SANASA GENERAL INSURANCE COMPANY LIMITED

POLICY ON RISK MANAGEMENT AND INTERNAL CONTROLS

1. OVERVIEW

The Board of Directors of this Company has adopted this Policy in conformity with the Listing Rules to establish a framework to identify, assess mitigate and monitor risks across all aspects of the Company's operations.

2. DEFINITIONS

The following words and expressions shall have the respective meanings given against each such word unless such meanings are inconsistent with or repugnant to the subject or context**:**

"**Articles**" the articles of association of the Company;

"**Board**" means the board of Directors of the Company;

"**CEO**" means an employee of the Company performing the functions of the chief executive officer of the Company and called by whichever name;

"**Company**" means Sanasa General Insurance Company Limited ; ;

"**Companies Act**" means the Companies Act No. 07 of 2007 as amended from time to time;

"**Directors**" means the directors presently serving on the Board of the Company, and includes alternate directors appointed in accordance with the Articles;

"**Listing Rules**" means the Listing Rules of the Colombo Stock Exchange;

"**Policy**" means this policy on risk management and internal control;

"**Whistleblower Protection Officer**" means any officer designated to receive complaints/disclosures in accordance with the Policy on Whistleblowing.

3. PURPOSE

The Policy aims to ensure that risks are managed effectively with adequate internal controls to protect the interests of all stakeholders, maintain business continuity and enhance the Company's resilience in the face of uncertainties.

4. SCOPE

This Policy applies to the Company and to all Directors, including the CEO and employees of the Company, to the extent applicable.

5. GOVERNANCE AND RESPONSIBILITY

5.1 The Board of Directors has the ultimate oversight of the Company's risk management activities. The implementation and oversight of the risk management framework is delegated by the Board to the Risk Management Committee.

5.2 In carrying out their respective duties and responsibilities, the Audit/Risk Committee must guide the management in,

(a) identifying and assessing potential risks associated with the Company's activities, including strategic, operational, financial and regulatory risks;
(b) implementing measures to mitigate and control identified risks to an acceptable level;
(c) the regular monitoring and review of risk exposure and mitigation efforts to adapt to changing circumstances;
(d) fostering a risk-aware culture within the Company, where all employees are encouraged to report potential risks and contribute to risk management efforts.

5.3 The Company's risk management framework must comply with the applicable laws, regulations and industry standards. Additionally, employees must adhere to the Company's Policy on Internal Code of Business Conduct and Ethics for all Directors when identifying, assessing and managing risks.

5.4 Employees must receive regular training on risk management principles, processes and tools to their relevant roles. Awareness seminars and workshops may be conducted to promote a culture of risk awareness and encourage proactive risk reporting.

5.5 The risk management framework must be periodically reviewed on an annual basis and updated to reflect changes in the business environment, emerging risks and lessons learned from past experiences. Feedback from stakeholders including employees, customers and suppliers may be sought to identify areas of improvement.

5.6 [*Include any other policy, requirement or standard that is currently being followed by the Company which the Company wishes to continue post listing*]

6. RISK IDENTIFICATION AND ASSESSMENT

6.1 Risks must be identified through regular risk assessments, which may include workshops, surveys, and consultation with relevant stakeholders. This step aims to identify sources of risks, areas of impact, events, their causes and potential consequences.

6.2 Risks must be categorized based on their nature, severity, and likelihood of occurrence.

6.3 Risk assessments must consider both internal and external factors, including market conditions, regulatory changes, technological advancements, and competitive landscape.

7. RISK MITIGATION AND INTERNAL CONTROL

7.1 Upon identification and assessment, risks must be prioritized based on their potential impact and likelihood.

7.2 The Company must ensure that high-priority risks, are treated in one of the following ways:

(a) Risk Avoidance – Avoiding the risk by deciding not to commence/continue with the activity that gives rise to the identified risk;
(b) Risk Reduction – Involves reducing the severity or loss or the likelihood of the loss from occurring.
(c) Risk Transfer – Sharing the burden of loss or the benefit of gain from an identified risk with another party.
(d) Risk Acceptance – Involves accepting the loss or benefit from a risk when it occurs.

7.3 All risks that are not avoided or transferred are retained by default.

7.4 Internal controls must be periodically tested on an annual basis and reviewed to ensure their effectiveness and compliance with the applicable regulations and industry standards.

8. REPORTING

8.1 Key risk indicators must be established to monitor changes in risk exposure, effectiveness of internal controls and identify emerging risks.

8.2 Regular risk reporting must be provided to the Board of Directors and senior management to keep them informed of the company's risk profile, control environment and compliance status.

8.3 Any significant changes in risk exposure or unforeseen events must be promptly reported to the CEO who may escalate the matter to the Risk Committee, if necessary.

9. REVIEW AND MONITORING

9.1 The Audit / Risk Management Committee will from time to time review this Policy, monitor its implementation to ensure continued effectiveness and compliance with regulatory requirements and good corporate governance practice and will make recommendations on any proposed revisions as may be required to the Board for its review and final approval.

9.2 Upon the Board's approval, the said revision or amendment will be deemed to be effective and form part of this Policy.

9.3 This policy is to be read in conjunction with the Articles and other relevant Company policies, including:

(i) Policy on Internal Code of Business Conduct and Ethics for all Directors and Employees;
(ii) Policy on Control and Management of Company Assets and Shareholder Investments; and
(iii) Policy on Anti-Bribery and Corruption.

Date of Approval: 24th September 2024