SATIN Creditcare Network Limited

Document Control

Document Name	Policy for Protecting Personal data of Aadhaar Number Holders
Document Reference No.	22
Version Number	1.2
Created by	Pravupada Pandit, Saurabh Mishra
Reviewed by	Vikas Umrao, Gaurav Gupta, Ashok Rawat
Approved by	Anil Kwatra, Vikas Wadhera
Effective From	01/04/2026

Revision History

Created Date	Ver	Description (First Release/Revision)	Created by	Reviewed by	Approved by	Board Approval
28/01/2026	1.2	Annual Policy Review	Pravupada, Saurabh	Vikas Umrao, Gaurav Gupta	Anil Kwatra, Vikas Wadhera, Ashok Rawat	21/03/2026
12/12/2024	1.1	Annual Policy Review	Pravupada, Saurabh	Vikas Umrao	Anil Kwatra, Dhiraj Jha, Gaurav Gupta	12/03/2025
20/03/2024	1.0	Adoption/First Version	Ravi Anand	Vikas Umrao	Anil Kwatra, Dhiraj Jha	22-03-2024

Statement of Confidentiality

This document is confidential in nature and contains information that is proprietary and confidential to Satin Creditcare Network Limited (SCNL) which shall not be disclosed outside SCNL, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of Satin Creditcare Network Ltd is prohibited.

Table of Contents

1. Abbreviation Table

For the purpose of this Policy, the following abbreviations shall have the meanings assigned to them below. Unless the context otherwise requires, these abbreviations shall be read consistently across this document.

Abbreviation	Description
ADV	Aadhaar Data Vault
AML	Anti-Money Laundering
ASA	Authentication Service Agency
AUA	Authentication User Agency
CERT-In	Indian Computer Emergency Response Team
CIDR	Central Identities Data Repository
CISO	Chief Information Security Officer
CBO	Chief Business Officer
CIO	Chief Information Officer
CRO	Chief Risk Officer
DPDP Act	Digital Personal Data Protection Act, 2023
e-KYC	Electronic Know Your Customer
HSM	Hardware Security Module
ISO	International Organization for Standardization
IT Act	Information Technology Act, 2000
KUA	e-KYC User Agency
NBFC-MFI	Non-Banking Financial Company – Microfinance Institution
NDA	Non-Disclosure Agreement
OTP	One-Time Password
PDP	Personal Data Protection
PID	Personal Identity Data
RBI	Reserve Bank of India
SCNL	Satin Creditcare Network Limited
SMS	Short Message Service
SPDI	Sensitive Personal Data or Information
STQC	Standardisation Testing and Quality Certification
UIDAI	Unique Identification Authority of India
UID Token	Unique Identification Token issued by UIDAI
VID	Virtual ID

2. Introduction

Satin Creditcare Network Limited ("SCNL" or "the Company"), as a regulated Non-Banking Financial Company - Microfinance Institution (NBFC-MFI), recognises the fundamental importance of privacy, confidentiality, and security of personal data, particularly identity information linked to Aadhaar numbers. Aadhaar-based authentication and e-KYC are sensitive processes governed by strict statutory and regulatory safeguards. Any misuse, unauthorised access, or breach of Aadhaar-related personal data can cause serious harm to individuals and expose the Company to regulatory, legal, and reputational risks.

This Policy establishes a comprehensive framework for lawful, fair, transparent, and secure handling of Aadhaar-related personal data across the Company, ensuring compliance with applicable laws, regulatory directions, and industry best practices.

3. Objective

The objective of this Policy is to:

- Ensure protection of personal data of Aadhaar number holders processed by SCNL
- Establish clear governance, accountability, and control mechanisms for Aadhaar data
- Ensure compliance with the Aadhaar Act, UIDAI Regulations, RBI directions, and IT laws
- Embed privacy-by-design and data minimisation principles across systems and processes
- Protect the rights and interests of customers, borrowers, and other Aadhaar number holders

4. Scope And Applicability

This Policy applies to:

- All employees, officers, directors, consultants, agents, and contractual staff of SCNL
- All systems, applications, devices, and processes involving Aadhaar authentication or e-KYC
- All Aadhaar-related personal data collected, processed, stored, transmitted, or archived by SCNL

The Policy covers Aadhaar numbers, Virtual IDs, UID Tokens, demographic data, authentication transaction logs, and any identity information as defined under the Aadhaar Act and applicable regulations.

5. Relevant Provisions of Law and Judicial Pronouncements

For the purpose of ensuring continued compliance with the legal and regulatory requirements governing the use and protection of Aadhaar-related identity information, reference shall be made to the following statutes, regulations, judicial pronouncements, and regulatory instruments, as amended or supplemented from time to time:

- The judgment of the Hon'ble Supreme Court of India delivered in September 2018 in relation to Aadhaar and the protection of privacy and identity information.
- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- The Aadhaar and Other Laws (Amendment) Act, 2019.
- The Aadhaar (Authentication) Regulations, 2016.
- The Aadhaar (Data Security) Regulations, 2016.
- The Aadhaar (Sharing of Information) Regulations, 2016.

All circulars, notifications, advisories, standards, and directions issued by the Unique Identification Authority of India (UIDAI) from time to time.

6. Purpose

The purpose of this Policy is to establish a comprehensive and uniform framework within the Company for the protection, processing, storage, and management of personal data of Aadhaar number holders in a lawful, fair, and secure manner.

This Policy seeks to guide all stakeholders, officers, employees, and authorised personnel of the Company in ensuring strict compliance with the applicable provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; the Aadhaar and Other Laws (Amendment) Act, 2019; the Aadhaar (Authentication) Regulations, 2016; the Aadhaar (Data Security) Regulations; the Aadhaar (Sharing of Information) Regulations, 2016; the Information Technology Act, 2000 and the rules framed thereunder, as amended from time to time.

Further, this Policy aims to ensure that Aadhaar-related personal data is collected and processed solely for lawful and permitted purposes, safeguarded against unauthorised access, misuse, alteration, or disclosure, and handled in a manner that upholds the privacy, dignity, and rights of Aadhaar number holders while supporting the Company's regulatory obligations and operational requirements.

7. Governance and Policy Review

This Policy shall be owned and administered by the Operational Excellence & Process Re-Engineering Department. Any amendments shall be undertaken based on regulatory changes, audit observations, or operational requirements, with approval from the designated authority/committee. The Board of Directors shall review this Policy at least once every year.

8. Terms And Definitions

For the purposes of this Policy, unless the context otherwise requires, the following terms shall have the meanings assigned to them below. Words importing the singular shall include the plural and vice versa.

a) Aadhaar Number

"Aadhaar number" means an identification number issued to an individual under sub-section (3) of Section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and includes any alternative virtual identity generated under sub-section (4) of that section.

Reference: Section 2(a) of the Aadhaar Act, 2016 and Section 3(i)(a) of the Aadhaar and Other Laws (Amendment) Act, 2019.

b) Aadhaar Data Vault (ADV)

"Aadhaar Data Vault" means a separate, secure database, vault, or system where Aadhaar numbers and any associated identity information are mandatorily stored, and which serves as the sole repository for such data.

Reference: UIDAI Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25 July 2017.

c) Anonymisation

"Anonymisation" means an irreversible process of transforming or converting personal data into a form in which an individual cannot be identified, directly or indirectly, and which meets the prescribed standards of irreversibility.

Reference: Section 3(2) of the Personal Data Protection Bill, 2019.

d) Authentication

"Authentication" means the process by which the Aadhaar number, along with demographic information, biometric information, or OTP of an individual, is submitted to the Central Identities Data Repository (CIDR) for verification, and such repository verifies the correctness or otherwise of such information based on its records.

Reference: Section 2(c) of the Aadhaar Act, 2016.

e) Authentication Service Agency (ASA)

"Authentication Service Agency" or "ASA" means an entity providing the necessary infrastructure and secure network connectivity to enable a requesting entity to perform Aadhaar authentication using the facilities provided by UIDAI.

Reference: Regulation 2(f) of the Aadhaar (Authentication) Regulations, 2016.

f) Authentication User Agency (AUA)

"Authentication User Agency" or "AUA" means a requesting entity that uses the Yes/No authentication facility provided by UIDAI.

Reference: Regulation 2(g) of the Aadhaar (Authentication) Regulations, 2016.

g) Authority

"Authority" means the Unique Identification Authority of India (UIDAI) established under sub-section (1) of Section 11 of the Aadhaar Act, 2016.

Reference: Section 2(e) of the Aadhaar Act, 2016.

h) Biometric Information

"Biometric information" means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.

Reference: Section 2(g) of the Aadhaar Act, 2016.

i) Central Identities Data Repository (CIDR)

"Central Identities Data Repository" or "CIDR" means a centralised database containing Aadhaar numbers issued to individuals, along with the corresponding demographic and biometric information and other related records.

Reference: Section 2(h) of the Aadhaar Act, 2016.

j) Consent

"Consent" means the free, informed, specific, clear, and capable-of-withdrawal permission given by the data principal for processing of personal data, obtained through an affirmative action and in accordance with applicable data protection laws.

Reference: Section 11 of the Personal Data Protection Bill, 2019.

k) De-identification

"De-identification" means the process by which identifiers are removed, masked, or replaced with a fictitious name or code such that the data principal cannot be directly identified without additional information.

Reference: Section 3(16) of the Personal Data Protection Bill, 2019.

l) Demographic Information

"Demographic information" means information relating to the name, date of birth, address, and such other details as may be specified for issuance of an Aadhaar number, excluding race, religion, caste, tribe, ethnicity, language, income, medical history, or entitlement records.

Reference: Section 2(k) of the Aadhaar Act, 2016.

m) e-KYC User Agency (KUA)

"e-KYC User Agency" or "KUA" means a requesting entity that, in addition to being an AUA, is authorised to use the e-KYC authentication facility provided by UIDAI.

Reference: Regulation 2(l) of the Aadhaar (Authentication) Regulations, 2016.

n) Global AUA

"Global AUA" means an Authentication User Agency authorised to access full e-KYC data, including Aadhaar numbers, and permitted to store Aadhaar numbers within its systems.

Reference: UIDAI Circular No. 1 of 2018, dated 10 January 2018.

o) Local AUA

"Local AUA" means an Authentication User Agency authorised to access only Limited KYC and not permitted to store Aadhaar numbers within its systems.

Reference: UIDAI Circular No. 1 of 2018, dated 10 January 2018.

p) Hardware Security Module (HSM)

"Hardware Security Module" or "HSM" means a secure physical computing device used to generate, store, and manage cryptographic keys for signing authentication requests and decrypting e-KYC response data.

Reference: UIDAI Circular No. 11020/204/2017 – UIDAI (Auth-I), dated 22 June 2017.

q) Identity Information

"Identity information" in respect of an individual includes the Aadhaar number, biometric information, and demographic information.

Reference: Section 2(n) of the Aadhaar Act, 2016.

r) Limited KYC

"Limited KYC" means an Aadhaar-based service that does not return the Aadhaar number and provides only a UID Token and limited demographic information, as permitted to Local AUAs.

Reference: UIDAI Circular No. 1 of 2018, dated 10 January 2018.

s) PID Block

"PID Block" means the Personal Identity Data element comprising demographic information, biometric information, and/or OTP collected during Aadhaar authentication.

Reference: Regulation 2(n) of the Aadhaar (Authentication) Regulations, 2016.

t) Personal Data

"Personal data" means any data relating to a natural person who is directly or indirectly identifiable and includes any inference drawn for profiling purposes.

Reference: Section 3(28) of the Personal Data Protection Bill, 2019.

u) Personnel

"Personnel" means all employees, officers, directors, consultants, agents, and contractual staff engaged by the requesting entity.

Reference: Regulation 2(1)(f) of the Aadhaar (Data Security) Regulations, 2016.

v) Processing

"Processing" means any operation performed on personal data, including collection, recording, storage, use, disclosure, retrieval, restriction, erasure, or destruction.

Reference: Section 3(31) of the Personal Data Protection Bill, 2019.

w) Reference Key

"Reference Key" means an additional key mapped to an Aadhaar number stored within the Aadhaar Data Vault for secure referencing.

Reference: UIDAI Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25 July 2017.

x) Requesting Entity

"Requesting Entity" means an agency or person submitting Aadhaar number and related identity information to CIDR for authentication.

Reference: Section 2(u) of the Aadhaar Act, 2016.

y) Resident

"Resident" means an individual who has resided in India for a period of one hundred and eighty-two days or more during the twelve months immediately preceding the date of application for enrolment.

Reference: Section 2(v) of the Aadhaar Act, 2016.

z) Sensitive Personal Data or Information

"Sensitive personal data or information" means personal information relating to passwords, financial details, health conditions, biometric information, medical records, or any information prescribed under applicable law.

Reference: Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

aa) UID Token

"UID Token" means a unique, 72-character alphanumeric string issued by UIDAI in response to authentication or Limited KYC requests, specific to each Aadhaar number and requesting entity.

Reference: UIDAI Circular No. 1 of 2018, dated 10 January 2018.

bb) Virtual ID (VID)

"Virtual ID" or "VID" means a temporary, revocable alternative identity issued by UIDAI in lieu of an Aadhaar number.

Reference: Section 3(4) of the Aadhaar Act, 2016 and Section 4 of the Aadhaar and Other Laws (Amendment) Act, 2019.

9. Personal Data Collection

The Company shall collect personal data, including Aadhaar number or Virtual ID, strictly and directly from the Aadhaar number holder for the limited purpose of carrying out Aadhaar-based authentication or e-KYC in connection with the provision of its services.

Collection of Aadhaar-related personal data shall be undertaken only in accordance with applicable law, regulatory permissions granted by the UIDAI, and the disclosures made to the Aadhaar number holder at the time of such collection.

9.1. Specific Purpose for Collection of Personal Data

The identity information of an Aadhaar number holder, including Aadhaar number or Virtual ID, shall be collected solely for the purpose of establishing the identity of the individual through Aadhaar authentication and for conducting e-KYC in connection with customer onboarding, account opening, or such other services as may be lawfully permitted.

Such identity information shall be collected, processed, and used strictly in accordance with the Aadhaar Act, 2016, the rules and regulations framed thereunder, and other applicable regulatory requirements. Under no circumstances shall Aadhaar-related personal data be used for purposes beyond those explicitly disclosed to the Aadhaar number holder.

Even where consent is obtained, identity information shall not be used for any secondary or additional purpose unless such use is expressly permitted under the Aadhaar Act and related regulations. SCNL shall implement appropriate organisational and technical controls to ensure that identity information is not used beyond the scope defined in the disclosure notice and consent provided by the Aadhaar number holder.

9.2. Notice and Disclosure of Information to Aadhaar Number Holder

Prior to the collection of Aadhaar-related personal data, SCNL shall provide a clear, explicit, and comprehensible notice to the Aadhaar number holder. Such notice shall, inter alia, disclose the purpose for which the personal data is being collected, the nature of information that may be returned by UIDAI upon authentication, and whether submission of Aadhaar is mandatory or voluntary for the specified purpose.

Where submission of Aadhaar is mandatory, the legal provision mandating such submission shall be clearly disclosed. Where Aadhaar submission is voluntary, or where an Aadhaar number has not been assigned, alternate and viable means of identification shall be offered in accordance with applicable law and RBI directions.

The notice shall further inform the Aadhaar number holder of the option to use Virtual ID in lieu of Aadhaar number, the name and address of SCNL as the requesting entity, and the grievance redressal mechanism available to the Aadhaar number holder.

SCNL shall ensure that the Aadhaar number holder is notified of the authentication transaction through appropriate means such as SMS, email, or other approved channels, and shall maintain verifiable logs evidencing such notification.

9.3. Obtaining Consent

Consent of the Aadhaar number holder shall be obtained after providing the requisite disclosure and prior to undertaking Aadhaar authentication or e-KYC. Such consent may be obtained in physical form or through electronic means, including web-based or mobile application interfaces, as may be applicable.

SCNL shall maintain proper records evidencing the disclosure provided and the consent obtained from the Aadhaar number holder. The mechanism, format, and process for obtaining and recording consent shall be vetted and formally approved by the Legal Department to ensure compliance with applicable laws and regulatory expectations.

9.4. Processing of Personal Data

The identity information collected from the Aadhaar number holder shall be processed solely for the purpose of Aadhaar authentication by securely transmitting such information to the CIDR in accordance with UIDAI specifications.

Aadhaar authentication and e-KYC shall be carried out only for the specific purposes declared to UIDAI and permitted by UIDAI. These purposes shall be clearly communicated to the Aadhaar number holder at the time of authentication through the disclosure notice.

SCNL shall not use Aadhaar-related personal data, including e-KYC information, for any purpose other than those permitted under applicable RBI KYC and AML Master Directions and those disclosed to the Aadhaar number holder at the time of authentication.

Demographic details received from UIDAI as part of the e-KYC response shall be used solely for the purpose of identifying the individual and providing the relevant services for which such authentication was undertaken, and only for the duration necessary to fulfil such purpose.

9.5. Retention of Personal Data

Authentication transaction logs shall be retained for a period of two years, after which such logs shall be archived for a further period of five years or for such longer period as may be required under applicable laws, regulations, or internal policies, whichever is later.

Upon expiry of the applicable retention period, and except where retention is required pursuant to a court order, regulatory directive, or pending legal or regulatory proceedings, such authentication transaction logs shall be securely deleted in a manner that ensures irretrievability.

9.6. Sharing of Personal Data

Aadhaar-related identity information shall not be shared in any manner that is inconsistent with the Aadhaar Act, 2016, the Aadhaar and Other Laws (Amendment) Act, 2019, UIDAI regulations, or circulars issued by UIDAI from time to time.

Biometric information, where collected, shall not be transmitted over any network unless encapsulated within an encrypted PID block in accordance with UIDAI specifications.

SCNL shall not require or permit Aadhaar numbers to be transmitted over the internet or any electronic medium unless such transmission is secured through encryption and complies with UIDAI-prescribed standards, except where transmission is necessary for correction of errors or redressal of grievances in a lawful and secure manner.

10. Data Security

The Company shall implement robust technical, organisational, and administrative safeguards to ensure the confidentiality, integrity, and availability of Aadhaar-related personal data throughout its lifecycle. All security controls shall be aligned with the Aadhaar Act, 2016, UIDAI regulations and circulars, applicable RBI directions, and recognised information security standards.

10.1. Secure Collection and Transmission

Aadhaar number or Virtual ID shall be collected only through secure applications and transmitted exclusively over encrypted and secure communication channels in accordance with UIDAI specifications. Identity information received from UIDAI as part of the authentication or e-KYC response shall be stored in a secure manner, protected against unauthorised access, alteration, or disclosure.

Where biometric authentication is undertaken, biometric information shall be captured only through UIDAI-registered and STQC-certified devices. Such devices shall encrypt biometric data at the point of capture, and the encrypted data shall be transmitted to UIDAI over secure channels without intermediate storage.

OTP-based authentication data shall similarly be captured through secure applications and encrypted at the client device level prior to transmission to UIDAI, in strict compliance with UIDAI technical standards.

10.2. Prohibition on Storage of Core Aadhaar Data

Aadhaar numbers or Virtual IDs submitted by residents, customers, or individuals for authentication, and the corresponding PID blocks generated during the authentication process, shall not be retained under any circumstances. SCNL shall retain only those parameters explicitly returned by UIDAI as part of the authentication or e-KYC response, in accordance with applicable regulations.

As a Local Authentication User Agency (Local AUA), SCNL shall not store Aadhaar numbers of customers or residents in its systems, except where expressly permitted by UIDAI, thereby ensuring enhanced privacy and security of identity information.

10.3. Encryption and Key Management

All e-KYC information received from UIDAI shall be stored only in encrypted form. The encryption mechanisms employed shall meet UIDAI-prescribed standards and follow current industry best practices.

Cryptographic keys used for digitally signing authentication requests and for encryption or decryption of identity information stored within the Aadhaar Data Vault shall be generated, stored, and managed exclusively within HSMs, in compliance with UIDAI and Aadhaar Data Vault circulars.

10.4. Certified Devices, Applications, and Audits

SCNL shall use only STQC-certified and UIDAI-approved biometric devices for Aadhaar authentication, wherever biometric authentication is deployed.

All applications, systems, and interfaces used for Aadhaar authentication or e-KYC shall be tested for compliance with the Aadhaar Act, 2016 and UIDAI technical specifications prior to deployment in production. Any modification or change impacting the processing of Aadhaar-related personal data shall be subject to re-testing.

Such applications and systems shall be subjected to independent information systems audits at least annually by auditors certified by STQC, CERT-In, or any other UIDAI-recognised body.

10.5. Access Control and Confidentiality Obligations

Access to authentication applications, authentication servers, audit logs, source code, and information security infrastructure shall be restricted strictly to authorised personnel on a need-to-know basis. SCNL shall maintain and periodically review access control lists to ensure continued appropriateness of access rights.

All employees, contractual staff, consultants, service providers, and other personnel handling Aadhaar-related identity information shall be bound by appropriate confidentiality and non-disclosure obligations through contractual agreements and internal policies.

10.6. Incident Management and Breach Reporting

In the event of any actual or suspected breach of Aadhaar-related identity information, SCNL shall promptly notify UIDAI in accordance with applicable regulations. Such notification shall include details of the nature and impact of the breach, the number of Aadhaar number holders and records affected, contact details of the designated Privacy Officer, and the remedial measures taken or proposed to mitigate the breach and prevent recurrence.

SCNL shall maintain documented incident response procedures and ensure timely coordination with regulatory authorities, auditors, and internal stakeholders.

10.7. Authentication Logs and Records

Authentication transaction logs received from the CIDR shall be securely stored and shall include only the minimum information permitted under UIDAI regulations. In the case of Local AUAs, where storage of Aadhaar number is not permitted, the corresponding UID Token shall be stored in lieu of the Aadhaar number.

Such logs shall include details of the authentication response parameters, the disclosure of information provided to the Aadhaar number holder at the time of authentication, and the record of consent obtained. Under no circumstances shall PID information be stored.

10.8. Information Security Governance

SCNL shall maintain a comprehensive Information Security Policy aligned with ISO/IEC 27001 standards, UIDAI-specific information security requirements, and the Aadhaar Act, 2016. This policy shall govern the protection of identity information and shall be periodically reviewed and updated to address evolving security risks and regulatory requirements.

Aadhaar numbers, wherever permitted to be stored, shall be stored only within an Aadhaar Data Vault implemented strictly in accordance with UIDAI specifications.

11. Rights of the Aadhaar Number Holder

The Company recognises and upholds the statutory rights of Aadhaar number holders in relation to the processing of their Aadhaar-related personal data, subject to the limitations prescribed under applicable laws and regulations.

11.1. Right to Access and Correction

An Aadhaar number holder shall have the right to obtain access to identity information and authentication transaction records maintained by SCNL in relation to such Aadhaar number holder, and to request correction or updation of such information where it is found to be inaccurate or incomplete.

Notwithstanding the above, collection, storage, or further sharing of core biometric information is expressly prohibited under Section 29 of the Aadhaar Act, 2016. Accordingly, Aadhaar number holders shall not be entitled to access, obtain, or request correction of core biometric information.

SCNL shall establish and maintain a defined process enabling Aadhaar number holders to view identity information held by the Company and to submit requests for updation, subject to successful authentication of the Aadhaar number holder. Where the requested updation pertains to data maintained by UIDAI, the Aadhaar number holder shall be appropriately informed of the procedure to approach UIDAI for such correction.

11.2. Right to Withdraw Consent

An Aadhaar number holder shall have the right to withdraw consent given to SCNL for the storage of e-KYC data, to the extent permitted under applicable law.

Upon receipt of a valid request for withdrawal of consent, and subject to regulatory or legal retention requirements, SCNL shall delete the stored e-KYC data in a secure and verifiable manner and provide an acknowledgement of such deletion to the Aadhaar number holder.

11.3. Right to Grievance Redressal

An Aadhaar number holder shall have the right to lodge a complaint or grievance relating to the processing of Aadhaar-related personal data with the designated Privacy Officer of the Company.

The Privacy Officer shall be responsible for monitoring Aadhaar data processing activities and for ensuring that such processing is carried out in compliance with the Aadhaar Act, UIDAI regulations, and this Policy. Grievances shall be examined and addressed in a timely and transparent manner in accordance with the Company's grievance redressal framework.

11.4. Aadhaar Number Holder Access Request

The Company shall establish and maintain a structured and documented process to receive, examine, and respond to requests from Aadhaar number holders relating to access, correction, or other lawful exercise of rights in respect of their Aadhaar-related personal data.

As a mandatory safeguard, the identity of the Aadhaar number holder shall be duly authenticated through appropriate and secure means prior to granting access to, or acting upon, any request relating to identity information or authentication records.

All access requests received from Aadhaar number holders shall be formally recorded, tracked, and responded to within a reasonable and defined timeframe, in accordance with applicable laws, regulatory expectations, and internal service standards.

SCNL shall ensure that the handling of such access requests is carried out in full compliance with the Aadhaar Act, UIDAI regulations, applicable data protection and privacy laws, and the provisions of this Policy.

12. Privacy by Design

The Company shall adopt the principle of Privacy by Design as a core component of its governance framework for processing Aadhaar-related personal data. Privacy considerations shall be embedded at the earliest stages of design and throughout the lifecycle of all systems, products, processes, and technologies that involve the collection, processing, or storage of identity information of Aadhaar number holders.

SCNL shall ensure that no database, record, or repository containing Aadhaar numbers or Aadhaar-related identity information is made public or disclosed, whether in physical or electronic form, unless such Aadhaar numbers have been appropriately redacted, masked, or blacked out in accordance with applicable legal and regulatory requirements.

Prior to the launch or implementation of any new or modified process involving the processing of Aadhaar-related identity information, the Company shall ensure that a compliant disclosure of information or privacy notice is provided to the resident, customer, or individual concerned, and that valid consent is obtained and recorded in accordance with the Aadhaar Act, 2016 and UIDAI regulations.

To ensure ongoing compliance, SCNL shall conduct periodic self-assessments, including at least quarterly reviews, to verify adherence to disclosure and consent requirements and to identify any gaps requiring corrective action.

The Company shall implement appropriate organisational and technical measures, including anonymisation, de-identification, data minimisation, and purpose limitation, to ensure that the collection and processing of identity information remain adequate, relevant, and strictly limited to the lawful purposes for which such data is processed.

13. Governance And Accountability Obligations

The Company shall establish a robust governance and accountability framework to ensure effective oversight, lawful processing, and continuous compliance in relation to Aadhaar-related personal data.

13.1. Privacy Governance Structure

The Company shall constitute a Privacy Committee to provide strategic direction, oversight, and guidance on matters relating to privacy, data protection, and Aadhaar compliance. The Privacy Committee shall review privacy risks, regulatory developments, audit outcomes, and major incidents, and shall recommend appropriate corrective and preventive measures.

SCNL shall designate a Privacy Officer responsible for developing, implementing, maintaining, and monitoring an organisation-wide privacy governance and accountability framework to ensure compliance with applicable laws, UIDAI regulations, and this Policy. The name and contact details of the Privacy Officer shall be communicated to UIDAI and other relevant external authorities through appropriate channels.

13.2. Role, Independence, and Expertise of the Privacy Officer

The Privacy Officer shall function independently and shall be involved in all matters relating to the processing of Aadhaar-related identity information. The Privacy Officer shall possess adequate expertise in data protection and privacy laws, UIDAI regulations, and industry best practices.

The Privacy Officer shall advise senior management and the Board, as applicable, on privacy obligations, regulatory risks, and compliance requirements, including matters involving high-risk processing and the need for data protection or privacy impact assessments.

13.3. Risk Management and Incident Oversight

The Privacy Officer shall be responsible for identifying, assessing, and mitigating privacy and data protection risks arising from the processing of Aadhaar-related personal data.

In the event of any privacy or data security incident, the Privacy Officer shall coordinate incident response, regulatory communication, remediation measures, and internal reporting, ensuring compliance with UIDAI and other applicable regulatory requirements.

13.4. Audit, Assurance, and Compliance Monitoring

The Privacy Officer shall ensure that Aadhaar authentication operations, systems, and applications are subjected to independent audits at least annually by auditors empanelled with CERT-In, STQC, or any other UIDAI-recognised body.

In addition, internal audits relating to Aadhaar data processing and compliance with the Aadhaar Act, 2016 and this Policy shall be conducted at least on a quarterly basis through the Internal Audit function. The outcomes of such audits shall be monitored, documented, and tracked for timely corrective action.

13.5. Training, Awareness, and Capacity Building

The Privacy Officer shall ensure periodic training and awareness programmes for all personnel involved in processing Aadhaar-related identity information. Such training shall emphasise lawful processing, disclosure obligations, consent requirements, data security practices, and the legal and reputational consequences of non-compliance or data breaches.

Front-end personnel interacting with Aadhaar number holders shall receive regular training to ensure accurate communication of disclosures, proper consent capture, and secure handling of identity information. Aadhaar-specific training shall also be provided to developers, system administrators, and technical personnel based on their respective roles. Completion of all training programmes shall be documented and retained for audit and regulatory purposes.

13.6. Policy Communication and Continuous Review

The Privacy Officer shall be responsible for formally communicating this Policy, and any amendments thereto, to all relevant stakeholders, employees, and service providers required to comply with its provisions. Any change to the Policy shall be disseminated promptly and effectively.

The Privacy Officer shall facilitate periodic privacy performance reviews in consultation with the Privacy Committee and other stakeholders. Such reviews shall consider audit findings, privacy incidents, regulatory changes, UIDAI directives, and ongoing privacy initiatives, with a view to strengthening the Company's privacy governance framework.

14. Transfer of Identity Information Outside India is Prohibited

In strict compliance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the regulations framed thereunder, Aadhaar-related identity information processed by the Company shall not be hosted, stored, processed, or transferred outside the territory of India under any circumstances.

All systems, databases, applications, and infrastructure used for Aadhaar authentication or e-KYC shall be located within India, and no cross-border access, transmission, or storage of Aadhaar-related identity information shall be permitted, whether directly or indirectly.

15. Grievance Redressal Mechanism

The Company shall maintain an accessible, transparent, and effective grievance redressal mechanism to address complaints and concerns of Aadhaar number holders relating to the processing of Aadhaar-related personal data.

Aadhaar number holders may submit grievances or complaints to the Company's designated Privacy Officer through multiple channels, including the Company's website, mobile application, telephone, SMS, or such other communication channels as may be made available from time to time.

SCNL shall take reasonable and appropriate measures to ensure that Aadhaar number holders are adequately informed of the identity, role, and contact details of the Privacy Officer. The contact details of the Privacy Officer, along with the prescribed format or procedure for filing grievances, shall be prominently displayed on the Company's website and other commonly used communication platforms.

Where interactions with Aadhaar number holders occur through non-electronic or physical modes, SCNL shall ensure that the name and contact details of the Privacy Officer are displayed prominently through posters or notice boards at such locations to facilitate easy access to the grievance redressal mechanism.

In the event that a grievance is not resolved to the satisfaction of the Aadhaar number holder through consultation with the Company's management or the Privacy Officer, the Aadhaar number holder shall have the right to seek redressal through the mechanisms prescribed under Section 33B of the Aadhaar Act, 2016, without prejudice to any other remedies available under applicable law.

16. Responsibility for Implementation and Enforcement of the Policy

The effective implementation, monitoring, and enforcement of this Policy shall be supported by clearly defined roles and accountability at senior management levels within the Company.

The overall responsibility for independent monitoring and enforcement of this Policy, including oversight through audits, reviews, and compliance assessments, shall vest with the Chief Audit Officer, Mr. Amarjit Singh. The Chief Audit Officer shall ensure that adherence to this Policy is periodically evaluated and that any non-compliance or control gaps are reported to the appropriate management and governance forums for corrective action.

Responsibility for the implementation and operationalisation of the controls prescribed under this Policy shall rest with the Chief Business Officer, Mr. Anil Kwatra. This shall include ensuring that business processes, systems, and operational practices are aligned with the requirements of this Policy and applicable regulatory provisions.

The review and approval of disclosures provided to Aadhaar number holders, consent clauses, consent collection mechanisms, and consent logging processes shall also be the responsibility of the Chief Business Officer. Such reviews shall be undertaken to ensure continued compliance with the Aadhaar Act, UIDAI regulations, and this Policy.

17. Contact Details

For any queries, requests, or grievances relating to the processing of Aadhaar-related personal data, Aadhaar number holders may contact the designated Privacy Officer of SCNL.

Name of the Privacy Officer:

Mr. Sunil Yadav (Sr. Vice President - Chief Information Officer)

Contact Number: +91 99118 97867

Email Address: sunil.yadav@satincreditcare.com

18. Policy Approval, Review, and Sign-Off Matrix

Author	Designation	Date	Signature
Pravupada Pandit	Sr. Associate - Operational Excellence & Customer Services		
Saurabh Mishra	Sr. Associate - Operational Excellence & Customer Services		

Reviewer	Designation	Date	Signature
Vikas Umrao	Lead: Operational Excellence & Customer Services		
Ashok Rawat	Chief Information Security Officer		
Gaurav Gupta	Head - Operational Excellence & Process Re-Engineering		

Approving Authority	Designation	Date	Signature
Anil Kwatra	Chief Business Officer		
Vikas Wadhera	Chief Risk Officer		

End***