SBFC FINANCE LIMITED

SBFC_32_IT_Aadhar_Data_Privacy_Policy_v2.2

(Internal)

Disclaimer: No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, recording, photocopying or otherwise outside of SBFC Finance Limited without the prior permission of SBFC Finance Limited.

Document Control

Authorization

Document Title: Aadhar Data Privacy Policy

Document Code: SBFC_32_IT_Aadhar_Data_Privacy_Policy_v2.2

Document Classification: Internal

Item	Description	Approved Date
Author	Shivaji Manwadkar (Senior Manager)	25-01-2025
Recommended by	Gunjan Dedhia (Head Applications & Support)	
Reviewed by	Namrata Sajnani (Chief Compliance Officer)	
	Ganesh Vaidya (Chief Technology Officer)	
	Murali Singh (Data Protection Officer)	
	Kalpesh Surjiani (vCISO)	
	Pankaj Poddar (Chief Risk Officer)	
	Aseem Dhru (MD & CEO)	
Approved by	Board	

Document Approval History

Version	Approved (by)	Date	Signature/Email/Meeting	Remarks
1.0	Board	02-06-2023	Meeting	Initial Version
1.1	CTO	09-12-2023	Meeting	We have refined the versioning control
2.0	Board	25-01-2024	Meeting	Annual Review
2.1	CTO	12-11-2024	Email	CCO changed from Jay Mistry to Namrata Sajnani.
2.2	Board	25-01-2025	Meeting	Updated as per ISO 27701:2019

Table of Contents

1.Purpose

This policy outlines the Information Security Policy and Information Security Controls applicable to the SBFC FINANCE LIMITED acting as Authentication User Agency (AUA)/KYC User Agency (KUA). In addition to the SBFC FINANCE LIMITED's Information Security Policy and Cyber Security Policy, the UIDAI security policy outlines the additional security controls and specific measures to protect the Aadhaar data collected, stored, and processed by the SBFC FINANCE LIMITED. SBFC FINANCE LIMITED shall ensure the security of UIDAI information assets handled by SBFC FINANCE LIMITED 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 a review mechanism to ensure that the AUAs/KUAs adhere to all provisions of the UIDAI Information Security Policy for AUAs/KUAs.
3. Aadhaar-related data collection should be strictly aligned with specific purposes as defined under the DPDP Act. Collecting data beyond the intended purpose, such as for targeted advertising or unrelated profiling, should be prohibited.
4. Ensure that only the minimum necessary personal data is collected for Aadhaar-related services, aligning with the data minimization principle in the DPDP Act.

2. Scope

To design suitable controls to ensure the privacy and security of the Biometric information of the customer as well as the 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.

3. Distribution

The Aadhaar Data Privacy Policy shall be distributed among following departments:

- IT Department
- Information Security Dept
- Risk and Compliance Dept
- Operations

4. Introduction

The Unique Identification Authority of India has been established by the Government of India with the mandate to the Authority is to issue a 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 the presentation of their fingerprints/ iris authentication or non-biometrically using a One Time Password (OTP) sent to registered mobile phone or e-mail address.

KUA uses demographic data, and/or biometric data in addition to the resident's UID. They use Aadhaar authentication to provide services such as E-KYC verification and fetching demographic information for verification of load applicants. Since the AUAs handle sensitive resident information such as Biometric information, Aadhaar number, E-KYC data etc. of the residents, it becomes imperative to ensure its security.

5. Aadhar Card 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 uses 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.

  Note:- Individuals shall have the right to withdraw their consent for the use of their Aadhaar data, and such withdrawal should be respected immediately. This is a core right under the DPDP Act, ensuring individuals have control over their personal data.
- SBFC FINANCE LIMITED 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 SBFC FINANCE LIMITED has been defined and formulated.

6. Data Privacy on Aadhar and Biometrics

The submission of Aadhaar details by a customer to the SBFC FINANCE LIMITED is voluntary and the SBFC FINANCE LIMITED shall not insist a customer to produce their Aadhaar details for availing any of the services. In cases where an Aadhaar number is offered voluntarily by the customer to the SBFC FINANCE LIMITED, the SBFC FINANCE LIMITED shall seek a declaration by the customer towards the same.

- For cases where e-KYC verification is required, the SBFC FINANCE LIMITED shall get 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.
- The biometric details whenever captured by the SBFC FINANCE LIMITED 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 SBFC FINANCE LIMITED shall use STQC certified devices for demographic details received from UIDAI shall be stored for future reference, the biometric details shall not be stored by the SBFC FINANCE LIMITED 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 mask Aadhaar Number, timestamp etc., but shall not capture/store the PID (Personal Identity Data) associated with the transaction.
- Aadhar enrolment and updating entails the process of capturing the personal information of the customers along with their Biometric details. To protect data privacy, the enrolment application sought by the SBFC FINANCE LIMITED from the customer to assist in internal data entry process shall be returned to the resident/shall be destroyed internally.
- The data so captured shall be sent to UIDAI as a straight through process. SBFC FINANCE LIMITED shall not store the data captured (both biometric and personal information) in any manner and form.

7. Human Resources

- The SBFC FINANCE LIMITED shall appoint a SPOC/team for all UIDAI-related activities and communication with UIDAI.
- Induction as well as periodic functional and information security training shall be conducted for all SBFC FINANCE LIMITED personnel for UIDAI related services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
- All employees accessing UIDAI information assets shall be made aware of UIDAI information security policy and controls.

8. Asset management

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

9. 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 endpoint 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 authentication request shall be digitally signed by either SBFC FINANCE LIMITED or ASA as per the mutual agreement between them.
- While establishing a secure channel to the AADHAAR Authentication Server (AAS the SBFC FINANCE LIMITED 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 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:

a) key generation.

b) key distribution.

c) Secure key storage.

d) key custodians and requirements for dual Control.

e) prevention of unauthorized substitution of keys.

f) Replacement of known or suspected compromised keys.

g) Key revocation and logging and auditing of key management related activities.

- HSM is being deployed in the SBFC FINANCE LIMITED’s network corporate Tier 4 Data Centre to store the encryption keys for the Aadhaar vault and other Aadhaar-related key management processes. 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.

10. Physical and Environment Security

- The SBFC FINANCE LIMITED servers involved in the 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 centers where Aadhaar data is collected, processed, stored, and disposed.

11. Operational Security

- The SBFC FINANCE LIMITED 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:
  a. Aadhaar Number against which authentication is sought.
  b. Specified parameters of authentication request submitted.
  c. Specified parameters received as authentication response.
  d. The record of disclosure of information to the Aadhaar number holder at the time of authentication.
  e. Record of the consent of Aadhaar number holder for the resident.
  f. Details of the authentication transaction such as API Name, AUA / KUA Code, 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 the SBFC FINANCE LIMITED 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 SBFC FINANCE LIMITED, 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 an NTP server or must be managed centrally and a procedure shall be made to check for and correct any significant variation.
- The SBFC FINANCE LIMITED's server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities.
- SBFC FINANCE LIMITED shall implement only those changes related to Aadhaar which are approved by UIDAI for execution.

12. Grievance Redressal and Data Protection Officer (DPO)

For any concerns, discrepancies, or grievances related to the processing and use of your information, you may contact the grievance officer, or the Data Protection Officer (DPO), who would also be handling the responsibility of Aadhar Officer appointed by SBFC. The DPO is responsible for ensuring compliance with applicable data protection laws, addressing privacy-related concerns, and safeguarding PII rights.

You can reach the DPO at:
Email: murali.singh@sbfc.com
Address: 103, 1st Floor, C&B Square, Sangam Complex,

Andheri Kurla Road, Village Chakala,

Andheri (East), Mumbai - 400059

13. Communication Strategy

- In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometric reader and the device performing the encryption shall be secured against all security threats/attacks.

- Terminal devices shall provide different logins for operators. These users shall be authenticated using some additional authentication scheme such as passwords, AADHAAR authentication, etc.
- Each terminal shall have a unique terminal ID. This number must be transmitted with each transaction along with UIDAI assigned institution code for the SBFC FINANCE LIMITED as specified by the latest UIDAI API documents.
- A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transaction processed.
- The network between SBFC FINANCE LIMITED and ASA shall be secured. SBFC FINANCE LIMITED shall connect with ASAs through leased lines or similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.
- The SBFC FINANCE LIMITED Authentication server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the SBFC FINANCE LIMITED Authentication server from all sources other than AUAs / KUAs PoT terminals.
- Use of web-based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy.
- UIDAI should be informed about the ASAs, that SBFC FINANCE LIMITED has entered into an agreement.
- SBFC FINANCE LIMITED shall be responsible for reporting any security weaknesses, any incidents, possible misuse, or violation of any of the stipulated guidelines to UIDAI immediately.

14. Compliance

- SBFC FINANCE LIMITED shall comply with all terms and conditions outlined in the UIDAI AUA / KUA agreement and AUA / KUA compliance checklist.
- SBFC FINANCE LIMITED shall ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis and on a need basis to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request.
- If any non-compliance is found because of the audit, management shall:
  a) Determine the causes of the non-compliance.
  b) Evaluate the need for actions to avoid recurrence of the same.
  c) Determine and enforce the implementation of corrective and preventive action.
  d) Review the corrective action taken.
- SBFC FINANCE LIMITED shall use only licensed software for UIDAI related infrastructure environment. Record of all software licenses shall be kept and updated regularly.
- SBFC FINANCE LIMITED and its partners shall ensure compliance with all the relevant laws, rules, and regulations, including, but not limited to, ISO27001:2013 Standard, Information Technology Act 2000 and 2008 amendments, Aadhaar Act, 2016 and Regulations.

- E-KYC should be used as a facility using only biometric and OTP modalities by the AUAs.
- Separate license keys must be generated by all AUAs for their SUB-AUAs from the UIDAI portal.
- SBFC FINANCE LIMITED shall have authentication servers routing to CIDR hosted in Data Centers within India. SBFC FINANCE LIMITED shall adhere to all the notifications, guidelines and circulars published by UIDAI. The compliance team of SBFC FINANCE LIMITED shall be responsible for the communication of the published information by UIDAI to all its personnel.
- Individuals should have the right to access their Aadhaar data, request corrections, and challenge any inaccuracies. This aligns with the DPDP Act's provision that data principals (individuals) should have the right to correct or update their data.

15. Change Management

- SBFC FINANCE LIMITED shall document all changes to UIDAI Information Processing facilities/ Infrastructure/ processes.
- SBFC FINANCE LIMITED shall implement only those changes related to Aadhaar which are approved by UIDAI for execution.
- Change log/ register shall be maintained for all changes performed.

16. Application Security

- All of the applications developed by AUA/KUA, or authentication applications being used by AUA/KUA developed by third party vendors must adhere to Aadhaar Authentication Application Security Standard (AAASS). The standard applies to all entities that perform Aadhaar authentication and store, process or transmit Aadhaar number holder data.
- Application shall be certified by STQC or CERT-In empaneled.
- Source code review shall be conducted on the application and the report of the same shall be maintained.
- Aadhaar Authentication Application Security Standard includes technical and operational requirements set by the Unique Identification Authority of India (UIDAI) to protect Aadhaar number holder data.
- Prior to deployment of the application in the production environment, the requesting entity shall ensure that the application meets all the requirements of the AAASS satisfactorily.

17. Enforcement

1. All staffs (Permanent, Temporary, Contractors and Third-Party staff) are required to comply with this policy and any personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

2. Staff having knowledge of any misuse or malpractice of SBFC IT Systems and their associated information processing facilities must report to their respective managers immediately and subsequently report as Information Security Incident for necessary action