Introduction

This policy outlines the framework for cybersecurity and data privacy for Sai Silks Kalamandir. We are committed to protecting our customers' personal and financial information and ensuring the security of our IT systems. This policy applies to all employees, contractors, and third-party service providers.

Objectives

1. **Protect Customer Data:** Ensure the confidentiality, integrity, and availability of customer data.
2. **Comply with Regulations:** Adhere to relevant data protection laws and industry standards.
3. **Prevent Cyber Threats:** Implement measures to prevent, detect, and respond to cybersecurity threats.

Scope

This policy covers:

- All data collected, processed, and stored by the company.
- All IT systems, networks, and devices used in the business operations.
- All employees, contractors, and third-party service providers who have access to company data and systems.

Data Collection and Use

- **Data Minimization:** Collect only the data necessary for business operations.
- **Consent:** Obtain explicit consent from customers before collecting their personal data.
- **Purpose Limitation:** Use data only for the purposes specified at the time of collection.

Data Protection Measures

1. **Encryption:** Encrypt sensitive data both in transit and at rest.
2. **Access Control:** Implement role-based access controls to limit data access to authorized personnel only.
3. **Data Masking:** Use data masking techniques to anonymize sensitive data in non-production environments.

Network and System Security

1. **Firewalls and Antivirus:** Install and maintain firewalls and antivirus software on all company devices.
2. **Intrusion Detection Systems (IDS):** Use IDS to monitor network traffic for suspicious activities.
3. **Regular Updates:** Ensure all systems and software are regularly updated with the latest security patches.

Employee Training and Awareness

1. **Security Training:** Provide regular cybersecurity training to all employees.
2. **Phishing Awareness:** Educate employees on recognizing and reporting phishing attempts.
3. **Incident Reporting:** Establish clear procedures for reporting security incidents.

Incident Response

1. **Incident Response Team:** Establish an incident response team to handle security breaches.
2. **Response Plan:** Develop and maintain an incident response plan outlining steps to be taken in case of a data breach.
3. **Notification:** Notify affected customers and relevant authorities in the event of a data breach.

Vendor Management

1. **Due Diligence:** Conduct thorough due diligence on third-party vendors before engaging their services.
2. **Contracts:** Include data protection clauses in contracts with third-party vendors.
3. **Monitoring:** Regularly monitor and audit third-party vendors for compliance with data protection requirements.

Compliance and Monitoring

1. **Regulatory Compliance:** Ensure compliance with relevant data protection laws, such as GDPR, CCPA, etc.
2. **Internal Audits:** Conduct regular internal audits to assess compliance with this policy.

3. **Continuous Improvement:** Review and update this policy periodically to address emerging threats and regulatory changes.

1. **Retention Policy:** Establish data retention policies that define how long data should be kept.
2. **Secure Disposal:** Ensure secure disposal of data that is no longer needed, using methods such as shredding or secure deletion.

Policy Review

This policy will be reviewed annually or whenever there are significant changes to our business practices or applicable laws and regulations.