SAMHI HOTELS LIMITED

RISK MANAGEMENT POLICY

1. PREAMBLE

Pursuant to Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations") and Section 134(3) of the Companies Act, 2013, SAMHI Hotels Limited ("**Company**") has developed a risk management framework wherein, key risks have been identified, measurement criteria of the key risks indicators defined and mitigation plans detailed. The Board has approved this risk management policy ("**Policy**") on **27th March, 2023.**

This Policy shall come into force with effect from the date the SEBI Listing Regulations take effect with respect to the Company.

2. LEGAL FRAMEWORK OF THE POLICY

(a) The Companies Act, 2013 ("**Companies Act**") lays down the following:

(i) As per Section 134 of the Companies Act, the report of the board of directors of a listed company must include a statement indicating the development and implementation of a risk management policy for the company including the identification of elements of risk, if any, which in the opinion of the board of directors of the company, may threaten the existence of the company;

(ii) The audit committee of a listed company shall act in accordance with the terms of reference specified in writing by the board of directors of the company, which shall, inter-alia, include the evaluation of risk management systems as per Section 177 of the Companies Act;

(iii) Further, the independent directors of a company, should satisfy themselves that systems of risk management are robust and defensible as per Schedule IV of the Companies Act.

(b) It has therefore become mandatory for the companies such as the Company, to prepare a comprehensive framework of risk management for the assessment of risks and to determine the responses to these risks, such that the board of director of the Company ("**Board**") feels, may threaten the existence of the Company.

3. OBJECTIVES OF THE POLICY

(a) The risk and safety management system adopted by the Company will enable the Company to identify problem areas with respect to regulations, competition, business risk, development risks, investments, acquisition and retention of talent, health & safety. business risk, *inter- alia*, further includes financial risk, political risk, fidelity risk, legal risk, employee, guest, asset safety and safety of community and to establish a prevention system to safeguard the future.

(b) The Board determines the Company's tolerance for risk and is committed to a risk management system that balances the need to preserve long term values, prudently manages the hotel properties, maintain good relationships with partners and joint ventures, and facilitates a culture of innovation.

4. CONSTITUTION OF RISK MANAGEMENT COMMITTEE

(a) The Board has appointed a risk management committee ("**Committee**") comprising of directors and key senior executives of the Company. The Committee:

(i) identifies new risks facing the Company and reviews existing risks for continuity and relevance;

(ii) identifies key risk owners who will be responsible for managing individual risks;

(iii) recommends key risk indicators ("**KRI**(**s**)") and measurement criteria;

(iv) periodically reviews the Policy and risk management framework of the Company;

(v) recommends mitigation plans as identified by individual key risk owners; and

(vi) the status of each risk along with mitigation plans is presented to the Board.

5. APPLICABILITY

This Policy is applicable to all the businesses of the Company.

6. 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 to enable management to take informed decisions. If deemed fit by the Management, the Company may engage reputable third parties to perform certain functions and support the Company in the risk management process, from time to time.

Broad outline of the framework is as follows:

(a) Risk Identification: Management identifies areas that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. 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:

(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, 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.
- 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 include:

- 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 in political environment.

(b) Root Cause Analysis: Root cause analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.

(c) Risk Scoring: An analysis of all internal processes and support functions is done to determine the likelihood and impact of risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on 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.

(d) Risk Categorisation:

The identified risks are further grouped in to (a) High; (b) Medium; and (c) Low risks.

- High Risk - Represents critical control weaknesses requiring prompt action to mitigate

information systems or business process vulnerabilities. Adequate compensating controls do not exist to mitigate risk exposure or may not be sufficient given the impact of a risk occurrence should it occur.

- Medium Risk - Represents moderate control weaknesses requiring near-term management focus to strengthen existing controls. Some compensating controls are present but additional controls are necessary to further mitigate risk exposure.
- Low Risk - Represents minor control weaknesses requiring management focus to enhance existing controls. Compensating controls are present to mitigate exposure (or if not the impact of a risk occurrence is minor) but opportunities exist to enhance controls or improve operating efficiency.

(e) 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 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.

(f) 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 self-assessments throughout the year.

(g) 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.

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.

(h) Risk reporting:

Periodically, key risks are reported to the Board or 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.

(i) 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.

7. 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 in managing risks in accordance with the Board's policies. • Ensure that senior management monitors the effectiveness of internal control system • 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: • Formulation of a detailed risk management policy which 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; and (c) business continuity plan; • 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, as and when amended from time to time, including the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.

8. AMENDMENT

The Board and the Committee may review, amend, abrogate, modify or revise any or all provisions

of this Policy from time to time. However, amendments in the Companies Act or in the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, that mandatorily apply to the Company shall be deemed to be incorporated in this Policy and shall be binding.

9. DISCLAIMER CLAUSE

The Company cautions the readers that the risks outlined above are not exhaustive and are for information purposes only. The Company is not an expert in assessment of risk factors, risk mitigation measures and management's perception of risks. The readers are therefore requested to exercise their own judgment in assessing various risks associated with the Company.