continuity Plan (BCP):

The BCP ensures that personnel and assets are protected and are able to function quickly in the event of a disaster. The BCP is generally conceived in advance and involves input from key stakeholders and personnel.

BCP involves defining any and all risks that can affect the company's operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters— fire, flood, or weather-related events—and cyber-attacks. Once the risks are identified, the plan to include:

- ✓ Determining how those risks will affect operations
- ✓ Implementing safeguards and procedures to mitigate the risks
- ✓ Testing procedures to ensure they work
- ✓ Reviewing the process to make sure that it is up to date

Review:

This Policy shall be reviewed **at least once in a year** or earlier if required due to regulatory changes or business exigencies. Any amendments shall be recommended by the Risk Management Committee and approved by the Board.

This Policy was further reviewed at the Meeting of the Risk Management Committee held on 18th May, 2026.