CUSTOMER DATA STORAGE, RETENTION, ARCHIVAL AND DESTRUCTION POLICY

OF

SHRI RAM FINANCE CORPORATION PRIVATE LIMITED

SHRI RAM FINANCE
CORPORATION PVT. LTD.
EMPOWERING FINANCIAL STRENGTH

1. PREAMBLE

Shri Ram Finance Corporation Pvt. Ltd. ("SRFC" or "the Company"), a Non-Banking Financial Company (NBFC), recognizes that customer information is a critical business asset and is committed to protecting the confidentiality, integrity, availability, and privacy of customer data throughout its lifecycle.

This Policy establishes a comprehensive framework governing the collection, storage, processing, retention, archival, sharing, and destruction of customer information in compliance with applicable regulatory requirements and industry best practices.

2. OBJECTIVE

The objectives of this Policy are to:

a) Ensure protection of customer information against unauthorized access, disclosure, alteration, loss, or misuse.

b) Define categories of customer data permitted to be collected and stored.

c) Establish retention periods for customer records based on regulatory, legal, and business requirements.

d) Define secure archival and destruction procedures.

e) Establish accountability for data governance and oversight.

f) Ensure compliance with applicable RBI directions and statutory requirements.

3. REGULATORY REFERENCES

This Policy is framed considering:

- RBI Master Direction – Information Technology Framework for NBFC Sector.
- RBI Master Direction – Know Your Customer (KYC).
- RBI Digital Lending Guidelines.
- RBI Guidelines on Outsourcing of Financial Services.
- Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023.
- Applicable contractual, legal, and regulatory obligations.

4. SCOPE

This Policy applies to:

- All customer information collected, processed, stored, transmitted, archived, or destroyed by SRFC.
- All employees, directors, officers, consultants, contractors, and outsourced service providers.

- All business applications, databases, infrastructure, and storage repositories maintained by the Company.

5. DATA GOVERNANCE PRINCIPLES

SRFC shall adhere to the following principles:

Data Minimization

Only information necessary for legitimate business, regulatory, legal, and operational purposes shall be collected and retained.

Purpose Limitation

Customer information shall be collected and processed only for lawful and authorized purposes.

Security by Design

Appropriate technical and organizational controls shall be implemented throughout the information lifecycle.

Accountability

All departments handling customer information shall be accountable for compliance with this Policy.

6. CUSTOMER DATA CATEGORIES

The Company may collect and maintain the following categories of information:

6.1 Identity Information

- Name
- Photograph
- Date of Birth
- Gender
- Signature
- Customer Identification Number

6.2 KYC Information

- PAN
- Aadhaar (as permitted by law)
- Passport
- Driving Licence
- Voter ID
- CKYC Identifier

6.3 Contact Information

- Address

- Mobile Number
- Email Address

6.4 Financial Information

- Bank Account Details
- Income Documents
- Credit Bureau Information
- Loan Repayment Information

6.5 Transaction Information

- Loan Applications
- Sanction Details
- Repayment History
- Collection Records

6.6 Digital Lending Information

- Consent Records
- Key Fact Statements
- Digital Acceptance Records
- Audit Logs

7. DATA STORAGE REQUIREMENTS

7.1 Storage Standards

Customer information shall be stored only on:

- Company-owned infrastructure;
- RBI-compliant cloud environments approved by the Company;
- Authorized data centres located within India.

Customer information shall not be stored on unauthorized devices, removable media, personal systems, or unapproved cloud platforms.

7.2 Security Controls

The Company shall implement:

- Encryption of sensitive information at rest and in transit.
- Role-based access controls.
- Multi-factor authentication for privileged users.

- Database activity monitoring.
- Security logging and audit trails.
- Backup and recovery mechanisms.
- Vulnerability Assessment and Penetration Testing (VAPT).

7.3 Data Masking

Sensitive information such as PAN, Aadhaar Number, and Bank Account Number shall be masked wherever operationally feasible.

8. ACCESS CONTROL

Access to customer information shall be governed by:

- Need-to-Know Principle.
- Least Privilege Principle.
- Role-Based Access Control (RBAC).

User access shall be:

- Formally approved.
- Periodically reviewed.
- Revoked immediately upon employee separation or transfer.

9. CUSTOMER DATA RETENTION

Customer information shall be retained only for as long as necessary to fulfil business, legal, audit, and regulatory requirements.

Record Category	**Minimum Retention Period**
KYC Documents	5 Years after closure of relationship
Customer Identification Records	5 Years
Loan Application Files	10 Years
Loan Agreements	10 Years after closure
Repayment Records	10 Years
Collection Records	10 Years
Customer Communications	8 Years
Digital Lending Records	10 Years
CKYC Records	10 Years

Record Category	Minimum Retention Period
Audit Logs	Minimum 2 Years
Security Logs	Minimum 180 Days Online and Archived

Where any investigation, litigation, audit, inspection, or regulatory proceeding is pending, relevant records shall be preserved until closure of such proceedings.

10. DATA ARCHIVAL

Data no longer required for active operations but required for retention shall be archived in secure repositories.

Archived records shall:

- Remain encrypted.
- Be protected against unauthorized modification.
- Be recoverable when required.
- Maintain audit trails.

11. DATA SHARING AND THIRD-PARTY MANAGEMENT

Customer information may be shared only:

- With customer consent where required;
- To comply with legal or regulatory obligations;
- With authorized service providers under valid contractual arrangements.

All vendors shall:

- Execute confidentiality and data protection agreements.
- Maintain security controls equivalent to SRFC standards.
- Permit audits and inspections.
- Certify deletion of customer information upon contract termination.

12. DATA DESTRUCTION POLICY

Upon completion of the applicable retention period and subject to legal hold requirements, customer information shall be securely destroyed.

Electronic Records

Approved methods include:

- Secure deletion;
- Cryptographic erasure;

- Database purging;
- Media sanitization.

Physical Records

Approved methods include:

- Cross-cut shredding;
- Pulverization;
- Secure destruction through authorized agencies.

13. DATA DESTRUCTION REGISTER

The Company shall maintain a Data Destruction Register capturing:

- Description of records destroyed;
- Retention period completed;
- Date of destruction;
- Destruction method;
- Approval authority;
- Evidence of destruction.

14. EXCEPTIONS AND LEGAL HOLD

Destruction activities shall be suspended where records are required for:

- RBI inspections;
- Internal or external audits;
- Litigation;
- Law enforcement investigations;
- Regulatory proceedings.

15. ROLES AND RESPONSIBILITIES

Board of Directors

- Approve this Policy.
- Provide oversight on data governance.

IT Strategy Committee

- Monitor implementation and compliance.

CISO / Head – IT

- Ensure implementation of technical controls.

- Monitor policy compliance

Compliance Department

- Monitor regulatory adherence.

Business Functions

- Ensure proper handling of customer information.

Internal Audit

Independently assess effectiveness of controls and compliance

16. POLICY VIOLATIONS

Any violation of this Policy may result in:

- Disciplinary action;
- Termination of employment or contract;
- Regulatory reporting;
- Legal proceedings as applicable.

17. REVIEW OF POLICY

This Policy shall be reviewed annually or earlier in case of:

- Regulatory changes;
- Significant business changes;
- Technology changes;
- Security incidents.

18. BOARD APPROVAL

This Policy has been reviewed and approved by the Board of Directors of Shri Ram Finance Corporation Private Limited and shall remain effective until amended or replaced.

****