RISK MANAGEMENT POLICY

Under Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI LODR")

RISK MANAGEMENT POLICY

1. PREAMBLE

Section 134(3)(n) of the Companies Act, 2013 requires that the report by the Board of Directors laid at the general meeting shall include a statement on the development and implementation of a risk management policy for the company. Section 177(4)(vii) of the Companies Act, 2013 ("Act") provides that Audit Committee shall evaluate the internal financial controls and risk management systems of the company. Regulation 17(9) (a) of SEBI LODR, inter alia, mandates laying down the procedures for risk assessment and minimization. Further Regulation 17(9)(b), provides the Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the company. Accordingly, the Board of Directors (the "**Board**") of Smartworks Coworking Spaces Limited has adopted this policy .

2. DEFINITIONS

"**Company**" means Smartworks Coworking Spaces Limited.

"Risk" means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may or may not be avoidable by pre-emptive action.

"Risk Management" is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

"Risk Management Committee" means the Committee formed by the Board as under Regulation 21 of the SEBI LODR.

"**Senior Management**" means officers and personnel of the Company who are members of its core management team comprising all members of management one level below the Chief Executive Director or Managing Director or Whole Time Director or Manager, including the functional heads and shall specifically include company secretary and Chief Financial officer.

Words and expressions used and not defined in this Policy shall have the meaning ascribed to them in the SEBI LODR, the Securities and Exchange Board of India Act, 1992, as amended, the Securities Contracts (Regulation) Act, 1956, as amended, the Depositories Act, 1996, as amended, or the Companies Act, 2013 and rules and regulations made thereunder.

3. RISK MANAGEMENT COMMITTEE

The Board has formed a Risk Management Committee (RMC) in line with the requirements of the Listing Regulations. The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

4. ROLES AND RESPONSIBILITIES

The Risk Management Committee shall be responsible for framing, implementing and monitoring the risk management policy for the company including evaluating the adequacy of risk management systems and ensuring that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;The Audit Committee shall review risk management systems on an annual basis.

5. RISK MANAGEMENT SYESTEM/PROCESS

The Risk Management process involves the following phases:

- Risk identification
- Risk analysis
- Risk assessment
- Risk mitigation

Risk Identification

Risk identification involves identification of sources of risk, areas of impacts, events (including changes in circumstances), their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity.

The internal as well as external risks for the Company can be broadly categorized into:

i. Financial risk
ii. Operational risk
iii. Sectoral risk
iv. Sustainability risk (ESG related risks)
v. Information risk
vi. cyber security risk
vii. any other risk as may be determined by the Committee

Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk
- the trigger events that would lead to the occurrence of the risks
- the positive and negative consequences of the risk
- the likelihood that those consequences can occur

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

Risk Assessment

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 measured based on a risk element's potential impact on revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize.

Risk Mitigation

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:

1. Risk Avoidance (eliminate, withdraw from or not become involved)
   Risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. Risk Reduction (optimize - mitigate)
   Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

3. Risk Sharing (transfer – outsource or insure)
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk.

4. Risk Retention (accept and budget)
   Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are

retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

In addition to the broad steps and processes outlined above, the Company has in place a Enterprise Risk Management Framework also to identify, assess, monitor, and manage risks applicable to its operations and business activities.

6. RISK MONITORING & REPORTING

a. All the Head of Departments/Senior Management Personnel ("HODs") under the guidance of the Managing Director/Whole time Director has the responsibility for over viewing management's processes and results in identifying, assessing and monitoring risk associated with Company's business operations and the implementation and maintenance of policies and control procedures to give adequate protection against key risk. In doing so, the HOD considers and assesses the appropriateness and effectiveness of management information and other systems of internal control, encompassing review of any external agency in this regard and action taken or proposed resulting from those reports. Setting up of proper internal control systems to analyse the probable risks and mitigating it pro-actively.

b. 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.

c. The statutory auditors carries 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.

d. The Board shall include a statement in Board's report indicating the 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.

7. BUSINESS CONTINUITY PLAN

Business continuity plan covers readily identifiable risks, including technical problems, fires, natural disasters and other emergencies. It includes maintaining business functions or quickly resuming them in the event of a major disruption, whether caused by a fire, flood or any other act of god, which is out of reasonable control. A business continuity plan outlines procedures and instructions an organization must follow in the face of such disasters; it covers business processes, assets, human resources, business partners, etc. The business continuity plan may be reviewed and amended by the Risk Management Committee.

8. AMENDMENTS AND REVIEW OF THIS POLICY

This Policy shall be reviewed by the Risk Management Committee periodically, at least once in two years, including by considering the changing industry dynamics and evolving complexity. Any subsequent amendment and modification in the Act or the Listing Regulations and any other laws in this regard shall automatically apply to this Policy.

In case of any amendment(s), clarification(s), circular(s) etc. issued by the relevant authorities, not being consistent with the provisions laid down under this policy, then such amendment(s), clarification(s), circular(s), etc. shall prevail upon the provisions hereunder and this policy shall stand amended accordingly from the effective date as laid down under such amendment(s), clarification(s), circular(s), etc.

9. EFFECTIVE DATE

This policy shall be effective from the date of its adoption by Board of Directors.

Version Control:

Sr. No.	Version No.	Date of approval
1.	**V1**	July 31, 2024
2.	**V2**	June 25, 2026