Policy Title	Risk Management Policy ("Policy")
Entity	South City Projects (Kolkata) Private Limited *(formerly known as South City Projects (Kolkata) Limited)* ("Company")
Effective Date	From the date of approval by the Board of Directors of the Company i.e., August 3, 2026.
Applicability	This policy is applicable to the Company.
Introduction & Purpose	The purpose of the risk management policy is to provide guidance with regards to managing risks so as to support the achievement of corporate objectives and comply with applicable regulations. A risk management policy is a critical component of effective governance and strategic management, which helps our organization navigate uncertainties and make informed decisions to achieve our strategic objectives. This policy is framed in line with the requirement of Section 134(3) and Section 177(4) of the Companies Act, 2013, and other applicable laws, including any rules, regulations or guidelines, framed thereunder (including any amendment or re-enactment thereof). An element of risk is associated with all activities carried out by the Company and a practice of risk management enables the Company to proactively identify, assess and remediate the risks posed to the Company. The responsibility of managing risk lies with all employees associated with the Company. This policy outlines the Company's risk management process and sets out the responsibilities of the Board of Directors (BOD), its designated committees, if any, senior management and others within the Company. The specific objectives of the Risk Management Policy are: • **Board visibility:** To enable visibility and oversight of the Board on risk management system and material risk exposures of the Company. • **Risk identification and evaluation**: To ensure all risks across the Company are identified that could impede the Company's ability to achieve its objectives. To ensure all risks are evaluated through a standardized process and consolidated across the organization to priorities the impact on the Company. • **Risk reporting and continuous improvement:** To ensure that risks are reported internally as well as external stakeholders as per relevance and

	significance. To establish a process of continuous improvement in risk management by regularly reviewing and updating risk assessments and mitigation strategies. • **Risk appetite:** To establish and maintain the risk appetite of the Company within the defined threshold levels by tracking the early warning indicators / risk indicators.
Risk (as defined in **Standard of Internal Audit (SIA) 13 issued by the Institute of Internal Auditors)**	Risk is an event which can prevent, hinder and 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 disadvantages, 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. **Strategic Risk** are associated with the primary long-term purpose, objectives and direction of the business. **Operational Risks** are associated with the on-going, day-to-day operations of the enterprise. **Compliance Risks** are risks associated with the compliance with various Acts, Rules, Regulations and other compliances applicable to the Company. **Financial Risks** are related specifically to the processes, techniques and instruments utilized to manage the finances of the enterprise, as well as those processes involved in sustaining effective financial relationships with customers and third parties. **Knowledge Risks** are associated with the management and protection of knowledge and information within the enterprise. **Inherent Risks**: The risk that an activity poses if no controls or other mitigating factors were in place (the gross risk or risk before controls). The risk management process focuses on areas of high inherent risk, with these documented in the Risk Register. **Residual Risks:** Upon implementation of treatments there will still be a degree of leftover risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances. **Significant Risk:** Significant risks include those risks that have a high likelihood and high impact or where there is limited ability for mitigation by the Company. These risks are identified and assessed based on the Company's expertise, judgement and knowledge.

	Risk Appetite: Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
Importance of Risk Management	A certain amount of risk taking is inevitable if the organization has to achieve its objectives. Effective management of risk helps to manage innovation and improve performance by contributing to: a) Certainty and fewer surprises, b) More effective management of change, c) More efficient use of resources, d) Better management at all levels through improved decision making, e) Reduced waste and fraud, and better value for money, f) Management of contingent and maintenance activities.
Approach to Risk Management	Enterprise risk management philosophy is to enable the achievement of the Company's strategic objectives by identifying, analyzing, assessing, mitigating, monitoring, preventing, and governing any risks or potential threat to these objectives. While the achievement of strategic objectives is a key driver, our values, culture and our obligation & commitment to employees, customers, investors, regulatory bodies, partners, and the community around us are the foundation on which our risk management philosophy is based. The systematic and proactive identification of risks and mitigation thereof shall enable effective or quick decision-making, enable business continuity, and shall improve the performance of the organization.
Organization Structure	- BOD - Designated Committee(s) if any or Senior management - Risk Owners
Responsibility of BOD	The BOD of the Company shall authorise, a designated committee if any, or senior management, to discharge the function of a risk management committee. The BOD may define the role and responsibility designated committees, if any, or senior management, which shall include the monitoring and reviewing of the risk management plan and such other functions as it may deem fit including ESG and cyber security, as applicable. The Board, has the responsibility to review and ensure that: a) The ACB has, once in two years, reviewed the risk management framework / policy to satisfy itself that it continues to be sound and effectively identifies all areas of potential risk b) Adequate policies and processes have been designed and implemented to manage identified risks c) A regular program of audits is undertaken to test the adequacy of and compliance with prescribed policies; and proper remedial action is undertaken to redress areas of weakness.

Responsibilty of Designated Committee / Personnel	The designated committee, if any, or designated personnel shall carry out the roles and responsibilities as applicable to Debt Listed entities. The designated committee, if any, or designated personnel 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 is necessary The role of the committee shall, *inter alia,* include the following: a) To formulate a detailed risk management policy which should include: i. 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 Committee. ii. Measures for risk mitigation including systems and processes for internal control of identified risks. iii. Business continuity plan. b) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company; c) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems; d) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity; e) To keep the BOD informed about the nature and content of its discussions, recommendations and actions to be taken; The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the ACB. The designated committee, if any, or designated personnel shall coordinate its activities accordingly, so that there is no overlap with the other activities, as per the framework laid down by the BOD.
Chief Risk Officer	The CRO, if any and in his absence, the Chief Financial Officer (**"CFO"**), performing the functions of the CRO, will work with members of ACB and

	risk owners in establishing and implementing the risk management process effectively in their areas of responsibilities. The CRO, if any, shall provide inputs and insights in the establishment, monitoring and structuring risk management processes and further monitor its compliance in accordance with relevant provisions of the policy. *Key roles and responsibilities:* a) Ensure updation of risk management policy pursuant to the organization's risk management purpose. b) Validate that the risk management policy is implemented in each department and that all significant risks are recognized, acknowledged, and effectively managed. c) Act as convener in meetings d) Discuss with risk owners and finalize the ownership of risk registers, thereby entrusting a person with the responsibility of completion of the risk register. e) Coordinate with Risk Owners for periodic update of risk registers. f) Advise the Risk Owner in identifying and assessing risks, creating mitigation plans, and developing key risk indicators. g) Assess ratings of identified enterprise risks and prioritize them for its presentation to the Designated Committee(s) or Designated personnel as the case may be. h) Update the Designated Committee(s) or Designated personnel as the case may be on a periodic basis with updates in risk policy, new risks identified, focus risks, mitigation plans. i) Act as a coordinator between the BOD and the Designated Committee(s) or Designated personnel as the case may be. j) Present the key business risks faced by the organization and their mitigation plans to the Board on behalf of the Designated Committee(s) or Designated personnel as the case may be. k) Create a framework for holistic enterprise view to risk management process and ensure inter department dependencies are addressed. l) Sign off risk assessment templates in coordination with Risk Owners.
Risk Owner(s)	Risk Owners are head of respective function/department/location or business leaders responsible for overseeing the management, monitoring, response and emerging changes related to their assigned risks. *Key roles and responsibilities of Risk Owner(s):* a) Ownership of risk in their respective function / department. b) Ensure that risks for their respective functions/department/location are identified and assessed as per risk assessment framework c) Understand and take responsibility for the management of risk in their business units/functional areas

	d) Ensure risk registers are maintained and updated on a quarterly basis. Ensure effective and efficient coverage of applicable risks e) Assess ratings of identified enterprise risks and prioritize them for the presentation to the Designated Committee(s) or Designated personnel as the case may be f) Facilitate the identification and implementation of risk mitigation plans g) Track and measure the effectiveness of the mitigation plans and ensure risk mitigating plans are mapped against prioritized risks. h) Approve risk assessments and mitigation of risks of respective function / department for validation by the CRO.
General Responsibilities	Every staff member is responsible for effective management of risk including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk reduction strategies including the promotion and training of the risk management process to staff. Risk management processes should be integrated with other planning processes and management activities.
Risk Management Procedure	Risk management is a continuous process that is accomplished throughout the life cycle of a company. It is an organized methodology for continuously identifying business objectives; information assets; and the underlying assets (e.g., hardware, software, databases, networks and facilities) and measuring the unknown; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction. Effective risk management depends on risk management planning; early identification and analyses of risks; early implementation of corrective actions; continuous monitoring and reassessment; and communication, documentation, and coordination. The assessment of countermeasures should be performed through a cost benefit analysis where controls are selected to reduce the risk to a level acceptable to the management. This process may be based on the following: a) The cost of the control compared to the benefit of minimizing the risk b) Management's risk appetite c) Preferred risk-reduction methods
Risk Management Methodology	The methodology adopted by the Company for managing and treating its risks and that of Company is defined as follows: **Risk Identification:** This involves continuous identification of events that may have negative impact on the Trust's ability to achieve goals.

Identification of risks, risk events and their relationship are defined on the basis of discussion with the risk owners and secondary analysis of related data, previous internal audit reports, past occurrences of such events etc.

In line with SEBI LODR, the Company shall classify all applicable enterprise risks for the Company in the below stated broad categories:

- **Sectoral Risks**: Key sectoral risks applicable to all entities in the real estate sector

- **Operational Risks**: Inadequate or failed processes or people capabilities
- **Financial Risks**: Related to Financing / financial transactions
- **Information Risks**: Possible information / data leakage, misuse, or loss
- **Cyber Security Risk**: Cyber threats / frauds
- **Sustainability (ESG)**: Related to environment, social and governance
- Others

Note- Legal & Compliance related risks may be classified under Governance (ESG risk) or Operational risk, as applicable.

Risk Prioritization: Once risks have been identified, risks should be prioritized by evaluating the uncertainty of risk events or conditions in terms of:

- **Impact:** Severity of a risk, if it were to occur.

- **Likelihood:** Probability of a risk occurring.

- **Velocity:** Rapidness of a risk manifesting itself, once it starts to unfold.

Risk Criticality Score (using the rating scale)

The risk criticality score determines what risks are reported at the senior management level and the Designated Committee(s) or Designated personnel as the case may be. For the Company, a rating scale is suggested to capture the management's assessment of the potential impact, likelihood and velocity.

Impact X Likelihood + Velocity = Risk Criticality Score

Risk Mitigation: Risk mitigation options are analyzed to determine the appropriate risk treatment strategy, considering cost-benefit analysis. Risk Owners identify response options considering cost-benefit analysis when designing risk responses.

Each risk response could be categorized into one of the 4Ts – Terminate, Take, Treat, or Transfer - also called the 4T's of risk strategy.

<table>
<tr><td></td><td>Risk response categories can be summarized as follows:

Risk Avoidance, risk reduction, risk acceptance and risk transfer

<table>
<tr><th>Category</th><th>Risk Responses</th></tr>
<tr><td>Terminate/ Avoid</td><td>Actions to exit the activity that causes the risk. For example, risks Avoid classified with High Impact as well as High Likelihood could be handled in this manner.</td></tr>
<tr><td>Take/Accept</td><td>Take no action to affect likelihood and impact; accept and live with the risk exposure. For example, risks classified with Low Impact and Low Likelihood could be handled in this manner</td></tr>
<tr><td>Treat/ Reduce</td><td>Actions to reduce the risk exposure by reducing the likelihood, impact, or both</td></tr>
<tr><td>Transfer/ Share</td><td>Actions to reduce the likelihood or impact by transferring the full or portion of the risk to another entity/ counterparty</td></tr>
</table>
</td></tr>
<tr><td></td><td>Monitor Risk: Risk management uses the output of a risk assessment and implements countermeasures to reduce the risks identified to an acceptable level. This policy provides a foundation for the development of an effective risk register, containing both the definitions and the guidance necessary for the process of assessing and mitigating risks identified within functions and associated processes.

In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of consolidated risk register along with the business justification and their status shall be continuously monitored and periodically presented to ACB.</td></tr>
<tr><td>Risk Reporting</td><td>Process of risk reporting:

CRO or an independent firm of Chartered accountants will place the Risk register with significant risks, the key indicators, the risk category and the effectiveness of the mitigation plans. On an ongoing basis, when a new or emerging risk is identified, Risk owners of respective departments will notify CRO.

After reviewing the Risks, the CRO will determine whether the risk identified warrants inclusion in the risk register.
Risk included in the risk register in the half year will be reported to Board or designated personnel, if any, in the next meeting.

Risk reporting of adverse events:</td></tr>
</table>

	All adverse events and near misses must be recorded and reported. All adverse events, as may be decided as significant by risk owner in consultation with CRO, should be reported, even if some time has passed since the event occurred. The company will periodically review its risk profile. The objective of this review is to assess movement in existing risks and identify any new or emerging risks.
Risk Training, Awareness, Communication & Culture	The commitment from Company extends to providing comprehensive training programs for employees at all levels, clearly delineating roles and responsibilities, and elevating awareness of risk across the organization. Emphasis is placed on open communication channels, efficient reporting procedures, and feedback mechanisms to instill a proactive approach to risk management. Leadership is committed to actively supporting and exemplifying the desired risk culture, integrating risk considerations into performance management processes. The organization encourages continuous learning, measurement of risk management initiatives, and the assimilation of lessons learned to continually fortify the ability to identify, assess, and manage risks effectively. Through these concerted efforts, the aim is to cultivate a positive risk culture where every employee is empowered to contribute to collective success by actively participating in risk management processes.
Business Continuity Plan	The The Board, designated committees / personnel, if any, shall ensure that a detailed business continuity plan is implemented which will inter alia cover the identification of risk, determination of such risks that will have an impact on the Company business operations, implement safeguards and procedures to mitigate such risks, testing procedures for mitigating the risks and reviewing the processes.
Review / Amendment	This policy may be reviewed by the Board from time to time. However, any subsequent amendment / modification in the SEBI LODR or the Companies Act, 2013 or any other governing Act/Rules/Regulations or re-enactment, impacting the provisions of the Policy shall automatically apply to the Policy and the relevant provision(s) of the Policy shall be deemed to be modified and/or amended to that extent, even if not incorporated in the Policy.