

SRI SAI SAMARDHA SOLUTIONS PVT. LTD

Regd. Off: Plot No. 46 A, Western Hills, Addagutta Society,
Near Narayana Concept School, Opp JNTU University, KPHB Colony, Hyderabad-72.
E-mail : sankarbabu@ssst.in.net

DATA PROTECTION & PRIVACY POLICY

Effective Date: 18-06-2022

Last Reviewed Date: 24-04-2026

Reviewed By: Yalamanchi Sankar Babu

Designation: CEO

Signature: _____

SRI SAI SAMARDHA SOLUTIONS PVT. LTD

Regd. Off: Plot No. 46 A, Western Hills, Addagutta Society,
Near Narayana Concept School, Opp JNTU University, KPHB Colony, Hyderabad-72.
E-mail : sankarbabu@ssst.in.net

LEGAL STATEMENT & SCOPE

This Policy enforces physical, electronic, and managerial safeguards to govern the collection, processing, transmission, storage, and overall security of all personal, institutional, corporate, and client data maintained in physical formats or logical databases during operational delivery by **Sri Sai Samardha Solutions Pvt. Ltd.** It also governs the reporting, investigation, and containment of workplace physical security incidents, near-miss occurrences, and system privacy breaches. Scope extends to all units, employees, faculty, staff, contractors, sub-vendors, and personally owned employee devices (BYOD) accessing sensitive operational data.

Sri Sai Samardha Solutions Pvt. Ltd. is committed to providing a safe, secure, and compliant working environment for all personnel, vendors, and sub-contractors. The organization maintains a formal process to report, investigate, and remediate all workplace accidents, security incidents, and near-miss occurrences. This framework ensures adherence to all applicable local and national laws, identifies underlying contributing factors, and executes necessary corrective actions to prevent recurrence.

PURPOSE

To establish operational guidelines, so far as reasonably practicable, for reporting, investigating, and applying appropriate control measures whenever an accident, information security incident, or near-miss occurrence arises. The primary objective is to maintain safe systems of work and secure operational environments across all **Sri Sai Samardha Solutions Pvt. Ltd.** sites.

1. ORGANIZATIONAL GOVERNANCE & ACCOUNTABLE ROLES

Direct organizational oversight and accountability are established under the following structure:

- **Operational Responsibilities:**
 - a) Mitigating and controlling the overall operational impact of all system security incidents.
 - b) Protecting, preserving, and effectively utilizing incident-related information for internal forensic analysis, regulatory disclosures, and notifications.
 - c) Ensuring all employees, contractors, and sub-contractors are fully aware of their operational roles and duties regarding security incident handling.

SRI SAI SAMARDHA SOLUTIONS PVT. LTD

Regd. Off: Plot No. 46 A, Western Hills, Addagutta Society,
Near Narayana Concept School, Opp JNTU University, KPHB Colony, Hyderabad-72.
E-mail : sankarbabu@ssst.in.net

- d) Guaranteeing compliance with all applicable statutory laws and regulations governing personal data handling.
- e) Identifying root causes and sources of security incidents or unauthorized disclosures to minimize future risks of recurrence.
- **Chief Executive Officer (CEO - Sankar Babu):** Holds ultimate executive accountability for policy approval, organizational compliance, and regulatory/client escalations.
- **Data Governance & Security Lead (IT & Operations Lead):** Accountable for daily operational compliance, access permissions, system monitoring, and serving as the primary liaison for client TPR risk audits.
- **System & Network Administrator:** Responsible for implementing network boundary controls, active firewalls, SSL certificates, and technical encryption standards.
- **All Employees & Operators:** Accountable for strict adherence to data protection standards, credential confidentiality, and immediate reporting of potential data events.

2. DATA PRIVACY PRINCIPLES & PURPOSE LIMITATION

- **Privacy Event Definition:** A Privacy Event includes any breach of confidentiality, infringement of rights, unauthorized disclosure, right-of-publicity violations, false light, or intrusion upon seclusion.
- **Legitimate Collection:** Personal data is collected solely for specified, necessary operational purposes (e.g., employee rosters, transport logistics, operational analytics, billing).
- **Purpose Limitation:** Personal data shall not be used or processed beyond the explicit purpose specified at collection without prior written authorization.
- **Data Minimization:** Data collection is strictly restricted to the minimum required to fulfil contractual obligations.

3. TECHNICAL DATA SECURITY CONTROLS

- **Encryption in Transit:** All personal or sensitive client data transmitted over internet connections must utilize Secure Socket Layer (SSL) / TLS protocols supporting a minimum of 128-bit encryption technology.
- **Encryption at Rest:** Sensitive identifiers and verification records (including eKYC data are encrypted at rest utilizing the AES-256-bit encryption standard.

SRI SAI SAMARDHA SOLUTIONS PVT. LTD

Regd. Off: Plot No. 46 A, Western Hills, Addagutta Society,
Near Narayana Concept School, Opp JNTU University, KPHB Colony, Hyderabad-72.
E-mail : sankarbabu@ssst.in.net

- **Physical Entry Controls:** Physical entry to all company facilities and server infrastructure is restricted exclusively to authorized personnel utilizing encrypted key-card access. Unauthorized visitors are strictly prohibited from entering operational areas.
- **Network & Server Protection:** Web servers, databases, and operational endpoints operate behind active firewalls and are continuously monitored to prevent unauthorized access, erasure, or modification.
- **Active anti-virus and anti-malware** software is deployed and maintained across all company PCs, laptops, and server infrastructure

4. SECURE COMMUNICATIONS PROTOCOL

- **Ordinary Email Restrictions:** Unencrypted ordinary email shall not be used to transmit sensitive personal information, credentials, or confidential financial metrics.
- **Secure Facilities:** Any dispatch of sensitive data must occur via encrypted channels, secure client portals, or secure email transmission facilities.

5. DATA RETENTION & STATUTORY COMPLIANCE

- **Retention Period:** Personal and corporate data will not be retained longer than necessary for contractual execution, statutory compliance, or legal requirements.
- **Sanitization & Disposal:** Decommissioned data or hardware undergoes secure electronic wiping or physical destruction in compliance with applicable statutory guidelines.
- **Statutory Alignment:** This Policy strictly complies with the **Digital Personal Data Protection (DPDP) Act, 2023**, the **Information Technology Act, 2000**, and applicable **CERT-In Cyber Security Directions**. Security incidents meeting statutory thresholds will be reported to CERT-In within 6 hours of identification.

6. THIRD-PARTY DISCLOSURES & PRIOR CLIENT APPROVAL

- **Prior Written Authorization:** The organization shall not transfer, disclose, or sub-process any client personal or corporate data to any third party or fourth party without prior notice and formal written approval from the client.

SRI SAI SAMARDHA SOLUTIONS PVT. LTD

Regd. Off: Plot No. 46 A, Western Hills, Addagutta Society,
Near Narayana Concept School, Opp JNTU University, KPHB Colony, Hyderabad-72.
E-mail : sankarbabu@ssst.in.net

- **Binding Obligations:** Approved third parties must execute a formal Data Processing Agreement enforcing confidentiality and equivalent security standards.

7. SECURITY INCIDENT & DATA BREACH MANAGEMENT

System users must report all information security concerns to the company's designated external IT security provider. Any serious information security incident must be escalated immediately to Executive Management at sankarbabu@ssst.in.net.

- **Incident Reporting Parameters:** Management shall formally log the incident, capturing:
 1. **Type of Incident**
 2. **Detailed Description of the Incident**
 3. **Date and Time of Notification**
 4. **Identity of the user reporting the incident**
- **Internal Reporting:** Any suspected or confirmed loss, unauthorized access, or compromise of data must be reported to the Data Governance Lead within 1 hour.
- **Client Escalation:** Impacted clients will be formally notified in writing or via direct telephonic communication immediately or within 24 hours of confirming any data breach or security incident impacting client data.
- **Executive Management,** alongside the designated response team, will establish and execute the necessary corrective activities for incident containment and remediation.
- **Resolution Timelines:** Upon breach detection, emergency containment measures shall be initiated within **4 hours**. Full containment and mitigation will be completed within **24 to 48 hours** based on incident severity. A complete Root Cause Analysis (RCA), Impact Assessment, and resolution report will be documented and submitted to affected clients within **7 business days**.
- **External IT Provider Reporting:** All serious information security incidents must be immediately reported to both Executive Management and the company's designated IT Security leads.
- **Immediate Device Seizure Protocol:** Upon detection of an incident, management is authorized to immediately seize all company-issued laptops, storage media, or access

SRI SAI SAMARDHA SOLUTIONS PVT. LTD

Regd. Off: Plot No. 46 A, Western Hills, Addagutta Society,
Near Narayana Concept School, Opp JNTU University, KPHB Colony, Hyderabad-72.
E-mail : sankarbabu@ssst.in.net

devices assigned to involved personnel for digital forensic examination.

- **Media Restraints & Evidence Retention:** Employees shall not release any devices, media, or records to external parties without prior written authorization. All evidence and incident logs must be securely retained until final case resolution.
- **Upon detection,** reported incidents are immediately assigned to a dedicated expert team possessing specialized domain knowledge within the concerned department.

8. COMPLIANCE, AUDITS & GOVERNANCE

- **Independent Audits:** The organization undergoes annual internal privacy assessments and fully cooperates with client-led independent audits.
- **Mandatory Security Training:** The Information Security team shall conduct periodic audits and mandatory data protection training on a regular basis for all employees, operators, and management personnel.
- **Penalties:** Non-compliance with this policy leads to immediate disciplinary action, up to and including termination of employment and legal prosecution.

9. GRIEVANCE REDRESSAL & INCIDENT REPORTING CONTACTS

Clients and data subjects may report security incidents, data breaches, or privacy grievances directly to our designated Grievance Officer:

- **Grievance Officer:** **Sankar Babu (CEO)**
- **Email:** sankarbabu@ssst.in.net
- **Phone:** **+91 88973 22777 / +91 8885004540**
- **Website:** <https://sssspvtltd.in>
- **Response SLA:** Incident reports are acknowledged within 2 hours; privacy grievances are resolved within 7 business days.

**** This Policy operates in full accordance and compliance with all applicable State Government rules, guidelines, and statutory requirements. ****