



Risk Management Policy

(Pursuant to Section 134(3)(n) of the Companies Act, 2013 and Regulations 17(9) and 21 read with Paragraph C of Part D of Schedule II to the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (“SEBI Listing Regulations”), as amended)

{Approved by the Board of Directors of Elitecon International Limited at its meeting held on 18 September, 2026}

TABLE OF CONTENTS

S. No.	Contents
1	Preamble and Background
2	Legal Framework
3	Objectives of the Policy
4	Scope and Applicability
5	Key Definitions
6	Risk Management Principles
7	Risk Appetite Statement
8	Risk Governance Structure
9	Risk Management Committee - Composition, Meetings and Powers
10	Risk Universe
11	Risk Management Process
12	Risk Assessment Matrix
13	Risk Register and Risk Dashboard
14	Risk Assurance
15	Business Continuity Plan and Crisis Management
16	Internal Controls and Compliance Integration
17	Risk Reporting and Escalation
18	Review of Policy and Framework
19	Disclosure and Records
20	Alignment with Other Policies
21	Limitation

1. Preamble and Background

Elitecon International Limited (“**Company**”) recognises that an effective risk management framework is an integral part of sound corporate governance and is essential for protecting stakeholder interests, supporting informed decision-making, achieving strategic objectives and ensuring continuity of critical business operations. The risk management framework of the Company shall be proportionate to the nature, scale and complexity of its business operations, regulatory environment, organizational structure and risk profile.

Risk management is not intended to eliminate all business risks. Its purpose is to ensure that risks are identified in a timely manner, evaluated objectively, managed within an approved risk appetite, escalated at the appropriate level and monitored through adequate controls, reporting and governance mechanisms.

The Board of Directors has adopted this Risk Management Policy to provide a structured framework for risk identification, risk assessment, risk mitigation, internal control, business continuity, monitoring and reporting across the Company and, to the extent applicable, its subsidiaries and controlled operations.

2. Legal Framework

In addition to the requirements expressly set out in applicable law, this Policy establishes the Company's internal framework for identification, assessment, prioritisation, mitigation, monitoring, reporting and escalation of risks and shall be implemented in a manner proportionate to the Company's business and risk profile.

This Policy has been framed having regard to the following provisions and regulatory expectations:

- a. Section 134(3)(n) of the Companies Act, 2013, requiring the Board's Report to include a statement indicating development and implementation of a risk management policy, including identification of elements of risk which, in the opinion of the Board, may threaten the existence of the Company;
- b. Section 134(5)(e) of the Companies Act, 2013 relating to directors' responsibility for internal financial controls and adequacy and operating effectiveness of such controls, as applicable;
- c. Section 177 of the Companies Act, 2013, to the extent the Audit Committee is required to evaluate internal financial controls and risk management systems;
- d. Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, requiring the listed entity to lay down procedures to inform the Board about risk assessment and minimisation procedures and making the Board responsible for framing, implementing and monitoring the risk management plan;
- e. Regulation 21 of the SEBI Listing Regulations relating to constitution, role, powers and functioning of the Risk Management Committee for applicable listed entities;
- f. Schedule II, Part D, Para C of the SEBI Listing Regulations specifying the role of the Risk Management Committee, including formulation of a detailed risk management policy, monitoring and reviewing risk management systems, business continuity and reporting to the Board;
- g. Applicable provisions of the SEBI Listing Regulations, SEBI circulars, Companies Act, 2013, Secretarial Standards, securities laws, accounting standards, tax laws, FEMA, labour

laws, environmental and sustainability requirements, consumer/product laws and other laws applicable to the business and operations of the Company.

In case of any inconsistency between this Policy and applicable law, the applicable law shall prevail. The Policy shall be deemed to be modified to the extent necessary to comply with any amendment, circular, notification or clarification issued by the competent authority.

3. Objectives of the Policy

The objectives of this Policy are to:

- a. establish a structured and consistent enterprise-wide risk management framework;
- b. identify internal and external risks faced by the Company, including strategic, financial, operational, sectoral, sustainability, information, cyber security, legal, compliance and reputational risks;
- c. define the governance structure for risk oversight by the Board, Risk Management Committee, Audit Committee, senior management and functional heads;
- d. provide a methodology for risk identification, assessment, prioritisation, mitigation, monitoring and reporting;
- e. establish appropriate risk appetite, risk tolerance levels, escalation thresholds and key risk indicators for material risks, wherever considered appropriate
- f. ensure that risk mitigation measures, internal controls and business continuity processes are aligned with the Company's business strategy and stakeholder expectations;
- g. enable informed decision-making by ensuring that material risks and emerging risks are placed before the appropriate forum on a timely basis;
- h. promote a culture of risk awareness, ethical conduct, regulatory compliance, accountability and transparency across the Company; and
- i. support sustainable growth, protection of stakeholder value and continuity of critical operations.

4. Scope and Applicability

This Policy applies to the Company and, to the extent applicable and legally permissible, to its subsidiaries, joint ventures, business units, branches, manufacturing/trading operations, distribution networks, finance and treasury functions, compliance functions, information systems and other operational areas under the control or supervision of the Company. The Company shall establish appropriate mechanisms for identifying, assessing, monitoring and reporting material risks arising at subsidiary or controlled-entity level which may have a material impact on the Company or the consolidated group.

Where the Company has overseas subsidiaries, investments, operations or material exposures outside India, the risk management framework shall, where relevant, take into consideration country risk, foreign exchange risk, regulatory risk, geopolitical risk and other risks arising from such exposure.

The Policy shall apply to directors, key managerial personnel, senior management, employees, consultants, retainers and other persons acting on behalf of the Company, to the extent relevant to their role and responsibility.

Detailed standard operating procedures, delegation matrices, internal financial control processes, compliance trackers, authority levels, insurance arrangements, business continuity plans and crisis response protocols may be maintained separately and shall operate in support of this Policy.

5. Key Definitions

For the purpose of this Policy, unless the context otherwise requires:

Term	Meaning
Board	The Board of Directors of Elitecon International Limited.
Company	Elitecon International Limited.
Risk	The effect of uncertainty on objectives, including events or circumstances that may adversely impact strategy, operations, financial position, reputation, compliance status, stakeholder value or business continuity.
Risk Appetite	The nature and level of risk that the Company is willing to accept in pursuit of its strategic and business objectives.
Risk Management Committee / RMC	The Risk Management Committee constituted by the Board in accordance with Regulation 21 of the SEBI Listing Regulations, as applicable.
Risk Owner	A person or function responsible for managing, monitoring and reporting a specific risk or group of risks.
Key Risk Indicator / KRI	A metric, trigger or signal used to monitor exposure to a particular risk or emerging risk trend.
Material Risk	A risk which may have a significant impact on the Company's operations, financial position, regulatory standing, stakeholder confidence, reputation, market conduct or continuity of business.
Inherent Risk	The level of risk assessed before taking into account the effect of existing controls or mitigation measures.
Risk Tolerance	The acceptable variation around the Company's approved risk appetite within which a risk may be managed without requiring escalation to a higher level.
SEBI Listing Regulations	The SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended from time to time.

6. Risk Management Principles

The Company shall follow the following guiding principles for risk management:

- risk management shall be integrated with strategic planning, budgeting, capital allocation, business expansion, financial reporting and compliance processes;
- material risks shall be identified, assessed and reported in a timely and evidence-based manner;
- risk ownership shall be clearly allocated to responsible functions or individuals;
- risks shall be managed through preventive, detective and corrective controls;
- risk mitigation shall be proportionate to the likelihood, impact, cost, regulatory sensitivity and business criticality of the risk;
- the Company shall maintain a no tolerance approach for fraud, bribery, wilful non-compliance, market abuse, manipulation, insider trading, deliberate financial misreporting, unauthorised use of confidential information and conduct that materially damages stakeholder trust;
- the Company may accept reasonable commercial and strategic risks where such risks are evaluated, documented, approved at the appropriate level and aligned with the Company's objectives;
- risk management shall include both downside protection and opportunity evaluation; and
- the risk framework shall be periodically reviewed to reflect changing industry dynamics, regulatory developments, business complexity and emerging risks.

7. Risk Appetite Statement

The Company recognises that risk-taking is inherent in business growth, expansion, innovation and capital deployment. However, such risk-taking must be disciplined, transparent and within a governance framework approved by the Board.

The Risk Appetite Statement shall be approved by the Board, on the recommendation of the Risk Management Committee, and shall be reviewed periodically in light of the Company's strategy, financial position, regulatory environment, risk profile and changing business circumstances.

The indicative risk appetite of the Company shall be as follows:

Risk Area	Risk Appetite / Approach
Legal, regulatory and listing compliance	No appetite for wilful or reckless non-compliance. All statutory, listing, exchange, SEBI, Companies Act, tax, FEMA and other regulatory obligations shall be tracked and complied with within prescribed timelines.
Financial reporting and internal controls	Low appetite for errors, misstatements, unsupported accounting judgements, delayed consolidation, deficient documentation or weak internal financial controls.
Business expansion and strategic initiatives	Measured appetite, subject to due diligence, Board / Committee approvals, capital discipline, risk assessment, legal review and post-implementation monitoring.
Liquidity, leverage and treasury	Prudent appetite, with focus on preserving solvency, timely debt servicing, adequate working capital, cash-flow visibility and compliance with covenants.
Operational execution	Moderate appetite for process innovation and expansion, subject to adequate SOPs, vendor controls, quality assurance, insurance, escalation and monitoring.
Cyber security and confidential information	Low appetite for cyber incidents, data loss, unauthorised access, misuse of unpublished price sensitive information, SDD weaknesses or technology disruption.
Fraud, ethics and market conduct	Zero tolerance for fraud, bribery, corruption, market manipulation, insider trading, false disclosures, suppression of information or retaliation against whistle-blowers.
Reputation and stakeholder communication	Low appetite for avoidable reputational harm, misleading communication, inconsistent public statements, defective stock exchange

	disclosures or stakeholder grievance escalation.
--	--

Where quantitative risk appetite or tolerance limits are considered necessary, such limits may be prescribed by the Board, Risk Management Committee or the appropriate management authority pursuant to the framework approved by the Board.

8. Risk Governance Structure

The Company shall follow a layered governance structure for risk oversight and accountability.

8.1. Board of Directors

- a. The Board shall be responsible for framing, implementing and monitoring the risk management plan of the Company.
- b. The Board shall approve this Policy and material amendments thereto.
- c. The Board shall review material risks, significant risk incidents, risk mitigation status and recommendations of the Risk Management Committee / Audit Committee.
- d. The Board may entrust monitoring and review of the risk management plan to the Risk Management Committee and, where relevant, to other committees in accordance with applicable law and the framework approved by the Board, without diluting the statutory role of the Risk Management Committee or the Board's overall responsibility for the Company's risk management framework.

8.2. Risk Management Committee

- a. The Risk Management Committee shall be constituted and function in accordance with Regulation 21 and Paragraph C of Part D of Schedule II of the SEBI Listing Regulations, as applicable to the Company.
- b. The Committee shall formulate, monitor and periodically review this Policy and the risk management systems of the Company.
- c. The Committee shall ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
- d. The Committee shall oversee implementation of the Policy and evaluate adequacy of risk management systems.
- e. The Committee shall keep the Board informed about the nature and content of its discussions, recommendations and actions to be taken.
- f. The Committee may seek information from any employee, obtain outside legal or professional advice and secure attendance of external experts, wherever necessary.
- g. The appointment, removal and terms of remuneration of the Chief Risk Officer, if any, shall be subject to review by the Committee.
- h. For clarity, neither the SEBI Listing Regulations nor this Policy requires the Company to appoint a Chief Risk Officer. This provision shall apply only if the Company has appointed or proposes to appoint a Chief Risk Officer.
- i. The RMC shall coordinate its activities with the Audit Committee and other committees of the Board wherever there is an overlap in responsibilities, in accordance with the framework approved by the Board.

8.3. Audit Committee

Nothing contained in this Policy shall restrict the independent responsibilities of the Audit Committee under applicable law:

- a. The Audit Committee shall evaluate internal financial controls and risk management systems, as required under applicable law.
- b. The Audit Committee shall coordinate with the Risk Management Committee where there is overlap relating to financial reporting risk, internal controls, fraud risk, audit observations, related party transactions, compliance weaknesses or whistle-blower matters.
- c. The Audit Committee may, in accordance with applicable law review significant audit findings, control deficiencies and corrective action plans and may report material matters to the Board.

8.4. Senior Management and Functional Heads

- a. Senior management shall be responsible for implementation of the risk management framework within their respective areas.
- b. Functional heads shall identify, assess, mitigate, monitor and report risks in their functions and shall maintain adequate records of controls, approvals and escalations.
- c. Management shall periodically update the Risk Register, prepare risk dashboards and place material risks before the Risk Management Committee / Board, as applicable.
- d. Risk owners shall remain accountable for the risks assigned to them notwithstanding delegation of individual mitigation activities.

8.5. Company Secretary and Compliance Officer

- a. The Company Secretary / Compliance Officer shall support the Board and Committees in matters relating to listing compliance, stock exchange disclosures, corporate governance, statutory filings, investor grievance reporting, preservation of records, insider trading controls and secretarial compliance.
- b. The Company Secretary / Compliance Officer shall ensure that risk-related decisions requiring stock exchange disclosure or Board / Committee reporting are identified and escalated appropriately.

8.6. Risk Owners and Employees

- a. Every employee and risk owner is responsible for identifying and escalating risks, control failures, suspected fraud, compliance breaches, information security incidents and any matter that may materially affect the Company.
- b. Employees shall comply with applicable policies, SOPs, authority limits, code of conduct, confidentiality obligations, insider trading code and statutory requirements.

9. Risk Management Committee - Composition, Meetings and Powers

The composition, quorum, meeting frequency and powers of the Risk Management Committee shall be in accordance with Regulation 21 of the SEBI Listing Regulations and any amendment thereto. Without prejudice to the applicable law:

- a. the Committee shall have a minimum of three members;
- b. a majority of members shall be members of the Board;
- c. at least one member shall be an independent director and where the Company has outstanding SR equity shares, at least two thirds of the Risk Management Committee shall comprise independent directors;
- d. the Chairperson of the Committee shall be a member of the Board;

- e. senior executives may be members of the Committee;
- f. the Committee shall meet at least twice in each financial year, and not more than 210 days shall elapse between any two consecutive meetings;
- g. the quorum for a meeting 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 in attendance;
- h. the Committee may invite executives, internal auditors, statutory auditors, legal advisors, consultants, IT/cyber experts, insurance advisors or other persons to attend meetings; and
- i. the Committee shall coordinate with other committees where there is overlap of responsibilities.

10. Risk Universe

The risk universe of the Company may include, without limitation, the following categories. The list is indicative and shall be updated based on business evolution, industry dynamics, regulatory developments and management assessment.

The following risk categories constitute the Company's indicative risk universe and shall not be construed as exhaustive. The RMC may add, remove, combine or reclassify risk categories based on the Company's business activities, emerging risks, regulatory developments and risk profile.

Risk Category	Illustrative Risk Areas
Strategic and business risk	Business model risk, expansion roadmap, competition, pricing pressure, portfolio concentration, market entry, acquisition/integration risk, subsidiary performance, execution risk and dependence on key business assumptions. Country and geopolitical risk arising from operations, investments, customers, suppliers or counterparties located outside India, wherever applicable.
Subsidiary and Group Risk	Risks arising from the financial, operational, regulatory, legal, tax, governance, liquidity, foreign exchange, country and other exposures of subsidiaries and controlled entities, including risks arising from inter-company transactions, guarantees, investments, funding arrangements and dependency on subsidiaries or key group entities.
Financial risk	Revenue volatility, profitability, liquidity, leverage, interest rate risk, foreign exchange exposure, commodity price movement, working capital, credit risk, receivables, impairment, taxation, accounting judgements and covenant compliance. Foreign exchange and currency risk arising from import, export, overseas investments, subsidiaries or other foreign currency exposures, wherever applicable.
Operational risk	Supply chain disruption, vendor concentration, procurement, manufacturing/trading operations, warehousing, logistics, distribution, inventory, process failure, quality control, insurance adequacy and operational efficiency. Supply chain and inventory risk, including supplier concentration, disruption in availability

	of critical inputs, inventory obsolescence, excess or slow-moving inventory, logistics disruption and dependency on key vendors.
Product, customer and consumer risk	Product quality, packaging, labelling, safety, consumer complaints, recall risk, customer concentration, distributor/dealer disputes and service-level failures.
Legal and regulatory risk	Companies Act, SEBI Listing Regulations, SAST, PIT, ICDR, stock exchange filings, secretarial compliance, tax, FEMA, labour, environmental, consumer/product, contract and litigation risks.
Market conduct and disclosure risk	UPSI handling, structured digital database, trading window, stock exchange disclosure, investor communication, rumours, media statements, misleading information and stakeholder grievances.
Governance, ethics and fraud risk	Fraud, bribery, conflict of interest, related party transactions, internal control override, whistle-blower complaints, delegation of authority breach and misappropriation.
Information and cyber security risk	Cyber attacks, data leakage, system downtime, unauthorised access, weak access controls, IT vendor risk, ransomware, confidential information misuse and disaster recovery gaps.
Sustainability and ESG risk	BRSR/BRSR Core readiness, energy/water/waste data, labour practices, health and safety, supply chain responsibility, community impact, climate-related risk and ESG disclosures.
Human capital risk	Key managerial personnel dependency, succession planning, talent retention, conduct risk, training gaps, workplace safety, POSH and employee relations.
Reputational risk	Adverse regulatory developments, media reports, market rumours, investor complaints, social media escalation, governance concerns and brand perception.
Product, customer and consumer risk	Product quality, packaging, labelling, safety, consumer complaints, recall risk, customer concentration, distributor/dealer disputes and service-level failures.
Business continuity and crisis risk	Natural disaster, fire, pandemic, geopolitical disruption, technology outage, plant/warehouse disruption, key vendor failure and emergency response.

11. Risk Management Process

The Company shall follow a structured risk management process comprising risk identification, assessment, prioritisation, mitigation, monitoring, reporting and review.

11.1. Risk Identification

- Risks shall be identified through business planning, management reviews, audit observations, regulatory updates, compliance trackers, financial reviews, operational reviews, investor/stakeholder feedback, whistle-blower complaints, cyber alerts, legal cases, industry developments and external events.
- Each function shall identify risks relevant to its area and submit them for consolidation in the Risk Register.

11.2. Risk Assessment

- a. Identified risks shall be assessed based on likelihood and impact as the primary scoring parameters. Additional factors such as velocity, persistence, controllability and regulatory/reputational sensitivity may be considered as qualitative modifiers when determining the overall risk priority.
- b. Impact may be evaluated across financial, operational, legal, compliance, reputation, customer, sustainability and business continuity parameters.
- c. The Company may use qualitative and/or quantitative assessment methods depending on the nature of the risk.

11.3. Risk Prioritisation

- a. Risks shall be prioritised as Critical, High, Medium or Low based on likelihood and impact.
- b. Critical and High risks shall be placed before senior management and, where material, before the Risk Management Committee / Board.
- c. Medium and Low risks shall be monitored at the functional level and escalated if exposure increases.

11.4. Risk Mitigation

- a. Mitigation strategies may include risk avoidance, reduction, transfer, sharing or acceptance with monitoring.
- b. Controls may include approvals, segregation of duties, maker-checker controls, SOPs, insurance, contractual protections, compliance calendars, system controls, training, audits, due diligence, legal review, vendor controls, hedging, cash-flow controls and crisis protocols.
- c. Residual risk after mitigation shall be reviewed and tracked.

11.5. Monitoring and Review

- a. Risk owners shall monitor key risks and relevant KRIs at such frequency as may be appropriate to the nature and materiality of the risk.
- b. The frequency of monitoring shall be higher for Critical and High risks and may be reduced for Low risks where the existing control environment remains effective.
- c. Significant deviations, breaches, incidents or emerging risks shall be escalated immediately to senior management and, where material, to the Risk Management Committee / Board.
- d. Corrective action plans shall have clear ownership, timelines and status tracking.

12. Risk Assessment Matrix

The matrix is an indicative framework. The RMC may approve separate quantitative thresholds or risk-specific assessment methodologies where the nature of the relevant risk requires a more appropriate assessment approach.

The following indicative matrix may be used by the Company to classify risks. The matrix is illustrative and may be supplemented by quantitative thresholds approved by management / Committee.

Score	Likelihood	Illustrative Description
1	Rare	May occur only in exceptional circumstances.

2	Unlikely	Could occur, but not expected under normal circumstances.
3	Possible	May occur at some time based on current controls and exposure.
4	Likely	Expected to occur in certain circumstances or has occurred previously.
5	Almost certain	Expected to occur frequently or exposure is already materialising.

Score	Impact	Illustrative Description
1	Insignificant	Limited operational inconvenience; no material financial, legal or reputational impact.
2	Minor	Manageable impact; limited delay, cost or localised process failure.
3	Moderate	Noticeable financial/operational impact; management attention required; potential compliance concern.
4	Major	Significant financial, legal, regulatory, operational or reputational impact; Committee/Board attention may be required.
5	Severe	Potential threat to business continuity, solvency, listing compliance, regulatory standing, stakeholder confidence or existence of the Company.

Risk Rating	Combined Score / Classification	Indicative Response
Critical	20-25 or management-classified critical	Immediate escalation to senior management and RMC / Board, detailed action plan, close monitoring and periodic reporting.
High	12-19	Action plan required; risk owner to report progress; RMC review where material.
Medium	6-11	Functional-level mitigation and periodic review; escalate if trend worsens.
Low	1-5	Routine monitoring through existing controls.

13. Risk Register and Risk Dashboard

The Company shall establish and maintain a comprehensive Risk Register and Risk Dashboard for identification, assessment, monitoring, mitigation and reporting of material, significant and emerging risks faced by the Company and, where applicable, its subsidiaries. The Risk Register may be maintained in electronic form and may be updated periodically by risk owners under supervision of senior management.

The Risk Register / dashboard should generally capture the following information:

Field	Description
Risk ID	Unique identification number for the risk.
Risk Category	Strategic, financial, operational, compliance, cyber, ESG, reputational etc.
Risk Description	Brief description of the risk event, cause and possible impact.
Risk Owner	Function / individual accountable for monitoring and mitigation.
Inherent Risk Rating	Risk level before considering mitigation controls.
Existing Controls	Preventive, detective and corrective controls already in place.

Residual Risk Rating	Risk level after considering existing controls.
Mitigation Action Plan	Additional actions required, if any.
Timeline and Responsibility	Target date and accountable person/function.
KRI / Trigger	Metric or event that signals increase in risk exposure.
Status	Open / ongoing / under review / mitigated / closed.
Escalation Required	Whether the risk requires senior management / RMC / Board escalation.

14. Risk Assurance

- a. The Company shall establish appropriate mechanisms for obtaining reasonable assurance regarding the effectiveness of risk management processes and controls.
- b. Such assurance may be obtained through internal audit, management review, compliance review, control self-assessment, independent assurance, specialist review, external professional advice or such other mechanisms as may be appropriate.
- c. Material control deficiencies, recurring risk incidents and significant deviations from approved mitigation plans shall be subject to appropriate corrective action and escalation.

15. Business Continuity Plan and Crisis Management

The Company shall maintain a business continuity approach proportionate to the scale and complexity of its operations. The business continuity plan shall be maintained separately and shall include procedures to respond to events that may disrupt critical operations.

The business continuity and crisis response framework shall cover, as applicable:

- a. identification of critical business processes, systems, vendors, personnel and locations;
- b. emergency response, incident command and communication protocols;
- c. alternate operating arrangements for critical functions;
- d. data backup, disaster recovery and cyber incident response;
- e. inventory, logistics, customer/distributor communication and vendor continuity;
- f. regulatory and stock exchange disclosure assessment for material incidents;
- g. insurance notification and claim documentation;
- h. employee safety and stakeholder communication; and
- i. periodic testing, simulation or review of business continuity arrangements.

16. Internal Controls and Compliance Integration

The Company shall maintain systems and processes for internal control of identified risks, including internal financial controls, compliance controls, operational controls, information technology controls and such other controls as may be appropriate to the Company's risk profile.

The Company shall endeavour to maintain the following control environment:

- a. clearly defined authority matrix and approval limits;
- b. segregation of duties and maker-checker controls for financial, secretarial, regulatory and operational processes;
- c. documented SOPs for material functions;
- d. Compliance Calendar for Companies Act, SEBI Listing Regulations, stock exchanges, tax, FEMA and other applicable laws;

- e. periodic review of statutory filings, stock exchange disclosures and corporate actions;
- f. structured digital database and controls for unpublished price sensitive information;
- g. vendor and customer due diligence for material relationships;
- h. review of related party transactions and arm's length documentation, wherever applicable;
- i. internal audit / management audit / legal review for selected high-risk areas;
- j. information security controls, access management and data backup;
- k. training and awareness for employees on compliance, ethics, insider trading, disclosure and information security; and
- l. whistle-blower and grievance mechanisms for reporting concerns.

17. Risk Reporting and Escalation

The Company shall establish reporting channels so that material risks and risk incidents are escalated without delay. The following matters shall ordinarily be escalated to senior management and, depending on materiality, to the Risk Management Committee / Board:

- a. material regulatory notices, proceedings, investigations, exchange queries or potential non-compliance;
- b. material financial misstatement, internal control weakness or suspected fraud;
- c. material deviation in business plan, liquidity position, debt covenant, cash flows or profitability;
- d. cyber security incident, data breach, system compromise or significant technology outage;
- e. material product quality, consumer safety, recall, vendor, customer or operational incident;
- f. material litigation, tax demand, penalty, show cause notice or claim;
- g. adverse media coverage, investor grievance escalation or reputation-sensitive event;
- h. significant breach of code of conduct, whistle-blower complaint, bribery/corruption allegation or conflict of interest; and
- i. any event that may require disclosure to stock exchanges under Regulation 30 or any other applicable provision.

18. Review of Policy and Framework

The Risk Management Committee shall periodically review this Policy at least once every two years, including by considering changing industry dynamics, regulatory developments, evolving business complexity and the Company's risk profile.

The Policy may be reviewed earlier if there is any material change in business operations, market capitalisation applicability, regulatory requirements, Board direction, risk incident, change in control, major acquisition/divestment, expansion into new business lines, significant subsidiary restructuring or other event considered material by the Board or Committee.

Any material amendment to this Policy shall be recommended by the Risk Management Committee and approved by the Board, unless such amendment is administrative, clerical or required to reflect an automatic change in law.

19. Disclosure and Records

The Company shall make such disclosures regarding risk management, risk management committee, internal controls, Board's Report statement, corporate governance report, annual report, BRSR/BRSR Core and website disclosure as may be required under applicable law.

Minutes of the Risk Management Committee and Board meetings, risk registers, action trackers, incident reports, audit observations and related documents shall be maintained in accordance with applicable law, the Company's document preservation policy and internal requirements. Confidential risk information, unpublished price sensitive information, commercially sensitive information and privileged legal advice shall be handled strictly on a need-to-know basis, except where disclosure is required under applicable law or by a competent regulatory, judicial or governmental authority.

20. Alignment with Other Policies

This Policy shall be read together with other policies and frameworks of the Company, including:

- a. Code of Conduct for Directors and Senior Management;
- b. Code of Conduct for Prevention of Insider Trading and Fair Disclosure Code;
- c. Policy for Determination of Materiality of Events / Information;
- d. Policy on Related Party Transactions;
- e. Whistle Blower / Vigil Mechanism Policy;
- f. Dividend Distribution Policy;
- g. Policy for Preservation of Documents and Archival Policy;
- h. Nomination and Remuneration Policy;
- i. Corporate Social Responsibility Policy, if applicable;
- j. Internal Financial Control framework and delegation of authority matrix;
- k. BRSR / sustainability data management framework; and
- l. Any other policy, SOP, manual or guideline approved by the Board / Committee / management.

21. Limitation

This Policy provides the governance framework for risk management. It does not guarantee elimination of risks or prevention of losses. Risk management depends on timely identification, quality of information, effectiveness of controls, business judgement, external environment, regulatory developments and conduct of persons responsible for implementation.

The Board and Committees may exercise business judgement and discretion in applying this Policy, subject to applicable law and fiduciary duties.