SATIN Creditcare Network Limited

Document Control

Document Name	Policy on Model Authentication Compliance
Document Reference No.	21
Version Number	1.2
Created by	Pravupada Pandit, Saurabh Mishra
Reviewed by	Vikas Umrao, Gaurav Gupta, Ashok Rawat
Approved by	Anil Kwatra, Dhiraj Jha
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, Ashok Rawat	Anil Kwatra, Vikas Wadhera	21/03/2026
18/12/2024	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

Document Control 1
Revision History 1
1. Abbreviation Table 5
2. Introduction 6
3. Purpose and Objective 6
4. Scope And Applicability 6
5. Governance and Policy Review 6
6. Terms And Definitions 6
7. Human Resources 10
7.1. Roles, Accountability and Regulatory Liaison 10
7.2. Personnel Due Diligence, Confidentiality and Access Eligibility 10
7.3. Training, Awareness and Access Lifecycle Management 11
8. Asset Management 11
8.1. Asset Identification, Ownership and Inventory Management 11
8.2. Asset Usage, Protection and Hardening Controls 11
8.3. Asset Movement and Secure Disposal 12
9. Access Control 12
9.1. Authorisation Principles and Least Privilege Access 12
9.2. Access Lifecycle Management and Periodic Review 12
9.3. Privileged Access Controls and Operator Authentication 13
10. Password Policy 13
10.1. Password Issuance, Confidentiality and Change Management 13
10.2. Password Complexity and Reuse Restrictions 13
10.3. Secure Storage, Transmission and Account Lockout Controls 14
11. Cryptography and Security of Aadhaar Number 14
11.1. Encryption and Protection of Personal Identity Data 14
11.2. Cryptographic Key Management and Digital Signing Controls 14
11.3. Aadhaar Number Minimisation, Masking and Tokenisation 15
12. Physical and Environmental Security 15
12.1. Data Centre Security and Access Management 15
12.2. Asset Protection, Movement Control and Environmental Safeguards 15
12.3. Workplace Security, Clear Desk Practices and Emergency Controls 16
13. Operations Security 16
13.1. Operational Readiness and Standard Operating Procedures 16
13.2. Segregation of Duties and System Integrity Controls 16
13.3. Infrastructure Security, Patch Management and Monitoring 17
13.4. Data Handling, Logging and Aadhaar Data Vault Controls 17
13.5. Usage Restrictions, Session Controls and Hosting Requirements 17

14. Communications Security 18
14.1. Device and Transaction Identification Controls 18
14.2. Secure Network Connectivity and Perimeter Protection 18
14.3. Communication Usage Controls and Acceptable Practices 18
15. Information Security Incident Management 18
15.1. Incident Identification and Regulatory Reporting 19
15.2. Third-Party Incident Awareness and Accountability 19
15.3. Incident Investigation and Root Cause Analysis 19
16. Compliance 19
16.1. Regulatory Compliance and Authorisations 19
16.2. Audit, Assurance and Oversight 20
16.3. Non-Compliance Management, Controls and Continuous Monitoring 20
17. Change Management 20
18. Policy Approval, Review, and Sign-Off Matrix 21

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
API	Application Programming Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
BGV	Background Verification
CERT-In	Indian Computer Emergency Response Team
CIDR	Central Identities Data Repository
CCTV	Closed-Circuit Television
e-KYC	Electronic Know Your Customer
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
KUA	e-KYC User Agency
NDA	Non-Disclosure Agreement
NTP	Network Time Protocol
OTP	One-Time Password
PID	Personal Identity Data
PoT	Point of Transaction
POS	Point of Sale
RCA	Root Cause Analysis
SCNL	Satin Creditcare Network Limited
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSL	Secure Sockets Layer
STQC	Standardisation Testing and Quality Certification
UIDAI	Unique Identification Authority of India
UID Token	Unique Identification Token issued by UIDAI
UUID	Universally Unique Identifier
VA	Vulnerability Assessment
VID	Virtual ID
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	Extensible Markup Language

2. Introduction

Satin Creditcare Network Limited ("SCNL" or "the Company") leverages Aadhaar-based authentication and e-KYC mechanisms as part of its customer onboarding, servicing, and regulatory compliance processes, strictly in accordance with applicable law. Given the sensitive nature of identity information involved in such processes, the Company recognises the critical importance of maintaining the highest standards of information security, data protection, and regulatory compliance.

This Policy on Model Authentication Compliance establishes a comprehensive governance and control framework governing Aadhaar authentication and related identity verification models deployed by SCNL. The Policy is designed to ensure that all authentication models, systems, applications, infrastructure, and processes operate in a secure, lawful, auditable, and transparent manner, aligned with regulatory expectations and industry best practices.

3. Purpose and Objective

The primary purpose of this Policy is to define a structured and enforceable framework for secure and compliant use of Aadhaar-based authentication models within SCNL. The objectives of this Policy include safeguarding the confidentiality, integrity, and availability of Aadhaar-related data; ensuring lawful and consent-based processing of identity information; establishing clear roles, responsibilities, and accountability across the authentication ecosystem; mitigating operational, legal, and reputational risks arising from misuse or compromise of authentication systems; and enabling effective regulatory oversight, auditability, and continuous improvement of authentication controls.

4. Scope And Applicability

This Policy applies to all Aadhaar authentication and e-KYC models, systems, applications, devices, infrastructure, personnel, and third parties involved in Aadhaar-based authentication activities undertaken by or on behalf of SCNL. The Policy covers Global AUAs, Local AUAs, Sub-AUAs, Business Correspondents, technology service providers, and any other outsourced entities participating in the authentication ecosystem.

All employees, contractual staff, consultants, and third-party personnel with access to Aadhaar-related systems or information are required to comply with this Policy.

5. 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.

6. 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.

7. Human Resources

7.1. Roles, Accountability and Regulatory Liaison

SCNL shall establish a clearly defined human resource governance framework for all Aadhaar-related authentication activities, recognising that personnel handling Aadhaar data constitute a critical element of the overall security and compliance ecosystem.

The Company shall designate both a Technical SPOC and a Management SPOC for Aadhaar authentication related operations and regulatory coordination. These SPOCs shall be responsible for liaison with the UIDAI and for ensuring timely communication, reporting, and compliance with all applicable Aadhaar-related laws, regulations, and directives. Any change in the designated SPOCs shall be promptly intimated to UIDAI in the prescribed manner.

7.2. Personnel Due Diligence, Confidentiality and Access Eligibility

All employees, contractual staff, and agencies involved in handling Aadhaar-related information, systems, or infrastructure shall be subject to mandatory background verification and shall execute appropriate confidentiality and non-disclosure agreements prior to being granted access. The Company acknowledges that UIDAI or any agency authorised by UIDAI may verify or validate such background verification and confidentiality arrangements as part of its supervisory or audit processes.

Where Aadhaar authentication activities are carried out through Business Correspondents, Sub-AUAs, or other third-party service providers, SCNL shall obtain formal undertakings from such entities confirming that background verification and confidentiality requirements have been duly completed for their respective personnel handling Aadhaar-related data. Access to Aadhaar authentication infrastructure shall be granted strictly on a need-to-know basis and only after completion of all prescribed due diligence and contractual safeguards.

7.3. Training, Awareness and Access Lifecycle Management

SCNL shall ensure that comprehensive information security and Aadhaar compliance training is imparted to all relevant personnel at the time of induction and thereafter on a periodic basis. Such training shall cover the requirements of the Aadhaar Act, 2016, the Aadhaar Regulations, UIDAI information security policies, and all relevant circulars, advisories, and technical guidelines issued from time to time. In addition to general awareness programmes, specialised and role-based training shall be conducted for personnel involved in specific functions within the Aadhaar authentication ecosystem.

Training programmes shall be conducted at least on a half-yearly basis and additionally whenever there are material changes in the authentication ecosystem, regulatory requirements, or internal processes. Records of all training sessions shall be maintained for audit and compliance purposes.

Upon cessation of employment, transfer, or change of role of any personnel handling Aadhaar-related authentication data, all user credentials, system access rights, and associated privileges shall be revoked or deactivated within twenty-four hours. This requirement shall apply equally to employees, contractual staff, and third-party personnel and shall be periodically reviewed to ensure effectiveness.

8. Asset Management

SCNL shall maintain a comprehensive asset management framework for all information assets supporting Aadhaar authentication services. Given the sensitivity of Aadhaar-related information, all assets used for authentication including applications, systems, databases, networks, devices, and infrastructure shall be formally identified, labelled, classified, and protected throughout their lifecycle in accordance with applicable regulatory and security requirements.

8.1. Asset Identification, Ownership and Inventory Management

All information assets deployed for Aadhaar authentication purposes shall be clearly identified and recorded in a centrally maintained asset inventory. The inventory shall capture relevant details such as asset type, location, custodian, ownership, and classification and shall be updated on a regular basis or upon any material change.

Ownership and accountability for each authentication-related asset shall be clearly defined and documented to ensure appropriate control, maintenance, and oversight. Asset classification shall reflect the criticality and sensitivity of Aadhaar-related information processed or stored by the asset.

8.2. Asset Usage, Protection and Hardening Controls

SCNL shall implement appropriate technical and administrative controls to prevent unauthorised access, loss, damage, theft, or compromise of assets containing Aadhaar-related information. Aadhaar data, including identity information, shall not be transferred to or stored on personal devices or unauthorised electronic media or storage systems under any circumstances.

All devices and systems used for Aadhaar authentication, including point-of-sale devices, tablets, desktops, laptops, servers, and databases, shall be deployed only after completion of system hardening in accordance with approved baseline configurations. Where UIDAI has prescribed specific hardening or security standards, such requirements shall be strictly followed;

in all other cases, SCNL shall define and enforce its own hardening standards aligned with industry best practices.

Biometric capture for Aadhaar authentication shall be performed exclusively through STQC-certified Registered Devices. This requirement shall apply equally to SCNL, its Sub-AUAs, Business Correspondents, and any other authorised third-party service providers involved in the authentication ecosystem.

8.3. Asset Movement and Secure Disposal

SCNL shall establish documented procedures for the secure movement, repair, sanitisation, and disposal of assets used for Aadhaar authentication operations. Prior to any equipment being sent outside SCNL premises for repair, maintenance, or replacement, the equipment shall be sanitised to ensure complete removal of any Aadhaar-related data. A movement log shall be maintained for all such assets and shall be subject to periodic review.

Information systems, storage media, and documents containing Aadhaar-related information shall be disposed of in a secure manner that prevents data reconstruction or unauthorised recovery. Disposal procedures shall be aligned with regulatory expectations and internal information security policies and shall be auditable.

9. Access Control

SCNL shall implement a robust access control framework to ensure that only duly authorised individuals are permitted to access information facilities processing Aadhaar-related information. Such facilities include, but are not limited to, authentication applications, audit logs, authentication servers, source code repositories, and information security infrastructure. Access shall be governed through formally maintained Access Control Lists and shall be subject to continuous oversight.

9.1. Authorisation Principles and Least Privilege Access

Access to Aadhaar-related systems and information assets shall be granted strictly on the basis of defined roles and responsibilities and in accordance with the principle of least privilege. SCNL, its Sub-AUAs, Business Correspondents, and other authorised third-party personnel shall be provided only such access as is necessary to perform their designated functions.

Common or shared user IDs and group user IDs shall not be permitted, as they undermine accountability and auditability. Any exceptional requirement for shared access, where no viable alternative exists, shall be approved by senior management of SCNL and formally documented, along with compensating controls to mitigate associated risks.

9.2. Access Lifecycle Management and Periodic Review

Access rights and system privileges for all personnel handling Aadhaar-related information shall be revoked within twenty-four hours of separation, transfer, or cessation of authorised engagement. Following deactivation, user IDs that are no longer required shall be deleted in a controlled manner to prevent reuse or misuse.

SCNL shall conduct periodic reviews of access rights to Aadhaar-related information facilities at least on a quarterly basis. Such reviews shall validate the continued appropriateness of access in relation to job roles and responsibilities, and review reports shall be documented and retained for audit and regulatory inspection purposes.

9.3. Privileged Access Controls and Operator Authentication

Administrative and privileged access to Aadhaar-related systems shall be strictly controlled and monitored. Procedures shall be established for the secure storage, handling, and management of administrative credentials for critical information systems. Where manual storage is unavoidable, credentials shall be secured in fire-resistant safes or approved password vaults, with access logs maintained and reviewed periodically.

Users shall not be granted local administrative rights on their systems as a default practice. In cases where administrative access is required for operational reasons, such access shall be time-bound, documented, and restricted from modifying local or system-level security configurations.

For assisted devices or applications where operators perform authentication-related functions on behalf of residents, robust operator authentication mechanisms shall be implemented. Such mechanisms may include password-based authentication, Aadhaar authentication, smart card–based authentication, or other secure authentication methods approved by SCNL, ensuring traceability and accountability of all operator actions.

10. Password Policy

SCNL shall implement a strong password management framework to protect access to Aadhaar authentication systems, applications, and information assets. Password controls shall form a foundational element of the Company's access security architecture and shall be enforced consistently across all Aadhaar-related environments.

10.1. Password Issuance, Confidentiality and Change Management

Initial passwords shall be issued through secure mechanisms and shall be mandatorily changed by users upon first login. All user credentials, including those of administrators and privileged users, shall be treated as confidential information and shall not be shared, displayed, transmitted, or otherwise disclosed in any form.

Passwords shall be changed immediately whenever there is any indication or suspicion of compromise, unauthorised disclosure, or system security breach. In addition, passwords shall be refreshed at defined intervals, with privileged and administrative accounts subject to more frequent change requirements than standard user accounts.

10.2. Password Complexity and Reuse Restrictions

Passwords used for accessing Aadhaar-related systems shall adhere to defined complexity standards to reduce the risk of guessing, brute-force, or credential-stuffing attacks. Such passwords shall have a minimum length of eight characters and shall not be based on easily identifiable personal information such as names, dates of birth, telephone numbers, or similar attributes.

Passwords shall be constructed to avoid predictable patterns, including consecutive identical characters or exclusively numeric or alphabetic sequences. Each password shall include a combination of uppercase and lowercase letters, numeric characters, and special characters. Reuse of the last five passwords shall be prohibited, and usernames shall not be used as passwords under any circumstances. Users shall also be restricted from using the same password across multiple UIDAI or Aadhaar-related access points.

10.3. Secure Storage, Transmission and Account Lockout Controls

Passwords shall not be hardcoded into source code, scripts, executables, configuration files, or automation tools. Where passwords are stored within systems or databases, they shall be protected using strong encryption or hashing mechanisms and shall never be stored or transmitted in clear text or in any reversible format.

Passwords shall not be embedded in automated login processes, including macros or function keys. Systems shall enforce account lockout controls such that a predefined number of consecutive failed login attempts three in the case of Aadhaar-related systems results in automatic account locking. Locked accounts shall be restored only through controlled administrative processes, including password reset and user identity verification by authorised system administrators.

11. Cryptography and Security of Aadhaar Number

SCNL shall implement robust cryptographic and data protection controls to ensure the confidentiality, integrity, and lawful use of Aadhaar numbers and associated identity information throughout the authentication lifecycle. All cryptographic mechanisms shall strictly adhere to UIDAI technical specifications and applicable regulatory standards.

11.1. Encryption and Protection of Personal Identity Data

Personal Identity Data including demographic and biometric information of the resident, shall be encrypted in accordance with the latest UIDAI-prescribed API specifications. Such encryption shall be performed at the point of capture on the endpoint authentication device and shall remain intact throughout transmission, processing, and exchange within the authentication ecosystem, including communication with Authentication Service Agencies.

The encrypted PID block shall not be stored in any system or device, except where buffered authentication is expressly permitted. In such exceptional cases, storage shall be strictly time-bound and shall not exceed twenty-four hours, after which the PID data shall be securely deleted from all local systems and storage media.

11.2. Cryptographic Key Management and Digital Signing Controls

All authentication requests shall be digitally signed to ensure authenticity, non-repudiation, and integrity of the transaction. Such digital signing may be performed by SCNL and/or the Authentication Service Agency, in accordance with the contractual and operational arrangements approved by UIDAI.

Cryptographic keys used for digital signing of authentication requests and for decryption of e-KYC XML responses shall be generated, stored, and managed exclusively within Hardware Security Modules. The HSMs deployed for this purpose shall be compliant with FIPS 140-2 standards and shall adhere to all provisions prescribed under UIDAI Circular No. 11020/204/2017 dated 22 June 2017, as well as any subsequent guidelines or notifications issued by UIDAI.

SCNL shall establish a comprehensive key management framework governing the entire lifecycle of cryptographic keys, including key generation, secure distribution, controlled storage, assignment of custodianship under dual control mechanisms, prevention of unauthorised substitution, timely replacement of compromised or suspected compromised keys, key revocation, and maintenance of detailed logs and audit trails for all key management activities.

11.3. Aadhaar Number Minimisation, Masking and Tokenisation

Where SCNL provides authentication services to Sub-AUAs, the client application used for Aadhaar authentication shall be developed, owned, and digitally signed by SCNL to ensure application integrity and regulatory accountability.

Aadhaar numbers shall be stored only within a secure Aadhaar Data Vault, where permitted, and the reference key used within the Aadhaar Data Vault shall be generated using a Universally Unique Identifier scheme to prevent guessing, correlation, or reverse engineering of Aadhaar numbers.

Display of full Aadhaar numbers shall be strictly restricted to the Aadhaar number holder or to authorised personnel with a demonstrable business requirement and appropriate approval. In all other cases, Aadhaar numbers shall be masked by default, with only the last four digits visible.

SCNL shall implement and progressively enhance the use of Virtual ID, UID Token, and Limited e-KYC mechanisms within its authentication systems to minimise direct handling of Aadhaar numbers and reduce the risk of data exposure. Integration of Virtual Tokens and UID Tokens into SCNL's services shall be undertaken in accordance with UIDAI specifications and applicable regulatory guidance.

12. Physical and Environmental Security

SCNL shall implement comprehensive physical and environmental security controls to protect Aadhaar-related infrastructure, information systems, and processing facilities against unauthorised access, damage, disruption, or loss. Such controls shall be commensurate with the criticality and sensitivity of Aadhaar-related information and shall align with UIDAI security requirements and industry best practices.

12.1. Data Centre Security and Access Management

All servers and infrastructure processing or storing Aadhaar-related information shall be housed within secure cabinets located in SCNL's designated Data Centres. Data Centres hosting Aadhaar-related systems shall be fully secured, access-controlled, and monitored at all times.

Physical access to Data Centres and other restricted areas shall be limited strictly to authorised personnel and shall be governed through pre-approval mechanisms. Entry and exit details, including the identity of the individual, date, time, and purpose of access, shall be recorded and retained for audit and regulatory review. Security personnel shall be deployed during and beyond office hours to ensure continuous monitoring and protection of critical infrastructure.

Closed-circuit television surveillance shall cover AUA and KUA servers and other critical Aadhaar-related infrastructure within the Data Centre. Signage clearly identifying restricted areas and entry requirements shall be prominently displayed at all relevant access points, particularly in areas where Aadhaar authentication servers are physically hosted.

12.2. Asset Protection, Movement Control and Environmental Safeguards

The movement of all incoming and outgoing assets associated with Aadhaar authentication within the Data Centre shall be formally documented and tracked. Lockable cabinets or safes shall be provided for secure storage of critical Aadhaar-related equipment, documents, and storage media.

Environmental safeguards, including fire doors, fire detection and suppression systems, and related safety mechanisms, shall be deployed, clearly labelled, and maintained in operational condition. Preventive maintenance activities, including periodic audits of fire safety equipment and surveillance systems such as CCTV, shall be conducted at least on a quarterly basis to ensure continued effectiveness.

Controls shall be designed and implemented to protect power supply lines, network cables, and related infrastructure from unauthorised access, interception, tampering, or physical damage.

12.3. Workplace Security, Clear Desk Practices and Emergency Controls

SCNL shall enforce a clear desk and clear screen policy across all Aadhaar-related work areas to minimise the risk of unauthorised access, accidental disclosure, or loss of sensitive information. Information systems shall be configured with screen savers or equivalent technological controls to automatically lock unattended systems after a defined period of inactivity.

Emergency preparedness and response measures shall be established to address physical security incidents, environmental hazards, or other disruptions affecting Aadhaar-related infrastructure. Appropriate controls, including intrusion detection mechanisms and evaluation plans, shall be implemented to enable timely detection, response, and recovery in the event of an emergency.

13. Operations Security

SCNL shall establish and maintain a comprehensive operations security framework to ensure that Aadhaar authentication systems and processes operate in a secure, reliable, and fully compliant manner. Operational controls shall safeguard Aadhaar-related information against unauthorised access, misuse, disruption, or compromise throughout its lifecycle.

13.1. Operational Readiness and Standard Operating Procedures

SCNL shall complete the Aadhaar on-boarding process as prescribed by UIDAI prior to commencement of any Aadhaar authentication activities. Formal and documented Standard Operating Procedures shall be established for all Aadhaar-related information systems and services. These procedures shall define routine operational activities, system maintenance requirements, escalation mechanisms, and actions to be taken in the event of system failures, security incidents, or service disruptions.

13.2. Segregation of Duties and System Integrity Controls

Personnel engaged in development, testing, or operational functions shall not be assigned responsibilities related to system administration, audit log management, or security review where such overlap could compromise data security or independence of controls. Where segregation of duties is not feasible due to operational constraints, compensating controls such as enhanced monitoring, supervisory oversight, and periodic review of audit trails shall be implemented.

SCNL shall ensure that no personnel intentionally create, introduce, or deploy malicious code or any logic designed to impair system performance, compromise security, or enable unauthorised access to Aadhaar-related information. Test and production environments shall be physically and/or logically segregated to prevent unauthorised changes or data leakage.

13.3. Infrastructure Security, Patch Management and Monitoring

A formal patch management process shall be implemented to ensure timely application of security updates at both application and server levels. Periodic vulnerability assessments shall be conducted to identify and remediate weaknesses in Aadhaar-related infrastructure.

All systems and hosts connecting to Aadhaar authentication services or processing resident identity information shall be protected using endpoint security controls, including anti-virus and anti-malware solutions. Network security controls such as intrusion detection systems, intrusion prevention systems, and web application firewalls shall be deployed to safeguard Aadhaar infrastructure.

Event logging shall be enabled to capture critical user activities, system exceptions, and security events. Audit logs shall be monitored regularly, retained securely, and made accessible only to authorised personnel. All system clocks shall be synchronised using a centralised time source to ensure integrity of logs.

13.4. Data Handling, Logging and Aadhaar Data Vault Controls

SCNL shall comply fully with all consent-related requirements under the Aadhaar Act, 2016, Aadhaar Regulations, and UIDAI circulars. Aadhaar authentication transaction logs shall be maintained strictly in accordance with regulatory requirements and shall not contain Personal Identity Data.

Biometric data collected during Aadhaar authentication shall not be stored in client applications or terminal devices under any circumstances. No resident or transaction data shall be retained on endpoint devices after completion of authentication.

Where e-KYC data is received, such data shall be stored only in encrypted form and only after obtaining explicit consent from the resident. Sharing of e-KYC data with Sub-AUAs or other entities shall be undertaken only after obtaining specific approval from UIDAI and strictly in accordance with applicable regulations.

Where SCNL operates as a Global AUA or KUA, Aadhaar numbers and related data shall be stored only within a secure Aadhaar Data Vault located in a highly restricted and isolated network zone. All Aadhaar data stored in the Data Vault shall remain encrypted, and UIDAI-prescribed Data Vault guidelines shall be strictly followed.

13.5. Usage Restrictions, Session Controls and Hosting Requirements

Aadhaar numbers shall not be used as domain-specific identifiers within internal systems. Domain-specific identifiers shall be decoupled, revoked, or reissued as necessary to prevent correlation or misuse. Separate licence keys shall be generated for Sub-AUAs as prescribed by UIDAI, and SCNL's e-KYC licence key shall not be shared with any third party.

SCNL and its ecosystem partners shall ensure that Aadhaar-related identity information is not displayed, disclosed, or published to unauthorised persons or external agencies, nor mapped with unrelated datasets. Aadhaar authentication servers shall be hosted only in data centres located within India.

User sessions shall be terminated upon completion of authentication activity, and automated lock-out mechanisms shall be implemented for workstations, servers, and network devices to prevent unauthorised access due to inactivity.

14. Communications Security

SCNL shall implement robust communications security controls to ensure the confidentiality, integrity, and authenticity of Aadhaar authentication data transmitted across networks. All communication channels supporting Aadhaar authentication shall be secured against unauthorised access, interception, tampering, or misuse, in accordance with UIDAI specifications and applicable regulatory requirements.

14.1. Device and Transaction Identification Controls

Each authentication device deployed for Aadhaar authentication shall be assigned a unique device code in accordance with UIDAI specifications. This unique device identifier shall be transmitted with every authentication transaction, along with the UIDAI-assigned institution code for SCNL, as prescribed under the latest UIDAI API documentation.

In addition, each authentication transaction shall be assigned a unique transaction number generated automatically by the authentication device. Such transaction numbers shall be sequential or incremented in a controlled manner to ensure traceability, auditability, and prevention of replay or duplication attacks.

14.2. Secure Network Connectivity and Perimeter Protection

All network communication between SCNL, its Sub-AUAs, Business Correspondents, service providers, and Authentication Service Agencies shall be conducted over secure and trusted communication channels. Wherever feasible, connectivity with ASAs shall be established through leased lines or equivalent private and secure network links.

In circumstances where public networks are utilised, secure communication protocols such as Secure Sockets Layer or Virtual Private Network technologies shall be implemented to encrypt data in transit and protect against interception or unauthorised access.

Servers supporting Aadhaar authentication services shall be hosted behind appropriately configured firewalls. Firewall rules shall be designed to restrict incoming network traffic strictly to authorised sources, including SCNL's designated Point of Transaction terminals, and to block all unauthorised access attempts.

14.3. Communication Usage Controls and Acceptable Practices

Use of communication tools, including web-based email services, for Aadhaar-related activities shall be restricted to official purposes only and shall comply with SCNL's acceptable usage policies and information security guidelines. Personnel shall be prohibited from using unauthorised communication channels for transmission of Aadhaar-related information.

SCNL shall periodically review communication security controls to ensure their continued effectiveness and alignment with evolving regulatory requirements and threat landscapes.

15. Information Security Incident Management

SCNL shall maintain a structured and responsive information security incident management framework to ensure timely identification, reporting, investigation, and remediation of Aadhaar-related security incidents. The framework shall be designed to minimise impact, ensure regulatory compliance, and prevent recurrence.

15.1. Incident Identification and Regulatory Reporting

SCNL shall promptly identify, assess, and report any security weaknesses, suspected incidents, unauthorised access, misuse, or violation of Aadhaar-related security requirements. All reportable incidents shall be communicated to the Unique Identification Authority of India without delay and in the manner prescribed under applicable regulations.

Any confirmed or suspected confidentiality breach or security incident involving Aadhaar-related information shall be reported to UIDAI within twenty-four hours of detection, irrespective of whether the incident originates within SCNL's systems or within the ecosystem of its Sub-AUAs, Business Correspondents, or service providers.

15.2. Third-Party Incident Awareness and Accountability

SCNL shall ensure that all Sub-AUAs, Business Correspondents, and other third-party service providers involved in Aadhaar authentication are aware of, and comply with, prescribed Aadhaar incident reporting obligations. Contractual arrangements with such entities shall incorporate incident reporting requirements, escalation timelines, and cooperation obligations for investigation and remediation.

SCNL shall retain overall accountability for Aadhaar-related incident reporting and regulatory coordination, irrespective of whether the incident occurs within its own environment or that of an outsourced or partner entity.

15.3. Incident Investigation and Root Cause Analysis

For all material or significant Aadhaar-related security incidents, SCNL shall conduct a detailed Root Cause Analysis to identify underlying technical, procedural, or human factors contributing to the incident. Where incidents involve Sub-AUAs or third-party service providers, such entities shall be required to support the investigation and provide necessary information.

Based on the findings of the Root Cause Analysis, SCNL shall implement appropriate corrective and preventive actions to mitigate identified risks, strengthen controls, and reduce the likelihood of recurrence. Records of incidents, investigations, and remediation actions shall be maintained for audit and regulatory review.

16. Compliance

SCNL shall ensure continuous compliance with all applicable legal, regulatory, and contractual requirements governing Aadhaar authentication activities, supported by robust audit, oversight, and corrective action mechanisms.

16.1. Regulatory Compliance and Authorisations

SCNL shall comply at all times with the Aadhaar Act, 2016, the Aadhaar Regulations, 2016, the UIDAI agreement, and all circulars, advisories, technical specifications, and directions issued by UIDAI from time to time. Prior approval of UIDAI shall be obtained before appointment of any entity as a Sub-AUA, and necessary permissions shall be regularised for existing Sub-AUAs where applicable. All Aadhaar authentication applications deployed by SCNL and its Sub-AUAs shall clearly display the SCNL logo to ensure accountability and traceability in accordance with UIDAI requirements.

SCNL and its ecosystem partners, including Sub-AUAs, Business Correspondents, and service providers, shall ensure compliance with all applicable laws, regulations, and UIDAI-prescribed guidelines governing Aadhaar authentication activities.

16.2. Audit, Assurance and Oversight

All applications used for Aadhaar authentication shall be subjected to information systems audits conducted by auditors certified by STQC or CERT-In, and the corresponding compliance audit reports shall be submitted to UIDAI as prescribed. Sub-AUAs shall be permitted to access Aadhaar authentication services only through duly audited and approved client applications.

SCNL shall ensure that its Aadhaar authentication operations and supporting systems are audited at least annually by information systems auditors certified by recognised authorities. In addition to audits initiated by SCNL, UIDAI may conduct audits of SCNL's systems and operations, either directly or through auditors appointed by UIDAI, and SCNL shall extend full cooperation for such audits.

16.3. Non-Compliance Management, Controls and Continuous Monitoring

Any instances of non-compliance identified through audits, inspections, or regulatory reviews shall be promptly addressed by management through identification of root causes, evaluation of measures to prevent recurrence, and implementation of appropriate corrective and preventive actions, followed by review of their effectiveness.

SCNL shall ensure that only duly licensed software is deployed within Aadhaar-related infrastructure environments, with accurate records of software licences maintained and updated on an ongoing basis. Fraud analytics capabilities shall be deployed to analyse Aadhaar authentication transactions for detection and prevention of fraudulent activity. Further, SCNL shall conduct periodic audits of Sub-AUAs, Business Correspondents, and other third-party service providers involved in Aadhaar authentication to ensure end-to-end compliance with applicable regulatory and UIDAI requirements.

17. Change Management

SCNL shall establish and maintain a structured change management framework for all Aadhaar authentication related applications, infrastructure, processes, and information processing facilities. All changes, whether technical, procedural, or operational in nature, shall be formally documented, reviewed, and approved prior to implementation to ensure that security, compliance, and system integrity are not compromised.

A centralised change log or change register shall be maintained to record details of all changes performed, including the nature of the change, approval authority, implementation date, and post-implementation status. Change records shall be retained in an auditable manner and shall be made available for internal review, regulatory inspection, and UIDAI audits as required.

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***