DATA PREVENTION POLICY (Applicable to SME Companies to ensure data protection, information security, and prevention of unauthorized access or disclosures)

1. Objective

The objective of this Data Prevention Policy is to safeguard confidential, proprietary, and personal data handled by the Company in the course of its operations. This policy aims to ensure compliance with applicable data privacy and cybersecurity regulations and to prevent unauthorized access, loss, misuse, or disclosure of such data.

2. Scope

This policy applies to all employees, directors, contractors, interns, consultants, and any third parties who have access to the Company's data, IT systems, networks, or physical storage. It covers:

- Electronic data
- Physical documents
- Personal identifiable information (PII)
- Financial and operational records
- Intellectual property and proprietary business information

3. Data Classification

All Company data shall be classified into the following categories:

✓ Confidential: Internal business operations, financials, employee and client data, trade secrets.

✓ Restricted: Regulated or sensitive data requiring legal compliance (e.g., PAN,

Aadhaar, financial details).

✓ Public: Data cleared for public distribution, including information disclosed under statutory filings.

4. Key Principles for Data Prevention

- Access Control: Data access shall be role-based and granted only on a need-to-know basis.

- Data Encryption: Sensitive electronic data must be encrypted both in transit and at rest.

- Secure Disposal: Physical documents and electronic files no longer required must be disposed of securely (e.g., shredding, data wipe tools).

- Monitoring and Logging: All critical systems shall be logged and monitored for unauthorized access or anomalies.

- Email and USB Restrictions: Restrictions shall be placed on external data transfers via email or portable storage devices.

- Password Protocols: Complex password policies and multi-factor authentication shall be enforced.

- Data Backups: Periodic data backups must be maintained in secure, isolated environments.

5. Employee Responsibilities

Employees must:

⇨ Handle data responsibly and maintain confidentiality.

⇨ Avoid sharing passwords or leaving systems unattended.

⇨ Report any suspected data breach or phishing attempt immediately to the IT/Admin department.

⇨ Undergo regular data security and privacy training.

6. Third Party and Vendor Obligations

All third-party service providers and vendors handling Company data must:

❖ Sign a Non-Disclosure Agreement (NDA).

❖ Adhere to this policy and relevant legal standards.

❖ Implement security controls consistent with Company guidelines.

SAKETH SEVVENSTAR INDUSTRIES LIMITED

Plot No. PAP - D 146 - 147, Turbhe MIDC, TTC Industrial Area, S Central Road, Opp. Balmer Lawrie Van Leer Co., Turbhe, Navi Mumbai - 400 705, Maharashtra - India. **Tel:** + 91 022 2762 0641/42/43 | **E-Mail:** info@sssipl.in
GST No.: 27ABCCS7341C1ZI | **CIN No.:** U27300MH2019PTC331404 | **PAN No.:** ABCCS7341C1ZI