CREDITACCESS GRAMEEN LIMITED

POLICY ON KNOW YOUR CUSTOMER (KYC), ANTI-MONEYLAUNDERING (AML) AND COUNTERING FINANCING OF TERRORISM (CFT)

Revision History

Version	Author	Description of Changes	Release Date
1	Chief Audit Officer (CAO)/ Chief Compliance Officer (CCO)	First version	April 1, 2017
2	Chief Audit Officer (CAO)/ Chief Compliance Officer (CCO)	(a) Inclusion of definitions section (b) Prescribing procedures & steps to be followed on identification of PEPs, High-Risk customers, etc. (c) Screening of Prohibited list of individuals/entities	June 25, 2021
3	Chief Audit Officer (CAO) / Chief Compliance Officer (CCO)	(a) Obtaining voluntary consent from customer for authentication / offline verification as required under RBI Directions read with the Aadhaar Act,2016 & PML Act, 2002 & Regulations made thereunder.	Dec 21, 2021
4	Chief Audit Officer (CAO) / Chief Compliance Officer (CCO)	Amendment made to Scope and insertion of new clause "Record Keeping"	March 23, 2022
5	Chief Audit Officer (CAO) & Chief Compliance Officer (CCO)	(a) Revised based on amendment to Master Direction (MD) on KYC by RBI dated April 28, 2023 and May 04, 2023 (b) Incorporated relevant provisions of PFRDA Circular on KYC/AML/CFT	July 21, 2023
5	Chief Audit Officer (CAO) & Chief Compliance Officer (CCO)	Re-adoption	April 01, 2024
6	Chief Compliance Officer	(a) Removal of point (i) and (ii) where link to ISIL (Da'esh) & Al-Qaeda Sanctions List and Taliban Sanctions List are given. Frequent updates in these lists by MHA are captured and are available in RBI's KYC Master Direction. So, it is proposed to give reference to RBI's KYC MD instead of giving the link directly in our policy (b) 'Chief Audit Officer' under point (vi) being revised to 'Chief Audit Officer/ Head – Internal Audit' and newly added point – (viii) Principal Officer	Oct. 25, 2024
7	Chief Compliance Officer	Updation of 'Para 13' on 'Principal Officer' to align it with extant, applicable RBI Regulations	Jan. 24, 2025

8	Haridarshini. A, Chief Customer Service Officer	Revised to align with the Master Direction (MD) on KYC by RBI dated November 28, 2025. Language alignment & structuring across the policy document for improved clarity, consistency, and readability	April 16 2026
9	Haridarshini. A, Chief Customer Service Officer	Revised to align with the Master Direction (MD) on KYC by RBI dated November 28, 2025. Language alignment & structuring across the policy.	October 22, 2026

Version Control

Version	Author	Reviewed by	Approved by
1	CAO / CCO	MD & CEO	Board of Directors
2	CAO / CCO	MD & CEO	Board of Directors
3	CAO / CCO	MD & CEO	Board of Directors
4	CAO / CCO	MD & CEO	Board of Directors
5	CAO and CCO	MD & CEO	Board of Directors
5	CAO and CCO	Managing Director	Board of Directors
6	CCO	Managing Director	Board of Directors
7	CCO	Managing Director	Board of Directors
8	Principal Officer	MD &CEO	Board of Directors
9	Haridarshini-CCSO	Devika Praveen-CCO Gururaj Rao-COO Ganesh Narayanan, MD & CEO	Board of Directors

Contents

1. Introduction: 5
2. Objective: 5
3. Scope: 5
4. Definitions: 5
5. Customer Acceptance Policy: ..... **Error! Bookmark not defined.**
6. Risk Management: 6
7. Customer Identification Procedure (CIP): 8
8. Customer Due Diligence CDD) Procedure: 9
9. Prohibited List of Individuals/Entities: 144
10. Data Secrecy, Sharing of Information and Record Keeping: 155
11. Periodic Review and Assessment, Compliance Monitoring, Risk Management: 166
12. Hiring of Employees and Employee Training: 166
13. Customer Education: 166
14. Designated Director: 177
15. Principal Officer: 177
16. Reporting: ..... **Error! Bookmark not defined.**7
17. CKYC Dissemination and Implementation: 188

POLICY ON KNOW YOUR CUSTOMER (KYC), ANTI-MONEY LAUNDERING (AML) AND COUNTERING FINANCING OF TERRORISM (CFT)

1. Introduction:

CreditAccess Grameen Limited being a Non-Banking Financial Company – Micro Finance Institution ("NBFC-MFI") registered with RBI, is subject to the applicable Direction issued by RBI, as amended from time to time. Further, also being an entity registered as Point of Presence (PoP) to transact in pension schemes under National Pension System as per the Pension Fund Regulatory and Development Authority (Point of Presence) Regulations, 2018, including amendments, if any, for the time being in force, is obliged to have Know Your Customer / Anti-Money Laundering / Countering Financing of Terrorism (KYC/AML/CFT) policy.

2. Objective:

The objective of KYC, AML and CFT policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering (ML)/ Terrorist Financing (TF) activities.

3. Scope:

This policy is applicable to various stakeholders including employees and customers of the Company.

4. Definitions:

(i) "Aadhaar Act, 2016" shall refer to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, as amended from time to time.

(ii) "Act" or "Rules" means the Prevention of Money Laundering Act, 2002 and Prevention of Money Laundering (Maintenance of Records) Rules, 2005, and the same shall also be referred to as "PML Act" and "PML Rules", respectively.

(iii) "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.

(iv) "Customer/Borrower" means a person who is engaged in a financial transaction or activity with the Company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting. It shall mean and include the applicant and co-applicants.

(v) "Designated Director" means a person whom the NBFC designates to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include the Managing Director or a whole-time Director, whom the Board of Directors has duly authorised.

(vi) "Digital KYC" has the same meaning as defined under RBI Directions.

(vii) "MBDF" means the Member's Basic Data Form

(viii) "Officially Valid Documents" or "OVDs" means the passport, the driving license, 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, including amendments to RBI Directions, from time to time.

(ix) "PFRDA Regulations" means the provisions which are applicable to the Company under the Pension Fund Regulatory and Development Authority (Point of Presence) Regulations, 2018, as amended from time to time

(x) "RBI Directions" means provisions which are applicable to the Company under RBI (NBFCs– Know Your Customer) Directions, 2025, as amended from time to time or such other Circulars, Notifications or guidelines issued by RBI from time to time on KYC / AML / CFT requirements.

(xi) "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, including the Heads of States / Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations and important political party officials.

(xii) "Principal Officer" means a Company's nominated officer at the management level, responsible for furnishing information as per rule 8 of the PMLA Rules.

(xiii) Senior Management – shall have the same meaning as defined in Section 178 of Companies Act 2013.

(xiv) "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:

a) 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
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to have no economic rationale or bona fide purpose; or
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

(xv) ''Video based Customer Identification Process (V-CIP)" Means an alternative method by which an authorised official of the NBFC conducts customer identification with facial recognition and customer due diligence. This process involves a 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 which the customer furnished, through independent verification and by maintaining an audit trail of the process and considers on par with face-to-face CIP for the purpose of KYC Directions.

The phrase customer, borrower, client and subscriber are used interchangeably in this Policy, and they shall be considered to have the same meaning, as per RBI Directions or PFRDA Regulations.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Act, Rules, PFRDA (Point of Presence) Regulations, 2018 and RBI Directions, as the case may be.

5. Customer Acceptance Policy

The Company shall:

(1) not to extend any facility to an anonymous or fictitious customer.

(2) not extend any facility without applying appropriate CDD measures, either due to non-cooperation of the customer or unreliability of the documents / information furnished by the customer. The Company shall consider filing an STR, if necessary, when it is unable to comply with

the relevant CDD measures in relation to the customer.
(3) mandatory information as per application form and details of ID, address proof, PAN/Form-97 to be collected for extending the facility.
(4) obtain additional information, if any, with the explicit consent of the customer.
(5) apply the CDD procedure at the Unique Customer Identification Customer (UCIC) level. Thus, if an existing KYC-compliant borrower desires to avail any of our product or service there shall be no need for a fresh CDD exercise as far as identification of the borrower is concerned.
(6) The circumstances in which a customer is permitted to act on behalf of another person

- Acceptance of terms and conditions by the group leader on behalf of the members or any other action, the Company may stipulate in line with Regulatory guidelines.

(7) put in place a suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists.
(8) verify the Permanent Account Number (PAN) (if obtained) from the verification facility of the issuing authority.
(9) verify the Goods and Services Tax (GST) number from the search / verification facility of the issuing authority, where the GST details are available.

The members of general public should not be denied a financial facility, especially those who are financially or socially disadvantaged, including the Persons with Disabilities (PwDs). The Company should not reject an application for onboarding or periodic updation of KYC without application of mind. The officer concerned should duly record the reason(s) for rejection.

Further, where the Company suspects money laundering or terrorist financing, and 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.

Further, the Company is also guided by the policy to enable any of the digital channels, such as Grameen MAHI – Self Service Android App ("App"), for accepting the loan applications/ references from the existing customers and adopt a detailed SOP in this regard.

6. Risk Management:

The Company shall have a risk-based approach as outlined below:

(A) For the purpose of RBI Directions:

(i) Customers shall be categorised as low, medium and high-risk category, based on the risk assessment framework adopted by the Company.
(ii) Risk categorisation shall be undertaken based on parameters such as customer's identity, social status, financial status, nature of business activity, and information about the clients' business and its location, geographical risk covering customers as well as transactions. Further, the risk categorization of a customer and the specific reasons for such categorization will be kept confidential and will not be revealed to the customer to avoid tipping off.
(iii) All microfinance customers of the Company will be categorized as low-risk customers for the following reasons:

a. All such customers belong to low-income households.
b. Their identity, residential addresses and the source(s) of income are verified and are further confirmed through personal visits by Company's officials.
c. The customers belong to the lower socio-economic strata with annual household income to be eligible for MFI loans as per RBI guidelines.

However, any circumstances leading to classification/downgrading of Micro Finance customers into other than Low category will be covered as part of Customer Risk Categorisation Framework.

(iv) Non-GL Borrowers will be classified into different risk category based on their profile in line with Customer Risk Categorisation Framework.

Further, any individual PEPs as per the RBI definition will be categorized as high-risk and subjected to Enhanced Due Diligence. However, there is remote possibility of PEPs applying for the loan facilities offered by the Company. Thus, screening of applicants against PEPs list is considered as not applicable/ not carried out. If the existing customer subsequently becomes a PEP, then the Senior Management shall approve such customers to continue the business relationship with the Company.

A periodic review/assessment of all customers for risk categorization to be carried out bi-annually.

Further, The risk categorisation of customers shall be undertaken in accordance with the Customer Risk Categorisation Framework", as amended from time to time.

(B) For the purpose of PFRDA Regulations:

(i) Subscriber's risk profile for accounts under pension schemes regulated/ administered by PFRDA shall be categorized as lower risk, moderate risk and higher risk.
(ii) Risk categorization shall be undertaken based on whether contribution is mandatory contribution, voluntary with low contribution, contribution on voluntary basis, contributions which are a withdrawable account.
(iii) In addition to the above, the nature of accounts, source and mode of contribution, regularity in the flow of contribution, withdrawals, residence status of the subscriber, Politically Exposed Person, shall also be considered while assessing the risk profile of the subscribers.

Basis the group lending (GL) customer profile, the low-ticket size of the loans offered by the Company, low contribution on voluntary basis by the PFRDA subscribers, they are considered as low-risk customers.

7. Customer Identification Procedure (CIP)

The Company to undertake customer identification at the time of commencing the account-based relationship i.e. while selling its own products and/or selling third-party products as agents.

To ensure customer acceptance is in accordance with the applicable provisions of Aadhaar Act, 2016 and Regulations made thereunder with respect to authentication, offline verification, digital KYC, Video Based Customer Identification Process (VCIP), e-KYC, KYC Identifier allotted by the CKYCR or such other forms of verification of Aadhaar number or such other permissible OVDs, as may be made permissible to the Company, from time to time.

8. Customer Due Diligence (CDD) Procedure

For undertaking CDD, the Company shall obtain the following from an individual while establishing an account-based relationship

A. As part of the customer acceptance process (physical mode), to procure the following documents:

(i) Photograph of customer along with Co-applicant, if applicable.

(ii) <u>Photo IDs:</u>

- Voter's ID issued by Election Commission of India
- Proof of possession of Aadhaar Number/ copy of Aadhaar (redacted)*
- Driving License
- Passport
- Job card issued by NREGA duly signed by an officer of the State Government
- Letter issued by the National Population Register containing details of name and address.

*Provided the customer voluntarily provides his/her Aadhaar number, wherever applicable, either in physical or electronic form, for authentication or offline verification, digital KYC, Video Based Customer Identification Process (V-CIP), e-KYC authentication, KYC Identifier allotted by the CKYCR, or in such other form or in such manner as may be specified by the Regulations under the Aadhaar Act, 2016, as amended from time to time.

(iii) PAN or equivalent e-document to be obtained as per the provisions of IT Rule 159 as amended from time to time. Form 97 to be obtained from persons who do not have PAN or equivalent e-document thereof.

(iv) <u>Address Proof:</u>

A copy of any one of the following documents as address proof:

- Aadhaar Card (redacted)
- Voter's ID issued by Election Commission of India
- Driving License
- Passport
- Job card issued by NREGA duly signed by an officer of the State Government
- Letter issued by the National Population Register containing details of name and address.

Where the above documents furnished by the customer do not have updated current address, the following documents may be collected for the limited purpose of proof of address: -

- Utility bill, which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill).
- Property or Municipal tax receipt.
- Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings if they contain the address.
- 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 license agreements with such employers allotting official accommodation.

The customer should submit the updated KYC documents with current address within a period of three months of submitting the documents specified above.

B. Verification of KYC/ OVDs by Kendra Managers

(i) Both Photo ID and address proof should be verified with the original and a digital image of the same should be captured by the Kendra Manager ("KM") in respective digital applications/platform.

(ii) In case digital copies are obtained, the company official should submit an undertaking after verifying with the original and affixing the branch seal. The undertaking should be signed by the customer as well.

(iii) In case photocopies are obtained, both photo ID and address proof (photocopies) should be self-attested by the customer. Further, it should be duly attested by the company official after verifying with the original and affixing the branch seal.

(iv) The Photo ID and Age proof are to be collected for spouse of the customer. This must be taken at the time of enrolment of new customers.

(v) <u>Periodic KYC updation:</u>

a. In all cases where the Company has already obtained valid KYC documents from the customers, there is no need to obtain fresh set of documents if there is no change, while giving fresh/repeat loans. However, the KYC documents once submitted will remain valid for a period of ten (10) years in case of low-risk customers and five (5) years in case of medium risk customers, from the date of establishing the account-based relationship/ last KYC updation.
   In case of customers categorized as high risk, a fresh set of KYC documents shall be obtained once in every two (2) years.

b. In case of no change in the KYC information, the Company should obtain a self-declaration from the customer in this regard through the customer's registered email-id, mobile number or other digital channels, letter, etc.
   Same process to be followed in case of change in address details of the customer. However, the Company may obtain a copy of OVD or deemed OVD, as defined in para 8(iv) above, for the purpose of proof of address, declared by the customer at the time of updation / periodic updation.

c. The Company may use Aadhaar OTP based e-KYC in non-face-to-face mode for updation / periodic updation. The Company should ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

d. The Company shall issue due notice/ advance intimations to customers for the periodic updation of KYC, as prescribed by RBI and shall maintain appropriate records of such

communications for audit purposes.

e. Further, the Company to provide facility for periodic updation of KYC updation at branches for submission of recent photograph/ KYC documents, that requires physical presence of the customer at the base branch (where account is maintained).
f. Company should provide an acknowledgment to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation.
g. For customers, where the Permanent Account Number (PAN) is not available, the equivalent e-document thereof or Form No. 97 as defined in rule 159 of Income-tax Rules 2026 shall be obtained.

C. Video based Customer Identification Process (V-CIP).

1. V-CIP Infrastructure

(i) The Company shall comply with the RBI guidelines on minimum baseline cyber security and resilience framework for NBFCs, as updated from time to time as well as other general guidelines on IT risks. The Company shall house the technology infrastructure on its own premises, and the V-CIP connection and interaction shall necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall comply with relevant RBI guidelines. The Company shall ensure that ownership of data in cloud deployment model rests with the Company only and all the data including video recording is transferred to the Company's exclusively owned / leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and the cloud service provider or third-party technology provider assisting the V-CIP shall retain no data.

(ii) The Company shall 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 consent shall be recorded in an auditable and alteration-proof manner.

(iii) The V-CIP infrastructure / application shall be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

(iv) The video recordings shall contain the live GPS co-ordinates (geo tagging) of the customer undertaking the V-CIP and date and time stamp. The quality of the live video in the V-CIP shall be adequate to allow identification of the customer beyond doubt.

(v) The application shall have components with face liveness / spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company.

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

(vi) The Company can use appropriate artificial intelligence (AI) technology to ensure that the V-CIP is robust.

(vii) Based on experience of detected / attempted / near-miss cases of forged identity, the company shall regularly update the technology infrastructure including application software as well as workflows.

(viii) The V-CIP infrastructure shall be subject to necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gaps reported under this process is to be mitigated by the Company before rolling out process of V-CIP implementation. Such tests/Audits shall be conducted by empaneled auditors of Indian Computer Emergency Response Team (CERT-In). Such tests shall also be carried out Annually in conformance to internal / regulatory guidelines.

(ix) The Company shall subject the V-CIP application software and relevant APIs / webservices to appropriate testing of functional, performance, and maintenance strength before being used in live environment. Such application shall be rolled out only after closure of any critical gaps found during such tests.

2. V- CIP Procedure:

The Company to formulate a clear workflow and standard operating procedure for V-CIP and ensure adherence to it. The V-CIP process should be operated only by officials of the Company specially trained for this purpose. The official shall be capable of carrying out liveness checks 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 the video, reconnecting calls, etc., may not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then the Company may not initiate a fresh session. However, in case of call drop / disconnection, fresh session shall be initiated.

(iii) The Company shall vary the sequence and / or type of questions, including those indicating the liveness of the interaction, during video interactions to establish that the interactions are real-time and not pre-recorded.

(iv) The Company shall reject the account opening process if it observes any prompting at the customer end.

(v) The Company shall factor in the fact that the V-CIP customer is an existing or new customer, or if the case relates to one rejected earlier or if the name appears in some negative list, at an appropriate stage of workflow.

(vi) Company's authorised official performing the V-CIP shall record audio and video as well as capture a photograph of the customer present for identification and obtain the identification information using any one of the following:

(a) OTP based Aadhaar e-KYC authentication with borrower's consent.

(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.

(vii) The Company should ensure redact or blackout of the Aadhaar number

(viii) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, the Company shall ensure that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP.

(ix) Further, in line with the prescribed period of three working days for usage of Aadhaar XML file / Aadhaar QR code, the Company shall ensure that it undertakes video process of the V-CIP 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. However, the Company shall ensure that no incremental risk is added due to this.

(x) If the address of the customer is different from that indicated in the OVD, the Company shall capture suitable records of the current address, as per the existing requirement. The Company shall ensure that it also confirms the economic and financial profile / information submitted by the customer from the customer undertaking the V-CIP in a suitable manner.

(xi) The Company shall capture a clear image of PAN card displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The Company shall verify the PAN details from the database of the issuing authority, including through DigiLocker.

(xii) The use of printed copy of equivalent e-document, including an e-PAN is not valid for the V-CIP.

(xiii) The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar / OVD and PAN / e-PAN 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.

(xiv) The Company shall make all accounts opened through V-CIP operational only after subjecting them to concurrent audit to ensure the integrity of process and its acceptability of its outcome.

(xv) The Company shall appropriately comply with all matters not specified under the paragraph but required under other statutes such as the Information Technology (IT) Act.

3. V-CIP Records and Data Management

(i) The Company shall store the entire data and recordings of V-CIP in a system / system located in India, in a safe and secure manner and bears the date and time stamp that affords easy historical data search.

(ii) The Company shall also preserve the activity log along with the credentials of the official

performing the V-CIP.

D. Ongoing Due Diligence of Customers

The Company shall conduct ongoing due diligence and transaction monitoring for all GL and RF customers, irrespective of their risk category, to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

E. Enhanced due diligence of customers:

In case of Medium/High-Risk customers, the Company shall carry out enhanced due diligence procedures prescribed under applicable RBI Directions, PML Rules 2005 and PFRDA Regulations to gather sufficient information including information about the changes in nature of activity, sources of funds etc.

In addition, the Company shall ensure following measures with respect to "High Risk" customers:

(i) The identity of the person should have been verified before accepting him/her as a customer.
(ii) The decision to offer any facility is taken at a senior level/product head in accordance with the Customer Acceptance guidelines.
(iii) In the event of an existing customer subsequently categorised as "High-Risk", senior management's approval is obtained to continue the business relationship.
(iv) Enhanced monitoring on an on-going basis.

9. Prohibited List of Individuals/Entities:

I. Obligations under the Unlawful Activities (Prevention) (UAPA) Act, 1967:

(1) The Company shall ensure that in terms of section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967 and amendments thereto, it does not have any account in the name of individuals / entities appearing 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). The details of the two lists are as under:

(i) The 'ISIL (Da'esh) & Al-Qaida Sanctions List', established and maintained pursuant to Security Council resolutions 1267 / 1989 / 2253, which includes names of individuals and entities associated with Al-Qaida, is available at www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list

(ii) The 'Taliban Sanctions List', established and maintained pursuant to Security Council resolution 1988 (2011), which includes names of individuals and entities associated with the Taliban is available at https://www.un.org/securitycouncil/sanctions/1988/materials.

(2) The Company shall also ensure to refer to the lists as available in the Schedules to the

Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The Company shall verify the aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, on a daily basis, and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the NBFC for meticulous compliance.

(3) The Company shall report the details of accounts resembling any of the individuals / entities in the lists to FIU-IND in addition to advising the Ministry of Home Affairs (MHA) as required under UAPA notification dated February 2, 2021

II. Obligations under Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act, 2005):

The NBFC shall ensure meticulous compliance with the 'Procedure for Implementation of section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005' laid down in terms of section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India.

Accordingly, Company to ensure compliance to all guidelines issued in this regard by RBI from time to time

III. Further, the Company will verify the UNSCR 1718 Sanctions List of Designated Individuals and Entities, as available at Implementation of UNSC Sanctions (DPRK) | Ministry of External Affairs , Government of India (https://www.mea.gov.in/implementation-of-unsc-sanctions-dprk) to 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.

Further, the Company's customers are monitored periodically by screening them against the lists provided under RBI Directions and PFRDA Regulations, as amended from time to time.

10. Data Secrecy, Sharing of Information and Record Keeping:

I. Data Secrecy, Sharing of Information

(1) The Company shall maintain secrecy regarding the customer information that arises out of the contractual relationship between the NBFC and the customer.

(2) The Company shall treat information collected from customers for the purpose of opening of account as confidential and shall not divulge details thereof for the purpose of cross-selling, or for any other purpose without the express permission of the customer.

(3) While considering the requests for data / information from Government and other agencies, the Company shall satisfy itself 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.

(4) The exceptions to the said rule shall be as under:

(i) Where disclosure is under compulsion of law,

(ii) Where there is a duty to the public to disclose,

(iii) Where the interest of the NBFC requires disclosure, and

(iv) Where the disclosure is made with the express or implied consent of the customer.

II. Record Keeping

The customer identification records and account information shall be maintained and preserved in accordance with the Prevention of Money Laundering Act, 2002 and the applicable Rules made thereunder. Transaction records shall be retained for at least eight years from the date of the transaction and customer identification and address records shall be preserved for at least eight years after business relationship has ended. Further, Company shall also maintain records of all transactions mentioned under para 16 of this policy.

Records shall contain sufficient details to enable reconstruction of individual transactions, including the nature, amount, date, and parties involved, and should be maintained in hard or electronic form in a manner that permits their prompt retrieval and production to competent authorities when requested/needed.

11. Compliance of KYC policy: Role of Internal Audit

Internal audit department or the external auditor appointed by the Company should periodically verify compliance with the extant policies, procedures and controls related to money laundering activities based on overall risk assessment. Company should also upgrade its questionnaire and system from time to time in accordance with the extant PML Act and PML Rules. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. Company should submit audit notes and compliance to the Audit Committee of the Board on quarterly basis.

12. Hiring of Employees and Employee Training:

The Company shall, as an integral part of its personnel recruitment/ hiring process, ensure for adequate screening of individuals while hiring of employees. The basic training undertaken for each new loan officer and regular refresher training conducted at branches would ensure that field staff are adequately trained in KYC, AML and CFT procedures. The Company will review the training adequacy at regular intervals to ensure that training is different for frontline staff, compliance staff and staff dealing with new customers.

The Company should ensure the proper staffing of the audit function with persons adequately trained and well-versed in KYC / AML / CFT policies of the NBFC, regulation and related issues.

13. Customer Education:

Customers would be trained on the necessity and importance of KYC documents during Compulsory Group Training. Apart from these, regular awareness activities shall be undertaken

through Kendra Announcements, Jagruthi Campaign etc.

14. Designated Director:

To ensure compliance with the obligations under the Act and Rules, the Company shall nominate a Director on their Boards as "Designated Director".

The name, designation, address and contact details of the Designated Director, including changes thereon, shall be communicated to the FIU-IND, the Reserve Bank of India, the Pension Fund Regulatory and Development Authority (PFRDA) and such other statutory/ regulatory authorities, as may be required from time to time.

15. Principal Officer:

As required under RBI Directions, the Company shall appoint a senior management officer to be designated as Principal Officer who is located at the Head/Corporate Office of the Company. To discharge his/ her responsibilities, the Principal Officer shall have timely access to all customer identification data and other CDD information, transaction records and other relevant information. The role and responsibilities of the Principal Officer shall include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Act and Rules, as amended from time to time.

The name, designation, address and contact details of the Principal Officer shall be communicated to the FIU- IND, the Reserve Bank of India, the Pension Fund Regulatory and Development Authority (PFRDA) and such other statutory/ regulatory authorities, as may be required from time to time.

16. Reporting:

The Company shall ensure reporting of the following transactions/instances

(i) **CTR -** All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency

(ii) **CTR -** Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which have taken place within a month and the monthly aggregate which exceeds Rupees Ten Lakh or its equivalent in foreign currency.

(iii) **CCR -** All cash transactions where forged or counterfeit currency notes or banknotes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions.

The transactions specified in clauses (i) to (iii), if any, above shall be reported by the 15th day of the succeeding month.

(iv) **STR -** All suspicious transactions whether made in cash and in manner as mentioned in the Act and Rules shall be reported within 7 working days from the date of occurrence of such transaction.

(v) Any instance of forged identity detected during the V-CIP process shall be reported as a cyber event under extant regulatory guidelines (CERT-In).

(vi) **Match found during the screening of following sanction list**

a. Under UNSC Sanctions Lists - the Company shall immediately report the transaction/details, together with full particulars of the funds, financial assets or economic resources involved, to the Central Nodal Officer (Joint Secretary (CTCR), Ministry of Home Affairs).
b. Under Weapons of Mass Destruction (WMD) list - the Company shall immediately report the transaction/details, together with full particulars of the funds, financial assets or economic resources involved, to the Central Nodal Officer (Joint Secretary (CTCR), Ministry of Home Affairs), Director, FIU-India, and simultaneously provide a copy of such communication to the concerned State Nodal Officer (Principal Secretary/Secretary, Home Department) and the Reserve Bank of India (RBI), in accordance with applicable regulatory requirements.

17. CKYC Dissemination and Implementation:

All regulatory instructions related to Central KYC Records Registry (CKYCR) will be formally disseminated across all locations and business segments wherever applicable for information and necessary implementation.

****