KNOW YOUR CUSTOMER (KYC) GUIDELINES AND ANTI-MONEY LAUNDERING (AML) MEASURES

AGRIM HOUSING FINANCE PRIVATE LIMITED

{REGISTERED WITH NATIONAL HOUSING BANK (NHB) HAVING CERTIFICATE OF REGISTRATION RECEIVED FROM THE RESERVE BANK OF INDIA DATED JULY 03, 2020 HAVING REGISTRATION NUMBER DOR-00183 }

1. INTRODUCTION

As part of the best corporate practices, and good governance, AGRIM HOUSING FINANCE PRIVATE LIMITED (hereinafter referred to as "the Company" or "AGRIM HFC") has adopted **'Know Your Customer' (hereinafter referred to as "KYC")' and 'Anti Money Laundering (hereinafter referred to as "AML") Measures' (referred to as "Guidelines")** for lending/ credit/ operations/ financial dealings in compliance with governing laws.

These guidelines aim at preventing the Company from being used intentionally or unintentionally by criminal elements for committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism. Accordingly, the Company had prepared the policy on 'Know Your Customer and Anti-Money Laundering /CFT Measures' which are applicable to Company and Satellite Offices/ branches and are duly complied with by all the Officials Managers, and the staff dealing with the customers. Considering the importance of the measures, the top management will be directly involved in the various aspects of accounting related issues.

2. GOVERNING LAWS

The Finance (No.2) Act, 2019, has amended the National Housing Bank Act, 1987 conferring certain powers for regulation of Housing Finance Companies (HFCs) with Reserve Bank of India (RBI). The provisions of the said Act came into force w.e.f. August 09, 2019. Consequently, RBI vide a Press Release dated August 13, 2019, informed that the HFCs will henceforth be treated as one of the categories of Non-Banking Financial Companies (NBFCs) for regulatory purposes.

The Master Direction – Know Your Customer (KYC) Direction, 2016 issued by the Reserve Bank of India has consolidated directions on Know Your Customer (KYC), Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) and is applicable to all Regulated Entities of RBI. As HFCs are also entities to be regulated by the RBI after the said transfer of regulation, RBI, on May 19, 2020, decided to extend the said Master Direction to all HFCs and repealed the instructions/guidelines/regulations issued by the National Housing Bank from time to time in this regard. Accordingly, the Master Direction – Know Your Customer (KYC) Direction, 2016; last dated May 04, 2023; issued by the Reserve Bank of India applies to AGRIM HFC.

The KYC Policy framed hereunder is to be read and followed in conjunction with Know Your Customer (KYC) Direction, 2016, as amended from time to time, issued by the RBI or any other applicable law in force and in the event of any inconsistency, the latter shall prevail.

The Company shall further ensure compliance with the provisions of the Prevention of Money-Laundering Act, 2002, and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

3. OBJECTIVES OF KYC POLICY

In view of the foregoing, Key objectives of the KYC and AML Policy are as under:

(a) To establish a regulatorily compliant KYC mechanism to on-board customers;

(b) To ensure compliance throughout the life-cycle of customers as per the laid down norms

(c) To prevent the Company's business channels/products/services from being used as a channel for Money Laundering("**ML**")/ Terrorist Financing("**TF'**);

(d) To establish a framework for adopting appropriate AML procedures and controls in the operations/business processes of the Company;

(e) To ensure compliance with the laws and regulations in force from time to time;
(f) To protect the Company's reputation;
(g) To lay down KYC-AML compliance norms for the employees of the Company.

4. NAME OF THE POLICY & ITS APPLICABILITY AND EFFECTIVE DATE.

a) Name of the Policy

This Policy shall be known as "Know Your Customer (KYC) Policy of AGRIM HOUSING FINANCE PRIVATE LIMITED".

b) Applicability:

This Policy shall be applicable to all categories of products and services offered by the Company and shall be followed by every branch, office, official, employee, service provider, attorney, or any other delegated authority acting or conducting business on behalf of the Company.

c) Effective Date :

The Policy shall come into force with immediate effect.

5. DEFINITIONS

A. Unless the context otherwise requires, the terms herein shall bear the meanings assigned to them below:

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. "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.

iii. " Beneficial Owner (BO)" means:

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, having controlling ownership interest or who exercise control through other means.

Explanation - For the purpose of this sub-clause-

(i) "Controlling ownership interest" means ownership of / entitlement to more than 25 percent of the shares or capital or profits of the company.

(ii) "Control" shall include the right to appoint a 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, having ownership of / entitlement to more than 15 percent of capital or profits of the partnership.
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, having ownership of/ entitlement to more than 15 percent 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.

c) 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 15% 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.

iv. "Certified Copy" ***of Officially Valid Document (OVD)***– means obtaining and comparing the copy of the proof of possession of Aadhaar Number where offline verification cannot be carried out or OVD so produced by the customer with the original and recording the same on the copy by the authorized officer under his unique number (such as PF No. or employee number etc.). The authorized officer will also attest to the duly signed photograph of the customer.

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 anyone of the following, may be obtained:

- authorized officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas Banks with whom the Company have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/ Consulate General in the country where the non-resident customer resides.

v. "**Central KYC Records Registry**" (CKYCR) means an entity defined under Rule 2(1) of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

vi. "**Customer**" means

- a person or entity that maintains an account and/ or has a business relationship with the Company;
- one on whose behalf the account is maintained (i.e. the beneficial owner);
- beneficiaries of transactions conducted by professional intermediaries, such as stock brokers, chartered accountants, solicitors, mutual funds etc. as permitted under the law; and
- any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company, say, a wire transfer or issuance of a high value demand draft as a single transaction.

vii. "**Customer Due Diligence**" (CDD) means identifying and verifying the customer and the beneficial owner.

viii. "Customer identification" means undertaking the process of CDD.

ix. "Designated Director" means a person so designated by the Board to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules thereunder and shall include the Managing Director or a whole-time Director (as defined under the Companies Act, 2013) duly authorized by the Board.

x. "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 Company as per the provisions contained in the Act.

xi. "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

xii. "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 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.

xiii. "Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by

the Central KYC Records Registry.

xiv. "**KYC Templates**" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individual and legal entities.

xv. "Non-face to face customers' means customers who opens accounts without visiting the branch/office of the Company or meeting the officials of the Company.

xvi. "Officially Valid Document" *(OVD)* 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 the 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 e-documents thereof 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 license agreements with such employers allotting official accommodation;

c) The customer shall submit OVD with a 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 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.

xvii "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)

xviii"**On-going Due Diligence**" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

xix. "Person" includes: a) an individual, b) a Hindu undivided family, c) a company, d) a firm, e) an association of persons or a body of individuals, whether incorporated or not, f) every artificial juridical person, not falling within any one of the above persons (a to e), and g) any agency, office or branch owned or controlled by any of the above persons (a to f).

xx. "Periodic Updation" means steps taken to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relent by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

xxi. "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g.,Heads of State/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important

political party officials, etc.

xxii. "Principal Officer" means an officer nominated by the Company for ensuring compliance, monitoring transactions, sharing and reporting information as required under the law/ regulations, and responsible for communicating and furnishing information to FIU-IND under PML Rules.

xxiii. "Shell Bank" means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.

xxiv. "**Suspicious transaction**" means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

(i) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the PML Act, regardless of the value involved; or

(ii) appears to be made in circumstances of unusual or unjustified complexity; or

(iii) appears to not have an economic rationale or bonafide purpose; or

(iv) 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.

xxv. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:

a) opening of an account;

b) deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;

c) entering into any fiduciary relationship;

d) any payment made or received, in whole or in part, for any contractual or other legal obligation; or

e) establishing or creating a legal person or legal arrangement.

xxvi. "UCIC" means Unique Customer Identification Code, i.e., unique customer-ID allotted to individual customers while entering into new relationships as well as to the existing customers. All the accounts of an individual customer will be opened under his / her UCIC.

xxvii. "Video based Customer Identification Process (V-CIP)" means a method of customer identification by an official of the Company by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose and to ascertain the veracity of the information furnished by the customer. Such a process shall be treated as a face-to-face process for the purpose of this KYC Policy. *(Wherever applicable)*

xxviii. "Walk in Customer" means a person who does not have an account-based relationship with the Company, but undertakes transactions with the Company.

B. All other expressions unless defined herein shall have the same meaning as having been assigned to them, under the RBI's Master Circular – Know Your Customer (KYC) Direction, 2016, the Reserve Bank of India Act, 1935, the Banking Regulation Act, 1949, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

6. KEY ELEMENTS

KYC & AML procedures enable the Company to know/understand its customers and their financial dealings better which in turn help manage risks prudently. The policy has the following key elements:

6A. CUSTOMER ACCEPTANCE POLICY

6A.1 The Company shall adhere to the following customer acceptance policy:

i) The Company shall not open an account in an anonymous or fictitious/ benami name.

ii) The Company shall not open an account where it is unable to apply appropriate customer due diligence (CDD) reiterated in this policy hereafter either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

iii) The Company shall not undertake a transaction or account-based relationship without following the CDD procedure. CDD procedure shall also be followed for all the joint account holders while opening a joint account.

The Company shall obtain the information/documents as specified in this policy under the heading 'customer due diligence procedures' for KYC purposes while opening an account and during the periodic updation. However, the documents specified in CDD procedure are in addition to and not in substitution of any other document which the Company may require or is required to obtained under the law for having account-based relationship with any legal person or entity including a company, partnership firm, trust, society, etc.

iv) The Company shall obtain Optional/ additional information only with the explicit consent of the customer after undertaking a transaction or establishing an account-based relationship.

v) The PAN, where obtained, shall be verified from the verification facility of issuing authority.

vi) The Company shall apply the CDD procedure at UCIC level where a UCIC (Unique Customer Identification Code) shall be allotted while entering into a new relationship with individual customers. Thus, if an existing KYC compliant customer of the Company desires to open another account or desires to avail additional loan facility, there shall be no need for a fresh CDD exercise.

vii) The Company shall permit a customer to act on behalf of another person/ entity only in accordance with the law and the circumstances in which customer is permitted to act is clearly spelt out.

viii) To ensure that identity of the customer, directly or indirectly, does not match with any individual terrorist or prohibited/unlawful organizations, whether existing within the country or internationally, or to ensure that the customer or beneficiary is not associated with or affiliated to any illegal or unlawful or terrorist organization as notified from time to time either by RBI, Government of India, State Government

or any other national or international body /organizations, the Company shall maintain a list of individuals or entities issued by RBI, United Nationals Security Council, UAPA or other regulatory & enforcement agencies. Identity of the customer to ensure non-resemblance will be verified from the said list in all the cases before acceptance.

ix) Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of Information Technology Act, 2000 (21 of 2000).

x) The Company shall not undertake further transactions like additional disbursements, issuance of cheques/ payment orders, additional Top Up loans etc. (except accepting dues, EMIs and inward funds), with the existing customers/ counter party, if proper KYC documents are not in place.

6A.2 Subject to the above norms and cautions, it will be ensured that the above norms and safeguards do not result in any kind of harassment or inconvenience to bonafide and genuine customers, especially those who are financially or socially disadvantaged, and they should not feel discouraged while dealing with the Company.

In such exceptional circumstances before rejection of service to customers on the issue of his identity, necessary approval from a level senior to the officer normally taking such decision should be obtained.

6B. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer identification means undertaking the process of Customer Due Diligence (CDD) i.e. identifying the customer and verifying his/her identity by using reliable, independent source documents, data, or information. The Company shall, therefore, obtain sufficient information necessary to establish, to its satisfaction, the identity of each new customer /beneficiary of the relationship/account, whether regular or occasional, and the purpose of the intended nature or relationship**.**

6B.1 The Company shall undertake identification of the customers in the following cases;

a) Commencement of an account-based relationship with the customer.

b) In case of any doubt about the authenticity or adequacy of the customer identification data, it has obtained.

c) While entering into the transaction:

i. of selling third party products as an agent;

ii. of selling the Company's own products and services;

iii. for a non-account based customer/ walk-in customer;

if the value of a single transaction or series of transactions that appear to be connected is more than rupees fifty thousand.

d) When it has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.

6B.2 The true identity and bona-fide of the existing customers and new potential customers opening accounts with the Company and obtaining basic background information would be of paramount importance. The Company will obtain sufficient identification data to verify

i. The identity of customer

ii. his/her address/location and

iii. his/her recent photograph.

AGRIM HFC needs to obtain information necessary to establish, the identity of new customers.

6B.3 Reliance on customer due diligence, if any, is done by the third party

The Company for the purpose of verifying the identity of customers, while entering into account-based relationship, may rely on customer due diligence done by a third party, subject to the following conditions:

a) Such third party has been duly appointed in writing by the Company for that purpose;

b) Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or the Central KYC Records Registry;

c) Copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available without delay to the Company as and when desired.

d) 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.

e) The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

6B.4 Officially Valid Document (OVD) Means:

1) The Passport,

2) The Driving License,

3) Proof of possession of Aadhaar Number,

4) The Voter identity Card issue by the Election Commission of India.
5) Job card issued by NREGA duly signed by an officer of State Government,

6) Letter issued by the UIDAI containing the details of name, address and Aadhaar No.,

7) Any other document as notified by the Central Government in consultation with regulator.

Note:

a. Where the customer submits his proof of possession of Aadhaar number as on 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 e-documents thereof 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. Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there 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.

In respect of low risk category of customers, where simplified measures are applied for verifying the identity of the clients, the following documents shall be deemed to OVD:

a) Identity Card with applicant's Photograph issued by the Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial institutions;

b) Letter issued by a Gazetted officer, with a duly attested photograph of the person.

6B.5 CUSTOMER DUE DILIGENCE

The Company shall obtain the information/documents as specified under for KYC purposes while opening an account and during the periodic updation. However, the documents specified are in addition to and not in substitution of any other document which the Company may require or is required to obtained under the law for having account based relationship with any legal person or entity including a company, partnership firm, trust, society, etc.

S.NO.	APPLICABILITY	DOCUMENT REQUIRED
1.	INDIVIDUALS INCLUDING - BENEFICIAL OWNER,	a. Recent photograph; b. Certified copy of Permanent Account Number (PAN) OR the equivalent e-document thereof;
	- AUTHORIZED SIGNATORY OR - THE POWER OF ATTORNEY HOLDER RELATED TO ANY LEGAL ENTITY	c. Certified copy of one of the OVDs as defined above to be taken for verification of the identity and the address OR the equivalent e-document thereof; and d. Other documents including in respect of the nature of the business and financial status of the client OR the equivalent e-document thereof, as may be required by the Company.
		NOTE:-
		i. If PAN is not available then Form No. 60 as defined in Income-tax Rules, 1962 may be taken; ii. Aadhaar Offline Verification- The Company, being a non-bank, may carry out offline verification of a customer if he is desirous of undergoing Aadhaar offline verification for identification purposes. However, where its customer submits his Aadhaar number, the Company will ensure such a customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under section 7 of the Aadhaar Act. Further, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identifies Data Repository, customer may give self-declaration to that effect to the company. iii. Authentication using e-KYC authentication facility provided by the UIDAI- As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI, it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the PMLA/ the Aadhaar Act/the KYC & AML Guidelines.

		iv. If the customer provides an equivalent e-document of any OVD, the Company should verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules made thereunder and take a live photo as specified under Digital KYC Process defined below.
2.	SOLE PROPRIETORSHIP FIRM	a. CDD of the individual (proprietor) shall be carried out. b. Additionally, any two of the following documents shall also be obtained as a proof of business/ activity in the Proprietary Firm: c. Registration certificate d. Certificate/ License issued by the municipal authorities under Shop and Establishment Act. e. GST and income tax returns. f. Certificate/ registration document issued by GST/ Professional Tax authorities. g. IEC (Importer Exporter Code) h. 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. i. Utility bills such as electricity, water, and landline telephone bills. **Note:** • Company is satisfied that it is not possible, may accept only one of those documents as proof of business activity. • Provided 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.
3.	PARTNERSHIP FIRM	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: (a) Registration certificate (b) Partnership deed (c) Permanent Account Number of the partnership firm (d) Documents, as specified in point 1 of this table, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf
4.	COMPANY	For opening an account of a company, certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: (a) Certificate of incorporation (b) Memorandum and Articles of Association (c) Permanent Account Number of the company (d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf

		Documents, as specified in point 1 of this table, relating to the beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf.
5.	TRUST	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: (a) Registration certificate (b) Trust deed (c) Permanent Account Number or Form No. 60 of the trust (d) Documents, as specified in point 1 of this table, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf.
6.	UNINCORPORATED BODIES OR ASSOCIATIONS	Certified copies of each of the following documents or the equivalent e-documents thereof shall be obtained: (a) Resolution of the managing body of such association or body of individuals; (b) Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals; (c) Power of attorney granted to transact on its behalf; (d) Documents, as specified in point 1 of this table, relating to the beneficial owner, the managers, officers or employees, as the case may be, holding an attorney to transact on its behalf; and (e) Such additional information as may be required by the Company, to collectively establish the legal existence of such an association or body of individuals. Explanation: i. Unregistered partnership firms/ trusts shall be included under the term 'Unincorporated associations'. ii. Term body of individuals' includes 'societies'
7.	HINDU UNDIVIDED FAMILY	Certified copies of each of the following documents shall be obtained: (a) Identification information, as mentioned under paragraph 7 in respect of the Karta and Major Coparceners, (b) Declaration of HUF and its Karta, (c) Recent Passport photographs duly self-attested by major co-parceners along with their names and addresses. (d) The Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962.
8.	JURIDICAL PERSON	Persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents or the equivalent e-documents thereof shall be obtained: (a) Document showing name of the person authorized to act on behalf of the entity;

		(b) Documents, as specified in point 1 of this table,, of the person holding an attorney to transact on its behalf; and (c) Such other documents as may be specified by the Company in writing to establish the legal existence of such an entity/ juridical person.

6B.6 Identification of Beneficial Owner

For opening an account of an entity who is not a natural, the beneficial owner(s) shall be identified and all reasonable steps in terms of sub-rule (3) of Rule 9 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 to be undertaken to verify his/ her identity keeping in view the following:

(a) Where the customer or the owner of the controlling interest is a company listed on a stock exchange or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

(b) In cases of trust/ nominee or fiduciary accounts where 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.

6C. RISK MANAGEMENT

"Risk Management" in the present context refers to money laundering, terrorist funding risk, credit, and financial risks associated with a particular customer from the Company's perspective. This risk is based on risk perceptions associated with customer profile and level of risk associated with the product & channels used by the customer.

6C.1. As per KYC policy, for acceptance and identification, customers are categorized broadly into low risk, medium risk, and high risk categories.

i) Low risk customers

For the purpose of this policy, will be individuals and entities whose identities and sources of wealth can be easily identified, have structured income and transactions in whose accounts by and large conform to the known profile. Illustrative examples of low risk customers could be:

(a) Salaried applicants with fixed salary paid by cheque/bank.
(b) People belonging to government departments,
(c) People working with government owned companies, regulators and statutory bodies etc.
(d) People belonging to lower economic strata of the society whose accounts show small balances and low turnover
(e) People working with Public Sector Units
(f) People working with reputed Public Limited companies & Multinational Companies.
(g) Self Employed professionals other then HNIs (High Net Worth Individuals).

(ii) Medium Risk customers would include:

(a) Salaried applicants with variable income/unstructured income
(b) Salaried applicants with salary paid by cash.
(c) Salaried applicants working with Private limited companies.
(d) Self Employed Non-Professional.
(e) Self Employed customers with sound business and profitable track record for a reasonable period.
(f) High Net worth Individuals with occupational track record of upto 3 years.
(g) Retired Person with Pension

(iii) High risk customers:

That are likely to pose a higher than average risk to us may be categorized high risk customers depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. The Company will examine the case in details based on the risk assessment.

Examples of high risk customers requiring higher due diligence may include:

(a) Non-resident customers,
(b) Retired Person without Pension
(c) High net worth individuals, without an occupational track record of more than 3 years.
(d) Trusts, charities, NGOs and organizations receiving donations.
(e) Companies having close family shareholding or beneficial ownership,
(f) Firms with 'sleeping partners'
(g) Politically exposed persons (PEPs) of foreign origin,
(h) Non-face to face customers
(i) Those with dubious reputation as per available public information, etc

Further, in addition to the Income Source of the Applicant as stated above, following factors will also to be taken care off to Identify Customer Risk:

a. LTV
b. Age of Applicant
c. Mortgage Type
d. Education of Applicant
e. CIBIL

The Company through its Board, will time to time review the Risk weights to be assigned to all the Factors decided, to reach at the Customer Rating, to determine level of Risk.

For customer acceptance, KYC is a pre-requisite for a risk grading. Company would involve the senior management & seek its approval to continue business relationship with the customer. However, exceptions will be made for financially and socially disadvantaged. Stricter norms will be applied to persons having dubious records or whose record is not easily verified. The Recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) standards should also be used in risk assessment.

6C.2 Money Laundering and Terrorist Financing Risk Assessment by the Company

6C.2A The money laundering and terrorist financing risk for the Company are likely to be low due to the following reasons:

a) The Company does not operate in other countries /geographies;
b) The Company does not source/originate loans from other countries/geographies, and its customer base consists of Indian nationals only;
c) The Company extends loans to identified borrowers for which rigorous KYC checks have been put in place.
d) The Company verifies the end use of the loan
e) The Company does not offer banking, liabilities and insurance products; and
f) The Company offers loans/credit facilities with defined end-use.

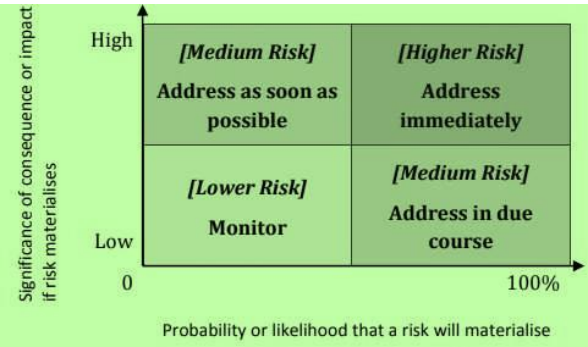
6C.2B However, in accordance with the regulatory requirements, the Company will carry out money laundering and terrorist financing exercise periodically to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk to which the Company may be exposed to. Such internal risk assessment shall be commensurate to its size, geographical presence, the complexity of activities/structure, etc.

6C.2C The exercise undertaken by the Company shall be properly documented, and the assessment process will consider various relevant risk factors and will take cognizance of overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share. Accordingly, it will frame its mitigation plan also. It should involve the relevant functions and have the following stages:

a) Identification: Development of a list of potential risk factors drawn from known/suspected threats or vulnerabilities. For this purpose, various important aspects of the KYC Policy (non-compliance of which may pose a threat to Company) will be identified along with the risks which the Company may be exposed to due to the same.

b) Analysis- Implementation of key requirements under the KYC Policy should be analyzed. This stage should analyse the likelihood and the impact of each of the identified risks. It will help in assigning priority/ importance to each of the risks.

c) Evaluation- It should involve taking the results found during the analysis process to determine priorities for addressing the risks. These priorities should contribute to the development of a strategy for their mitigation. A typical Risk Evaluation matrix would be as under:



6C.2D The Company shall conduct the money laundering and terrorist financing Risk Assessment at least once in a year or at such other intervals as may be decided by the Board.

The outcome of the ML and TF Risk Assessment will be put up to the Audit Committee.

6D.1 MONITORING OF TRANSACTIONS/ ON-GOING DUE DILIGENCE

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce its risk only if it has an understanding of the normal and reasonable activity of the customer so that it can identify transactions that fall outside the regular pattern. The Company will put in place a process to identify and review complex and unusual transactions/ patterns which have no apparent economic or visible lawful purpose, or transactions that involve large amounts of cash or are inconsistent with the normal and expected activity of the customer.

The Extent of monitoring shall be aligned with the risk category of the customer, and high risk customer will be subjected to more intensified monitoring.

Explanation: High risk accounts have to be subjected to more intensified monitoring.

A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.

6D.2 PERIODIC UPDATION

Periodic updation shall be carried out at least once in every two years for high-risk customers, once in every five years for medium risk customers and once in every eight years for low-risk customers as per the following procedure:

(a) The Company shall carry out

i. Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals except those who are categorised as 'low risk'. In the case of low-risk customers, when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

ii. In case of Legal entities, the company shall review the documents sought at the time of opening of account and obtain fresh certified copies.

(b) PAN verification from the verification facility available with the issuing authority.

(c) Authentication of Aadhaar Number already available with the Company with the explicit consent of the customer in applicable cases.

(d) In case identification information available with Aadhaar does not contain the current address, an OVD containing the current address may be obtained.

(e) The Company may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication/Offline Verification unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

(f) The Company shall ensure to provide acknowledgment with date of having performed KYC updation.

(g) The time limits prescribe the above will also be applicable to accounts where a PEP is a beneficial owner.

(h) **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 the Company or customer's mobile number registered with the RE. Company may adopt a confirmation from customers registered mobile number by providing documents using advanced methods like confirmation by sending images on Whatsapp or as a link in SMS and reply confirming Yes will be treated as Re-KYC.

(i) **Change in address:**

- **For Individual Customers:** 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 the company, customer's mobile number registered with the company, digital channels (such as online banking / internet banking, mobile application of company), 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.

- **For Company:** A fresh Process will be carried out as per the Customer Identification Process laid above for onboarding the new customer.

(j) In case there is any updated document provided by the customer for updation of the KYC details digitally, then company will update the information based on the document submitted digitally. Any such document digitally then needs to be collected from the customer within 30 days from any such document submitted by the customer, which can not be verified digitally with any of the government records.

6D.5 SIMPLIFIED NORMS FOR SELF HELP GROUPS (SHGS)

(a) CDD of all the members of SHG shall not be required while opening the account of SHG.

(b) CDD all the office bearers of SHG shall suffice.

(c) No separate CDD under paragraph 7of the members or office bearers is necessary at the time of extending credit to SHGs.

7.Video based Customer Identification Process ("V-CIP")

The Company is currently not in the practice of Video Based Customer Identification Process.

But, the company may undertake live V-CIP, to be carried out by an official of the Company, for the establishment of an account-based relationship with an individual customer, after obtaining his informed consent.

The Company, if implements V-CIP, will adhere to the following requirements:

(a) The official of the Company performing the V-CIP should record video as well as capture photographs of the customer present for identification and carry out the Offline Verification of Aadhaar for identification.

(b) It should capture a clear image of the 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 should be verified from the database of the issuing authority.

(c) The live location of the customer (Geotagging) should be captured to ensure that customer is physically present in India.

(d) The official should check that photograph of the customer in the Aadhaar/PAN details matches with the customer undertaking the V-CIP, and the identification details in Aadhaar/PAN match with the details provided by the customer.

(e) The sequence and/or type of questions during video interactions should be varied in order to establish that the interactions are real-time and not pre-recorded.

(f) In case of offline verification of Aadhaar using an XML file or Aadhaar Secure QR Code, it should be ensured that the XML file or QR code generation date is not older than 3 days from the date of carrying out V-CIP.

(g) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process.

(h) It will be ensured that the process is seamless, real-time, secured, and end-to-end encrypted audio-visual interaction with the customer, and the quality of the communication is adequate to allow identification of the customer beyond doubt. The Company will carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

(i) To ensure security, robustness, and end to end encryption, the Company will carry out software and security audit and validation of the V-CIP application before rolling it out.

(j) The audio-visual interaction should be triggered from the domain of the Company itself. The V-CIP process should be operated by officials specifically trained for this purpose. The activity log, along with the credentials of the official performing the V-CIP should be preserved.

(k) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption is not leading to the creation of multiple files, then there is no need to initiate a fresh session by the Company. However, in case of call drop / disconnection, fresh session shall be initiated.

(l) The Company should ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp.

(m) The Company will endeavor to take the assistance of the latest available technology, including Artificial Intelligence (AI) and face matching technologies, to ensure the integrity of the process as well as the information furnished by the customer.

(n) The Company should ensure to redact or blackout the Aadhaar number.

(o) Where cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the RE 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 no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

(p) 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.

8.Digital KYC Process

In case Digital KYC Process is adopted by the Company, it will ensure compliance with the following requirements:

(a) It will use an Application to 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 Company.

(b) The access to such Applications should be controlled by the authorized persons of the Company. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism defined by the Company.

(c) The customer, for the purpose of KYC, shall visit the location of the Authorized Official of the Company ("Authorized Official") vice-versa. The original OVD should be in possession of the customer.

(d) It should be ensured that the Live photograph of the customer is taken by the Authorized Official, and the same photograph is embedded in the Customer Application Form (CAF). Further, 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 timestamp (HH:MM:SS) should be put on the captured live photograph of the customer.

(e) The Application should have the feature that only a 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 photographs should be of white colour, and no other person shall come into the frame while capturing the live photograph of the customer.

(f) 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 should be there while capturing the live photograph of the original documents.

(g) The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.

(h) Thereafter, all the entries in the CAF should 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.

(i) 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 the customer's own mobile number. Upon successful validation of the OTP, it will be treated as a customer

signature on CAF. However, if the customer does not have his/her own mobile number, then the 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 the Authorized Official should not be used for customer signature. The Company will check that the mobile number used in the customer signature shall not be the mobile number of the Authorized Official.

(j) The Authorized Official should provide a declaration about the capturing of the live photograph of the 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 official mobile number. Upon successful OTP validation, it shall be treated as the Authorized Official's signature on the declaration. The live photograph of the Authorized Official shall also be captured in this authorized officer's declaration.

(k) Subsequent to all these activities, the Application should give information about the completion of the process and submission of activation request to the activation officer of the Company, and also generate the transaction-id/reference-id number of the process. The Authorized Official shall intimate the details regarding transaction-id/reference-id number to the customer for future reference.

(l) The Authorized Official should check and verify that: (i) information available in the picture of the document is matching with the information entered by the Authorized Official 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.

(m) On Successful verification, the CAF shall be digitally signed by the Authorized Official, who will take a print of CAF, get signatures/thumb-impression of customers at an appropriate place, then scan and upload the same in the system. Original hard copy may be returned to the customer.

(n) No Originally seen and verified stamping required if any of the KYC process is completed digitally by the Authorised Official of the company

(o) **Non Face to Face Updation of KYC;s:** Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section 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 Company for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

- In case Company 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.
- 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. Company shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
- Apart from obtaining the current address proof, Company 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. Verification done by an external agency appointed by Company will be treated valid.
- Company shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
- Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP or Physical Process by Authorised Official of Company.

9. EFFECTIVE CONTROL AND TRAINING

9A. Internal Audit

The Company's Internal Audit and Compliance functions shall evaluate and ensure adherence to the KYC policies and procedures. As a general rule, the Compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Management under the supervision of Board/ Audit Committee shall ensure that the audit function is staffed adequately with skilled/ trained individuals.

Internal Auditors will specifically check and verify the application of KYC procedures at the branches/ offices 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 in quarterly meetings or with their normal reporting frequency.

9B. Training & Development

The Company shall have an ongoing employee training programs as under:-

- Individually at the time of joining of new employee and
- Of all the concerned employees atleast twice a year.

Ongoing training make sures that the staff members are adequately trained in KYC procedures & Anti-Money Laundering measures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers so that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

9C. Customer Education

The Company shall educate the customer on the objectives of the KYC programme so that customer understands and appreciates the motive and purpose of collecting such information. The Company shall made KYC guidelines available on website, displayed in branches/ office and prepare specific literature/ pamphlets, etc., which can be made available to customer upon request, to educate the customer about the objectives of the KYC programme.

9D. Introduction of New Technologies

The Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favour anonymity, and take measures, if needed, to prevent their use in money laundering activities as and when online transactions are started/ accepted by the Company.

9E. KYC for the Existing Accounts

The Company shall apply the KYC norms to the existing customers of loan accounts on the basis of materiality and risk envisaged by it for those existing loan accounts.

9F. Non-Cooperation by the customer in respect of KYC norms

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the Company shall follow-up with the existing identified customers for KYC compliance, Closure decision (if at all) will depend upon the internal assessment and its decision will be taken at a senior management (VP & above), only after issuing due notice to the customer

explaining the reasons.

9G. Applicability to branches/offices and subsidiaries outside India

The KYC guidelines shall also apply to the branches/ offices and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF recommendations, to the extent local laws permit as and when the Company opens overseas branches/ offices. When local applicable laws and regulations prohibit implementation of these guidelines, the same shall be informed to National Housing Bank and RBI.

9H. Appointment of Designated Director

1. The Board has designated the Managing Director as the Designated Director to ensure overall compliance with the obligations imposed under this Policy in the matter of KYC compliance or imposed under Chapter IV of the PML Act and the Rules.
2. The name, designation, and address of the designated director shall be communicated to the FIU-IND.
3. The Board shall not nominate the Principal Officer as the Designated Director.
4. The Designated Director, in consultation with the Principal Officer, shall be responsible for setting up the policies for implementation of the KYC program and shall issue subsidiary policies or documents for operationalizing the policy.
5. The Designated Director shall allocate responsibilities of officials/departments for ensuring compliance with the KYC Policy.

9I. Appointment of Principal Officer

1. The Company has designated, Senior Manager- Accounts & Finance as "Principal Officer" who shall located at Head/ Corporate office and will be responsible for monitoring and reporting of all transactions and sharing of information as required under the law.
2. The name, designation, and address of the Principal Officer shall be communicated to the FIU-IND and NHB.
3. The Board shall not nominate the Designated Director as the Principal Officer.
4. The Principal Officer shall assist the Designated Director for setting up various policies for implementation of the KYC Program.
5. The Principal Officer shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

9J. Appointment of Senior Management

1. Senior Management for the purpose of KYC compliance shall mean Designated Director, Principal Officer, and head of each department in the Company.
2. Senior Management shall assist the Principal Officer/Designated Director in the effective implementation of the KYC Program and submit compliance status report to them.

10. RECORD MANAGEMENT

10A Maintenance of records of transactions

(a) Record-keeping requirements- The Company shall ensure the maintenance of proper record of transactions required under PMLA as mentioned below:

(i) maintain all necessary records of transactions between the Company and the customer, both domestic and international, for at least five years from the date of the transaction;

(ii) preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of the business relationship, for at least five years after the business relationship is ended;

(iii) make available the identification records and transaction data to the competent authorities upon request;

(iv) introduce a system of maintaining a proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);

(v) all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

(vi) all series of cash transactions integrally connected to each other which have been individually valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month, and the monthly aggregate exceeds Rs.10 lakh or its equivalent in foreign currency;

(vii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions;

(viii) all suspicious transactions whether or not made in cash and by way of—

(A) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of—

- cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
- travellers cheques, or transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
- any other mode in whatsoever name it is referred to;

(B) credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;

(C) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:—

(a) payment orders, or

(b) cashiers cheques, or

(c) demand drafts, or

(d) telegraphic or wire transfers or electronic remittances or transfers, or

(e) internet transfers, or

(f) Automated Clearing House remittances, or

(g) lock box driven transfers or remittances, or

(h) remittances for credit or loading to electronic cards, or

(i) any other mode of money transfer by whatsoever name it is called;

(D) loans and advances including credit or loan substitutes, investments and contingent liability by way of—

(a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or

(b) purchase and negotiation of bills, cheques and other instruments, or

(c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or

(d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;

(E) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

(ix) records pertaining to the identification of the customer and his/her address; and

(x) should allow data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

(b) The records should contain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

(i) the nature of the transactions;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted; and

(iv) the parties to the transaction.

(c) Maintenance and Preservation of records- The Company will:

(i) maintain all necessary records of transactions between it and the customer, both domestic and international, for at least five years from the date of transaction.

(ii) Preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of the business relationship, for at least five years after the business relationship is ended.

(iii) maintain and preserve the following records for the required time period as prescribed under the PMLA, either in hard or soft format:

a) all necessary records of transactions referred above; which will permit reconstruction of

individual transactions so as to provide, if necessary, evidence for the prosecution of persons involved in criminal activity;

b) records pertaining to the identification of the customer and his address obtained while opening the account and during the course of the business relationship.

(iv) Make available the identification records and transaction data to the competent authorities upon request.

(v) Introduce a system of maintaining a proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005).

11. REPORTING REQUIREMENT TO FINANCIAL INTELLIGENCE UNIT-INDIA (FIU-IND)

11.1 In accordance with the requirements under the PMLA, the principal officer of the Company will furnish the following reports, as and when required, to the Director, Financial Intelligence Unit-India (FIU-IND):

(a) Cash Transaction Report (CTR)- If any such transactions detected, Cash Transaction Report (CTR) for each month by 15th of the succeeding month.

(b) Counterfeit Currency Report (CCR)- All such cash transactions where forged or counterfeit Indian currency notes have been used as genuine as Counterfeit Currency Report (CCR) for each month by 15th of the succeeding month.

Additionally, the Company will submit 'Statement showing the details of Counterfeit Banknotes detected' to the NHB within 7 days from the last day of the respective quarter. Even in the case of 'Nil' instance also, the statement is to be submitted to the NHB

(c) Suspicious Transactions Reporting (STR)- The Company will monitor transactions to identify potentially suspicious activity. Such triggers will be investigated, and any suspicious activity will be reported to FIU-IND. The Company will file the Suspicious Transaction Report (STR) to FIU-IND within 7 days of arriving at the conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. However, in accordance with the regulatory requirements, the Company will not put any restriction on operations in the accounts where an STR has been filed.

11.2 The Company will maintain confidentiality in investigating suspicious activities and while reporting CTR/ CCR/ STR to the FIU-IND/ higher authorities and ensure that there is no tipping off to the customer at any level.

11.3 The Company shall also endeavor to install robust software, throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

FIU-IND does not accept NIL Cash/ Suspicious Reports if no such transaction occurred during a particular period, thus no reporting is required in that case.

12. COMPLIANCE UNDER FOREIGN CONTRIBUTION (REGULATION) ACT, 1976

The Company shall ensure that the provisions of Foreign Contribution and Regulation Act, 1976, wherever applicable, are duly adhered to.

FCRA regulate the acceptance and utilization of foreign contribution or foreign hospitality received by certain

specified persons or associations such as candidates for election, journalist, Judges/Government servants, political party, etc. However, law permits certain persons or associations to accept the foreign contribution with the approval of the Central Government, as per the provisions of FCRA. In those cases, copy of approval or letter of intimation shall be taken from the customer.

13. SECRECY OBLIGATIONS AND SHARING OF INFORMATION

13.1 Officials of the Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer and requests for data/information from Government and other agencies, the Company shall first 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 mutual dealing except in following circumstances:

i. Where disclosure is under compulsion of law,
ii. Where there is a duty to the public to disclose,
iii. the interest of the Company requires disclosure, and
iv. Where the disclosure is made with the express or implied consent of the customer.

13.2 The Company shall maintain the confidentiality of information as provided in Section 45NB of the RBI Act, 1934.

13.3 The Company shall not use the information collected from the customer for the purpose of cross selling or for any other purpose without the express permission of the customer.

14. SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

The Company will capture the KYC information/ details as per KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

15. REPORTING REQUIREMENT UNDER FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA) AND COMMON REPORTING STANDARDS (CRS)

The Company, if applicable, will adhere to the provisions of Income Tax Rules 114F, 114G, and 114H. If the Company becomes a Reporting Financial Institution as defined in Income Tax Rule 114F, it will take requisite steps for complying with the reporting requirements in this regard.

16. COMPLIANCE WITH SECTION 51A OF UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967

The Company will ensure compliance with Section 51A of UAPA Act, 1987 by screening the prospective and existing account holders for UN Sanction List or any other list as per UAPA Act, 1987. In the event, any account holder resembles the name of as per the list, it will be reported to FIU-IND and Ministry of Home Affairs. Further, other requirements including the freezing of assets, shall be followed by the Company.

17. ADHERENCE TO THE KYC AND AML GUIDELINES BY THE COMPANY'S AGENTS

(a) The Company's agents or persons authorized by it, for its business, will be required to be compliant with the applicable KYC & AML Guidelines.

(b) All requisite information shall be made available to the RBI/ National Housing Bank to verify the compliance with the applicable KYC & AML Guidelines.

(c) The books of accounts of persons authorized by the Company, including agents, etc., so far as they relate to the business of the company, shall be made available for audit and inspection whenever required.

18. SELLING THIRD PARTY PRODUCTS

The Company acting as agents while selling third party products as per regulations in force from time to time shall comply with the following:

(a) the identity and address of the walk-in customer shall be verified for transactions above rupees fifty thousand as required under paragraph 4 of this Policy.

(b) transaction details of the sale of third party products and related records shall be maintained as prescribed.

(c) Anti-money Laundering (AML) software capable of capturing, generating and analyzing alerts for the purpose of filing CTR / STR in respect of transactions relating to third party products with customers including walk-in customers shall be available.

(d) transactions involving rupees fifty thousand and above shall be undertaken only by:
i. debit to customers' account or against cheques; and
ii. obtaining and verifying the PAN given by the account based as well as walk-in customers.

19. NO OUTSOURCING OF DECISION-MAKING FUNCTION

The Company shall not outsource decision-making functions of determining compliance with KYC norms.

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

(a) Company 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 January 30, 2023, by the Ministry of Finance, Government of India (Annex III of this Master Direction).

(b) In accordance with paragraph 3 of the aforementioned Order, Company shall ensure not to carry out transactions in case the particulars of the individual / entity match with the particulars in the designated list.

(c) Further, Company shall run a check, on the given parameters, at the time of establishing a relation with a customer and on a periodic basis to verify whether individuals and entities in the designated list are holding any funds, financial asset, etc., in the form of bank account, etc.

(d) In case of match in the above cases, Company shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer (CNO), designated as the authority to exercise powers under Section 12A of the WMD Act, 2005. A copy of the communication shall be sent to State Nodal Officer, where the account / transaction is held and to the RBI. Compnay shall file an STR with FIU-IND covering all transactions in the accounts, covered above, carried through or attempted.

It may be noted that in terms of Paragraph 1 of the Order, Director, FIU-India has been designated as the CNO.

(e) Company may refer to the designated list, as amended from time to time, available on the portal of FIU-India.

(f) In case there are reasons to believe beyond doubt that funds or assets held by a customer would fall under the purview of clause (a) or (b) of sub-section (2) of Section 12A of the WMD Act, 2005, REs shall prevent such individual/entity from conducting financial transactions, under intimation to the CNO by email, FAX and by post, without delay.

(g) In case an order to freeze assets under Section 12A is received by the company from the CNO, Company shall, without delay, take necessary action to comply with the Order.

(h) The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by

company along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

(i) Company 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.

(j) In addition to the above, REs shall take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and Section 12A of the WMD Act.

21. Hiring of Employees and Employee training

- Adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process shall be put in place.
- Company shall endeavour to 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. REs shall also strive to develop an environment which fosters open communication and high integrity amongst the staff.
- Quarterly employee training programme shall be put in place so that the members of staff are adequately trained in KYC/AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in KYC/AML/CFT policies of the Company, regulation and related issues shall be ensured.
- Top Officials of the company designated by CEO should attend the periodic trainings conducted by the regulator on KYC and AML policy and training program to be suitably amended based on the inputs received from such programs.

22. REVIEW OF POLICY.

1. The Policy will be reviewed annually by the Board.

2. Any amendment to the policy considered necessary for effective implementation of the KYC Program any time during the year shall be carried out by the Designated Director and shall be placed for ratification at the next meeting of the Board.

23. GENERAL

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship after assessing the account at senior management (VP & above) and above upon issuing notice to the customer explaining the reasons for account closure.

Versions history

Version	Date	Comments
V1.1	21 .10.2020	**To approve incorporated amendments in RBI's Master Direction - Know Your Customer (KYC) Direction, 2016 up to Sep 20, 2020**
V1.2	29.04.2021	**To approve incorporated amendments in RBI's Master Direction - Know Your Customer (KYC) Direction, 2016 up to April 01, 2021**
V1.3	30.03.2022	**To review and update the Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy**
V1.4	30.06.2023	**To review and update the Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy as per amended Master Directions dated May 04, 2023**