

POLICY ON PRESERVATION OF DOCUMENTS

POLICY ON PRESERVATION OF DOCUMENTS

Lendingkart Finance Limited
(effective from February 11, 2026)

POLICY ON PRESERVATION OF DOCUMENTS

Table of Contents

| | | |
|-----|--|---|
| 1. | PREAMBLE | 4 |
| 2. | OBJECTIVE..... | 4 |
| 3. | DEFINITIONS | 4 |
| 4. | COVERAGE..... | 4 |
| 5. | CHARTER..... | 5 |
| A. | DOCUMENTS TO BE PRESERVED PERMANENTLY..... | 5 |
| B. | DOCUMENTS TO BE PRESERVED FOR NOT LESS THAN EIGHT YEARS | 5 |
| C. | DISCLOSURE OF INFORMATION ON THE WEBSITE OF THE COMPANY. | 5 |
| D. | RETENTION OF RECORDS AS PER PML ACT AND APPLICABLE RBI REGULATIONS..... | 6 |
| 6. | MODES OF PRESERVATION | 6 |
| 7. | PRINCIPLE OF RESPONSIBILITY OF EMPLOYEES FOR PRESERVATION OF DOCUMENTS | 7 |
| 8. | REVIEW OF THE POLICY | 7 |
| 9. | DISPOSAL OF RECORDS | 7 |
| 10. | AMENDMENT IN LAW..... | 7 |

POLICY ON PRESERVATION OF DOCUMENTS

1. PREAMBLE

Lendingkart Finance Limited (hereinafter referred to as “LFL” or “the Company”) treats its corporate documents, whether physical or electronic, as precious resources and believes in judicious preservation of the same.

2. OBJECTIVE

This Policy has been framed in compliance with SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (including any amendment thereof for the time being in the force), Companies Act, 2013, Reserve Bank of India (Non-Banking Financial Companies - Know Your Customer) Directions, 2025 (“KYC Directions”), Prevention of Money-Laundering Act, 2002 (PML Act), the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules) and other applicable RBI regulations. Further objective of this policy is to ensure systematic identification, categorization, maintenance, review, retention, archival and destruction of documents received or created in the course of business.

3. DEFINITIONS

“**Act**” means the Companies Act, 2013 and the Rules framed thereunder, including any modifications, amendments, clarifications, circulars or reenactments thereof.

“**Board**” means the Board of Directors of the Company.

“**Board Committees**” means Audit Committee, Nomination & Remuneration Committee and other Committees directly reporting to the Board of Directors from time to time.

“**RBI Regulations**” means all regulations enacted by Reserve Bank of India as applicable to the Company.

“**SEBI Regulations**” means all regulations enacted by Securities and Exchange Board of India as applicable to the Company.

“**Records pertaining to the identification**” / “**Identification records**” shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

4. COVERAGE

This Policy is intended to guide the company and its officers on maintenance of any Documents, their preservation and disposal.

POLICY ON PRESERVATION OF DOCUMENTS

5. CHARTER

Various laws applicable to the Company requires maintenance of certain types of corporate records, usually for a specified period of time. In compliance with the provisions of applicable laws and in the best interest of Company and its stakeholders, time limit for preservation of documents and archival of documents uploaded on the website of the Company is categorized as follows:

A. DOCUMENTS TO BE PRESERVED PERMANENTLY

The Company shall endeavor to keep the document stated below, either in electronic form or physical form or both, till the existence of the Company (however, such document shall be mandatorily kept for a period specified in any applicable law):

- (i) **Board, Board Committees & Members' Meetings Minutes:** Minutes of meetings of all Board, Board Committees & Members' meetings.
- (ii) **Annual Reports and Balance Sheets:** Copies of Annual Reports and Balance Sheets of each financial year.
- (iii) Such other documents as may be required to be maintained permanently under the Act viz., Certificate of Incorporation/Commencement of business, Certificate issued by RBI, Insurance Regulatory and Development Authority of India (IRDAI) and/ or any other regulatory or statutory body(ies), Patents, trademark registrations, copyright registrations, Statutory Registers

Other Documents: Any key/ critical document including contracts, memos, letters and/ or any other document considered as critical in the opinion of the Board of Directors of the Company, including all current documents, in respect of which any suit or proceeding is pending before any judicial or quasi-judicial authority.

B. DOCUMENTS TO BE PRESERVED FOR NOT LESS THAN EIGHT YEARS

The Company shall keep/preserve all key statutory filings related to Act, RBI Regulations, SEBI Regulations, taxation laws etc. and all the other requisite documents, as may be prescribed by various applicable laws and/or deemed necessary by the Company, either in electronic form or physical form or both, as may be required, for 8 years or for such time period as may be prescribed under the applicable law.

Registers, records, and returns required to be maintained under the Code on Wages, 2019, Code on Social Security, 2020, and other applicable Labour Codes, shall be preserved in their original format (electronic or otherwise) for a period of not less than five years (or such longer period as prescribed by state-specific rules) from the date of the last entry.

POLICY ON PRESERVATION OF DOCUMENTS

C. DISCLOSURE OF INFORMATION ON THE WEBSITE OF THE COMPANY.

The information which has been disclosed by the Company to the Stock exchanges in terms of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 will be hosted on the website of the Company for a period of five years.

The content of the website of the Company will be reviewed on a quarterly basis. All information/disclosures on the website of the Company would be moved to the archival folder after a period of 5 years from the date on which such disclosures/ announcements were made. The archival folder would be available on the website for a period of two years. Thereafter the said information may be destroyed.

D. RETENTION OF RECORDS AS PER PML ACT AND KYC MASTER DIRECTIONS, 2025 :

In terms of the KYC Master Direction, PML Act, 2002 read with PML Rules, 2005, the Company shall:

- Maintain all necessary records of transactions between the Company and the customer for at least five years from the date of transaction.
- Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended.
- Make the identification records and transaction data available to the competent authorities upon request.
- Have a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules, 2005.
- Maintain all necessary information in respect of transactions prescribed under Rule 3 of PML Rules, 2005 enable reconstruction of individual transaction, including the following:
 - a. the nature of the transactions.
 - b. the amount of the transaction and the currency in which it was denominated.
 - c. the date on which the transaction was conducted; and
 - d. the parties to the transaction.
 - e. Recording of rejection reasons of the application, as and where applicable.
- The detailed guidelines for maintaining the records of the customer have been prescribed in the Record Retention SOP of the Company. Attached herewith as Annexure 1.
- The third party is regulated, supervised, or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act and as specified in the KYC-AML Policy of the Company. Attached herewith as Annexure 2.

POLICY ON PRESERVATION OF DOCUMENTS

- Records or the information of the customers due diligence carried out by the third party is obtained by the Company immediately from the third party or from the Central KYC Records Registry as specified in the KYC-AML Policy of the Company Attached herewith as Annexure 2.
- Have a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.
- In the event the Company undertakes Video-based Customer Identification Process (V-CIP), the entire data and recordings of V-CIP shall be stored in a system located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search.

Every information maintained, furnished or verified as outlined above shall be kept confidential, unless provided other wise under any law for the time being in force. Further, the Company shall ensure that in case of customers who are non-profit organizations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

E. RECORDS OF OUTSOURCED ACTIVITIES:

The Company shall maintain and preserve:

- A central record of all material outsourcing of financial services, updated promptly, for review by the Board and Senior Management.
- An inventory of IT services outsourced to service providers (including key entities involved in their supply chains).
- Records of due diligence reviews of service providers, monitoring reports, and audit findings related to outsourcing arrangements.

6. MODES OF PRESERVATION

The document may be preserved either in Physical form and/or Electronic Form.

The officer of the company who is / are generally expected to observe the compliance of requirements of applicable law shall be the person(s) responsible to preserve the documents.

POLICY ON PRESERVATION OF DOCUMENTS

The preservation of documents should be such as to ensure that there is no tampering, alteration, destruction, or anything which endangers the content, authenticity, utility or accessibility of the Documents.

The preserved Documents must be accessible at all reasonable times. Access may be controlled by the authorized person for preservation, so as to ensure integrity and confidentiality of the Documents and prohibit unauthorised access.

7. PRINCIPLE OF RESPONSIBILITY OF EMPLOYEES FOR PRESERVATION OF DOCUMENTS

All the Employees in the permanent roles of the Company are responsible for taking into account the potential impacts on preservation of the documents in their work area and their decision to retain/preserve or destroy documents pertaining to their area. Such policy bestowing responsibility on the Company's employees would immensely help Company's litigation preparedness tool helping the Company's and Outside legal counsel to track down documents to handle the legal cases.

The respective Departmental/Functional Heads of the company shall be responsible for maintenance, preservation and destroying of documents in respect of the areas of operations falling under the charge of each of them, in terms of this policy.

8. REVIEW OF THE POLICY

The policy shall be reviewed at yearly interval or earlier if considered necessary by the Board of Directors.

9. DISPOSAL OF RECORDS

After the expiry of the statutory retention period the preserved documents for both the physical and electronic records may be destroyed in such a mode after following due process.

Provided that, in compliance with the RBI (Non-Banking Financial Companies – Responsible Business Conduct) Directions, 2025, original movable/immovable property documents collected from borrowers shall be released/returned to the borrower within a period of 30 days after full repayment/settlement of the loan account. The Company shall preserve the acknowledgment of such return as proof of compliance.

10. AMENDMENT IN LAW.

Any subsequent amendment/ modification in the applicable laws in this regard shall automatically apply to this Policy.

POLICY ON PRESERVATION OF DOCUMENTS

Annexure 1

Record Retention – Standard Operating Procedure (SOP) Version 1.0

POLICY ON PRESERVATION OF DOCUMENTS

Index

| Sr No | <u>Particulars</u> | <u>Page No.</u> |
|--------------|---|------------------------|
| 1 | Definition | 4 |
| 2. | Purpose | 5 |
| 3. | Scope | 5 |
| 4. | Coverage | 6 |
| 5. | Record Retention Requirement | 6– 11 |
| 6. | Mode of Preservation | 11 |
| 7. | Ownership of Record Retention | 12 |
| 8. | Archival & Destruction of Data | 12 |
| 9. | Approval Matrix | 12 |
| 10. | Conclusion | 13 |

POLICY ON PRESERVATION OF DOCUMENTS

1. Definition

- 1.1 “Applicable Law” shall mean without limitation all laws, statutes, rules, regulations, direction, RBI direction, circular and notifications, byelaws, binding codes of conduct and guidelines, statutes, codes, ordinances, case law, judgments, decrees and consent orders, and requests, demands, directives or rulings by governmental, semi/quasi-governmental or regulatory agencies, whether local, national, international, or otherwise existing from time to time which are applicable to the person, act, or activity in question. It shall also include ordinance, order, treaty, judgment, decree, injunction, permit, or decision of any central, state, or local government, authority, agency, court, or other body having jurisdiction over the matter in question, as may be in force from time to time.
- 1.2 “Data Protection Legislation” means the legislation and regulations relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data (as defined below) or privacy of an individual including (without limitation):
 - (a) The Information Technology Act, 2000 (as amended from time to time) including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“Privacy Rules”), Digital Personal Data Protection Act 2023 (“DPDP Act”) (to the extent applicable and enforceable) and any other applicable rules framed thereunder.
 - (b) All other applicable industry guidelines (whether statutory or non-statutory), internal guidelines or codes of conduct relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an individual issued by any regulator to any of the Parties.
 - (c) Any other Applicable Law solely relating to the protection of Personal Data and processing, storage, usage, collection and/or application of Personal Data or privacy of an.
- 1.3 “Customer/ Borrower” shall mean the customer of the Company, its co-lenders and lending partners.
- 1.4 “Non-individual Customer” shall mean the customer that is not a single person, but rather a legal entity like a company, partnership, proprietorship, or other organization etc.
- 1.5 “Partners shall mean third-party partners of the Company outsourced as part of the Customer loan journey who has access to Customer data including storage.
- 1.6 “Personal Data” ” means any data which relates to a natural person (as defined under Applicable Law and Data Protection Legislation) who is identifiable by or in relation to such data, including but not limited to an individual who is a Customer of the Company, or co-lender, lending partner, in the form of documents, and documents or electronic files.
- 1.7 “SOP” shall mean the Record Retention Standard Operating Procedure.
- 1.8 Board: The Board of Directors of the Company.

POLICY ON PRESERVATION OF DOCUMENTS

- 1.9 Board Committees: Audit Committee, Nomination & Remuneration Committee and other Committees, constituted from time to time, reporting to the Board of Directors or whose minutes of meetings are placed before the Board of Directors.
- 1.10 Company: Shall mean Lendingkart Finance Limited.
- 1.11 Documents: Any record, whether physical or electronic, created or received in the course of business operations.
- 1.12 Identification Records: Updated records of the identification data, account files, business correspondence and results of any analysis undertaken.
- 1.13 PML Act: Prevention of Money-Laundering Act, 2002.
- 1.14 RBI Regulations: Regulations enacted by Reserve Bank of India as applicable to the Company.
- 1.15 SEBI Regulations: Regulations enacted by Securities and Exchange Board of India to the extent applicable to the Company.

Interpretation:

headings and captions are used for convenience only and shall not affect the construction or interpretation of any provisions of this SOP;

all words (whether gender-specific or gender neutral) shall be deemed to include each of the masculine, feminine and neuter genders;

any reference to an enactment or a statutory provision is a reference to that enactment or statutory provision as from time to time amended, modified, consolidated, replaced or re-enacted (with or without modification) and includes all subordinate legislation or regulations, instruments or orders made under such enactment; and

words in the singular shall include the plural and vice versa

- the time period prescribed in this SOP shall be deemed to be modified in case an extended time period is prescribed under the applicable law or internal policy of the Company.

2. Purpose

This SOP outlines the process and guidelines for maintaining records related to customer transactions, Know Your Customer (KYC) documentation, and business communications to ensure compliance with Applicable Laws, Data Protection Legislation, the Reserve Bank of India (RBI) Master Direction on Know Your Customer, 2016 (KYC Master Direction) and the regulations prescribed under The Prevention of Money-Laundering Act, 2002 ('PML Act'), Prevention of Money-laundering (Maintenance of Records) Rules 2005 ('PML rules'), SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, Companies Act, 2013.

According to RBI Master Direction on Know Your Customer, 2016 (KYC Master Direction), and PMLA guidelines, the Company is required to maintain records of **all**

POLICY ON PRESERVATION OF DOCUMENTS

transactions between the Company and the Customer for at least five (05) years from the date of the transaction and preserve records pertaining to the identification of the Customers and their addresses for at least five (05) years after the end of the business relationship.

3. Scope

This SOP applies to all Customer records, Personal Data and transaction-related documents maintained by Company. It covers the retention and preservation of Customer Personal Data including but not limited to identification details, transaction records, Customer communication, documents as part of Customer loan journey (loan offer, loan agreement, payments schedule, statement of accounts etc.), and any other documentation obtained during the Customer loan journey, throughout the business relationship, and after the closure or termination of such relationships (hereinafter referred to as the “Documents/ Records”).

The Records to be maintained under this SOP includes data for both individual and Non-individual Customers required by regulatory bodies such as RBI and PMLA and stored in compliance with Applicable Laws. The focus is to ensure that Records are preserved for the mandatory period of five (05) years after the end of the business relationship.

Even after the termination of the business relationship with the Customer, Company will ensure that Records are retained and preserved for the specified duration. These Records are to be securely stored and easily retrievable for compliance, audit requirements, disclosures to appropriate stakeholders and authorities and regulatory purposes.

This SOP applies to all employees (permanent and temporary), directors, officers, and any other individuals acting for or on behalf of the Company.

4. Coverage

This SOP is intended to guide the Company, its Partners, its employees and relevant departments on maintenance of any Documents, their preservation and disposal.

5. Record Retention Requirements

As per the **Para 46** of Reserve Bank of India (RBI) Master Direction on Know Your Customer, 2016 (KYC Master Direction) and the regulations as **per section 12 of PMLA** prescribed under:

The Prevention of Money-Laundering Act, 2002 (‘PML Act’) and Prevention of Money-laundering (Maintenance of Records) Rules, 2005 (‘PML Rules’), The Companies Act, 2013 and the Rules framed thereunder and in compliance with Applicable Laws, including any modifications, amendments, clarifications, circulars or reenactments thereof, the Company shall ensure the following types of records are retained and preserved for a minimum period prescribed under aforesaid guidelines and mentioned

POLICY ON PRESERVATION OF DOCUMENTS

hereunder:

List of Records :-

| Document Type | Description | Retention Period |
|--|--|--|
| Agreements | <ul style="list-style-type: none"> a) Lease/Rental Agreement – All facilities b) Vendor Agreements Tech & Non Tech Agreements c) AMC Agreements | Five Years after the end of the term of the contract |
| Customer Identification Data (Non-Individual) | <ul style="list-style-type: none"> (a) Customer identification data and documents (KYC). (b) Account files (e.g., Customer account statements). (c) Any supporting documents obtained from the Customer as part of the Customer loan journey. (d) Business correspondence between the Customer and the Company. (e) Results of analysis (e.g., credit underwriting, risk assessments). (ii) Documents related to field visit / personal discussion with the Customers. | Five (05) years following the termination of the business relationship or the closure of the account (whichever is later). |
| Customer Identification Data (Individual) | <ul style="list-style-type: none"> (a) -Customer identification data and KYC documents of the Customer (i.e., Individual Customer, related parties, proprietor, directors, partners, ultimate beneficial owner, shareholder, authorized signatory). (b) Supporting documents obtained for establishing an account relationship such as account statement. (c) Account files (e.g., Customer's bank account statements). | Five years following the termination of the business relationship or the closure of the account (whichever is later). |

POLICY ON PRESERVATION OF DOCUMENTS

| Document Type | Description | Retention Period |
|---|--|--|
| Transaction Related Documentation | <ul style="list-style-type: none"> (a) Nature of the transaction (e.g., loan disbursement, repayments, settlement, closure, etc.). (b) Mode of transaction (e.g., transfer, cash deposit, RTGS/NEFT, UPI, IMPS, etc.). (c) Amount of transaction and the currency used. (d) Date on which the transaction occurred. (e) Parties involved in the transaction (individual Customers or Non-Individual Customers) and transaction reference numbers. (b) Statement of accounts evidencing the transaction. | Five (05) years following the termination of the business relationship or the closure of the account (whichever is later). |
| Communications with Customers and related audit logs | <ul style="list-style-type: none"> (a) Loan offer letters, sanction letters, Key Fact Statements (KFS), repayment schedules, etc. (b) Loan application forms and acknowledgments of receipt. (c) Logs pertaining to consents and declarations obtained from the Customer (including acceptance of General Terms and Conditions applicable Terms and Conditions and Privacy Policy, etc.). (d) Communications regarding sanction letter, loan agreements, acceptance of General Terms & Conditions, and amendments from time to time. (e) Communications regarding penal interest or charges associated with the loan transaction or any modifications/changes in the rate of interest or charges. (f) Communications regarding changes in terms and conditions of the loan and loan account. | Five (05) years following the termination of the business relationship or the closure of the account (whichever is later). |

POLICY ON PRESERVATION OF DOCUMENTS

| Document Type | Description | Retention Period |
|--|---|--|
| | <ul style="list-style-type: none"> (g) Communications regarding loan closure, compromise settlement, restructuring, etc. (h) Audit log pertaining to e signature / digital signature and acceptance of loan documents including loan agreement. (i) Any complaints/ grievances related to the loan transaction received from the Customer and corresponding resolution provided via any mode. (j) Communication related to Re – KYC of the Customer and corresponding update received from the Customer. (k) Any Customer request, queries received by the Company along with corresponding resolution provided via any mode. (l) Any other communication as part of the Customer loan journey. | |
| Internal Customer due diligence | <ul style="list-style-type: none"> (a) Risk rating of the Customer and change logs of risk rating over the period along with rationale. (b) Sanction screening records. (c) Periodic risk review records. (d) Politically Exposed Person (“PEP”) and close associate of PEP screening and supporting document related to enhanced due diligence. (e) VKYC recordings. (f) Concurrent audit on KYC and VKYC (all logs and observations). (g) Suspicious Transaction Reports (“STR”) records and filings linked to the account. (h) List of financial frauds (actual / potential) linked to the Customer account. | Five (05) years following the termination of the business relationship or the closure of the account (whichever is later). |

POLICY ON PRESERVATION OF DOCUMENTS

| Document Type | Description | Retention Period |
|--|---|---|
| Collection/ Recovery/ Call logs & Communication | Calls, emails, WhatsApp messages, and other customer communication records during collection | Three (03) years from the date of the transaction. |
| Visit/ Collection Calls Feedback | Feedback and notes recorded during physical visits or borrower interactions | Three (03) years from the date of the transaction. |
| Settlement & Compromise Records | Documentation related to settlement offers, compromises, and closure communication | 5 years from the date of settlement/closure |
| Customer Complaints during Collection | Complaints received related to collection activities and their resolution | 5 years from closure of complaint |
| Recovery Agent Authorization & Training Records | Records of agent authorization, training certificates, and adherence to collection code of conduct and Fair Practice Code of the Company and any other undertaking of the Company | 5 years from the date of agent offboarding |
| <u>Legal Notices Dispatched/ Case Records / Litigation Actions (Collection) & Litigation Matter for Corporate Legal</u> | (a) For Collection: Copies of legal notices physically sent in Civil Litigation matters, show cause notice physically sent for Civil Litigations matters and Civil litigation records actions taken in relation to recovery against borrower like Arbitration Records (Wherever possible)/Arbitration Decree. (b) For Corporate Legal: Cases against and by the Company. Show cause notices from authorities | <u>Seven (07) years from the date of action taken or Five (05) years from the date of Disposal of Litigation/Resolution of Case whichever is later.</u> |
| Customer Record Maintenance | (a) Know Your Client (KYC) records of the customer (b) Copy of proposal form duly signed by the client. (c) Register containing list of clients, details of policy such as type of policy, premium amount, date of | Ten (10) years from the end of the year to which they relate. |

POLICY ON PRESERVATION OF DOCUMENTS

| Document Type | Description | Retention Period |
|--|--|--|
| | <p>issue of the policy, charges or fees received.</p> <p>(d) Register recording complaints / grievances against the Company along with all the details;</p> <p>(e) Register containing details of the specified persons of the Company viz. the name, address, telephone no., photograph, date of commencement of employment, date of leaving service, if any, and monthly remuneration paid to specified person;</p> <p>(f) Copies of correspondence exchanged with the IRDAI or any other record as may be specified by the IRDAI from time to time.</p> | |
| GST Return Records & Income Tax Records | <p>(a) GST Act :- Records related to the filing of the annual GST return.</p> <p>(b) Income Tax Act :- Records related to income tax returns, assessments, and supporting documents as required under the Income Tax Act.</p> | <p>(a) Seventy-two (72) months from the due date of furnishing the annual return.</p> <p>(b) Six (6) years from the end of the relevant assessment year.</p> |
| Records related to Appeal, Revision, or Investigation (under GST Act) | <p>Documents and records pertaining to any appeal, revision, or other proceedings, including those under investigation, as per the provisions of the GST Act. This includes correspondence, legal notices, rulings, and any other related documents associated with the process.</p> | <p>These records should be retained until the completion of the investigation, appeal, or revision, as per legal requirements.</p> |
| Reopened Assessment Records (Section 147, Income Tax Act) | <p>Documents and records pertaining to assessments reopened under Section 147 of the Income Tax Act, including notices, communications, and supporting materials.</p> | <p>Six (6) years from the end of the relevant assessment year, or as specified under the applicable provisions of the Income Tax Act.</p> |

POLICY ON PRESERVATION OF DOCUMENTS

| Document Type | Description | Retention Period |
|---|---|--|
| International and Specified Domestic Transaction Records | Documents and information pertaining to international and specified domestic transactions, including agreements, financial statements, transfer pricing documentation, and related correspondence. | Eight (8) years from the end of the relevant assessment year |
| Employee Details (Owner – HR) | Employee Personal Details - Letter, Promotion, Salary, Exit etc | 8 Years from the from the date of exit |
| Employee Details (Owner – HR) | All Salary Related documents | 3 years from the last entry (i.e from the date of full and final settlement) |
| Employee Details (Owner – HR) | Compliance Related (PF, Gratuity etc) | 7 Years with all challan etc in place |
| Employee Details (Owner – HR) | Income Tax - Employee Related | 6 years from the end of the relevant assessment year, i.e., for a total period of 8 previous years |
| Board and Committee Records: | <ul style="list-style-type: none"> Minutes of meetings of all Board, Board Committees, & other Committees whose minutes of meeting are placed before the Board. Attendance registers of Board/Committee meetings | Permanently |
| Corporate Documents: | <ul style="list-style-type: none"> Memorandum and Articles of the Company Register of members and index of members Register of charges Register of loans, guarantee, security and acquisition made by the company | Permanently |

POLICY ON PRESERVATION OF DOCUMENTS

| Document Type | Description | Retention Period |
|-----------------------------------|---|---|
| Financial Records: | <ul style="list-style-type: none"> Annual Reports and Balance Sheets of each financial year Audit reports | Permanently |
| Legal and Regulatory: | <ul style="list-style-type: none"> Key contracts, memos, letters and critical documents as determined by the Board (physical or electronic form). Documents subject to pending litigation (until finality is attained) (physical or electronic form). Certificate issued by RBI, IRDA and/ or any other regulatory or statutory body(ies) (physical or electronic form). Patents, trademark registrations, copyright registrations. | Permanently |
| Statutory Filings: | <ul style="list-style-type: none"> All key statutory filings related to Companies Act, RBI Regulations, SEBI Regulations, taxation laws Copies of annual returns prepared under the Companies Act, 2013 All event-based disclosures to stock exchanges | Atleast Eight (8) years |
| Financial and Tax Records: | <ul style="list-style-type: none"> Books of accounts together with vouchers (8 financial years) Tax records and related documentation Bank statements and reconciliations (11 years) | Atleast Eight (8) years |
| Website Disclosures: | <ul style="list-style-type: none"> Information disclosed to stock exchanges | 5 years on website + 2 years in archival folder |

POLICY ON PRESERVATION OF DOCUMENTS

6. Modes of Preservation

The Records shall be preserved in line with the Company’s policies either in physical form and/or electronic form.

7. Ownership of Record Retention

7.1 The Information Technology department is the custodian of all the Records stored electronically in Company’s system and the Partners system/ servers.

7.2 Individual departments/ stakeholders shall take the ownership of all the Records stored in the physical form.

8. Archival & Destruction of Records

Records that are no longer actively used but need to be kept for the required time will be archived securely. The archived data will be stored separately, protected from unauthorized access, and organized for easy retrieval when needed for audits, reviews, or other regulatory checks. The Records pertaining to the identification of the customers and their addresses will be maintained for at least Five (05) years following the termination of the business relationship or the closure of the account (whichever is later). After the minimum retention period, Records will be securely deleted in a way that prevents unauthorized recovery. However, in case of any pending litigation in court, legal disputes matter in which final decision is pending, ongoing LEA/police investigation and in compliance with Applicable Laws and Data Protection Legislation etc., all Records related to Customer loan account will be preserved and archived until final closure of such proceedings and decision in the matters, even if this goes beyond the minimum retention period of five (05) years. This will be in exceptional to the Company’s archival policy for Records retained in Mailbox.

9. Approval Matrix for deletion of records

| Department Name | Approval |
|------------------|--|
| Compliance Team | CCO (Chief Compliance Officer) |
| Legal Team | Head of Legal or Group General Counsel |
| Finance Team | CFO (Chief Financial Officer) |
| Cross- Sell Team | Head Business |

POLICY ON PRESERVATION OF DOCUMENTS

| Department Name | Approval |
|-----------------------------|--|
| Collections Team | Chief Collections Officer |
| Product Team | Head Product |
| Information Technology Team | Chief Information Officer |
| Risk Team | Chief Risk Officer |
| Secretarial Team | Company Secretary or Group General Counsel |
| Operations | Head Operations & Customer Service |

10. Conclusion

This SOP establishes clear processes for the preservation, retention, and lawful disposal of records, ensuring transparency, audit readiness, and operational integrity. Through comprehensive documentation and robust data protection practices, the Company aims to safeguard Customer information, meet all legal obligations, and uphold the trust and interests of its Customers while enabling efficient and compliant business operations.

Annexure 2

Know Your Customer and Anti Money Laundering Policy (KYC and AML Policy)

Version 1.5 approved on February 11, 2026

1. PREAMBLE

This Document sets out the salient features of Know Your Customer ('KYC') and Anti-Money Laundering ('AML') norms for Lendingkart Finance Limited ('LFL' or 'the Company').

2. BACKGROUND

In terms of the provisions of PML Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by the Government of India as notified by the Government of India, NBFC's being Regulated Entities (REs) are required to follow certain customer identification procedures and conduct customer due diligence while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions and take steps to ensure implementing the provisions of the aforementioned Act, Rules and Ordinance, including operational instructions issued in pursuance of such amendment(s).

Accordingly, KYC/AML/CFT Policy of the Company ('this Policy') has been prepared in line with the (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 (updated as on December 29, 2025) and incorporating LFL's approach to KYC, AML and CFT issues.

3. KEY SOURCES OF LAW

The key regulations that form the framework of the KYC-AML norms applicable to LFL are:

- a) The Prevention of Money Laundering Act, 2002 as updated from time to time ('PML Act/ PMLA').
- b) The Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ('PML Rules') as updated from time to time.
- c) Master Direction on Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025, dated November 28, 2025 (DOR.AML.REC.No.280/14.01.003/2025-26) as updated from time to time ('KYC Master Directions').

POLICY ON PRESERVATION OF DOCUMENTS

4. DEFINITIONS

The terms herein shall bear the meanings assigned to them below:

- A.** Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:
- i. "Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
 - ii. "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
 - iii. "Authentication," in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
 - iv. Beneficial Owner (BO)
 - a) Where the **customer is a company**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.
Explanation- For the purpose of this sub-clause-
 1. "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
 2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.
 - b) Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control through other means.
Explanation – For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.
 - c) Where the **customer is an unincorporated association or body of individuals**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
Explanation: Term 'body of individuals' includes societies.
Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
 - d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust

POLICY ON PRESERVATION OF DOCUMENTS

through a chain of control or ownership.

- v. "Certified Copy" - Obtaining a certified copy by the RE shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorized officer of the RE as per the provisions contained in the Act.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

- authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
 - branches of overseas banks with whom Indian banks have relationships,
 - Notary Public abroad,
 - Court Magistrate,
 - Judge,
 - Indian Embassy/Consulate General in the country where the non-resident customer resides.
- vi. "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- vii. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:
- a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,
 - b. the Managing Partner, if the RE is a partnership firm,
 - c. the Proprietor, if the RE is a proprietorship concern,
 - d. the Managing Trustee, if the RE is a trust,
 - e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and a person who holds the position of or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.
- Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.*
- viii. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorized officer of the RE as per the provisions contained in the Act.
- ix. "Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- x. "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital

POLICY ON PRESERVATION OF DOCUMENTS

locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

- xi. “Know Your Client (KYC) Identifier” means the unique number or code assigned to a customer by the Central KYC Records Registry.

Explanation: A customer can obtain his KYC Identifier through the following ways:

In the process of opening an account, once the customer’s KYC Identifier is generated by CKYCR and provided to LFL, the Company shall share the same with the concerned customer. The customer can also access his KYC Identifier on CKYCR Portal (www.ckycindia.in).

- xii. “Non-profit organisations” (NPO) means any entity or organisation constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-Tax Act, 1961 (43 of 1961) that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013.
- xiii. “Officially Valid Document” (OVD) means the passport, the driving licence, proof of possession of Aadhaar number, the Voter’s Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.

Provided that,

- a. where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
- b. where the OVD furnished by the customer does not have updated address, the following documents, or the equivalent-documents there of shall be deemed to be OVDs for the limited purpose of proof of address:-
 - i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
 - ii. property or Municipal tax receipt;
 - iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
 - iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
- c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at ‘b’ above
- d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there

POLICY ON PRESERVATION OF DOCUMENTS

is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

- xiv. "Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).
- xv. "Person" has the same meaning assigned in the Act and includes:
- an individual,
 - Hindu undivided family,
 - company,
 - an association of persons or a body of individuals, whether incorporated or not,
 - every artificial juridical person, not falling within any one of the above persons (a to e), and
 - any agency, office or branch owned or controlled by any of the above persons (a to f).
- xvi. "Principal Officer" means an officer at the management level nominated by the RE, responsible for furnishing information as per rule 8 of the Rules.
- xvii. "Suspicious transaction" means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:
- gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
 - appears to be made in circumstances of unusual or unjustified complexity; or
 - appears to not have economic rationale or *bona-fide* purpose; or
 - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.*
- xviii. A 'Small Account' means a savings account which is opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account are specified in Section 23.
- xix. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery, or the arrangement thereof and includes:
- opening of an account;
 - deposit, withdrawal, exchange, or transfer of funds in whatever currency, whether in cash or

POLICY ON PRESERVATION OF DOCUMENTS

- by cheque, payment order or other instruments or by electronic or other non-physical means;
 - c. the use of a safety deposit box or any other form of safe deposit;
 - d. entering into any fiduciary relationship;
 - e. any payment made or received, in whole or in part, for any contractual or other legal obligation; or
 - f. establishing or creating a legal person or legal arrangement.
- xx. "Video based Customer Identification Process (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- xxi. "Group": The term "Group" shall have the same meaning assigned to it as per (e) of sub-section (9) of section 286 of Income Tax Act, 1961 (43 of 1961)
- B.** Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:
- i. "Customer" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
 - ii. "Walk-in Customer" means a person who does not have an account-based relationship with the RE, but undertakes transactions with the RE.
 - iii. "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

Explanation: The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

- a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;
- (b) Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;
- (c) Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.
- iv. "Customer identification" means undertaking the process of CDD.

POLICY ON PRESERVATION OF DOCUMENTS

- v. “KYC Templates” means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
- vi. “Non-face-to-face customers” means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.
- vii. “On-going Due Diligence” means regular monitoring of transactions in accounts to ensure that those are consistent with LFL’s knowledge about the customers, customers’ business and risk profile, the source of funds / wealth.
- viii. “Periodic Updation” means steps taken to ensure that documents, data, or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.
- ix. “Regulated Entities” (REs) means
 - a. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co- operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as ‘banks’
 - b. All India Financial Institutions (AIFIs)
 - c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).
 - d. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
 - e. All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.
 - f. Asset Reconstruction Companies (ARCs)
- x. “Shell bank” means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.
- xi. “Wire transfer” means any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person..
- xii. “Domestic wire transfer” means any wire transfer where the ordering financial institution and beneficiary financial institution are located in India. This term, therefore, refers to any chain of wire transfer that takes place entirely within the borders of India, even though the system used to transfer the payment message may be located in another country.
- xiii. “Cross-border wire transfer” means any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries. This term also refers to any chain of wire transfer in which at least one of the financial institutions involved is located in a different country.

POLICY ON PRESERVATION OF DOCUMENTS

- xiv. Senior Management' are the same as defined in 'Explanation' to Section 178 of the Companies Act, 2013. "senior management" means personnel of the company who are members of its core management team excluding Board of Directors comprising all members of management one level below the executive directors, including the functional heads

5. KNOW YOUR CUSTOMER STANDARDS

A. Objective

The objective of "Know Your Customer (KYC)" guidelines is to prevent the company from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedure also enables to know / understand the customer and their financial dealings better which in turn helps to manage the risk prudently.

B. Scope

The policy applies to Company's customers, officers, employees, products, and services of the Company.

C. Appointment of Principal Officer and Designated Director

- i. As per the requirement of the PML Rules, a Principal Officer for the Company has been appointed and the details of the Principal Officer was informed to FIU India and RBI.

Principal Officer is responsible for ensuring compliance, monitoring transactions, and reporting any transactions/information as covered under the PML Act read with its Rules.

The details of the Principal Officer of the Company are as under:

Name : Aakanksha Singh

Designation: Chief Compliance Officer

Email ID : aakanksha.singh@lendingkart.com

- ii. As per the requirement of the PML Rules, a Designated Director for the Company has been appointed and the details of the Designated Director was informed to FIU India and RBI.

Designated Director is responsible to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

The details of the Designated Director of the Company are as under:

Name : Mr. Prashant Joshi

Designation : Managing Director & Chief Executive Officer

Email ID : prashant.joshi@lendingkart.com

POLICY ON PRESERVATION OF DOCUMENTS

D. The Company has framed its KYC policy incorporating the following four key elements:

- a. Customer Acceptance Principles;
- b. Customer Identification Procedures including due diligence;
- c. Monitoring of Transactions; and
- d. Risk management

E. Customer Acceptance Principles

The Company shall, for all customer transactions, verify and maintain the record of identity and address(es), both current and permanent addresses of the customer, the nature of business and financial status of the customer.

The Company needs to set out explicit criteria for acceptance of customers to ensure:

1. No account is opened, or transaction is executed in anonymous or fictitious/benami name(s);
2. No account is opened where the LFL is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The LFL shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
3. No transaction or account-based relationship is undertaken without following the CDD procedure.
4. The mandatory information to be sought for KYC purpose while opening an account and during the periodic updation, is specified.
5. Additional information, where such information requirement has not been specified in the internal KYC policy of LFL, is obtained with the explicit consent of the customer.
6. LFL shall apply CDD procedure at the Unique Customer Identification Code (UCIC) level. A Unique Customer Identification Code (UCIC) shall be allotted while entering into new relationship with Individual Customer, If an existing KYC compliant customer of a LFL desires to open another account or avail any other product or with LFL, there shall be no need for fresh CDD exercise as far as identification of the customer is concerned.
7. CDD Procedure is followed for all the joint account holders, while opening a joint account.
8. Circumstances in which, a customer is permitted to act on behalf of another person/entity, is clearly spelt out.

POLICY ON PRESERVATION OF DOCUMENTS

9. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanction list indicated in Chapter IX of KYC Master Direction.

Further, LFL shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at <https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm>, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government. Also take into consideration those individuals/entities from jurisdictions that do not or insufficiently apply the Financial Action Task Force (FATF) Recommendations as per the FATF statements circulated by RBI.

10. Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Rule 114B of the Income Tax Rules, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.
11. Where an equivalent e-document is obtained from the customer, LFL will verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000).
12. Where Good and Services Tax (GST) details are available, the GST number shall be verified from the search/ verification facility of the issuing Authority.

However, reasonable care shall be taken to ensure that the Customer Acceptance Policy does not result in denial of loan facility to members of the general public, especially those, who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection will be duly recorded by the officer concerned.

Where LFL forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.

F. Customer Identification Procedure ('CIP')

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data, or information in case of individual as well as corporate. The Company will obtain information, stated below, necessary to establish, to its satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship.

- a. The Company shall undertake the identification of customers in the following cases:
 - Commencement of an account-based relationship with the customer.

POLICY ON PRESERVATION OF DOCUMENTS

- When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
 - Selling third party products as agents, selling their own products, payment of due of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
 - When a LFL has reason to believe that a customer (account based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
 - LFL shall ensure that introduction is not to be sought while opening accounts.
- b. LFL shall obtain certified copy of proof of possession of Aadhar number or the OVD and a recent photograph where an equivalent document is not submitted done by a third party, subject to the following conditions:
- Records or the information of the customers due diligence carried out by the third party is obtained by the Company immediately from the third party or from the Central KYC Records Registry.
 - Adequate steps are taken by LFL to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
 - The third party is regulated, supervised, or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
 - The third party shall not be based in a country or jurisdiction assessed as high risk. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with LFL.

LFL shall not outsource the decision-making function of determining compliance with KYC norms.

G. Customer Due Diligence (CDD):

a. CDD in case of individuals:

For customers that are individuals or individuals who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity, the Company will obtain the following:

- i) PAN or Form 60 defined in Income-tax Rules, 1962
- ii) The proof of possession of Aadhaar number where offline verification can be carried out; or
- iii) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; or
- iv) the KYC Identifier with an explicit consent to download records from CKYCR;

POLICY ON PRESERVATION OF DOCUMENTS

- v) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by LFL.

While undertaking CDD in case of individuals, LFL shall ensure that the following is fulfilled where the customer has submitted:

- (i) proof of possession of Aadhaar where offline verification can be carried out, LFL shall carry out offline verification.
- (ii) an equivalent e-document of any OVD, LFL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under digital KYC process mentioned hereunder.
- (iii) any OVD or proof of possession of Aadhaar number where offline verification cannot be carried out, LFL shall carry out verification through digital KYC as specified hereunder.
- (iv) KYC Identifier under clause (ac) of the KYC Master Direction, the LFL shall retrieve the KYC records online from the CKYCR.
- (v) LFL shall obtain a certified copy of proof of possession of Aadhaar number or the OVD and a recent photograph where an equivalent document / e-document is not submitted.
- (vi) CDD methodologies adopted by the company shall form part of customer onboarding procedure (Standard Operating Procedure of Pre-terms)
- (vii) such other documents including in respect of the nature of business and financial status of the customer for e.g. Bank statement, GST Certificate etc, or the equivalent e-documents thereof as may be required by LFL.

Note: LFL shall ensure that the use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 and the regulations made thereunder.

Note: Aadhaar number is not mandatory for purposes of KYC. However, in case the customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016), the customer shall provide the Aadhaar number to the LFL. In other cases, customers may provide the Aadhaar number voluntarily.

Note: LFL official can perform biometric-based e-KYC authentication, including Aadhaar Face Authentication.

POLICY ON PRESERVATION OF DOCUMENTS

b. CDD in case of non - individuals:

For undertaking CDD, LFL shall obtain the following from an individual as well as Non *Individuals while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:*

| Types of entity | Type of document to be collected and verified |
|--|--|
| Sole Proprietary concerns ¹ | <ul style="list-style-type: none"> (i) Documents specified above for individuals relating to the Proprietor. (ii) Any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained: <ul style="list-style-type: none"> (a) Registration certificate including Udyam Registration certificate (URC) issued by the Government (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act. (c) Sales and income tax returns. (d)CST/VAT/ GST certificate (d) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. (e) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (f) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. (g) Utility bills such as electricity, water, landline telephone bills, etc |

¹ In cases where LFL is satisfied that it is not possible to furnish two such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, LFL, however, will undertake CPV/FI, collect such information as would be required to establish the existence of such firm, confirm, clarify, and satisfy itself that the business activity has been verified from the address of the proprietary concern.

POLICY ON PRESERVATION OF DOCUMENTS

| | |
|--|--|
| <p>Corporate (Limited/Private Limited Company)</p> | <p>For companies, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:</p> <ul style="list-style-type: none"> i) Certificate of incorporation ii) Updated memorandum and Articles of Association iii) PAN of the company iv) A resolution from the Board of Directors and power of attorney granted to its managers, officers, or employees apply, open, and operate the loan on its behalf. v) PAN & OVD of the person relating to beneficial owner, the managers, officers, or employees, as the case may be, holding an attorney to transact on the company's behalf. vi) the name of the relevant persons holding senior management position and vii) the registered office and the principal place of its business if it is different. |
| <p>Partnership firm</p> | <p>For partnership firm, certified copies of each of the following documents or e-documents shall be obtained:</p> <ul style="list-style-type: none"> i) Registration certificate ii) Partnership deed iii) PAN of the partnership firm iv) PAN & OVD of the person relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf v) The names of all partners and vi) Address of the registered office, and the principal place of its business, if it is different. |
| <p>Unincorporated association or a body of individuals & Unregistered trust/</p> | <p>For Unincorporated association or a body of individuals, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:</p> <ul style="list-style-type: none"> a. Resolution of the managing body & Power of Attorney granted to transact business on its behalf. b. Permanent Account Number or Form No 60 of the unincorporated association or a body of individuals. c. PAN & OVD of the person relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf. |

POLICY ON PRESERVATION OF DOCUMENTS

| | |
|-------|--|
| | d. Such information as may be required by the LFL to collectively establish the legal existence of such an association or body of individuals. |
| Trust | <p>For Trust, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained:</p> <ul style="list-style-type: none"> i) Registration certificate ii) Trust deed and iii) Permanent Account Number or Form No 60 of the trust. iv) PAN & OVD of the person relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf. v) The names of the beneficiaries, trustees, settlor, protector, if any and authors of the trust vi) The address of the registered office of the trust and vii) list of trustees and documents, as specified for individuals, for those discharging the roles as a trustee and authorized to transact on behalf of the trust. |

Note:

- In cases where the LFL is satisfied that it is not possible to furnish two such documents, LFL may, at their discretion, accept only one of those documents as proof of business/activity. Provided LFL undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
- The submitted documents must be verified with the original copies, and authorized officer of LFL should mark them as "Original Seen and Verified" ("OSV")
- The Company shall collect necessary documents and information in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by the RBI from time to time.
- The first 8 digits of Aadhaar Number need to be blackout or redacts before accepting from customer, where the authentication of Aadhaar number is not required.
- proof of possession of Aadhaar / Aadhaar number where offline verification can be carried out, LFL shall carry out offline verification
- an equivalent e-document of any officially valid document, LFL shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Video KYC/V-CIP as specified in the policy.
- any officially valid document or proof of possession of Aadhaar number under clause (ab) of sub-rule (4) where offline verification cannot be carried out, LFL shall carry out verification through Video KYC/V-CIP as specified in the policy.

POLICY ON PRESERVATION OF DOCUMENTS

- In case of trust, LFL will ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in the KYC Master Direction.
- Such other documents including in respect of the nature of business and financial status of the customer for e.g. Bank statement, GST Certificate etc, or the equivalent e-documents thereof as may be required by LFL.

c. **Identification of Beneficial Owner**

Beneficial Owner is defined in the Definitions section of this Policy.

According to the regulatory norms, the Company would take reasonable measures to identify the beneficial owners and thereafter verify the beneficial owner(s) in terms of Rule 9(3) of the PML Rules, keeping in view the below:

| Type of Entity | Criteria for Identification of Beneficial Owner |
|------------------------------------|--|
| Company | individual who has the ownership of/entitlement to more than 10% of share or capital or profits of the Company |
| Partnership Firm | individual/partner who has the ownership of/entitlement to more than 10% of the capital or profits of the Firm |
| Association or Body of Individuals | individual who has the ownership of/entitlement to more than 15% of the property or capital or profits of the association |
| Trust | individual who is the setter of the trust, the trustee, the protector, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership. |

Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities: , it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities. b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

d. **Simplified procedure for opening accounts by Non-Banking Finance Companies (LFL):**

In case a person who desires to open an account is not able to produce documents, as specified in CDD, LFL may at its discretion open accounts subject to the following conditions:

- LFL shall obtain a self-attested photograph from the customer.
- Th designated officer of LFL certifies under his signature that the person opening the account has affixed his signature or thumb impression in his presence.

POLICY ON PRESERVATION OF DOCUMENTS

- The account shall remain operational initially for a period of twelve months, within which usual CDD procedure as mentioned above shall be carried out.
- Balances in all their accounts taken together shall not exceed rupees fifty thousand at any point of time.
- The total credit in all the accounts taken together shall not exceed rupees one lakh in a year.
- The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case Directions (d) and (e) above are breached by him.
- The customer shall be notified when the balance reached rupees forty thousand or the total credit in year reaches rupees eighty thousand that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in all the accounts taken together exceeds the limits prescribed in points (d) and (e) above.
- The account shall be monitored and when there is suspicion of ML/TF activities or other high- risk scenarios, the identity of the customer shall be established as per Section 16 & 18 of the Master Direction.

H. KYC Process: Video based Customer Identification Process (V-CIP)

LFL may undertake live Video based customer identification process “V-CIP,” the same will be carried out by an authorized official of LFL for establishment of an account-based relationship obtaining his informed consent. LFL may undertake V-CIP to carry out:

- CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, authorized signatories, and Beneficial Owners (BOs) in case of Legal Entity (LE) customers.

In case of CDD of a proprietorship firm, LFL will also obtain the equivalent e-document of the activity proofs with respect to the proprietorship firm.

- Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication as per EDD section.
- Updation / Periodic updation of KYC for eligible customers.

LFL opting to undertake V-CIP, shall adhere to the following minimum standards:

(a) V-CIP Infrastructure

LFL will be complied with the RBI guidelines on minimum baseline cyber security and resilience framework for banks, as updated from time to time as well as other general guidelines on IT risks. The technology infrastructure will be housed in own premises of the LFL and the V-CIP connection and interaction shall necessarily originate from our own secured network domain. Any technology related outsourcing for the process will be compliant with relevant RBI guidelines.

POLICY ON PRESERVATION OF DOCUMENTS

Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the LFL only and all the data including video recording is transferred to the LFL's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the LFL.

- i) LFL will ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer's consent should be recorded in an auditable and alteration proof manner.
- ii) The V-CIP infrastructure / application will be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.
- iii) The video recordings will contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.
- iv) The application shall have components with face liveness / spoof detection as well as face matching technology with a high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the LFL.

Explanation: Making specific facial gestures, like blinking of eyes, smiling, frowning, etc. is not mandatory for liveness check. LFL will take due cognizance of special needs, if any, of the customer during liveness check.

- v) Appropriate artificial intelligence (AI) technology will be used to ensure that the V-CIP is robust.
- vi) Based on experience of detected / attempted / 'near-miss' cases of forged identity, the technology infrastructure including application software as well as work flows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.
- vii) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests should also be carried out periodically in conformance to internal / regulatory guidelines.
- viii) The V-CIP application software and relevant APIs / webservices will also undergo appropriate testing of functional, performance, maintenance strength before being used in live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal/ regulatory guidelines.

(b) V-CIP Procedure

POLICY ON PRESERVATION OF DOCUMENTS

- i. LFL has formulated a clear work flow and standard operating procedure for V-CIP and ensures adherence to it. The V-CIP process shall be operated only by officials of LFL specially trained for this purpose. The LFL staff is capable of carrying out liveness check and detect any other fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.
- ii. Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption does not lead to the creation of multiple files, then there is no need to initiate a fresh session by the Entity. However, in case of call drop / disconnection, fresh session shall be initiated.
- iii. The official of the LFL shall ensure that the sequence and/or type of questions including those indicating liveness of the interaction, during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.
- iv. Any prompting, observed at end of customer shall lead to rejection of the account opening process.
- v. The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at appropriate stage of work flow.

The authorize official of the LFL performing the V-CIP shall record audio - video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

- a) OTP based Aadhar e-KYC authentication.
 - b) Offline Verification of Aadhaar for identification.
 - c) KYC records downloaded from CKYCR, using the KYC identifier provided by the customer.
 - d) Equivalent e-document of Officially Valid Documents (OVDs) including documents issued through Digilocker
- vi. LFL shall ensure to redact or blackout the Aadhaar number.
 - vii. In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, LFL will ensure that the video process of the V-CIP is undertaken within three working days of downloading / obtaining the identification information through CKYCR / Aadhaar authentication / equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. LFL will ensure that no incremental risk is added due to this.

- viii. If the address of the customer is different from that indicated in the OVD, suitable records of the current address shall be captured, as per the existing requirement. It shall be ensured that the economic and financial profile/information submitted by the customer is also confirmed from the customer undertaking the V-CIP in a suitable manner.
- ix. LFL shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority (NDSL) including through Digilocker.
- x. Use of printed copy of equivalent e-document including e-PAN is not valid for the V- CIP.
- xi. The authorized official of the LFL shall ensure that photograph of the customer in the Aadhaar/OVD

POLICY ON PRESERVATION OF DOCUMENTS

- and PAN/e-PAN details matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e-PAN shall match with the details provided by the customer.
- xii. All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.
 - xiii. All matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act shall be appropriately complied with by LFL.

(c) V-CIP Records and Data Management

- i) The entire data and recordings of V-CIP will be stored in a system / system located in India. LFL will ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search. The extant instructions on record management, as stipulated in this Master Direction, shall also be applicable for V-CIP.

ii) The activity log along with the credentials of the official performing the V-CIP shall be preserved.

I. CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR)

- i) In terms of provision of Rule 9(1A) of PML Rules, the LFL shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.
- ii) Operational Guidelines for uploading the KYC data have been released by CERSAI.
- iii) LFL shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be. The templates may be revised from time to time, as may be required and released by CERSAI.
- iv) LFL was required to start uploading the KYC data pertaining to all new individual accounts opened on or after from April 1, 2017, with CKYCR as prescribed.
- v) LFL shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the PML Rules. The KYC records have to be uploaded as per the LE Template released by CERSAI.
- vi) Once KYC Identifier is generated by CKYCR, LFL shall ensure that the same is communicated to the individual/LE as the case may be.
- vii) In order to ensure that all KYC records are incrementally uploaded on to CKYCR, LFL shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates at the time of periodic updation as specified in this Policy, or earlier, when the updated KYC information is obtained/received from the customer.. Also, whenever the LFL obtains additional or updated information from any customer as per below paragraph (Vii (a)) or Rule 9 (1C) of the PML Rules, the LFL shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR. CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs an LFL regarding an update in the KYC record of an existing customer, the LFL shall retrieve the updated KYC records from CKYCR and update the

POLICY ON PRESERVATION OF DOCUMENTS

KYC record maintained by the LFL

vii)(a) For the purpose of establishing an account-based relationship, updation/ periodic updation or for verification of identity of a customer, the LFL shall seek the KYC Identifier from the customer or retrieve the KYC Identifier, if available, from the CKYCR and proceed to obtain KYC records online by using such KYC Identifier and shall not require a customer to submit the same KYC records or information or any other additional identification documents or details, unless–

- there is a change in the information of the customer as existing in the records of CKYCR; or
- the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms; or
- the validity period of downloaded documents has lapsed; or
- the LFL considers it necessary in order to verify the identity or address (including current address) of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the customer.

Explanation: The entity that has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and / or address of the customer, as applicable. Accordingly, any NBFC downloading and relying on such records from the CKYCR shall not be required to re-verify the authenticity of the customer's identity and / or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005. The NBFC downloading and relying on KYC records downloaded from the CKYCR shall remain responsible for all aspects of CDD procedure and provisions of these Directions, except verification of identity and / or address of the customer

- viii) LFL shall ensure that during periodic updation, the customers are migrated to the current CDD standard.
- ix) Where a customer for the purpose of establishing an account-based relationship, submits a KYC identifier to LFL, with an explicit consent to download records from CKYCR, then LFL shall retrieve the KYC records online from the CKYCR using the KYC identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless –
- There is change in KYC information of the customers as existing in the records of CKYCR.
 - The current address of the customer is required to be verified.
 - LFL considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
 - the validity period of documents downloaded from CKYCR has lapsed.

J. Digital KYC Process

- i) LFL shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the LFL.
- ii) The access of the Application shall be controlled by the LFL, and it should be ensured that the

POLICY ON PRESERVATION OF DOCUMENTS

- same is not used by unauthorized persons. The Application shall be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by LFL to its authorized officials.
- iii) The customer, for the purpose of KYC, shall visit the location of the authorized official of the LFL or vice-versa. The original OVD shall be in possession of the customer.
 - iv) LFL must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the LFL shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
 - v) The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.
 - vi) Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
 - vii) The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
 - viii) Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e- Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
 - ix) Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officers registered with the RE shall not be used for customer signature. LFL must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
 - x) The authorized officer shall provide a declaration about the capturing of the live photograph of

POLICY ON PRESERVATION OF DOCUMENTS

customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the LFL. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

- xi) Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the LFL, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.
- xii) The authorized officer of the RE shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document; and (iii) all of the necessary details in CAF including mandatory field are filled properly.
- xiii) On Successful verification, the CAF shall be digitally signed by authorized officer of the RE who will take a print of CAF, get signatures/thumb-impression of customer at appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

K. On-Going Due Diligence

- i. LFL shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, their business and risk profile, the source of funds/wealth.
- ii. Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:
 - (a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
 - (b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
- iii. The extent of monitoring shall be aligned with the risk category of the customer.
- iv. Periodic review of risk categorization of accounts will be carried out at least once in six months and the need for applying enhanced due diligence measures shall be put in place for high-risk customers

The transactions in the accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

For ongoing due diligence, LFL may consider adopting appropriate innovations including artificial intelligence

POLICY ON PRESERVATION OF DOCUMENTS

and machine learning (AI & ML) technologies to support effective monitoring.

L. Enhance Due Diligence

Enhance Due diligence (non-face to face customer onboarding)

Non-face-to-face onboarding facilitates the Entities to establish relationship with the customer without meeting the customer physically or through V-CIP.

Non-face-to-face modes includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs.

Following EDD measures shall be undertaken by entities for non-face-to-face customer onboarding (other than Aadhaar OTP based customer onboarding)

- a) In case Entity has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
- b) In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. LFL has laid down below process that shall be followed for mobile number change request for all such customers:
 - Customer contacts Lendingkart “Customer Support Team” through any of our authorized channel such as our email id, online chat, whatsapp, toll free number.
 - Security check shall be performed to validate the customer’s request by the “Customer Support Team.”
 - Post positive verification of the request, a ticket shall be raised in CRM with the change requested.
 - Details shall be updated in the system post which confirmation shall be sent to the customer.
- c) Apart from obtaining the current address proof, Entity shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
- d) obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- e) First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer
- f) customers to be categorized as high-risk customers and subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.
- g) LFL shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries specified by the FATF.
- h) As part of the Group’s commitment to ensuring compliance to PMLA Act, LTPL (Group company) will facilitate LFL in discharging its obligations under the PMLA by sharing relevant information required for the purposes of CDD and money laundering and terrorist financing risk management. This includes, but not limited to, transaction such as lead referrals being initiated which involves LTPL in any manner. While sharing information adequate safeguards will be undertaken to maintain the confidentiality,

POLICY ON PRESERVATION OF DOCUMENTS

security, prevent tipping-off, and lawful use of the information exchanged.

Accounts of Politically Exposed Persons (PEPs)

LFL may establish account-based relationship with PEPs (whether as customer or beneficial owner) provided that, apart from performing normal customer due diligence:

- LFL have in place appropriate risk management systems to determine whether the customer or beneficial owner is a PEP.
- Reasonable measures are taken by the LFL for establishing the source of funds/wealth.
- For any lending/business relationship with PEP, formal approval at senior level (Head of Credit & Head of Credit Risk/CRO) will be taken and the account will be closely monitored on an on-going basis.
- In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP; approval from Head of Credit Risk/CRO & Chief Compliance Officer (CCO) will be obtained to continue the business relationship.
- All PEP accounts would be classified as High Risk accounts and will be subject to enhanced monitoring on-going basis.

These instructions shall also be applicable to family members or close associates of PEPs.

Explanation: For the purpose of this Section, “Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions **by a foreign country**, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.

These customer due diligence measures will also apply to accounts of Domestic PEPs or family members and close associates of PEPs, identified during the onboarding process or through alerts received from the screening process.

6. PEP MONITORING

- In PEP and associated PEP match cases flagged as confirmed a) Probable Hit, or b) Confirmed Hit should be taken on board only subject to approval from Credit Head & Credit Risk Head/ CRO, and will be based on the Enhanced due diligence checks.
- Based on the approval or rejection, the appropriate action should be taken.
- PEP and associated PEP if onboarded, shall be tagged as “High Risk” at UCIC and Loan level and shall be subject to enhanced due diligence and continuous transaction monitoring.
- The enhanced due diligence shall include to obtain the following information
 1. Detailed information Source of Wealth and approximate net worth.
 2. Review official declarations of assets and income along with supporting documents.
 3. Access credit history to understand financial behavior and obligations.
 4. Record news articles from reputable sources that investigate corruption, wealth sources, or

POLICY ON PRESERVATION OF DOCUMENTS

scandals involving PEPs and their close associates.

In the event of an existing customer subsequently becoming a Politically Exposed Persons (PEP), the Business function shall raise that with the Credit Head and Credit Risk Head/ CRO for approval to continue with the business relationship based on above mentioned enhanced due diligence checks.

7. MONITORING OF TRANSACTIONS

- a. In terms of the Rules, the Company is required to report information relating to cash and suspicious transactions electronically to FIU India. LFL needs to comply with such reporting requirement by utilising the formats stipulated in the Master Directions and as prescribed by FIU-IND.
- b. The Cash Transaction Report (CTR) (for cash transactions and integrally connected cash transactions, transactions involving receipts by non-profit organizations, cash transactions where forged or counterfeit currency notes or bank notes have been used and cross border wire transfers, every month, as referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3 of the PML Rules) for each month shall be submitted to FIU-IND by 15th day of the succeeding month.
- c. The Suspicious Transaction Report (STR) shall be submitted within 7 working days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.
- d. In this regard, the Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.
- e. LFL shall keep in mind that any delay in furnishing of information would result into a violation of the requirement stipulated in the Rules.
- f. The Principal Officer will be responsible for timely submission of STR to FIU-IND. No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.
- g. Details of accounts resembling any of the individuals / entities in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC) shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 2, 2021.
- h. LFL shall not put any restrictions on operations in the accounts merely based on the STR filed.

LFL, its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the director is confidential. and its directors, officers, and employees (permanent and temporary) will be prohibited from disclosing ('tipping off') the fact that an STR or related information is being reported or

POLICY ON PRESERVATION OF DOCUMENTS

provided to the FIU- IND. However, such confidentiality requirement shall not inhibit sharing of information under section 4(b) of Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be the duty of all employees involved to ensure that there is no tipping off to the customer at any level.

8. RISK MANAGEMENT

For Risk Management, LFL shall have a risk based approach which includes the following.

- (a) Customers shall be categorised as low, medium, and high risk category, based on the assessment and risk perception of the RE.
- (b) Broad principals may be maid down by LFL for risk-categorisation of customers
- (c) LFL shall undertake the risk categorisation at borrowers level and the same shall be based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customer as well as transactions, type of products/ services offered, delivery channel used for delivery of products/ services, types of transactions undertaken – cash, cheque/ monetary instruments, wire transfers, forex transactions etc. . While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

The nature and extent of due diligence will depend on the risk perceived by LFL. However, while preparing customer profile LFL should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive and is in conformity with the guidelines issued by RBI in this regard. Any other information from the customer will be sought separately with his/her consent.

Customer Risk in this context refers to the money laundering and terrorist funding risk associated with a particular customer from LFL's perspective. This risk categorisation is based on AML/KYC risk perceptions associated with customer profile and not the level of credit risk.

The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment.

Risk categorization of Individual as well as Non-Individual customers (legal entities) into High, Medium and Low would be done based on following broad parameters:

POLICY ON PRESERVATION OF DOCUMENTS

- PEP
- Non Face-to-Face
- Sourcing Channel
- Mode of KYC
- Customer Visit etc.
- Credit Risk, which includes customers
- Industry/ business profile
- location
- Financials/Credit History etc.

Note: An Illustrative list of Risk Categorization parameters is given above.

AML AND CFT RISK ASSESSMENT FRAMEWORK

LFL shall carry out a 'Money Laundering' (ML) and 'Terrorist Financing' (TF) Risk Assessment for mitigation of AML risk covering the aspects specified below. Further, the periodicity of risk assessment exercise shall be determined by the Board or any committee of the Board of the LFL to which power in this regard has been delegated, in alignment with the outcome of the risk assessment exercise. However, it should be reviewed at least annually.

- Identification and assessment of money laundering and terrorist financing risks and take effective measures to mitigate those risks for clients, countries or geographic areas, products, services, transactions, or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, LFL shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with LFL from time to time.
- LFL shall properly document the outcome of the risk assessment exercise conducted and proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. **
- The placement of such results before the Board or relevant sub-committee of the Board to which power in this regard has been delegated and should be available to competent Authorities and self-regulating bodies.
- LFL shall apply a risk-based approach (RBA) for mitigation and management of risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard. LFL shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, LFL shall monitor the implementation of controls and enhance them if necessary.

POLICY ON PRESERVATION OF DOCUMENTS

9. UPDATION/ PERIODIC UPDATION Of KYC

LFL will adopt a risk-based approach with respect to periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. LFL shall undertake Periodic Updation at least once every two years for high-risk customers, once every eight years for medium risk customers and once every ten years for low-risk customers subject to the following conditions:

i. Individual Customers:

- (a) **No change in KYC information:** In case of no change in the KYC information, a self- declaration from the customer in this regard shall be obtained through customer's email id registered with LFL, customer's mobile number registered with LFL, digital channels (such as mobile/web-based application of LFL), letter etc.
- (b) **Change in address:** In case of a change only in the address details of the customer, a self- declaration of the new address shall be obtained from the customer through customer's email-id registered with LFL, customer's mobile number registered with LFL, digital channels (such as mobile/web-based application of LFL), letter etc., and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. Further, LFL shall obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, for the purpose of proof of change of address, declared by the customer at the time of periodic updation.

ii. Customers other than individuals:

- a) **No change in KYC information:** In case of no change in the KYC information of the LE customer, a self- declaration in this regard shall be obtained from the LE customer through its email id registered with LFL, digital channels (such as mobile/ web-based application of LFL), letter from an official authorized by the LE in this regard, board resolution etc. Further, LFL shall ensure during this process that Beneficial Ownership (BO) information available with LFL is accurate and shall update the same, if required, to keep it as up-to- date as possible.
- b) **Change in KYC information:** In case of change in KYC information, LFL shall undertake the KYC process equivalent to that applicable for onboarding a new LE customer.

iii. Additional measures: In addition to the above, LFL shall ensure that –

- a) The KYC documents of the customer as per the current CDD standards are available. This is applicable even if there is no change in customer information but the documents available with LFL are not as per the current CDD standards. Further, in case the validity of the CDD documents available with LFL has expired at the time of periodic updation of KYC, LFL shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- b) Customer's PAN details, if available with LFL, is verified from the database of the issuing authority at the time of periodic updation of KYC.
- c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant

POLICY ON PRESERVATION OF DOCUMENTS

document(s), including self-declaration from the customer, for carrying out periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of periodic updation of KYC are promptly updated in the records / database of LFL and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

- d) In order to ensure customer convenience, LFL may consider making available the facility of periodic updation of KYC at any branch, in terms of our internal KYC policy duly approved by the Board of Directors or any committee of the Board to which power has been delegated.
- e) LFL will adopt a risk-based approach with respect to periodic updation of KYC. Any additional and exceptional measures, which otherwise are not mandated under the regulatory guidelines may be , adopted by the LFL which shall be clearly specified in this internal KYC policy duly approved by the Board of Directors.

iv. LFL shall advise the customers that in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; customers shall submit the update documents within 30 days of the update to the documents for the purpose of updating the records at LFL end.

v. Due Notices for Periodic Updation of KYC (Effective January 01, 2026)

LFL will intimate its customers, in advance, to update their KYC. Prior to the due date of periodic updation of KYC, LFL will give at least three advance intimations, including at least one intimation by letter, at appropriate intervals to its customers through available communication options/ channels for complying with the requirement of periodic updation of KYC. Subsequent to the due date, LFL will give at least three reminders, including at least one reminder by letter, at appropriate intervals, to such customers who have still not complied with the requirements, despite advance intimations. The letter of intimation/ reminder may, inter alia, contain easy to understand instructions for updating KYC, escalation mechanism for seeking help, if required, and the consequences, if any, of failure to update their KYC in time. Issue of such advance intimation/ reminder will be duly recorded in the system against each customer for audit trail.

vi. In respect of an individual customer who is categorized as low risk, LFL will allow all transactions and ensure the updation of KYC within one year of its falling due for KYC or upto June 30, 2026, whichever is later. Accounts of such customers will be monitored regularly. This is also applicable to low-risk individual customers for whom periodic updation of KYC has already fallen due.

vii. Aadhar OTP based e-KYC and V-CIP are permitted for the purpose of updation/ periodic updation of KYC

10. MANDATORY PERMANENT ACCOUNT NUMBER (PAN) OR FORM 60:

a) In case of existing customers, LFL will obtain the Permanent Account Number or equivalent e-document thereof or Form No.60, by such date as may be notified by the Central Government, failing which LFL can temporarily cease operations in the account till the time the Permanent Account Number or equivalent e-documents thereof or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, LFL will give the customer an accessible

POLICY ON PRESERVATION OF DOCUMENTS

notice and a reasonable opportunity to be heard. Further, LFL will also incorporate an appropriate relaxation(s) for continued operation of accounts for customers who are unable to provide Permanent Account Number or equivalent e- document thereof or Form No. 60 owing to injury, illness, or infirmity on account of old age or otherwise, and such like causes. Such accounts would however, be subject to enhanced monitoring

Provided further that if a customer having an existing account-based relationship with LFL and gives in writing that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, LFL will close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Note – For the purpose of this Section, “temporary ceasing of operations shall mean the following: In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

11. EMPLOYEE'S HIRING & TRAINING

a. Hiring of Employees

LFL shall ensure adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process.

LFL shall ensure that the staff dealing with / being deployed for KYC/AML/CFT matters have, high integrity and ethical standards, good understanding of extant KYC/AML/CFT standards, effective communication skills and ability to keep up with the changing KYC/AML/CFT landscape, nationally and internationally. LFL shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.

Any inefficient or suspicious behavior of employees shall be dealt with suitably. It shall be ensured that there is no tipping off to the customer at any level.

b. Employees' Training

LFL shall have an ongoing employee training program so that the members of the Company are adequately trained in KYC/AML /CFT procedures and fully understand the rationale behind the KYC/AML policies and implement them consistently.

All necessary circulars, guidelines, notifications issued by the RBI or government authority in connection with KYC / AML /CFT procedures will be communicated to all relevant members of the Company by the compliance officer.

The training shall include all frontline staff, operations staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer

POLICY ON PRESERVATION OF DOCUMENTS

education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/ AML/CFT policy of LFL, regulation and related issues shall be ensured by the compliance officer.

12. CUSTOMER EDUCATION

The implementation of KYC procedures requires the Company to demand certain information from customers, which may be of personal nature, or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information.

LFL's front line staff will therefore personally discuss this with customers and if required, the Company may also prepare specific literature/ pamphlets, etc. to educate the customer on the objectives of the KYC program.

13. INTRODUCTION OF NEW TECHNOLOGIES

LFL shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

LFL shall also ensure,

- (a) to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- (b) adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

14. PRESERVATION OF RECORDS

The following steps shall be taken regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules.

- a. maintain all necessary records of transactions between the LFL and the customer, both domestic and international, for at least five years from the date of transaction;
- b. maintain all necessary information in respect of transactions prescribed under PML rule 3 so as to permit reconstruction of individual transaction, including the following:
 1. the nature of the transactions.
 2. the amount of the transaction and the currency in which it was denominated.
 3. the date on which the transaction was conducted; and

POLICY ON PRESERVATION OF DOCUMENTS

4. the parties to the transaction
 - c. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for atleast five years after the business relationship is ended;
 - d. make available swiftly, the identification records and transaction data to the competent authorities upon request;
 - e. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
 - f. evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.
 - g. The records of identity and address of their customer, and records in respect of transactions referred to in Rule 3 shall be maintained in hard or soft copy.

Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", "identification records," etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

14A. LFL shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, LFL shall register the details on the DARPAN Portal and also maintain such registration records for a period of five years after the business relationship between the customer and LFL has ended or the account has been closed, whichever is later.

15. INTERNAL CONTROL SYSTEM

- a. The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC & AML policy and procedures. The compliance function under the guidance of Compliance Head / officer will provide an independent evaluation of the Company's policy and procedure, including legal and regulatory requirements.
- b. The Company will ensure that its audit function is staffed adequately with individuals who are well-versed in such policies and procedures or hire the services of a reputed company engaged in providing quality services in the said field.
- c. Internal Auditors will specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard will be put up before the Audit Committee of the Board at quarterly intervals. Any gaps identified by the auditors need to be rectified under the supervision of the Business head or compliance Head / officer.

POLICY ON PRESERVATION OF DOCUMENTS

16. POLICY REVIEW AND UPDATION

The Board of Directors shall review this Policy annually or on a need-basis i.e. in the event of change in regulatory framework or for business or operational need (whichever is earlier). Such updates / changes to the Policy will be communicated to the relevant staff /personnel (both in-house or outsourced) and relevant stakeholders across the Company.

17. CONFIDENTIALITY AND SHARING OF INFORMATION

- a. The Company officials shall maintain confidentiality of information as provided in Section 45NB of RBI Act 1934.
- b. LFL shall maintain secrecy regarding the customer information which arises out of the contractual relationship between LFL and Customer.
- c. Information collected from customers for the purpose of opening of accounts shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling or any other purpose without the express permission of the customer.
- d. While considering the request for data/information from Government and other agencies, LFL shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
- e. The exceptions to the said rule shall be as under:
 - o Where disclosure is under compulsion of law
 - o Where there is a duty to the public to disclose
 - o The interest of company required disclosure
 - o Where the disclosure is made with the express or implied consent of the customer.

18. CONFLICT WITH THE ACT/ RULES/REGULATIONS

a. Conflict with the Act/ Rules/Regulations

The Prevention of Money Laundering Act, 2002, Rules and Regulations issued there on and any Regulation / Circular / Direction issued by the RBI shall have an overriding effect on the Policy.

19. KYC POLICY / SOP EXCLUSIONS

- a. KYC Framework is in place for day-to-day operations, covering procedural aspects such as the list of KYC documents required for various loan applicant types elaborating valid KYC documents and other related operational processes.
- b. Any deviation to the KYC should have a documented EDD (Enhanced Due Diligence) and approval from the process owner (unit head). Any permanent deviation taken on the process should have a documented approval from the compliance and Business Head.

POLICY ON PRESERVATION OF DOCUMENTS

- c. The KYC and AML guidelines from the regulator cannot be compromised under any condition.

20. *OMNIBUS CLAUSE*

All extant & future master circulars/directions/guidelines/guidance notes issued by Reserve Bank of India (RBI) from time to time would be the directing force for the KYC Policy of LFL and will super cede the contents of this KYC Policy.
