SAYAJI HOTELS (INDORE) LIMITED
Registered Address: H-1 Scheme No. 54, Vijay Nagar, Indore, Madhya Pradesh, India, 452010Email ID: cs@shilindore.com Website: www.shilindore.com
Phone No.: 0731-4750012

Risk Management Policy

Risk Management Policy

1. Introduction

Risk is an inherent aspect of the dynamic business environment and managing its potential consequences means anticipating those events that could generate adverse and costly outcomes for the organization, while taking actions to avert and/or diminish the effects of such events. Risk Management Policy helps organizations to put in place effective frameworks for taking informed decisions about risks. To minimize the adverse consequence of risks on business objectives, Sayaji Hotels (Indore) Limited (**"the Company"**) has framed this Risk Management Policy. The guidance provides a route map for risk management, bringing together policy and guidance from Board of Directors. The objective of this document is to articulate an effective Risk Management Policy and process for the Company to promote a proactive approach in identifying, evaluating, reporting, and mitigating risks associated with the business and, in turn, to ensure sustainable business growth with stability.

2. Regulatory Requirements:

Pursuant to Regulation 17(9)(b) and Regulation 21(5) of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 and Sections 134(3)(n) and 177(4)(vii) read with Schedule IV of the Companies Act, 2013, the Company has established a framework for identification, assessment, monitoring, and mitigation of risks. The Board oversees the implementation of the risk management policy and internal financial controls, while the Audit Committee reviews the adequacy and effectiveness of the risk management systems. Independent Directors also satisfy themselves that the financial controls and risk management systems are robust and effective.

Accordingly, the Risk Management Policy shall include:

- Framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, Environment, Social and Governance related risks), information, cyber security risks, legal and regulatory risks or any other risk as may be determined by the Board;
- Measures for risk mitigation including systems and processes for internal control of identified risks; and
- Business Continuity Plan.

3. Risk Organization Structure and Risk Management Framework:

The Board of Directors is responsible for overseeing the Company's risk management framework and ensuring timely identification, assessment, monitoring, and mitigation of key risks and opportunities in alignment with the Company's objectives. The Board also reviews the adequacy of internal control systems, financial controls, and compliance with applicable laws and regulations, and may seek assistance from external experts wherever required.

The Managing Director and senior management are responsible for implementing and monitoring the risk management framework across the organization. Risk management is integrated into business processes through continuous identification, evaluation, mitigation, and reporting of risks.

The Company has established an internal control and internal audit framework covering all major business functions and operating units, including operations, finance, procurement, human resources, revenue management, and safety. These systems are designed to ensure operational efficiency, safeguarding of assets, reliability of financial reporting, compliance with applicable laws, and effective management of business risks.

The Board periodically reviews the key risks and mitigation measures, and all significant business proposals are evaluated considering the associated risks and uncertainties.

3.1. Risk Identification:

The Company continuously identifies internal and external risks based on business processes, past experiences, audit observations, industry trends, and regulatory developments. Risks may include financial, operational, human resource, political, sectoral, ESG, legal, compliance, and cyber security related risks.

3.2. Risk Assessment and Analysis

Identified risks are evaluated based on their likelihood and potential impact. The Company assesses criticality of risks and prioritizes them for mitigation through appropriate controls, monitoring mechanisms, and management actions.

Key risks monitored by the Company include:

- Financial and operational risks
- Human resource risks
- Political and regulatory risks
- Environmental, Social and Governance (ESG) risks
- Sectoral and economic risks
- Legal and compliance risks
- Cyber security and information technology risks

3.3 Risk Mitigation and Control

The Company implements suitable mitigation measures, internal controls, review mechanisms, and contingency plans to manage identified risks. The internal audit function periodically reviews the effectiveness of such controls and reports key observations to the management and the Audit Committee.

3.4 Risk Appetite

The Company shall undertake its business activities within an acceptable level of risk consistent with its strategic objectives, financial strength, regulatory obligations and stakeholder expectations. Risks exceeding the Company's acceptable risk tolerance shall be appropriately evaluated and escalated to the Board of Directors for necessary guidance and decision.

3.5 Risk Monitoring and Reporting

Risks and mitigation measures are regularly monitored by the senior management and periodically reviewed by the Board to ensure effectiveness of the risk management framework and timely corrective actions, wherever necessary.

The Risk Reporting Matrix: A risk reporting matrix is matched with specific likelihood ratings and Out-turns ratings to a risk grade of low (yellow), medium (orange) and high (red).

S. No.	Out-turns	Likelihood			
		1	2	3	4
		Rare	Unlikely	Likely	Almost certain
4	High				
3	Medium				
2	Low				
1	Insignificant				

4. Business Continuity Plan (BCP)

4.1 Introduction

The Company has established a Business Continuity Plan ("BCP") to ensure continuity of critical business operations during emergencies, disruptions, or unforeseen events. The BCP provides a framework for minimizing operational disruptions and safeguarding the interests of stakeholders, employees, assets, and business operations.

4.2 Purpose of BCP

The purpose of the BCP is to enable the Company to respond effectively to disruptions and restore essential operations within a reasonable timeframe. The plan also aims to strengthen operational resilience and ensure business continuity during crisis situations.

4.3 Objectives of BCP

The key objectives of the BCP are to:

- Ensure continuity of critical business functions;
- Minimize operational, financial, and reputational impact arising from disruptions;
- Safeguard employees, assets, systems, and data;
- Establish effective communication and response mechanisms; and
- Facilitate timely recovery and restoration of normal operations.

4.4 Direction and Control

The Board of Directors is responsible for overseeing and reviewing the BCP framework, including disaster response, business impact assessment, recovery planning, and communication protocols. The Board or any authorized officer may activate the BCP, whenever required.

4.5 BCP Activation and Response

The Company continuously evaluates potential events that may impact business continuity, including natural disasters, fire, power or system failures, cyber security incidents, pandemics, civil disturbances, terrorism, supply chain disruptions, and other unforeseen events. Appropriate response and escalation procedures are implemented depending upon the nature and severity of the event.

4.6 Communication and Recovery Measures

The BCP provides for coordination and communication among management, employees, customers, suppliers, and other stakeholders during crisis situations. The Company also maintains recovery and contingency measures, including alternate operational arrangements, system restoration procedures, and business recovery protocols to ensure timely restoration of operations.

4.7 Review and Monitoring

The BCP is periodically reviewed and updated to align with operational requirements, regulatory expectations, and emerging business risks. The Company may also, wherever considered necessary, conduct testing or simulation exercises of the Business Continuity Plan to assess its effectiveness and implement appropriate improvements based on the observations.

5. Risk Management Committee:

Pursuant to Regulation 21 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, constitution of a Risk Management Committee is applicable to top 1,000 listed entities determined on the basis of market capitalization as at the end of the immediate previous financial year. As the Company does not fall within the aforesaid criteria as on date, the requirement of constitution of a Risk Management Committee is presently not applicable to the Company. However, the Board of Directors shall continue to oversee and monitor the risk management framework and processes of the Company in accordance with applicable provisions of law.

6. Policy review

a. This Policy is framed based on the provisions of the SEBI Regulations and any other applicable law

b. In case of any subsequent changes in the Regulations or any other applicable law which make the provisions in the Policy inconsistent with the Listing Regulations or any other applicable law, the Regulations and such law shall prevail over the Policy

and the provisions in the Policy shall be modified in due course to make it consistent with the law.

c. The Policy shall be reviewed once in every two years by the Board of Directors.

****

This Policy was approved by the Board of Directors at its meeting held on August 11th, 2023 and was last reviewed and amended on 16th May, 2026