



**CONTINENTAL
SECURITIES LTD.**

CONTINENTAL SECURITIES LIMITED
RISK MANAGEMENT POLICY



1. OBJECTIVE

This Policy establishes a structured framework for identification, assessment, mitigation, monitoring and reporting of risks, including cyber security and information security risks, which may impact the Company's business, operations, financial stability, compliance and reputation.

This Policy is framed in compliance with:

- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, including Regulations 17, 21 and 27 relating to Board responsibility, Risk Management Committee.
- Companies Act, 2013, including Sections 177 and 134 relating to Audit Committee, internal financial controls and Board responsibilities.

2. APPLICABILITY

This Policy applies to all directors, employees, functions, systems, and third-party service providers of the Company.

3. RISK MANAGEMENT FRAMEWORK

The Company shall adopt an enterprise-wide risk management system covering identification of risks across all functions, assessment based on likelihood and impact, prioritisation of material risks, implementation of mitigation measures and internal controls, continuous monitoring and periodic review, and maintenance of a Risk Register.

4. GOVERNANCE STRUCTURE

4.1 Board of Directors (Reg. 17 SEBI LODR)

The Board shall approve and oversee this Policy and the Risk Management Plan, define risk appetite and tolerance levels, integrate risk management into strategic planning, and periodically review the risk management framework, at least once every two years.

4.2 Risk Management Committee (Reg. 21 SEBI LODR)

The RMC shall oversee the enterprise risk management framework, identify and monitor strategic, financial, operational, compliance, and cyber risks, and recommend mitigation measures and internal controls. It shall also review the Risk Register and risk reports quarterly, coordinate with the Audit Committee on financial and control risks, and review cyber security risks and incidents.

4.3 Audit Committee (Section 177, Companies Act, 2013)

The Audit Committee shall evaluate internal financial controls and risk management systems, review audit findings and the adequacy of internal controls, and oversee reporting of material risks and cyber incidents.

4.4 Risk Management Function / CRO

The Company may appoint a Chief Risk Officer/Senior management personnel or designate a function, responsible for maintaining the Risk Register, coordinating risk identification and reporting, monitoring mitigation actions, and supporting reporting to the Risk Management Committee and the Board.

4.5 Functional Heads & Employees

All employees and functional heads shall identify and report risks in their respective areas, implement appropriate mitigation controls, and promptly escalate significant risks.

5. CYBER SECURITY AND INCIDENT MANAGEMENT

The Company shall implement appropriate measures to protect its IT systems and data from cyber threats, including access controls, encryption, firewalls, Multi-Factor Authentication (MFA), secure backups, disaster recovery and business continuity systems, third-party risk assessments, cyber security awareness, and continuous monitoring.

In case of a cyber incident, the Company shall identify, contain, and assess the incident, preserve evidence, and carry out root cause analysis. The incident shall be reported to the Audit Committee, Risk Management Committee, and the Board, and disclosed to stock exchanges and regulators, if required, under applicable laws. Corrective and preventive actions shall be implemented.

7. RISK MINIMISATION MEASURES

The Company shall implement strong internal financial controls in accordance with Sections 134 and 177 of the Companies Act, supported by internal and statutory audits, business continuity and disaster recovery plans, segregation of duties, access controls, a whistle blower mechanism, cyber insurance where feasible, and regular compliance and risk training.

8. DISCLOSURE & REPORTING

Material risks and cyber incidents shall be reported to the Board and Committees and disclosed to stock exchanges in accordance with SEBI (LODR) Regulations, 2015.

9. REVIEW & AMENDMENT

This Policy shall be reviewed annually or earlier, if required due to regulatory or business changes. Any amendment shall be approved by the Board of Directors in accordance with SEBI LODR and Companies Act, 2013.

-----**-----

Date of last review by the board:-08-05-2026.