LUMINA DATAMATICS LIMITED

RISK MANAGEMENT POLICY

Title	**Risk Management Policy**		
Department	Finance	Version	2.0
Date of Effect	October 24, 2024	Date of Next Review	October 24, 2027

1. INTRODUCTION:

For the remaining part of this documents Lumina Datamatics Limited will be referred as "the Company/ Lumina Datamatics". The policy provide framework for management of risks and mitigation of threats arising out of environment under which the Company operates. This is a continuous and evolving process with change in business environment.

2. OBJECTIVE OF THE POLICY:

- Develop an appropriate risk appetite.
- Adopt good practice in the anticipation, timely identification, evaluation and cost-effective control of risk in carrying out both normal and extraordinary business activities.
- Ensure that adverse risks are either avoided, reduced to an acceptable level, or managed and contained; and to do so in good time and on a continuous basis.
- Support individual members of staff and teams to take appropriate risk-based decisions, encouraging responsible intellectual risk-taking, informed by an understanding of risk and reward and supported by senior colleagues where necessary.
- Ensure business continuity wherever possible and respond effectively when this is threatened.
- Enable a robust audit trail to demonstrate that we are capable of managing risk.
- Focus risk assessment and management on the highest level of threats to our ability to achieve our strategic objectives; and opportunities to promote them.
- Assure funders/investors that there is a robust approach in place to assess and manage risk.

3. RISK FRAMEWORK:

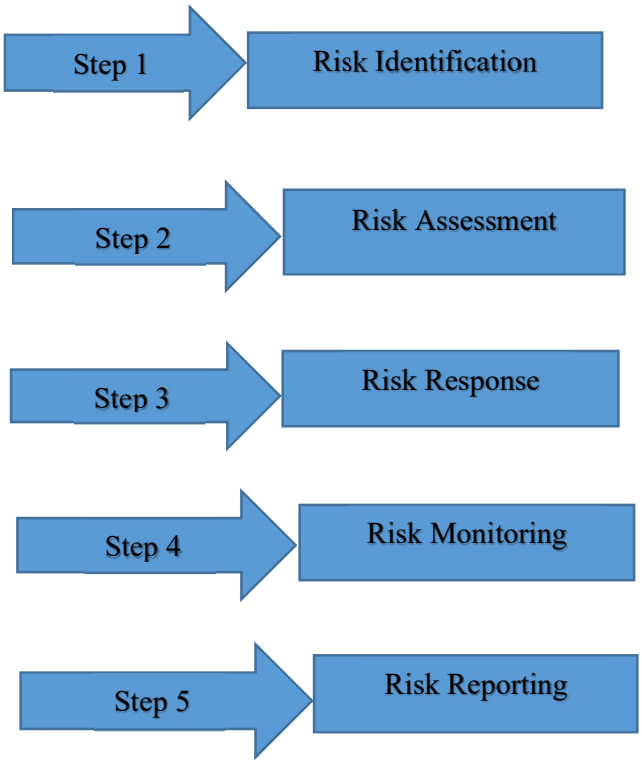
The risk framework of the Company shall include all its operational units and locations and projects and prospective investments. All investments made by the Company in its subsidiary companies shall also form part of this structure and process. The review of risks shall include the following but not limited to:

- Strategic Risks
- Financial Risks
- Compliance Risks
- Sectoral Risks
- Sustainability (Particularly ESG related) Risks
- Information technology Risks including Cyber Security Risks
- Operational Risks
- Business Continuity Plans

4. RISK GOVERNANCE ORGANISATION STRUCTURE:

Board of Directors	• Formulate, implement and monitor risk management framework • Ensuring risk management is integrated in to board reporting and annual reporting. • Ensuring that the company has mitigation strategies for all significant risks.
Audit Committee	• Mitigating risk in financial reporting process by ensuring proper internal control over financial reporting • Mitigating risk of non-compliances with various laws and regulations.
Management	• To Ensure that risk management framework is properly implemented and in place and working.

5. RISK MANAGEMENT PROCESS:



a. Risk Identification:

Identifying potential risks is an obvious first step in the risk management process. It's important to identify all risks that a business or organization may be exposed to. To do this, you'll want to employ as many methods as possible, including:

- Personal experience
- Recent history
- External research
- Interviews with industry professionals
- Group brainstorming sessions

b. Risk Assessment:

Once you identify a risk, you must assess how it will impact your project. This is typically done using two criteria: probability and impact. Risk probability states how likely a risk is to be realized, whilst risk impact states how severely the risk will affect your project if realized. It is common to assess these criteria using a qualitative scale (high/medium/low etc.), though some governance standards require quantitative assessment. Multiplying the two criteria together (either numerically or using a matrix) yields a result which is called the risk exposure or level of risk.

c. Risk Response:

Every project risk requires a response that is appropriate, achievable, and affordable. The risk level will very much determine the response. For example, you may choose to simply accept a low-level risk while a high-level risk demands a more aggressive response. Possible risk responses include:

- **Avoiding** the risk by not pursuing the activity that gives rise to the risk
- **Accepting** the risk and the consequences if it is realized
- **Mitigating** the risk by changing the probability and/or impact of the risk
- **Transferring** the risk to another party

Having defined the response, an action plan is typically required to execute the response.

d. Risk Monitoring:

Risks are not static; they change over time. The potential impact and probability of occurrence change, and what was once considered a minor risk can grow into one that presents a significant threat to the business and its revenue. Risk monitoring is the process of "keeping an eye" on the situation through regular risk assessments. It's important to understand that risk management is not a one-off event, it's a process that recurs through the life of an organization as it endeavours to anticipate threats and proactively handle them before they have an adverse impact.

e. **Risk Reporting:**

The Management should provide assurance to the Audit Committee with regards to the financial records, risk management and internal compliance.

Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk action plans is assessed to ensure changing circumstances do not alter risk priorities.

6. RESPONSIBILITY FOR RISK MANAGEMENT:

Responsibility holder	Responsibilities
Board	The Company's risk management architecture is overseen by the Board and the policies to manage risks are approved by the Board. Its role includes the following: ➢ Ensure that the organization has proper risk management framework; ➢ Define the risk strategy, key areas of focus and risk appetite for the Company; ➢ Approve various risk management policies including the code of conduct and ethics ; ➢ Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks.
Audit Committee	The Audit Committee assists the Board in carrying out its oversight responsibilities relating to the Company's (a) financial reporting process and disclosure of financial information in financial statements and other reporting practices, b) internal control, and c) compliance with laws, regulations, and ethics, (d) financial and risk management policies. Its role includes the following: ➢ Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls; ➢ Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies; ➢ Ensure that senior management monitors the effectiveness of internal control system; ➢ Help in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter frame policies for control and monitoring.

7. COMMUNICATION AND CONSULTATION:

Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the risk management process as well as on the process as a whole.

8. POLICY REVIEW:

This policy shall be reviewed periodically, at least once in three years, including by considering the changing industry dynamics and evolving complexity to ensure effectiveness and that its continued application and relevance to the business. Feedback on the implementation and the effectiveness of the policy will be obtained from the risk reporting process and other available information.

Approved by

For and on behalf of Board of Directors

Sd/-
Sameer Kanodia
Managing Director & CEO

****