CROISSANCE LIMITED

RISK MANAGEMENT POLICY

1. **Background**:

   The provisions of Section 134 (3) of the Companies Act, 2013 ("the Act") requires statement to be included in the Board's Report of the Company, on development and implementation of risk management policy of the Company including identification of risk factors which in the opinion of the Board may threaten the existence of the Company.

   In addition, the provisions of Section 177 (4) (vii) of the Companies Act, 2013 require that the Audit Committee shall act in accordance with the terms of reference specified in writing by the Board which shall interiliac include evaluation of risk management systems.

2. **Purpose and Scope:**

   The purpose of the policy is

   - To ensure protection of shareholder value through establishment of an integrated risk management framework for identifying, assessing, mitigating, monitoring, evaluating and reporting of all risks.

   - To provide clear and strong basis for informed decision making at all levels of the organization.

   - To continually strive towards strengthening the Risk Management & Compliance System through continuous learning and improvement.

3. **Applicability:**

   This policy applies to all employees of Company including management of the Company.

4. **Key Definitions**:

   - Risk Assessment: The systematic process of identifying and analyzing risks. The risk assessment consists of comprehensive study of threats and vulnerability and resultant exposure to various risks.

   - Risk Management: The structured way of protecting business and financial resources from risks and threats so that the objectives of the Company can be achieved without obstacles.

   - Risk Management Process: The application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, monitoring and communicating risk.

5. **Risk Management and key Activities:**

   Risk management, by and large involves reviewing the operations of the organization followed

by identifying potential threats to the organization including cyber security and the likelihood of their occurrence, and then taking appropriate actions to address the most likely threats.

The basic activities in any risk management system are:

(I) Risk identification.
(II) Risk assessment.
(III) Risk control.

Each of the risk needs to be assessed by the enterprise for its impact on profit and cash flow. Likelihood of occurrence and scope for mitigation or reduction including those relating to cyber security.

6. Risk Assessment and Control:

The Audit Committee and Board shall on periodic basis assess the external and internal risk factors across the organization. The risks are identified and formally reported through mechanism such as operation reviews and committee meetings. Internal control is exercised through policies and systems to ensure timely availability of information that facilitate pro-active risk management.

Certain identified risks are as follows:

i) Broad market trends and other factors beyond Company's control significantly reducing and harming the business, financial condition and results of operations.
ii) Failure in implementing its current and future strategic plans.
iii) Damage to reputation of the Company
iv) Risk management methods and insurance policies not being effective or adequate.
v) Changes in government policies relating to sector in which the Company operates.
vi) Changes in interest rates.
vii) Security risk and cyber-attacks.
viii) Insufficient systems capacity and system failures.

7. Review of policy:

The Board shall review the policy as and when required and ensure the policy to be in line with the regulatory requirements.

Company has adopted this updated Policy at its meeting held on 26th May, 2026.