
# Data Privacy Policy

## Document Control:

| | |
|---|---|
| **Document Title** | Data Privacy Policy |
| **Document ID Reference** | Satin/ISMS/InfoSec/Pol-30 |
| **Document Classification** | Internal |
| **Revision No.** | 2.1 |
| **Document Created on** | 10-12-2025 |
| **Document Approved / Publish Date** | 21-03-2026 |
| **Document Author** | Arpit Ankan |
| **Document Reviewer** | Ashok Rawat |
| **Document Approver** | Board of Directors |

## Revision History:

| Version | Date of Change | Author | Revision Description |
|---|---|---|---|
| 1.0 | 20-10-2023 | Roshani Singh | Updated as per ISO 27001:2022/ RBI Master Guidelines |
| 2.0 | 22-11-2024 | Arif Pasha | Revised document layout |
| 2.1 | 10-12-2025 | Arpit Ankan | Minor Changes, Updated as per UIDAI Guidelines |

## Related documents

| S. No | Document Reference No. | Document Name | Version |
|---|---|---|---|
| 1 | Satin/ISMS/InfoSec/Pol-01 | Policies for Information Security | 4.0 |

## Disclaimer:

This document is solely for the information of SCNL and should not be used, circulated, quoted or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without our prior written consent.

## TABLE OF CONTENTS

# 1 Introduction

The **Privacy Policy** outlines how SCNL collects, uses, stores, and protects personal and sensitive information in accordance with applicable privacy laws and regulations. As an organization committed to safeguarding the privacy and confidentiality of its customers, employees, and other stakeholders, SCNL ensures that all personal data is handled responsibly, securely, and transparently.

This policy establishes the principles and guidelines for how SCNL processes personal information, including the purposes for which it is collected, how it is used, and the measures in place to protect it from unauthorized access, loss, or misuse. It reflects SCNL's commitment to privacy and ensures that all data collection, storage, and processing practices align with relevant legal, regulatory, and ethical standards.

The **Privacy Policy** applies to all personal data collected by SCNL, whether through direct interactions (e.g., website forms, applications) or through automated systems (e.g., cookies, analytics), and covers all stakeholders, including customers, employees, vendors, and other third parties. By adhering to this policy, SCNL aims to maintain trust and transparency with all parties involved, ensuring that personal data is treated with the highest level of care and respect.

# 2 Objectives

The key objectives of the **Privacy Policy** are as follows:

**Ensure Compliance with Legal and Regulatory Requirements:**

- To ensure that SCNL adheres to applicable privacy laws, regulations, and industry standards, including DPDP and other relevant data protection frameworks, to protect personal and sensitive information.
- To ensure that SCNL complies with UIDAI regulations and Aadhaar data security requirements, enabling lawful, secure, and responsible handling of Aadhaar-related personal information.

**Safeguard Personal Data:**

- To implement adequate measures that protect personal data from unauthorized access, loss, theft, or misuse, ensuring the confidentiality, integrity, and availability of such information.

**Define Clear Data Usage Practices:**

- To establish clear and transparent guidelines for the collection, use, storage, and sharing of personal data, ensuring that data is used only for legitimate, clearly defined purposes.

**Provide Individuals with Control Over Their Data:**

- To empower individuals by providing them with the right to access, correct, delete, or restrict the processing of their personal data, and ensuring that their data rights are respected and upheld.

**Ensure Transparency and Accountability:**

- To communicate SCNL's privacy practices to all stakeholders, including customers, employees, and partners, and to be transparent about how their data is processed, shared, and protected.

**Minimize Data Retention Risks:**

- To establish guidelines for the retention and timely deletion of personal data that is no longer required for business or legal purposes, reducing the risks associated with excessive data retention.

**Maintain Data Accuracy and Integrity:**

- To ensure that personal data is accurate, up-to-date, and relevant for its intended use, minimizing the risk of errors or misuses that could affect individuals or SCNL's operations.

**Promote Privacy Awareness and Training:**

- To promote privacy awareness within the organization by educating employees on best practices, legal obligations, and SCNL's privacy policies, ensuring that all staff are equipped to handle personal data responsibly.

**Mitigate Privacy Risks and Respond to Incidents:**

- To proactively identify and mitigate potential privacy risks through regular risk assessments and audits, and to establish clear procedures for responding to data breaches or privacy incidents in a timely and effective manner.

**Support the Trust of Stakeholders:**

To build and maintain trust with customers, employees, and other stakeholders by demonstrating SCNL's commitment to protecting privacy and maintaining ethical practices in data handling.

# 3 Purpose

**Protect Personal Information:**

- Ensure that personal data collected from customers, employees, vendors, and other stakeholders is safeguarded against unauthorized access, misuse, or loss, maintaining confidentiality and integrity.

**Promote Transparency and Trust:**

- Build trust by clearly communicating how personal data is collected, used, stored, and shared, so that individuals understand their rights and SCNL's commitment to privacy protection.

**Ensure Legal Compliance:**

- Meet and exceed legal requirements related to data protection, including compliance with data privacy laws such as DPDP, and other local regulations, safeguarding SCNL from potential legal risks.

**Empower Individuals:**

- Provide individuals with the rights and mechanisms to manage and control their personal data, such as access, correction, and deletion, ensuring their privacy preferences are respected.

**Foster a Culture of Privacy:**

Establish a foundation for a privacy-conscious culture within SCNL by educating employees on privacy obligations, ensuring they handle personal data responsibly and securely in their daily activities.

# 4 Scope & Applicability

This policy is applied to:

- Information Assets that store the Hard copy/Electronic information
- All employees of SCNL
- All third-party employees who work on SCNL's premises or connect remotely from their networks to SCNL's network.

- Customer personal data refers to the specific types of information that SCNL collects, uses, and stores about its customers, such as names, addresses, email, Mobile numbers, Preferences, interests, Aadhaar card pan card and references.

## 5 RACI Matrix

| Data Privacy Policy | Responsible (R) | Accountable (A) | Consulted (C) | Informed (I) |
|---|---|---|---|---|
| **Policy development and maintenance** | CISO | CISO | CIO and All Department Head | IT Management Committee |
| **Policy approvals** | Board of Director | Board of Director | CISO | CIO |
| **Policy Enforcement** | CISO | CIO | All Department Head | IT Management Committee |
| **Policy Compliance Monitoring** | CISO | CISO | CIO | IT Management Committee |
| **Exception Approval** | CIO | CIO | CISO | IT Management Committee |

## 6 Policy Statement

- SCNL shall ensure privacy of personal information including sensitive personal information of its customers, employees, vendor employees & contracted employees/consultants /auditors.
- Personal information , i.e., any data that can directly or indirectly identify an individual such as:
  - Name, Age.
  - Contact information including email address
  - Demographic information such as postcode, email IDs, Mobile numbers, Preferences, and interests.
- SCNL must establish and maintain robust technical and security measures to prevent unauthorized or unlawful access to accidental loss, destruction, or damage of its sensitive information. To safeguard the confidentiality, integrity, and availability of SCNL's data, all web services and applications must be configured to operate within a secure virtual private network (VPN) environment. In addition, SSL/TLS certificates should be employed to ensure that all

communications over the internet are encrypted and transmitted securely via HTTPS, while file transfers should utilize secure FTP (SFTP) with TLS encryption to protect data in transit.

- To further enhance data security, SCNL will implement a range of strategies aimed at ensuring internal data privacy and protection. These strategies include the use of strong encryption technologies for both data at rest and data in transit, ensuring that sensitive and personally identifiable information (PII) is securely stored and transmitted. SCNL will also develop and enforce comprehensive organizational policies for handling sensitive data, including personal, financial, and confidential information, ensuring that all employees and stakeholders are aligned with data privacy standards.
- In addition, SCNL will invest in ongoing staff training and capacity-building programs to raise awareness of data protection best practices, legal compliance requirements, and the latest security threats. This continuous education will ensure that employees are equipped to handle data securely and in accordance with SCNL's internal policies and regulatory requirements. Regular audits and security assessments will be conducted to evaluate the effectiveness of these measures and identify potential vulnerabilities.

# 7 Responsibilities

| Roles | Responsibilities |
|---|---|
| **Business Head/Department Heads** | 1. Responsible for adherence and implementation of Data Privacy Policy.<br>2. Responsible for updating Critical Data register if any critical data is added, changed or removed.<br>3. Information Security team. |
| **Data Owners** | 1. Classifying and labeling information with the appropriate classification level.<br>2. Periodically reviewing the classification level of information and reclassifying them when appropriate.<br>3. Understand the uses and risks associated with the information for which they are accountable. This means that they are responsible in case of any improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security-related control deficiencies pertaining to the |

| Roles | Responsibilities |
|---|---|
| | information for which they are the designated Owner.<br>4. Responsible for choosing appropriate information systems, and relevant controls for information handled by these systems, consistent with policies and standards issued by the IT Department. |
| **Data Custodian** | 1. Individuals/staff members, in physical or logical possession of information from Owners.<br>2. Primary responsibility is to maintain the Confidentiality, Integrity and Availability of data.<br>3. Highlight any unaddressed risk to the Information owner. |

# 8 Procedures

## Data Privacy

Information Security team should conform to the following principles for Personal Information Collection:

- **Collection Limitation**: Personal information should be collected for specified and legitimate purposes only. The information SCNL collected data shall be used to provide the Service to the customer, to improve the quality of the Website and Service, and to communicate information about the Service. SCNL shall never sell Client information or trade or share with other companies or organizations for commercial purposes or otherwise, unless they have been expressly authorized by the customer, either in writing or in electronic form. The customer's Personal Information should be collected primarily from the customer. However, SCNL may also obtain information about customers from other sources to verify the information submitted by customers.
- **Purposes Specification:** The purposes, for which Personal information is collected, should be based on the approved business requirement. The purpose should be identified & specified at or before the time the information is collected. SCNL shall use the collected information to provide, improve, customize, support, and market its services.
  - SCNL services operates and provides services including customer support, improving and customizing services. SCNL understands how customers use their services and analyze the

information to evaluate and improve services, develop and test new services and features, and conduct troubleshooting activities.

- SCNL communicates with clients about SCNL's services and features. They should also inform clients about SCNL's terms and policies from time to time.

- **Personal information Quality:** Personal information should be relevant to and not excessive for the purposes for which it is collected and used. Personal information should be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.

- **Lawful Processing of customer data:** Personal data of customers will be securely stored, in manual or electronic form, and in accordance with the IT Act, 2022. In addition, data collected for a specific purpose, product, or service may be stored in SCNL with other information relating to an individual, and only in accordance with the data privacy principles mentioned above. The Data Fiduciary will be responsible for processing the data.
- **SCNL shall process information in the following cases-**
  - When the data subject has given consent to process his or her data for one or more specific purposes.
  - When Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering a contract.
  - Processing is necessary for compliance with a legal obligation to which SCNL is subject.
  - Processing is necessary to protect the vital interests of the data subject or another person.
  - The Data Custodian can process the personal data in case of a medical emergency involving a threat to life or immediate threat to the health of the Data Subject or any other individual.
  - A Data Subject has the right to complete, correct, update, and delete their personal data.
  - A Data Subject has the right to nominate, in the event of death or incapacity of the Data Subject, exercise the rights of the Data Subject.
- **Consent:** The knowledge and consent of the individual should be ensured for the collection/ receiving, usage, storage, or disclosure of personal information. SCNL's business operations shall be guided by the following:
  - The company shall request for consent in a manner, which is distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, where the data subject's consent should be given in the context of a written declaration.
  - SCNL shall inform the data subject of his/her right and the ease to withdraw his/her consent at any time.
  - To ensure effective identification, email addresses and passwords should be used.
  - Device IDs should be used to ensure that the right devices are being managed.

- SCNL shall request the consent of the data subject where the data may be transferred to a third party for any reason.
- SCNL shall only obtain personal information for the specific purpose of collection after which consent should be taken from the data subject to process his or her data.
- If the Data Subject's data is being used without their consent or in a wrong manner, then they're eligible to file a complaint.
- The consent Manager shall be accountable to the Data Subject and shall act on their behalf.

- **Limitation on Use and Retention:** Personal information should not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information should be kept only as long as it is necessary for the purposes for which it was collected and processed and in accordance with Personal information storage requirements under applicable IT Act 2022. The retention period of different types of data shall be defined and maintained based on the respective approved business requirements. Legal Dept. will advise the respective Business Head/Department Head for enforcement of the retention period of Personal Information.
- **Disclosure of Personal Information:** The information Security Team should not disclose, sell, or otherwise distribute to any third party any Personal information without prior consent of individual except under the following circumstances:
  - **Compliance with legal obligations**: SCNL may also disclose your personal information as required by law when it is considered in good faith that disclosure is necessary to protect the company's safety or the safety of others, to investigate fraud, or to respond to a government request. Where possible and legally permissible, SCNL shall communicate with the client in advance of any such disclosure. SCNL shall reject any third-party requests for personal information that are not legally binding.
  - **Third-party service providers** – SCNL may, from time to time, outsource some or all the operations of our business to third-party service providers. In such cases, it shall be necessary for SCNL to disclose personal information to those service providers. In some cases, the service providers may collect Personal Information directly from the individual(s) on SCNL's behalf. These service providers may have access to individuals' Personal information needed to perform their functions. However, SCNL shall ensure secure processes are followed by such service providers to access, use, and disclose personal information. As permitted or required by any law/statute/regulator, the personal information provided to the third-party service providers is disclosed:
    - To protect or defend SCNL's rights, interests, and property or the same of our associates and affiliates, or our affiliate's employees, consultants, etc.
    - For fraud-prevention purposes

- To prevent any people, including insurers and lenders who supply benefits or services to the individual.

- **Reasonable Security practices:** All appropriate technical, physical, and organizational measures should be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to data. SCNL follows the best security practices in line with ISO 27001 standards, to help in preventing unauthorized access to any customer's information.
- **Procedures and Guidelines for Data Privacy:** SCNL maintains physical, technological and procedural safeguards and security that comply with the IT Act, 2000. In addition, training procedures are in place for all employees of SCNL to ensure high standards in relation to Data Privacy. Below are some of the steps that SCNL has taken to ensure customer data privacy
  - The entire customer's data is classified as per SCNL data classification guidelines.
  - Access to sensitive data should be provided strictly on the basis of need to know.
  - Backup on removable storage media should be kept in a safe and secure environment.

# 9 Data Deletion

Data Deletion outlines the guidelines for the secure and systematic removal of data from SCNL's systems to ensure compliance with data protection regulations, safeguard privacy, and reduce the risk of unauthorized access to obsolete or unnecessary information.

- SCNL shall classify data based on sensitivity and relevance to determine the appropriate deletion procedures.
- SCNL shall adhere to applicable data protection laws and regulations, ensuring the right to be forgotten and compliance with privacy requirements.
- SCNL shall designate data owners for each dataset who are responsible for determining the appropriate retention period and overseeing the deletion process.
- SCNL shall utilize secure methods for data deletion, including permanent erasure techniques that prevent data recovery.
- SCNL shall establish specific timelines for data deletion based on regulatory requirements and business needs. Regularly review and update these timelines.
- SCNL shall communicate data deletion policies and procedures to relevant stakeholders, ensuring awareness and cooperation across the organization.

# 10 Data Masking

In adherence to SCNL's commitment to data privacy and confidentiality, it also includes provisions for the secure and responsible use of data masking techniques to safeguard sensitive information

during non-production activities. The primary objective is to ensure the protection of privacy and compliance with data protection regulations.

- SCNL shall clearly identify and classify sensitive data elements that require masking, such as personally identifiable information (PII), financial data, and other confidential information.
- SCNL shall extend data masking practices consistently across different environments, including development, testing, and staging, to maintain data integrity and privacy in various scenarios.
- SCNL shall implement appropriate data masking methods, such as substitution, shuffling, encryption, or tokenization, based on the sensitivity of the data and specific use cases.
- SCNL shall enforce access controls to restrict access to unmasked data, and implement robust logging mechanisms to capture details of data masking activities, supporting accountability and auditability

## 11 Transfer of Information

SCNL or any person on our behalf may transfer your Information including Personal Information /Sensitive Personal Data or Information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of Data protection that is adhered to by Us if such transfer is necessary for the performance of the lawful contract between us or any person on our behalf and you, or where you have consented to such transfer.

## 12 Correction of Discrepancies

SCNL or any person on its behalf shall permit you as and when requested by you to review the Information you had provided and ensure that any Personal Information or Sensitive Personal Data or Information found to be inaccurate or deficient shall be corrected or amended as feasible provided that SCNL shall not be responsible for the authenticity of the Personal Information or Sensitive Personal Data or Information supplied by the you to SCNL or any person acting on its behalf.

## 13 Option to withdraw Consent

SCNL or any person on its behalf shall, prior to the collection of Information including Sensitive Personal Data or Information, provide you an option to not to provide the data or Information sought to be collected. You shall, at any time while availing the services or otherwise, also have an option to withdraw your consent given earlier to SCNL. Such withdrawal of the consent shall be sent in writing to SCNL. In the case that you do not provide Information including Sensitive Personal Data or Information, or later on withdraw your consent, SCNL shall have the option not to provide you the services for which the said Information including Sensitive Personal Data or Information was sought.

## 14 Redressal of Grievances

SCNL shall address any grievances that you may have with respect to processing of Informations including Sensitive Personal Data or Information, in a time bound manner. For this purpose, SCNL designates **Mr. Vikas Umrao** as the Grievance Officer, and the contact detail of the Grievance Officer is **clientgrievance@satincreditcare.com**. The Grievance Officer shall redress the grievances expeditiously but within one month's time from the date of receipt of grievance. If you have any questions or concerns about our use of your Personal Information including Sensitive Personal Data or Information, please contact the Grievance Officer using the contact details provided in this Policy.

## 15 Exceptions and Limitations

Exceptions may be granted in cases where security risks are mitigated by compensating controls and in cases where security risks are at a low, acceptable level and compliance with minimum security requirements, not interfering with legitimate business needs. To request a security exception, follow the SCNL Exception Management Policy.

----------**End of Document**----------