RISK MANAGEMENT POLICY

1. BACKGROUND

Section 134(3) of the Companies Act, 2013 ("Act") requires a statement to be included in the report of the board of directors ("Board") of Brainbees Solutions Limited ("Brainbees" or the "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, may threaten the existence of the Company.

Furthermore, Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended ("Listing Regulations"), requires that the Company set out procedures to inform the Board of risk assessment and minimization procedures and makes the Board responsible for framing, implementing and monitoring the risk management plan of the Company.

This Policy shall come into force from the date of listing of equity shares of the Company on the stock exchanges.

2. OBJECTIVE AND PURPOSE

In line with the Company's objective towards increasing stakeholder value, a risk management policy has been framed, which attempts to identify the key events / risks impacting the business objectives of the Company and attempts to develop risk policies and strategies to ensure timely evaluation, reporting and monitoring of key business risks.

Risk Management Policy and Procedure this would promote a proactive approach in analysis, reporting and mitigation of key risks associated with the business in order to ensure a sustainable business growth and stability.

3. COVERAGE

The policy guidelines are devised in the context of the present business profile, future growth objectives and new business endeavors/ services that may be necessary to achieve the goals & the emerging global standards & best practices amongst the comparable organizations.

4. DEFINITIONS

a. **"Act"** means Companies Act 2013 and rules made thereunder as amended from time to time.
b. **"Company"** means Brainbees Solutions Limited.
c. **"Policy"** means Risk Management Policy.
d. **"Risk Management Committee"** or **"RMC"** or the **"Committee"** means a committee formed under regulation 21 of the Listing Regulations, as amended from time to time.

5. APPLICABILITY

This policy applies to all functions and units of Brainbees Solutions Limited and its subsidiaries.

6. RISK MANAGEMENT FRAMEWORK

Our risk management approach is composed primarily of three components:

A. Risk Governance
B. Risk Identification and mitigation
C. Risk Management Processes

A. Risk Governance:

- **Risk Management Committee**

The Company has a committee of the Board, namely, the Risk Management Committee, which was constituted with the overall responsibility of overseeing and reviewing risk management across the Company. The terms of reference of the Risk Management Committee are as follows:

The terms of reference of the Risk Management Committee are as follows:

a) To periodically review the risk management policy at least once in two years, including by considering the changing industry dynamics and evolving complexity;

b) To formulate a detailed risk management policy covering risk across functions and plan integration through training and awareness programmes;

c) The policy shall include:

(i) A framework for identification of internal and external risks specifically faced by the listed entity, in particular including financial, operational, sectoral, sustainability (particularly, environment, social and governance related risks), information, cyber security risks or any other risk as may be determined by the committee;
(ii) Measures for risk mitigation including systems and processes for internal control of identified risks;
(iii) Business continuity plan.

d) To approve the process for risk identification and mitigation;

e) To decide on risk tolerance and appetite levels, recognizing contingent risks, inherent and

residual risks including for cyber security;

f) 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 ofnon-compliance on an on-going basis;

g) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;

h) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;

i) To approve major decisions affecting the risk profile or exposure and give appropriate directions;

j) To consider the effectiveness of decision making process in crisis and emergency situations;

k) To balance risks and opportunities;

l) To generally, assist the Board in the execution of its responsibility for the governance of risk;

m) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;

n) To consider the appointment, removal and terms of remuneration of the chief risk officer (if any) shall be subject to review by the Risk Management Committee;

o) The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary;

p) The Risk Management 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 of directors;

q) To attend to such other matters and functions as may be prescribed by the Board fromtime to time; and

r) Such terms of reference as may be prescribed under the Companies Act and SEBI Listing Regulations.

- **The Business vertical and support function Heads** of the Company are owners of the risk of their functions and are responsible for managing risk on various parameters and ensure

implementation of appropriate risk mitigation measures. Risk & Internal Audit - Head of the Company is responsible for administration and compliance of this Policy.

- **The Risk Management team**
  - Provides oversight and continual reviews as explained in this policy.
  - Help the decision makers in the organization to take account of uncertainty.
  - Identify current and expected risk exposures of the organization and provide recommendations to address and drive the closures.
  - Enable compliance with the relevant legal and regulatory requirements.
  - Drive improvements and recommendation to achieve risk mitigation to improve financial stability of the organization.
  - Review of policy framework and have the changes approved through the auditcommittee and Board, as appropriate

B. Risk Identification and Mitigation:

- The Business vertical and support function Heads of the Company are responsible to identify the risks including the External and internal risk factors in the context of business objectives.

- Classification of Risk:

a) Financial / Operational / Preventable / Compliance risks:

- These are internal risks, arising from within the organization that are controllable and need to be eliminated or avoided.

- Examples –

  - Risks from employees' and managers' unauthorized, illegal, unethical, incorrect, or inappropriate actions
  - Retention of talent & succession planning
  - Control failures / gaps in IT / Manual process(s)
  - Security of assets – tangible and intangible
  - Safety of Human Resources
  - Compliance with labour / tax / corporate governance laws
  - Environmental, Social & Governance (ESG) related risk

b) External Risks

- External risks come up due to economic events that arise from outside of an institution's control.

- It arises from the external events that cannot be controlled by any an institution, cannot be forecasted with reliability, are normally beyond its control, and it is therefore difficult to reduce the associated risks.

- Examples –

  - Economic risk includes changes in market / national economic conditions viz economic recession, Gold price changes, significant change in global oil prices etc.
  - Political risk comprises of changes in the political environment that could hamper business environment.
  - Regulatory Risk includes changes in government policies on legal compliances
  - Natural risk factors include natural disasters – earthquake, flood etc - that affect normal business operations.
  - Employee strike or labour unrest.
  - Cyber security risks

c) Disruptive Risks

- Innovations to business models that disrupt the existing paradigm – eg. business models in the e-commerce space that threaten brick and mortar enterprises, technological disruptions (eg. quartz to mechanical, smart to quartz), Uber / Ola to taxi companies, etc.

- Demand shift due to technology / cross category threats.

d) Strategic Risks

- Risks taken on consciously linked to strategic choices to earn a higher return.

- New geography, category, manufacturing plants, new channels, for example business expansion plans in USA, Europe etc.

Examples of identified risks are:

- ✓ Broad market risk and other factors beyond the Company's control significantly
- ✓ Environmental risk like changes to Government policies, Geopolitical Issues, Financialpolicy, Import policies, etc
- ✓ Competition risk, Demand risk, supply chain management, Capacity management and inventory risk
- ✓ Technological change and security risks and cyber-attacks and other Fraud risks
- ✓ Supplier and critical service provider risk

- ✓ Reputation and PR risk
- ✓ Employment related risks
- ✓ Customer fraud risk
- ✓ Sustainability risk
- ✓ Legal and compliance risk
- ✓ Intellectual property risk
- ✓ Foreign exchange risk
- ✓ Financial risks including availability of funds, interest rate fluctuation, etc

Risk mitigation is an ongoing process that is deployed by business managers in the course ofbusiness. Risk mitigation process that may be regularly be deployed includes:

Review: Set up ERM (Enterprise Risk management) framework and periodicreview with senior management and board	Benchmark : Benchmark therisk policies with other peers	Internal control: Controls are exercised through policies and systems to ensure timely availability of information for pro-active risk management
Represent: Represent interest of organization through representative industry bodies for risk related to policies	Collaborate: work with other partners in eco system. For example: shift the shipment load to a different freight partner who has shipping linein the same area	Outsource the risk : For example Insurance
Reduce the risk: Example distributed supply chain	Educate and train: For example: IT security, FireSecurity	Redundancy: Back up sites for critical applications/business processes
Use Experts: For activities involving professional skills	Learn: Incident reporting, analysis and strengthen process by learning from own or other experiences	

C. Risk Management

Risk management is defined as the process of identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor,and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

- **Role of Risk Management Team**

The role of Risk Management team, through the process of revenue assurance and internal audit, includes:

- Review/discuss the Company's risk philosophy and the quantum of risk that the

Company, as an organization, is willing to accept in pursuit of stakeholder value;

- Review establishment and development of effective enterprise risk management
- Review and identify periodically key risk indicators. External and internal risk factors are assessed by responsible managers across the organization.
- Inquire about existing risk management processes
- Review the effectiveness of risk management processes in identifying, assessing and managing the Company's significant enterprise-wide risk exposures; Reviews to include operational risks; financial and reporting risks; compliance risks;
- Review of Cyber security

The risk management team will **identify** and formally **report** through mechanisms such asoperation reviews and committee meetings.

- **Overview of Process followed:**

  - Identify Key risk Business Areas subject to Risk
  - Prioritize risks: Based on factor of probability and impact
  - Set up Annual plans: Broken down by each quarter covering all the significant business vertical and business function, once in every two years cycle.
  - Risk identification: Risks are about events that, when triggered, cause problems. The aim of this step is to generate a comprehensive list of risks.
  - Risk analysis: Involves identifying causes and sources of risk and the trigger events that would lead to the occurrence of the risks.
  - Risk evaluation: To assess consequences of the risk and likelihood that those consequences can occur. The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.
  - Recommendations: To guide decisions on business risk issues.
  - Quarterly reporting, review and closure of risks through Action Taken reports.
  - Communication and consultation with external and internal stakeholders should take placeduring all stages of the risk management process.
  - Review of strategic risks arising out of adverse business decisions and lack of responsiveness to changes;
  - Develop comprehensive risk register: The aim is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate ordelay the achievement of objectives. Prepare risk registers for each function and business areas and provide unit-wise Risk Registers and Databases.
  - Enable Capability development (internal team or through the third party consulting firms)to perform the risk management process**.**

Any exceptions to this plan should be taken to Risk Management Committee for approval.

- **Risk Management Activity Calendar**

Forum	Timelines
Board of Directors	Annual
Audit Committee	Half Yearly
Risk Management Committee	Bi-annual
Executive Committee of Management	Quarterly
Risk Owners	Quarterly and Ongoing

D. Business Continuity Plan (BCP)

The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster. The BCP is generally conceived in advance and involves input from key stakeholders and personnel.

BCP involves defining any and all risks that can affect the company's operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters— fire, flood, or weather-related events—and cyber-attacks. Once the risks are identified, the plan should also include:

- Determining how those risks will affect operations
- Implementing safeguards and procedures to mitigate the risks
- Testing procedures to ensure they work
- Reviewing the process to make sure that it is up to date

7. MEETINGS/QUORUM

The RMC Meetings are required to be held twice in a year. The gap between 2 consecutive meetings cannot be more than 180 days on a continuous basis. The quorum for the meeting shall be either two members or one third of the members of the Committee, whichever is higher, including at least one member of the Board in attendance.

8. LIMITATION AND AMENDMENT

In the event of any conflict between the provisions of this Policy and of the Act or Listing Regulations or any other statutory enactments, rules, the provisions of such Act or Listing Regulations or statutory enactments, rules shall prevail over this Policy.

Any subsequent amendment / modification in the Listing Regulations, Act and/or applicable lawsin this regard shall automatically apply to this Policy.

9. REVIEW

This policy shall be reviewed periodically to ensure it meets the requirements of legislation & the needs of organization.

10. VERSION HISTORY

SR. NO.	VERSION	APPROVED BY	EFFECTIVE DATE	AMENDMENT SUMMARY
1	1.1			POLICY