DATA SECURITY AND PRIVACY POLICY

Technology is constantly evolving, and we at Raghav Productivity Enhancers Limited (RPEL) (called the "Company") remain committed to safeguarding the security and privacy of personal and business-related data collected from customers, suppliers, employees, and other stakeholders. This policy outlines our approach to data security and privacy in compliance with applicable laws and industry best practices.

PREAMBLE

This Data Privacy Policy is framed in accordance with the provisions of the Digital Personal Data Protection Act (DPDPA), 2023, enacted by the Government of India, and is aligned with applicable rules, standards, and regulatory directives governing the protection and processing of personal data.

By adhering to this policy, the Company seeks to uphold the right to privacy of its employees, customers, vendors, and other stakeholders. The principles outlined herein will serve as a guiding framework for the lawful, fair, and transparent processing of personal data and reinforce the Company's commitment to ethical data governance, digital responsibility, and compliance with prevailing data protection laws in India.

PURPOSE & OBJECTIVE

This policy establishes a framework for assessing and managing risks associated with data collection, processing, and storage. It outlines the necessary security measures, processes, and controls to protect sensitive information from unauthorized access, disclosure, alteration, or destruction.

Additionally, the policy ensures compliance with applicable laws, regulatory requirements, and industry best practices. By implementing stringent data protection measures, responsible data-sharing practices, and clear employee responsibilities, we strive to mitigate security threats and uphold trust in our operations.

Ultimately, this policy serves as a proactive guide to maintaining a secure data environment, reducing risks, and ensuring accountability in handling sensitive information.

To achieve this, it's important to follow basic Data Security Practices and stay proactive.

DATA PROTECTION MEASURES

To ensure the confidentiality, integrity, and availability of data, we implement the following security measures:

1. *Access Control* - Only authorized personnel have access to sensitive data.

2. *Encryption* - Data is encrypted during storage and transmission.
3. *Firewalls & Anti-Malware* - Regular security scans and software updates are maintained.
4. *Physical Security* - Restricted access to physical documents and secure storage of critical records.
5. *Regular Backups* - Data is regularly backed up to prevent loss due to system failures or cyber incidents.

DATA SHARING AND THIRD-PARTY ACCESS

The Company does not share personal data with third parties without the explicit consent of the data principal, unless required under statutory obligations, lawful orders, or in connection with a legal proceeding. All such data sharing is governed by appropriate data processing agreements and confidentiality clauses.

Where third-party vendors, processors, or service providers are engaged to carry out business operations involving personal data, Company ensures that they adhere to the obligations laid down in the DPDPA. These include implementing equivalent security standards, acting only on documented instructions, and ensuring no unauthorised secondary use of the data. For cross-border transfers, data may only be sent to countries or territories specifically notified by the Central Government, in accordance with the DPDPA framework.

EMPLOYEE RESPONSIBILITIES

1. Regularly Backup Your Data
2. Keep All Systems and Software Updated
3. Ensuring Antivirus Software is Installed and Regularly Updated
4. Email Protection
   a. Don't open emails from unknown senders.
   b. Keep email client apps updated.
5. Do not leave sensitive information lying around the office.
6. Do not leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.
7. Do not use free, unsecured Wi-Fi for shopping or banking on the Internet and even for logging into your social media profiles.
8. Do not click on links or download attachments from unwanted, unexpected emails, even if such emails look like they are from a known source.
9. Do not be tricked into giving away confidential information. It’s easy for an unauthorized person to call and pretend to be an employee or business partner.
10. Do not respond to phone calls or emails requesting confidential data.

11. Do not install unauthorized programs on your work computer. Malicious applications often pose as legitimate software. Contact your IT support staff to verify if an application may be installed.
12. Do not respond to pop-up ads that may come up on your screen. Close such pop-ups from the task manager.
13. Do not reply to e-mail(s) requesting financial or personal information. Please check the Email Address from where the mail has come before replying.

DATA RETENTION AND DISPOSAL

In compliance with the provisions of DPDPA, personal data is retained only for the duration necessary to fulfil the lawful purpose for which it was collected or for such period as mandated under applicable legal or regulatory obligations. Once the purpose has been served, or upon withdrawal of consent by the data principal, such data shall be deleted, anonymised, or otherwise lawfully disposed of, unless its retention is required to meet statutory obligations.

Data retention timelines are defined based on business need, legal risk, and contractual mandates. Secure data disposal protocols both physical and digital are enforced to prevent accidental disclosure or misuse of data after the retention period ends.

DATA BREACH RESPONSE

In the event of personal data breach likely to cause significant harm to any data principal, the Company shall promptly assess the scope and impact of the breach, contain and mitigate it, and report the incident to the Data Protection Board of India within the prescribed timeframe.

Data principals affected by such breaches will also be informed, where required, to enable them to take protective actions. All breaches are logged, investigated, and escalated as per internal policy, and corrective measures are implemented to prevent recurrence. Regular drills and reviews are conducted to ensure breach response readiness.

COMPLIANCE AND REVIEW

This policy shall be made available to employees and other concerned parties. This policy is reviewed periodically to ensure compliance with evolving legal and regulatory requirements. Non-compliance may result in disciplinary actions or legal consequences.

Approved by the Board on	30.04.2025
Effective from	01.04.2025
Version	1