CUSTOMER PRIVACY POLICY

CRISS FINANCIAL LIMITED

Policy Version: V 1.0
Policy Owner: Information Security Department

CUSTOMER PRIVACY POLICY

Version Control Sheet

The Version Control Sheet is critical to Customer Privacy Policy. It documents the history of policy changes, ensuring transparency, traceability, and accountability. This section outlines all revisions, including the nature of changes, approval details, and implementation dates.

Version Number	Amendment Date	Effective Date	Approved By
1.0			Board

Note: This is the first version, future versions will be tracked and maintained as per the above table.

Version Control Procedures:

1. **Document Control**: The Information Security Team is responsible for maintaining the master version of the Security Exceptions Policy and ensuring that all changes are accurately documented in the Version Control Sheet.

2. **Change Requests**: Any proposed changes to the policy must be submitted to the Information Security Team using a formal Change Request Form. This form should include the rationale for the change, an impact assessment, and any relevant supporting documentation.

3. **Review and Approval**: The Information Security Team and relevant stakeholders review all proposed changes. The ISC, CISO, and potentially the Board of Directors must approve the modifications for significant changes.

4. **Version Numbering**: Each approved change results in a new policy version, with an increment in the version number. Minor changes (e.g., clarifications or typo corrections) result in a minor version increment (e.g., from 1.1 to 1.2), while significant changes result in a major version increment (e.g., from 1.0 to 2.0).

5. **Distribution**: Once a new version is approved, the updated policy is distributed organization-wide through official channels, including email notifications, intranet postings, and relevant training sessions.

6. **Archiving**: Previous versions of the policy are archived in a secure repository, accessible only by authorised personnel. These archives are maintained for audit purposes and to provide a historical record of policy evolution.

7. **Review Cycle**: The policy is reviewed annually, or more frequently, if necessary, to ensure it remains aligned with organisational objectives, regulatory requirements, and the evolving threat landscape.

CUSTOMER PRIVACY POLICY

Preamble:

Criss Financial Limited, referred as CFL, recognizes that one of its fundamental responsibilities is to ensure that CFL protects personal information entrusted to the CFL by its customers. This is critical for the maintenance of the company's reputation and for complying with its legal and regulatory obligations to protect the CFL's customer information. The company also follows a transparent policy to handle personal information of its customers.

In this Policy, personal information means any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with the company, can identify such person (e.g., telephone number, name, address, transaction history etc.).

The Policy is in compliance with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the "IT Rules") contained in the Information Technology Act 2000.

This policy is also in compliance to Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices, RBI/DoS/2023-24/107, Master Direction DoS.CO.CSITEG/SEC.7/31.01.015/2023-24 for customer data and privacy.

Definitions used in the Policy

1. **Customer** refers to all members who have taken a loan from CFL or from any other bank/NBFC/Other financial institution through CFL acting as agent/banking correspondent. This includes those members who have a current loan outstanding and those who have taken a loan earlier.
2. **Information/Data** includes any financial and personal data collected from the members at the time of loan application.

    - Financial information includes any data collected from the customer regarding her businesses, income, expenses, loans outstanding, repayment history, guarantors, or collateral.
    - Personal information and personal identifiable information (PII) include any data collected from the customer that is about her family, health, consumption behavior, personal preferences, attitudes, beliefs or living conditions. PII includes KYC information collected via Aadhaar or any identity proofs mandated as primary and secondary by the RBI.

3. **Records** can be either a tangible object or digital information.
4. **Records Management** is the practice of maintaining the records of an organization from data collection stage till the data disposal stage. This includes classification, storage, securing and destruction or archival preservation of records.
5. **Credit Bureau** is an independent organization that compiles information from credit grantors and other sources regarding individuals' credit applications and payment behavior.

Principles of Policy Design

The privacy policy is meant to ensure that the personal information shared by the customer with CFL is not used against their interests by CFL or shared with a third party without their consent.

The following are the set of principles to be followed in each of these circumstances.

Environment	Action	Principle
Internal	Collecting information	Discretion and adherence to RBI regulations in the collection of documentation from customers
	Using customer information	Protection of customer interest from misuse internally
External	Sharing information with Third parties	Any sharing of information will be with customer's knowledge and consent

Implementation details:

CUSTOMER PRIVACY POLICY

Information collected at origination

Discretion and adherence to regulations in the collection of documentation from customers:

- Only those documents as required and as per KYC guideline norms for identity proof and address proof will be collected from customers
- Photos to be collected from the customer when applying for a loan. These are for CFL's records only and will be used by staff to identify customers. If a photo or picture of a customer is to be used as part of marketing or other material, written permission will be obtained from the customer. Additionally, CFL will not permit the re-use of customer photos by any other institution without written consent from the customer.
- Provided that documents/ data/ photos/ information collected by CFL from customers may be used by CFL to process loans of customers through any other bank/NBFC/Other financial institution where CFL is acting as agent/banking correspondent.
- Aadhaar data collected to be masked, and electronic information is stored in vaults – Aadhaar vault and LMS accordingly as per the applicable regulatory guidelines.

Sharing customer information externally

A. Disclosure / Sharing of customer's personal information only under the following circumstances:

- As per the legal requirements or to comply with any legal process
- As a part of reciprocal information exchange with other financial institutions (such as a credit bureau)
- To process loans with any other bank/NBFC/Other financial institution where CFL is acting as agent/banking correspondent.
- Disclosure / Sharing of customer's personal information by CFL in compliance with legal processes/regulatory authorities, self-regulatory organizations, and other government agencies.
- Ensuring MoUs with service providers/research agencies/external consultants etc. and non-disclosure agreements cover client confidentiality.
- Company borrows money from Banks/FI's/DFI's/Other financial institutions for on lending and in regard will have to share underlying loan details as part of book debts.
- Company's core includes raising funds by selling of receivables and to facilitate transaction, the information with respect to pools will be shared.

B. In any other circumstance, customer information will be shared only if:

- The customer has directed CFL to share it with a third party
- There is written permission from the customer authorizing the disclosure or as agreed in the loan documents

C. Customer Consent:

- Customer consent is taken during the loan origination.
- Customer must sign a consent form to provide his PII data in favour of CFL for processing the loan requirement.
- Consent of customer is explicitly taken before sending marketing communications and updates.
- Customer consent is taken wherever applicable with reference to data being shared to third party.

Aadhaar Data Security

Aadhaar Number captured in the system is by default masked in the Frontend and Backend of the Lending Management System and only privileged users can access this data and the system also gives an equal number which is again unique generated post dedupe of actual Aadhaar.

CUSTOMER PRIVACY POLICY

Training to customer on Privacy policy

In the customer training module:

- Customers are made aware of their privacy rights and responsibilities before they receive their loans.
- Their responsibilities include understanding CFL's privacy of customer data clause and their rights; keeping their information updated; storing their loan cards in a safe place; informing the company if their information has been misused; and keeping the group's financial data confidential
- Emphasizes the importance of keeping confidential information safe within the group
- It is explained to the borrowers that company can sell the loan to any other entity and share the information pertaining to such sale
- Access to information will be restricted and It will be on need basis and no download of the customer information is allowed

Channel for complaints

- Customers can contact the customer care number (which will be available on their loan card & Company's Website) to record any complaint.
- If any staff is proven to have breached the privacy policy, he or she will be served with penalties (ranging from fines to dismissal) as per the HR policy.

Promoting Awareness among the staff

- A well-defined access control mechanism is available to control information within the company
- Staff will be trained on the privacy policy and its implications during induction and other staff refresher trainings
- At the time of appointment, each staff will be made to sign a non-disclosure/confidentiality clause, thereby agreeing to protect CFL's and clients' data.

Monitoring

To ensure the effective implementation of privacy policy, regular monitoring to the extent of its adherence by employees is important. Internal Audit team will monitor any deviations to the policy during the branch audits and reports the same for corrective measures. External Audit team will also monitor as part of standard audit procedures.

Applicability

The company collects three types of information: personal, sensitive personal data and non-personal information means any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with the company, can identify such person (e.g., telephone number, name, address, transaction history etc.).

KYC, Sensitive personal data or information of a person (PII) means such personal information which consists of information relating to passwords, financial information such as loan account or credit card or debit card or other payment instrument details, sexual orientation, physical physiological and mental health condition, medical records and history, biometric information, details of nominees and national identifiers including but not limited to:

Aadhaar Card, Passport Number, Income/Household information, PAN, Election Voter ID etc. For customers enrolled in services provided by CFL, such as online bill payment, personal information mandatorily required for the transactions are collected.

Any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purpose of these rules.

CUSTOMER PRIVACY POLICY

The information customers provide online is stored, processed, used, deleted as per applicable guidelines.

Non personal information includes the IP address of the device used to connect to the company's website along with other information such as browser details, operating system used, the name of the website that redirected the visitor to the CFL's website, etc. Also, when someone browse our website or receive any of our emails as part of borrower's services or product promotion etc, the company and our affiliated companies, use cookies and/or pixel tags to collect information and store the online preferences.

Information Security Mechanisms and Records Management:

CFL maintains physical and electronic safeguards to protect customers' personal and financial information including their photos. The company has placed the following mechanisms in place to ensure information – both physical and electronic data storage, access, retrieval, sharing of data:

Records Management and Physical Data Security

- CFL keeps customers' physical files at the branch that received the initial loan application and other CFL's offices in a safe manner and only authorized branch staff are permitted to access the data. The company may engage the services of reputed third-party service providers for record/ data storage/ management purposes under SLAs agreed by CFL with such third parties in writing. Such SLAs would cover aspects of client data confidentiality and related compliance requirements
- Records may be transferred with in India from branches to other offices of the company/ third party service providers for record keeping purposes
- The database of customers who do not have any current loan outstanding with CFL are properly archived and kept and stored in the same manner as we store data/ documents of our customers.
- All customer data/ records/ documents/ information shall be maintained by CFL for such time as may be required as per applicable laws, including the Prevention of Money Laundering Act and rules thereunder
- Customer data for the rejected loans are stored for six months as per the internal policy of the CFL and those (physical/digital) copies are destroyed subsequently.

Information/IT Security Mechanisms

- Branches can enter or update the customer data but cannot access other branch data or files preventing unauthorized sharing of data. Staff at Headquarters can see data from all the branches, but rights to edit or update the data is given to select staff with specific login access controlled via defined access matrix.
- CFL has a policy that requires customer data base updates require the supervisors to authorize/ approve the updates.
- Each person who accesses the database uses an individual username and password. Users must change their passwords from time to time. Whenever an employee logs into the database, their name, the information they query, and the time when the request is made, are all recorded in a query log.
- CFL has a strong back-up system in which it uses a combination of hardcopy and digital backups of customer information. CFL's system backs-up all information on our cloud servers periodically. Only the IT team of CFL can access such data.
- Branches can't download anything which is uploaded into the system without authentication and authorization.

Response to Enquiries and Complaints

The company encourages customer enquiries, feedback and complaints which shall help it identify and improve the services provided to the Customer.

Scale Base Regulation

CUSTOMER PRIVACY POLICY

In accordance with para 5.6.5 of RBI's Scale Base Regulation 5.6.5, CFL shall immediately notify the Reserve Bank in the event of any breach of security and leakage of confidential customer-related information. In such events, the Company would be liable to the customer for any damages**.**