POLICY ON RISK MANAGEMENT

OF

SEMBCORP GREEN INFRA LIMITED

INDEX

1. Preamble

- Section 134(3)(n) of the Companies Act, 2013 ("**Act**") requires a statement to be included in the report of the board of directors of a company indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the board of directors of a company, may threaten the existence of the company.

- Further, Regulation 17(9) and Clause C, Part D of Schedule II of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("**LODR**") requires that companies set out procedures to inform the board of directors of the company of risk assessment and minimization procedures and make the board of directors responsible for framing, implementing and monitoring the risk management plan of the company. However, the provision of LODR to the extent incorporated in this policy shall be applicable to the Company from the date of listing of its shares on the Recognized Stock Exchange(s).

- Accordingly, the board of directors ("**Board**") of Sembcorp Green Infra Limited (formerly known as Sembcorp Green Infra Private Limited) ("**Company**") has adopted the Risk Management Policy ("**Policy**") for risk management and mitigation.

2. Objective

Sembcorp Green Infra Limited (SGIL), also referred to as the Company, is part of Sembcorp Industries Limited (SCI) group or Sembcorp Group. The company has adopted relevant governance, operational, financial, sustainability, cyber security and related policies and frameworks of the Sembcorp Group. The purpose of this Risk Management Policy (RMP) is to define SGIL's overall approach to manage its risks and provide a consistent approach in identifying and managing these risks. Comprehensive risk management framework provided by the RMP, and its effective implementation reinforce the long-term sustainability of the Company.

This Policy aims to provide a framework for the effective management of risk as required by the Act and in line with the LODR. Through this Policy, the Company intends to establish a robust framework for Identification, Reduction, Mitigation and Management of risks (such as Strategic, Financial, Operational, Compliance, Reputational, Sustainability and Technological Risks) that the Company may be subject to on periodical basis. It also prescribes the risk management governance structure along with the roles and responsibilities of various stakeholders within the organization.

Key objectives of the 'Policy" is to:

- Ensure achievement of the Company's vision & strategic priorities in line with its core values.
- To establish a framework for the company's risk management process and to ensure companywide implementation.
- Integrate risk management in the culture and strategic decision-making in the organization.
- To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed.
- To ensure proactive rather than reactive management.
- Enable compliance with appropriate regulations and adoption of leading practices.
- Anticipate and respond to changing economic, social, political, technological environmental and legal conditions in the external environment.

Managing Risk is an integral part of SGIL's business activity. In pursuit of its strategic objectives, the Company makes decisions and takes actions that have uncertain outcomes. For our business, a risk is defined as any possibility of realizing an outcome that is worse than the outcome desired. RMP provides the framework to proactively identify, analyze and report the Risks and their potential impact on the sustainability, growth, and performance of the Company. The Company employs different Risk Management approaches to limit the potential impact of these Risks. The Risk Management strategies include avoiding the risk, reducing the negative effect of the risk, transferring the risk to another party, and accepting some or all the consequences of a particular risk.

The scope of the policy extends to SGIL, and any entity, business and asset owned by it. This policy covers events within the company & events outside the company which have a bearing on the company's business. It applies to all employees of SGIL and to every part of SGIL's business and functions.

3. Risk Governance Structure

A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities for the management of risks on a day-to-day basis.

3.1 Roles and Responsibilities

3.1.1 Board of Directors

The Board of Directors (BoD) have overall responsibility for the governance of the Company's risk management. The BoD approves the company's risk policies, and oversees management in the design, implementation, and monitoring of risk management systems.
The composition and meeting frequency of the Board shall be governed by the Companies Act, 2013, the Articles of Association of the Company and, upon listing, applicable SEBI Listing Regulations. The Board shall periodically review risk management matters, including updates and recommendations placed by the Risk Management Committee.

3.1.2 Risk Management Committee of the Board

The Board has formed a committee, namely the Risk Management Committee ("Committee"), with the overall responsibility of overseeing and reviewing risk management across the Company.

The terms of reference of the Committee are as follows:

- To formulate a detailed risk management policy which shall include a framework for identification of internal and external risks specifically faced by the listed entity, including but not limited to financial, operational, strategic, sustainability (ESG related risks), cyber security risks or any other risk as may be determined by the committee, measures for risk mitigation including systems and processes for internal control of identified risks and a business continuity plan.
- To periodically review the risk management policy at least once in 2 (two) years, including by considering the changing industry dynamics and evolving complexity.

- To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- To approve the process for risk identification and mitigation
- To decide on risk tolerance and appetite levels, recognizing contingent risks, inherent and residual risks including for cyber security
- To monitor the Company's compliance with the risk structure. Assess whether current exposure to the risks it faces is acceptable and that there is an effective remediation of non-compliance on an on-going basis.
- To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company.
- To keep the Board of directors of the Company informed about the nature and content of its discussions, recommendations and actions to be taken.
- To approve major decisions affecting the risk profile or exposure and give appropriate directions.
- To consider the effectiveness of decision making process in crisis and emergency situations.
- To balance risks and opportunities
- To generally, assist the Board in the execution of its responsibility for the governance of risk
- To review and submit quarterly Risk Report to the Board.
- To consider the appointment, removal and terms of remuneration of the Chief Risk officer (if any)
- The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice outsiders with relevant expertise, if it considers necessary in order to carry out its functions effectively. The Committee shall coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board
- Any other similar or other functions may be laid down by Board from time to time and/or as may be required under the Act and the LODR.

3.1.3 Chief Risk Officer (if any)

The Chief Risk Officer (CRO) shall be nominated by the Managing Director who works with the project managers and functional heads to ensure effective implementation of an organization's risk management framework and process. However, appointment, removal and terms of remuneration of the Chief Risk Officer to be determined , if any, by the Risk Management Committee in alignment with Section 3.1.2.

Roles and Responsibilities of the CRO:

- Communicating and managing the establishment and ongoing maintenance of risk management policy pursuant to the organization's risk management vision.
- Designing and reviewing processes for risk management.
- Review of the quarterly risk reports submitted by risk management team.
- Communicating with the management and RMC regarding the status of risk management and reporting the key risks faced by the organization.

3.1.4 Risk Management Team

- Monitoring existing key business risks and emerging risks for the company

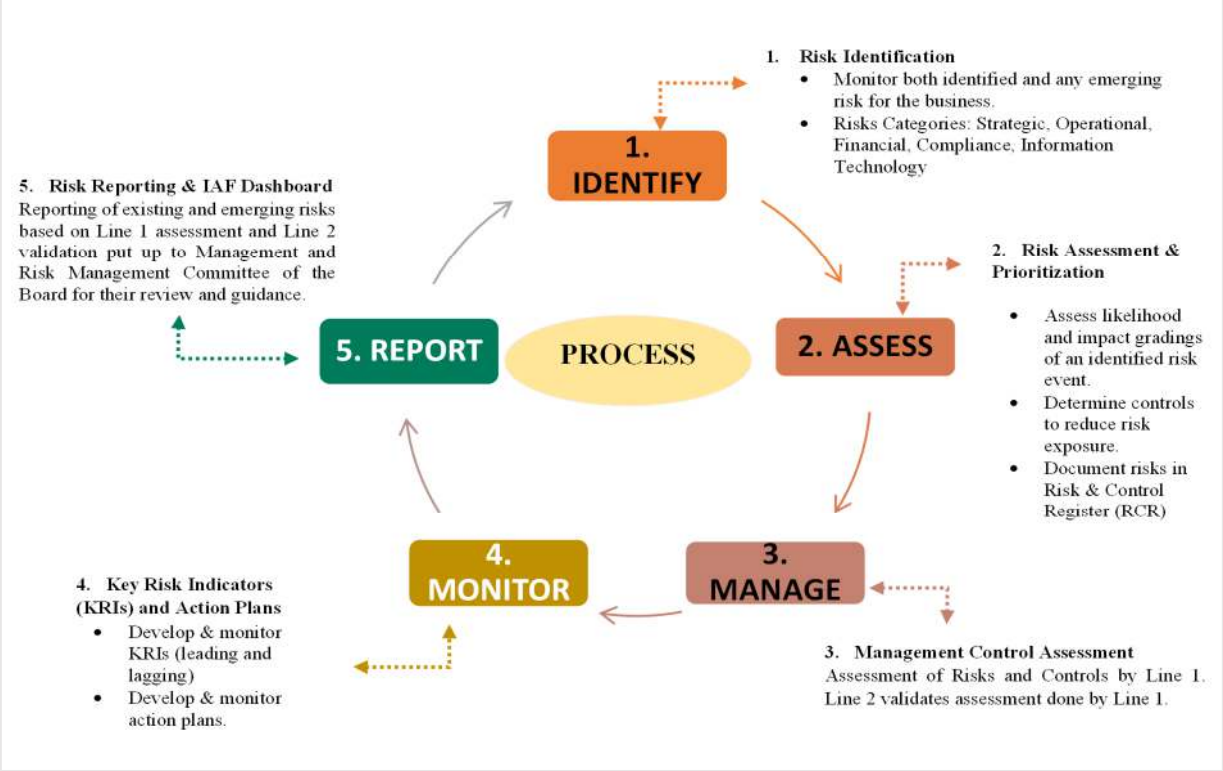
- Responsible for maintaining and updating risk related policies, framework, and RCR documents.
- Preparation and submission of quarterly risk reports to CRO and Management.

4. Integrated Assurance Framework (IAF) and Process

As part of the Risk management framework, the Company has adopted and implemented Integrated Assurance Framework (IAF) in line with Sembcorp Group, to put greater emphasis on the Three Lines of Defense model while managing risk. IAF is a comprehensive enterprise risk management framework where key risks are identified and deliberated by management with the support of the risk management function and reported periodically to the Committee of the Board, Management and Sembcorp Group. Robust mechanisms and systems have been put in place to identify and manage the inherent risks in our business and strategy, and to monitor the Company's risk exposure that could impact overall business sustainability and develop appropriate mitigations or controls.

The purpose of this framework is to identify risks in advance that have the potential impact on the Company's business or corporate standing or growth and manage them by calibrated action.
Under the IAF structure, the Three Lines of Defense work together to ensure that key strategic, financial, operational, compliance and information technology risks are reviewed and tested using a robust assurance process.

Risk and Control Register have been developed to document identification, analysis, and management of risks. The Risk and Control Register documents the risks, risk drivers, consequences, controls, mitigation, likelihood, risk rating, and identifies the key risks of the Company along with mitigation measures.



- **Risk Identification:** Risk Identification is a process of finding, recognizing, and describing risks. The risk is identified by keeping in mind some ascertainable criterion, for example,

  - What can go wrong?
  - What's the cause and effect?

  Risks can be identified under the following broad categories. This is an illustrative list and not necessarily an exhaustive classification.

  (a) Internal Risks:
  - Strategic risk
  - Project Execution risk
  - Health, Safety, Security & Environment risk
  - Compliance risk
  - Resource Variability
  - Financial risks
  - Operational risks
  - Key Commodity / Equipment price risk
  - Cyber Security & IT related risk
  - Technology Risk
  - Fraud, Bribery & Corruption risk
  - Reputation risk

  (b) External Risks:
  - Political & Regulatory Environment risks
  - Sustainability risks

- **Risk Assessment and Prioritization:**

  Risks so identified are assessed to classify them as per the criticality for the business. This would enable prioritization of risks and decide the right risk management strategies appropriate for the different class of risks. Wherever, applicable and feasible, the risk appetite is also defined, and adequate internal controls are installed to ensure that the limits are adhered to. In line with the Sembcorp Group Integrated Assurance Framework (IAF), risk appetite may be defined, wherever applicable and feasible, across five levels: **Zero, Low, Balanced, Open and Ambitious**. Residual risk exposures shall be monitored against the defined risk appetite levels and reported to Management, the Risk Management Committee and/or the Board, as applicable.The process of assessment is based on two parameters – risk impact and risk likelihood. Assessment of likelihood and impact gradings of an identified risk event is done post the identification of risks. Controls are determined to reduce risk exposure. The risks are then prioritized into Tier 1, 2 or 3. Tier 1 and Tier 2 risks shall be monitored quarterly through the IAF/RCR reporting process. Tier 3 risks shall be reviewed at least annually or earlier upon material changes, with significant escalations reported to Management, the RMC and/or the Board, as applicable.
  The identified risks are then documented in the Risk & Control Register (RCR).
  A 'Risk & Control Register' is a tool for recording business risk events encountered within the organization's operating environment in a standardized format describing risk, control, key risk indicators and action plans.

- **Risk Mitigation and Management Control Assessment (MCA):**

  - **Risk Mitigation:** The company has implemented required mitigation measures against each risk based on the risk framework. The Company has installed the following systems to firstly, shield the Company from the impact of the said risk:
    a. Involve all functions in the overall risk identification and mitigation exercise;
    b. Link the risk management process to the strategic planning and internal audit process;
    c. Creating and maintaining clear and comprehensive Documented Policies and Procedures
    d. Implementing strong IT Security Measures & cybersecurity protocols. Securing networks, databases, and sensitive data by regularly assessing vulnerabilities and patch software.
    e. Conducting regular internal audits. Auditing critical processes, financial transactions, and compliance areas and addressing control for weaknesses promptly.
    f. Implementing budget controls and expense approval processes.
    g. Frequent monitoring and assessing internal and external risk.

  - **Internal/ Management Control Assessment:** Management Control Assessment is the process to ensure/ verify that the Controls are adequate and effective. Based on the assessment of First Line of Defense, Second Line of Defense validates the Control ratings. Third Line of Defence (Internal audit) carries out periodic audit of adequacy and effectiveness of Controls.

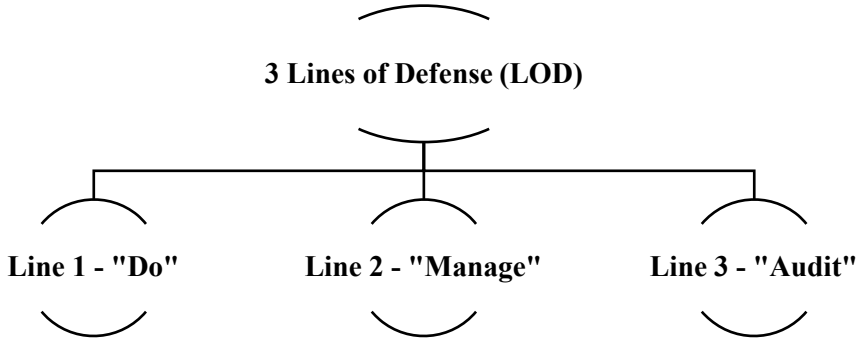
- **Key Risk Indicators (KRIs) and Action Plan:**
  Key Risk Indicators are measurable metrics to quantify and monitor any risk. They help to provide timely and objective warning about deterioration in any risk. Action Plans are management plans of action to improve controls and risk management. KRIs shall have defined thresholds, wherever applicable, to enable timely escalation of material risk movements to Management and the Risk Management Committee.

  - Develop & monitor KRIs (leading and lagging)
  - Develop & monitor Action Plans.

- **Risk Reporting and IAF Dashboard**: Reporting of existing and emerging risks based on First Line of Defense assessment and Second Line of Defense validation put up to Management and Risk Management Committee of the Board for their review and guidance.
  Reporting on MCA validation and KRI results and reporting on top risks for SCI Group & to the Company.

5. Three Lines of Defense Governance Structure

The 3 lines of Defense (LOD) risk reporting structure shall be followed by the organization:



Line 1

- Identify / evaluate risk and implement required controls.
- Monitor control adequacy and effectiveness.

Line 2

- Define Policies and Procedures
- Reviews & validates assessments and action plans, based on existing processes or controls.

Line 3

- Provide independent assessment of overall control of environment.
- Reporting to Senior Management & Audit Committee on key exceptions noted.

6. Periodical Risk Reporting

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the risks with their mitigation measures shall be updated on a regular basis. The following process shall be followed:

- Quarterly Risk reports for Risk Management Committee of the Board.
- Quarterly IAF update to SGIL Management and Sembcorp Group Risk.

7. Business Continuity Management (BCM)

SGIL has adopted and implemented the Incident Notification and Business Continuity Management Policy for the Sembcorp Group. The Incident Notification and BCM Policy outlines the framework for managing incident notifications and business continuity in SGIL. It comprises two key components:

- **Incident Notification**, which aims to minimise subjective judgement and ensure timely incident notifications by providing clear criteria on what constitutes a reportable incident and how it should be communicated.

- **Business Continuity Management (BCM),** which establishes the guidelines for crisis response and recovery. This ensures that the company is prepared and can respond and recover effectively from an incident or crisis to minimise its impact on the company and our stakeholders. Business Continuity Management shall be embedded in the Internal Controls and Crisis Management framework. The committee shall be responsible for laying out crisis response mechanism, communication protocols, and periodic training and competency building on crisis management. The Committee shall also conduct periodic disaster recovery mock drills to ensure that the organization is prepared to manage any crisis event quickly for business continuity

8. Information To the Board About Risk Assessment

- The Risk Management Committee shall, on a quarterly basis as may be required, submit a report to the Board of Directors setting out details of identified risks, impact of such risks on the Company and its stakeholders, measures taken by the Risk Management Committee to mitigate and manage the risks and outlook for the coming quarter.

- The Risk Management Committee shall periodically liaise with internal auditor and the audit committee with respect to any financial risks identified.

9. Disclosures

Board of Directors shall include a statement indicating development and implementation of a risk management policy for the Company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company in its Board Report**.**

10. Dissemination of the Policy

This Policy shall be made available on the Company's website at https://sembcorpindia.com and disclosed in the manner required under the LODR and other applicable laws.

11. Review And Amendment

The Board, the Audit Committee and The Risk Management Committee shall review the above list periodically, but atleast every 2 (two) years and make modifications to the said list as seen necessary.

Notwithstanding anything contained in this policy, the Company shall ensure compliance with additional requirements as may be prescribed under applicable laws either existing or arising out of any amendment to such applicable laws or otherwise and applicable to the Company from time to time.

This Policy is intended to be in conformity with the LODR and the Act as on the date of its adoption. However, if due to subsequent modifications in the LODR, the Act or any other applicable law, a provision of this Policy or any part thereof becomes inconsistent with the LODR, the Act or any other applicable law, then the provisions of such laws, as modified, shall prevail.

12. Effective Date

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

13. Contact

For queries related to this Policy, please contact:

Sr. No.	Name & Designation	Contact Number	Email address
1. 2.	Meenal Agarwal – Dy. Manager Avinash Roy - DGM	**124-6986700**	Meenal.agarwal@sembcorp.com Avinash.roy@sembcorp.com

****

Version Control:

Sr. No.	Version No.	Date of approval
1	V-1	29th July 2026