SAHANARATNABH LIMITED

(Formerly known as SAHANARATNABH PRIVATE LIMITED)

Registered Office: B WING, UNIT NO. 601, 602, 610, TANVIZ DAOMOND, IND EST, S.V.R.D. DAHISAR EAST, NEAR PETROL PUMP, NOVELTY SILK MILL, MUMBAI, 400068.
E-Mail: sahanaratnabh@gmail.com

RISK ASSESSMENT AND MANAGEMENT POLICY

Document Summary

Version Number	V1 – Effective from 16th July, 2026
Approved by	Board of Directors
Last date of renewal/ Version No.	N.A.
Current revision date/ Version No.	N.A.
Revision	Any revisions or modifications to this policy are to be formulated by the Chief Compliance Officer/Company Secretary and submitted to the Board for approval.

RISK ASSESSMENT AND MANAGEMENT POLICY

1. PREAMBLE

Pursuant to section 134(3)(n) of the Companies Act, 2013, this Risk Management Policy ("Policy") establishes the philosophy of **Sahanaratnabh Limited ("Company")** towards risk identification, analysis and prioritization of risks, development of risk mitigation plans and reporting on the risk environment of the Company. This Policy is applicable to all the functions, departments and geographical locations of the Company. The purpose of this Policy is to define, design and implement a risk management framework across the Company to identify, assess, manage and monitor risks. Aligned to this purpose is also to identify potential events that may affect the Company and manage the risk within the risk appetite and provide reasonable assurance regarding the achievement of the Company's objectives. This will present a wide approach to ensure that key aspects of risk that have a wide impact are considered in its conduct of business.

Risk is an event which can prevent, hinder or fail to further or otherwise obstruct the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise's ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

2. 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 objectives of the Policy can be summarized as follows:

(a) To safeguard the Company's and its subsidiaries'/ joint ventures' property, interests, and interest ofallstakeholders;

(b) To manage risks with an institutionalized framework and consistently achieving desired outcomes;

(c) To protect and enhance the corporate governance;

(d) To implement a process to identify potential / emerging risks;

(e) To implement appropriate risk management initiatives, controls, incident monitoring, reviews andcontinuousimprovement initiatives;

(f) Minimize undesirable outcomes arising out of potential risks; and

(g) To align and integrate views of risk across the enterprise.

3. COMPONENTS OF A SOUND RISK MANAGEMENT SYSTEM

The risk management system in the Company should have the following key features:

(a) Active board of directors, committee and senior management oversight;

(b) Appropriate policies, procedures and limits;

(c) Comprehensive and timely identification, measurement, mitigation, controlling, monitoring and reportingof risks;

(d) Appropriate management information systems at the business level;

(e) Comprehensive internal controls in accordance with current regulations and business size and scale; and

(f) A risk culture and communication framework

4. 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 entityare directed and managed by its Board and executive management.

5. RISK MANAGEMENT FRAMEWORK

The risk management committee formed by the Board shall periodically review the risk assessment and management 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 theirrespective areas of functioning.

6. RISK MANAGEMENT COMMITTEE

The Chairperson of the Risk Management Committee shall be a member of the Board of Directors and senior executives of the Company may be members of the Risk Management Committee.

The Risk Management Committee shall meet at least twice in a year. The quorum for a meeting of the Risk Management Committee shall be either two (2) members or one third of the members of the Risk ManagementCommittee, 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 one hundred and eighty (180) days shall elapse between any two consecutive meetings ofthe Risk Management Committee.

7. RISK MANAGEMENT PROCESS

Conscious that no entrepreneurial activity can be undertaken without assumption of risks and associated reward 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 decisions.

Broad outline of the framework is as follows:

a) Risk Identification: Management identifies potential events that may positively or negatively affectthe Company's ability to implement its strategy and achieve its objectives and performance goals.

Risks can be identified under the following broad categories. This is an illustrative list and notnecessarily anexhaustive classification.

(i) Internal risks include:

- Strategic Risk: Competition, inadequate capacity, high dependence on a single customer/vendor.
- Business Risk: Project viability, process risk, technology obsolescence/ changes, developmentofalternative products.
- Finance Risk: Liquidity, credit, currency fluctuation.
- Environment Risk: Non-compliances to environmental regulations, risk of health to people atlarge.
- Personnel Risk: Health & safety, high attrition rate, incompetence.

- Operational Risk: Process bottlenecks, non-adherence to process parameters/ pre-defined rules,fraud risk.
- 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, Data privacy and data availability.

(ii) External risks including:

- Sectoral Risk: Unfavorable consumer behavior in relation to the relevant sector etc.
- Sustainability Risk: Environmental, social and governance relates risks.
- Political Risk: Changes in the political environment, regulation/ deregulation due to changes inpoliticalenvironment.

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 measuredbased on a risk element's potential impact on revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion. 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 4as follows.

Impact	Score	Likelihood
Minor	1	Low
Moderate	2	Medium
High	3	High
Critical	4	Certain

The resultant "action required" is derived based on the combined effect of impact & likelihood and is quantified as per the summary below.

d) Risk Categorization:

The identified risks are further grouped in to (a) preventable; (b) strategic; and (c) external categoriesto homogenize risks.

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

(ii) Strategy 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 endeavours to focus on their identification and impact mitigation through 'avoid'/'reduce' approach that includes measures like business continuity plan / disasterrecovery 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, etc.

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

(i) Required action(s);

(ii) Required resources;

(iii) Responsibilities;

(iv) Timing;

(v) Performance measures; and

(vi) Reporting and monitoring requirements

The mitigation plan may also covers (i) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (ii) detective controls - responses to promptly revealundesirable 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.

Therefore, it is drawn with 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 ofthe risk events.

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.

"Fraud & Operations Risk" team works on a robust and dynamic real-time transaction monitoring mechanism via an automated rule engine already in place. This engine functions basis predefined set of rules. Our Operations Risk team comprises Risk Experts and Data Scientists who evaluate and monitor merchant transaction and market trends to raise alerts which are actioned as per the alert monitoring protocols.

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 outran 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 the Board or risk management committee with causes and mitigation actions 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 carry out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls 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 regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the CEO and the CFO, 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 describedabove, 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 functionalheads;

(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.

8. RESPONSIBILITY FOR RISK MANAGEMENT

Responsibility holder	Responsibilities
Board	The Company's risk management architecture is overseen by the Board and the policies to manage risks are approved by the Board. Its role includes the following: • Ensure that the organization has proper risk management framework • Define the risk strategy, key areas of focus and risk appetite for the company • Approve various risk management policies including the code of conduct and ethics • Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks
Audit Committee	The Audit Committee assists the Board in carrying out its oversight responsibilities relating to the Company's (a) financial reporting process and disclosure of financial information in financial statements and other reporting practices, b) internal control, and c) compliance with laws, regulations, and ethics (d) financial and risk management policies. Its role includes the following: • Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls; • Seeking regular assurance that the system of internal control is effective inmanaging risks in accordance with the Board's policies. • Ensure that senior management monitors the effectiveness of internal controlsystem. • Help in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter frame policies for control and monitoring.
Risk Management Committee	The Risk Management Committee, as constituted by the Board, is the key committee which implements and coordinates the risk function as outlined in this policy on an ongoing basis. Its role includes the following:

	• Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company; • Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems; • Periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity, and recommend for any amendment or modification thereof, as necessary; • Keep the Board of directors of the Company informed about the nature and content of its discussions, recommendations and actions to be taken; • Review the appointment, removal and terms of remuneration of the Chief Risk Officer (if any) • To implement and monitor policies and/or processes for ensuring cyber security; and any other similar or other functions as may be laid down by Board from time to time and/or as may be required under applicable law.

9. BUSINESS CONTINUITY PLAN

Business Continuity Plan (BCP) is a step-by-step guide to follow response to a natural or man-made crisis orany other incident that negatively affects the firm's key processes or service delivery. The objective of the Business Continuity Plan is to support the business process recovery in the event of a disruption or crisis. This can include short or long-term crisis or other disruptions, such as fire, flood, earthquake, explosion, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, Epidemic and Pandemic and other natural or man-made disasters.

10. 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.

11. DISCLAIMER CLAUSE

The risks outlined above are not exhaustive and are for information purposes only. Management is not an expert in assessment of risk factors, risk mitigation measures and

management's perception of risks. Readers are therefore requested to exercise their own judgment in assessing various risks associated with the Company.

12. PERIODICAL REVIEW OF EFFECTIVENESS

Effectiveness of risk management framework is ensured through periodical review of this Policy, provided that such review should be undertaken at least once in two years. As the risk exposure of any business may undergo change from time to time due to the changing industry dynamics, evolving complexity and continuously changing environment, the updation and review of this Policy will be done as and when required, by the risk management committee to ensure it meets the requirements of legislation and the needs of organization.

13. APPROVAL OF THE POLICY

The Board will be the approving authority for the company's overall risk management system. The Board will, therefore, approve this Policy and any amendments thereto from time to time.

14. EFFECTIVE DATE

This Policy is effective from the date of approval of its approval by the Board of Directors of the Company.

15. DISCLOSURES

The Company shall disclose the Policy on its website.

****

Footnote

1. The Board of Directors of SahanaRatnabh Limited at its meeting held on July 16, 2026, has adopted this Policy for the first time.



