ADITYA INFOTECH LIMITED

RISK ASSESSMENT AND MANAGEMENT POLICY

Version 1.0

Policy Version	Date of Board approval	Effective Date
Version 1.0	December 17, 2024	December 17, 2024

Table of Contents

RISK ASSESSMENT AND MANAGEMENT POLICY

PREAMBLE

Pursuant to Regulation 17(9) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("SEBI Listing Regulations") and Section 134(3) of the Companies Act, 2013, this Risk Assessment and Management Policy ("the Policy") establishes the philosophy of Aditya Infotech Limited ("Company"), towards risk identification, analysis and prioritization of risks, development of risk mitigation plans and reporting on the risk environment of the Company.

This Policy applies to all functions, departments, and geographical locations of the Company. Its primary purpose is to define, design, and implement a comprehensive risk management framework to identify, assess, manage, and monitor risks effectively. It also aims to identify potential events that could impact the Company, manage risks within the defined risk appetite, and provide reasonable assurance regarding the achievement of the Company's objectives. By adopting this approach, the Policy ensures that critical risk factors with significant impact are considered in the Company's business operations. This Policy has been adopted by the Board of Directors and may be amended from time to time with their approval.

DEFINITIONS

"**Company**" means Aditya Infotech Limited.

"**Risk**" refers to the possibility of an event or condition occurring that may negatively impact the achievement of objectives. It encompasses potential threats or uncertainties, whether arising from internal factors, such as system weaknesses or operational inefficiencies, or external factors, such as market fluctuations or regulatory changes. Risks can result in damage, injury, financial loss, or reputational harm and may require proactive management to mitigate or prevent their impact.

"**Risk Management**" is the process of identifying, assessing, prioritizing, and addressing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

"**Risk Management Committee**" means the Committee formed by the Board.

"**Risk Assessment**" means the overall process of risk analysis and evaluation.

"**Risk Register**" means a tool for recording the Risks identified under various operations.

RISK MANAGEMENT PROCEDURES

a) General

Risk management process includes four activities: Risk Identification, Risk Assessment, Risk Mitigation and Risk Monitoring & Reporting.

a) Risk Identification

The purpose of Risk identification is to identify internal and external risks specifically faced by the Company, 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 and identify all other events that can have an adverse impact on the achievement of the business objectives. All Risks identified are documented in the form of a Risk Register. Risk Register incorporates risk description, category, classification, mitigation plan, responsible function / department.

b) Risk Assessment

Assessment involves quantification of the impact of Risks to determine potential severity and probability of occurrence. Each identified Risk is assessed on two factors which determine the Risk exposure:

A. Impact if the event occurs
B. Likelihood of occurrence of event

Risk Categories: It is necessary that Risks are assessed after taking into account the existing controls, so as to ascertain the current level of Risk. Based on the above assessments, each of the Risks can be categorized as – low, medium and high.

c) Risk Mitigation

Risk mitigation plan drives policy development as regards risk ownership, control environment timelines, standard operating procedure, etc.

Risk mitigation plan is the core of effective risk management. The mitigation plan covers:

(i) Required action(s);
(ii) Required resources;
(iii) Responsibilities;
(iv) Timing;
(v) Performance measures; and
(vi) Reporting and monitoring requirements

The mitigation plan may also cover:

(i) preventive controls – a) responses to stop undesirable transactions, events, errors or incidents occurring; b) create awareness amongst the employees to avoid responding on undesirable messages, e-mails or transactions etc.;
(ii) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken;
(iii) corrective controls - responses to reduce the consequences or damage arising from crystallization of a significant incident.
(iv) Internal controls- the statutory auditors carry out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

Therefore, it is drawn with adequate precision and specificity to manage identified risks in terms of documented approach (accept, avoid, reduce, share) towards the risks with specific responsibility assigned for management of the risk events.

d) Risk Monitoring and Reporting:

To ensure that risks are kept within a reasonable range and that treatment measures have been taken and are working, monitoring of risks and treatment activities should be done on a frequent basis. A planned component of the risk management process with clearly defined roles should include ongoing monitoring and periodic reviews of the risk management process and its outcomes. Successful risk management depends on monitoring and review, thus it's important to specify who is in responsibility of carrying out these tasks. The monitoring and review's findings and observations are most helpful when they are well-documented and disseminated. In circumstances where the accepted risk of a particular course of action cannot be adequately mitigated, such risk shall form part of the consolidated risk register along with the business justification and their status shall be continuously monitored and periodically presented to the Risk Management Committee

BUSINESS CONTINUITY PLAN

Business Continuity Plan (BCP) is a step-by-step guide to follow response to a natural or man-made crisis or any other incident that negatively affects the firm's key processes or service delivery. The objective of the Business Continuity Plan is to support the business process recovery in the event of a disruption or crisis. This can include short or long-term crisis or other disruptions, such as fire, flood, earthquake, explosion, terrorism, tornadoes, extended power interruptions, hazardous chemical spills, Epidemic and Pandemic and other natural or man-made disaster.

AMENDMENT

Any change in the Policy shall be approved by the board of directors ("**Board**") of the Company. The Board shall have the right to withdraw and / or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Board in this respect shall be final and binding. Any subsequent amendment/modification in the Companies Act, 2013 or the Rules framed thereunder or the Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

SCOPE AND LIMITATION

In the event of any conflict between the provisions of this Policy and the Act or SEBI Listing Regulations or any other statutory enactments, modification or rules, the provisions of SEBI Listing Regulations / Act or statutory modification, enactments, rules shall prevail over this Policy and the part(s) so repugnant shall be deemed to be severed from the Policy and the rest of the Policy shall remain in force.

REVIEW OF THIS POLICY

This Policy shall be reviewed by the Risk Management Committee periodically, at least once in two years, including by considering the changing industry dynamics and evolving complexity.