Saraswat Bank

Saraswat Co-operative Bank Ltd.

(Scheduled Bank)

Aadhaar Data Privacy Policy – Addendum to IT Policy

Version 1.1

Effective From: 1st October 2022

Document ID: SCB/ITD/2022/ADPP/002

Document Classification: Confidential

Saraswat Co-operative Bank Ltd

Ekanath Thakur Bhavan, 953,

Appasaheb Marathe Marg,

Prabhadevi, Mumbai- 400 025

Document Control

Document Name	Aadhaar Data Privacy Policy
Classification	Internal and Confidential
Document#	Saraswat Co-op Bank – Aadhaar Data Privacy Policy v1.1
Version	1.1
Date Released	13st April 2023

Document Ownership

Prepared By:	Shiny Mithbaokar DGM (DBD)	**Document Owner**	Head – IT (Operations)
Reviewed By:	Srinivas Rao, Head - IT Infrastructure and Projects	**Recommended By:**	M. D. Operations
Approved By:	Board	**Date of Approval**	

Revision History

Sr. No.	Author	Date	Reason for Revision	Version Number
1	Head – IT Operations	23rd September 2022	1st Release – Aadhaar (Authentication and Offline Verification) Regulations, 2021	Version 1.0
2	Head – IT Operations	13st April 2023	2nd Release – Aadhaar (Authentication and Offline Verification) Regulations, 2021	Version 1.1

Distribution

Sr. No.	To	Date	Version Number
1	All employees and Customers	1st October 2022	Version 1.0
2	All employees and Customers	13st April 2023	Version 1.1

SARASWAT BANK – AADHAAR DATA PRIVACY POLICY

A. EXECUTIVE SUMMARY:

Saraswat Bank recognizes the security of UIDAI information in line with the Aadhaar Act 2016. The confidentiality, integrity, and availability of these shall be always maintained by these partners by deploying security controls in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards.

B. AADHAAR DATA PRIVACY POLICY:

Objective & Purpose:

To provide a framework of rules / regulations / standards / practices to the Aadhaar Data Privacy Policy to ensure that same are in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards.

This policy outlines the Information Security Policy and Information Security Controls applicable to the Bank acting as Authentication User Agency (AUA)/KYC User Agency (KUA). In addition to the bank's Information Security Policy and Cyber Security Policy, the UIDAI security policy outlines the additional security controls and specific measures to protect Aadhaar data collected, stored, and processed by the bank.

Bank shall ensure the security of UIDAI information assets handled by bank as listed below:

1. Providing AUAs/KUAs with an approach and directives for deploying security controls for all information assets used by them for providing services.

2. Establishing review mechanism to ensure that the AUAs/KUAs adhere to all provisions of the UIDAI Information Security Policy for AUAs/KUAs.

Coverage :

This policy covers the following broad areas which help establish, govern and manage Aadhaar Data Privacy Policy as directed by UIDAI on the basis of following circulars.

1. Aadhaar Regulations 2016
2. Aadhaar (Authentication and Offline Verification) Regulations 2021

I. Scope:

- Design suitable controls to ensure the privacy and security of the Biometric information of the customer as well as Aadhaar number and any other data received from the UIDAI in due course of authentication.
- To provide necessary guidelines to enable compliance with Aadhaar Act 2016 and any other applicable circulars or directions issued by the UIDAI.

II. Applicability:

The policy will apply to all departments/employees of the bank which access, process or store Aadhaar number and any other data received from the customers or UIDAI in due course of authentication.

III. Ownership:

The ownership of the Aadhaar Data Privacy Policy is with the Digital Banking Department.

IV. Review:

Aadhaar Data Privacy Policy shall be reviewed once in Two years or earlier, in the event of significant changes occur to ensure its continuing suitability, adequacy, effectiveness and regulatory compliances. Procedures and Processes will be reviewed and updated accordingly.

V. Approval :

Aadhaar Data Privacy Policy and its updates shall be placed by the Head DBD to the Board. Aadhaar Data Privacy Policy shall be reviewed & approved by the Board.

VI. Change / Version Control :

Head – DBD shall control the change and version of the policy document.

VII. Distribution :

The Aadhaar Data Privacy Policy shall be distributed among following departments

- IT Department
- Information Security Dept.
- Digital Banking Dept.
- Retail Dept.
- Risk Dept.
- Compliance Dept.
- Credit Card Dept.
- IBD
- Treasury
- Wholesale Banking

VIII. Enforcement and Compliance :

- Enforcement of the Aadhaar Data Privacy Policy shall be mandatory.
- Compliance with Aadhaar Data Privacy Policy is mandatory for all applicants as per applicability.

IX. Dispensation / Exception :

- Dispensation to be sought from Head - Digital Banking for any deviations to the Aadhaar Data Privacy Policy based on adequate business justification and recommendation / approval by respective Business Head / Function Head, unless otherwise specified in specific policy in this document.
- Head – DBD shall present such dispensations to MD-Operations for ratification.

X. Construction of this document :

The Aadhaar Data Privacy Policy has been developed in line with the Aadhaar Act 2016, UIDAI, Aadhaar Authentication Application Security Standards.

XI. Structure :

This document containing policies is structured as under :

Objective: This describes the objectives for having the relevant policy control in place.

Review & Maintenance: This defines the frequency of review and the person responsible for carrying out the review.

Broad Contours: The Policy Statement is intent of the management about the control requirement. This is a management direction for compliance by all those covered under the scope of this document.

C. POLICY :

a) Introduction :

- The Unique Identification Authority of India has been established by the Government of India with the mandate to the Authority is to issue unique identification number (called Aadhaar ID or UID) to Indian residents that is robust enough to eliminate duplicate and fake identities and can be verified and authenticated using biometrics in an easy and cost-effective manner.
- The UID has been envisioned as a means for residents to establish their identity easily and effectively, to any agency, anywhere in the country, without having to repeatedly produce identity documentation to agencies
- The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity biometrically through presentation of their fingerprints/ iris authentication or non-biometrically using a One Time Password (OTP) sent to registered mobile phone or e-mail address.

b) Definition

- Authentication User Agencies (AUA): Authentication User Agency is an organisation or an entity using AADHAAR authentication as part of its applications to provide services to residents.
- KYC User Agencies (KUA): KYC User Agency is an organisation or an entity using AADHAAR authentication and eKYC services from UIDAI as part of its applications to provide services to residents.

An AUA sends authentication requests to enable its services / business functions. An AUA connects to the CIDR through an ASA (either by becoming ASA on its own or contracting services of an existing ASA). AUA/KUA uses demographic data, and/or biometric data in addition to the resident's UID. They use Aadhaar authentication to provide services such as opening of bank account, LPG connection, etc. to residents. Since the AUAs handle sensitive resident information such as the Biometric information, Aadhaar number, eKYC data etc. of the residents, it becomes imperative to ensure its security.

c) Aadhaar Authentication Services:

- Aadhaar Authentication is defined as the process wherein, Aadhaar number along with the Aadhaar holder's personal identity information is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof based on the match with the Aadhaar holder's identity information available with it.
- The purpose of Authentication is to enable Aadhaar – holders to prove identity and for service providers to confirm the resident's identity claim to supply services and give access to benefits. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response.
- e-KYC Service: UIDAI also provides the e-KYC service, which enables a resident having an Aadhaar number to share their demographic information (i.e., Name, Address, Date of Birth, Gender, Phone & E-mail) and Photograph with UIDAI partner organization (called a KYC User Agency – KUA) in an online, secure, auditable manner with the resident's consent. The consent by the resident can be given via a Biometric authentication or One Time Password (OTP) authentication.

- The Bank has entered into a formal agreement with UIDAI to access Aadhaar authentication services, and e-KYC services. To protect the Aadhaar Beneficiary, the data privacy policy of the Bank has been defined and formulated.

d) Data Privacy on Aadhaar and Biometric details:

- The submission of Aadhaar details by a customer to the Bank is voluntary and the Bank shall not insist on a customer to produce their Aadhaar details for availing any of the services. In cases where Aadhaar number is offered voluntarily by the customer to the Bank, the Bank shall seek a declaration by the customer towards the same.
- Where customers are not willing to provide Aadhaar number for authentication Bank will provide alternative authentication mechanism to customers for availing the services.
- For cases where e-KYC verification is required, the Bank shall get an explicit consent from the resident for download of resident demographic details from UIDAI mentioning the purpose for which the details are sought.
- The consent shall be either in the form of an authorization letter or a provision to electronically record the consent in a software application.
- Biometric details shall also be captured by the Bank for the purposes of authentication, for example to authenticate a customer before permitting transaction through a Micro ATM / any other device, as an AEPS (Aadhaar Enabled Payment System) transaction.
- The biometric details whenever captured by the Bank shall be used only for data exchange with UIDAI which validates the captured biometric data against the biometric data maintained in CIDR (Central Identities Data Repository) against the specific Aadhaar number.
- The Bank shall use STQC certified devices for demographic details received from UIDAI will be stored for future reference, the biometric details shall not be stored by the Bank in any manner and form.
- A system log wherever required shall be maintained to extract the details in case of disputes. The logs should capture Aadhaar Number, timestamp etc., but will not capture/store the PID (Personal Identity Data) associated with the transaction.

e) Asset Management :

Authentication devices used to capture residents biometric should be STQC certified as specified by UIDAI.

f) Access Control :

The local security settings on all the systems shall be aligned and synced with the Active Directory or similar solutions for group policy enforcement.

g) Password Policy :

The password policy is applicable as per our Information Security Policy.

h) Cryptography :

- The Personal Identity data (PID) block comprising of the resident's demographic / biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication (for e.g., PoT terminal)
- The PID shall be encrypted during transit and flow within the AUA / KUA ecosystem and while sharing this information with ASAs.
- The encrypted PID block should not be stored unless in case of buffered authentication for not more than 24 hours after which it should be deleted from the local systems.
- The authentication request shall be digitally signed by either by Bank or ASA as per the mutual agreement between them.
- While establishing a secure channel to the AADHAAR Authentication Server (AAS the bank shall verify the following:
  - ✓ The digital certificate presented by the AAS has been issued / signed by a trusted Certifying Authority (CA).
  - ✓ The digital certificate presented by the AAS has neither been revoked nor expired.
  - ✓ The Common Name (CN) on the certificate presented by the AAS matches with its fully qualified domain name (presently, auth.uidai.gov.in).
- Key management activities shall be performed by all ASAs to protect the keys throughout their lifecycle. The activities shall address the following aspects of key management, including.

- ✓ key generation.
- ✓ key distribution.
- ✓ Secure key storage.

- ✓ key custodians and requirements for dual Control.
- ✓ prevention of unauthorized substitution of keys.
- ✓ Replacement of known or suspected compromised keys.
- ✓ Key revocation and logging and auditing of key management related activities.

- HSM shall be deployed in the Bank's network to store the encryption keys for the Aadhaar vault and other Aadhaar related key management process. Access to HSM shall be restricted and periodic access reviews must be conducted for HSM. HSM shall be working in FIPS 140-2 operational mode for all encryption activities.

i) Physical and Environmental Security

- The Bank servers involved in Aadhaar authentication mechanism should be placed in a secure lockable cage in the Data Centre.
- The facility should be manned by security guards during and after office hours
- CCTV surveillance shall cover the data centres where Aadhaar data is collected, processed, stored, and disposed.

j) Operations Security

- Bank shall complete the AADHAAR AUA / KUA on-boarding process before the commencement of formal operations.
- Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
- AUA / KUA employees shall not intentionally write, generate, compile copy, or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID information.
- All hosts that connect to the AADHAAR Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed on such hosts.
- Network intrusion and prevention systems should be in place – e.g., IPS, IDS, WAF, etc.
- AUAs / KUAs shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring.
- Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only.
- The authentication audit logs should contain, but not limited to, the following transactional details:
  - ✓ Aadhaar Number against which authentication is sought.
  - ✓ Specified parameters of authentication request submitted.
  - ✓ Specified parameters received as authentication response.
  - ✓ The record of disclosure of information to the Aadhaar number holder at the time of authentication
  - ✓ Record of the consent of Aadhaar number holder for the resident
  - ✓ Details of the authentication transaction such as API Name, AUA / KUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-id entity information.
- Logs shall not, in any event, retain the PID, biometric and OTP information.
- No data pertaining to the resident or the transaction shall be stored within the terminal device.
- The logs of authentication transactions shall be maintained by Bank for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.

- Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations governing the Bank, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes.

- All computer clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation.
- The Bank's server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities.
- Bank shall implement only those changes related to Aadhaar which are approved by UIDAI for execution.

k) MISUSE OF INFORMATION :

The Bank will inform the Authority and the Aadhaar number holder, without undue delay and in no case beyond 72 hours after having knowledge of misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information.

D. REGULATORY REFERENCES :

- Aadhaar Act 2016
- Requesting Entity Compliance Checklist_v_2.0
- Aadhaar (Authentication and Offline Verification) Regulations, 2021
- UIDAI Information Security Policy for AUA/KUA
- Various circulars issued by UIDAI

E. GLOSSARY :

KYC	Know Your Customer
MD	Managing Director
AUA	Authentication User Agency
ASA	Authentication Service Agency
CIDR	Central Identities Data Repository
KUA	Know your customer User Agencies
OTP	One Time Password
PID	Personal Identity Data
STQC	Standardisation Testing and Quality Certification Directorate