IKF Group

KYC & AML Policy and Anti-corruption and Anti-bribery Policy	
Date of Last Approval/Review	August 13, 2024
Date of Review	August 06, 2025
Prepared By	CCO & CRO
Proposed By	IKF Group
Approving Authority	Board of Directors
Version	V1 - 2025

Contents

1. Background

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. Accordingly, the Master Direction –Know Your Customer (KYC) Direction, 2016 issued by the Reserve Bank of India also applies to IKF Group.

The said Directions requires every NBFC/HFC to have a Know Your Customer (KYC) policy duly approved by its Board or by any committee of the Board to which power has been delegated. Paragraph 5 mandates the inclusion of the following four key elements in the KYC Policy, namely:

a) Customer Acceptance Policy;
b) Risk Management;
c) Customer Identification Procedures (CIP); and
d) Monitoring of Transactions.

Accordingly, in compliance with the aforesaid directions issued by the RBI, and in supersession of all its existing policies, executive orders, and instructions issued from time to time in this regard, the following KYC Policy has been approved by the Board of Directors of the Company.

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 (copy annexed as Annexure I) 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).

1.1. 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 frombeing 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.

1.2. 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 IKF Group" (applicable for both IKF Finance and IKF Home Finance).

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.

2. Definitions

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 than10 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 10 percent ~~10~~ percent of capital or profits of the partnership.

c) Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together or through one or more juridicalperson, 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.

d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10 percent 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 CommercialBanks 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-residentcustomer 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 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.

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 signedby 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 numberas 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 forensuring 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. "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.

xxiv. "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.

xxv. "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.

xxvi. "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)*

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

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.

3. Customer Acceptance Policy

a) 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 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.

iii) The Company shall not open an account where it is unable to apply appropriate customer due diligence (CDD) measures as specified in Chapter VI of the Know Your Customer Directions, 2016 and reiterated in this policy hereafter either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer.

iv) 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.

v) 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.

vi) 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.

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

viii) A Unique Customer Identification Code (UCIC) shall be allotted while entering a new relationship with individual customers.

ix) The Company shall apply the CDD procedure at the UCIC level. Thus, if an existing KYC compliant customer of the Company desiresto open another account or desires to avail additional loan facility,

x) There shall be no need for a fresh CDD exercise.

xi) The Company shall permit a customer to act on behalf of another person/ entity only in accordance with the law.

xii) 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.

b) 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.

4. Customer Identification Procedure (CIP)

Customer identification means 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.

However, the Company shall not seek an introduction while opening accounts.

a) 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 been 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 thatappear 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 thethreshold of Rs. 50,000/-

b) Reliance on customer due diligence is done by the third party

The Company for the purpose of verifying the identity of customers,while entering 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.

5. 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.

5.1 For Risk Management, the Company shall have a risk-based approach.

a) The Company shall categorize its customers based on the risk perceivedby the Company.
b) The Company shall categorize its customers into low, medium, and high-risk category, based on the assessment, profiling, and money laundering risk.
c) The parameters such as customer's identity, social/ financial status, nature of the business activity, and information about the clients' business and their location, etc. shall be considered for the risk assessment.
d) The ability to confirm identity documents through online or other services offered by issuing authorities shall also be factored in determining the riskcategory of the customer.
e) It is to be mentioned here that various other information collected about different categories of customers relating to the perceived risk, is non-intrusive and in accordance with this Policy.

5.2 However, the Company may use FATF Public Statement, the reportsand guidance notes issued by Government, RBI, or other authorities on KYC/AML procedures in risk assessment.

5.3 The following indicative parameters are to be used to determine the profile and risk category of customers:

a) Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd., etc.
b) Business Segment: Retail, Corporate etc.
c) Country of residence/ Nationality: Whether India or any overseaslocation/ Indian or foreign national.
d) Economic Profile: Asset size, Business Diversity, Risk bearing capacity, etc.
e) Account Vintage/ seasoning: Less than six months old etc.
f) Presence in regulatory negative/ PEP/ Defaulters/ Fraudster lists.
g) Suspicious Transaction Report (STR) filed for the customer.
h) AML alerts
i) Other parameters: like a source of funds, occupation, nature of the business, mode of operation, credit rating, etc. can also be used in addition of the above parameters.

The Company shall adopt all or majority of these parameters based on the availability of data.

5.3.1. An indicative list of customers' behavior and risks-based classification as also the risk-based transactions to be monitored by the Company will be prepared and made available by the Designated Director /Principal Officer.

5.4 For effective risk management, the Company shall ensure that it has an effective KYC program. The overall KYC program will cover proper management oversight, systems and controls, segregation of duties, training, and other related matters. Responsibilities will be explicitly allocated within the Company to ensure that the Company's policies and procedures are implemented effectively.

5.5 Money Laundering and Terrorist Financing Risk Assessment by the Company

5.5.1. The money laundering and terrorist financing risk for the Company arelikely 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 nationalsonly.
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.

5.5.2. 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.

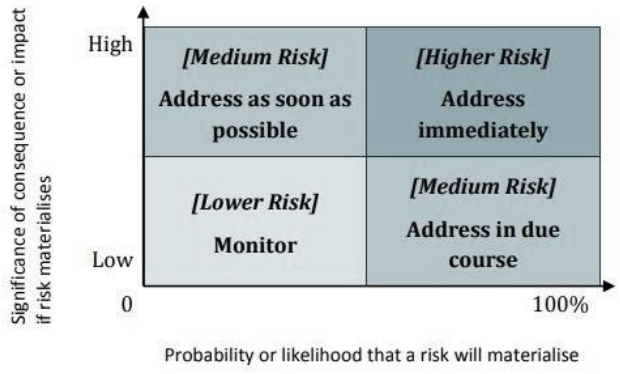
5.5.3. The exercise undertaken by the Company shall be properly documented, and the assessment process will consider various relevant risk factors and will take cognizance of overall sector-specific vulnerability, if any, that the regulator/supervisor may share. Accordingly, it will frame its mitigation 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 analyze 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:

5.5.4. 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.

5.5.5. The Company shall incorporate guidance issued by RBI, including risk indicators, and update its internal ML/TF Risk Assessment accordingly.

The outcome of the ML and TF Risk Assessment will be put up to theAudit Committee or such other Committee as may be decided by the Board.

6. 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.

7. Customer Due Diligence (CDD) Procedures

7.1. CDD procedure in case of individuals

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

(a) Recent photograph;

(b) Certified copy of Permanent Account Number (PAN) OR the equivalent e-document thereof;
(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.

  (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 provisionsof 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 (at sub-para).

  The Company may also carry-out KYC verification under Digital KYC Process defined below (at sub-para 7.1.3).

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

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

(l) 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.

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

(n) Only domain-based V-CIP systems shall be used as per RBI norms and concurrent audits shall validate compliance.

7.1.2. 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 inthe 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 photographof 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 filledin 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 ofthe 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.

7.1.3. Simplified procedure for opening accounts of Individuals

In case a person who desires to open an account is not able to produce anyof the OVDs, the Company may at its discretion open accounts subject tothe following conditions:

(a) The Company shall obtain a self-attested photograph from thecustomer.

(b) The authorized officer of the Company should certify under his signature that the person opening the account has affixed his signatureor thumb impression in his presence.

(c) The account shall remain operational initially for a period of 12 months, within which CDD, as prescribed above, should be carried out.

(d) Balances in all their accounts taken together shall not exceedRs.50,000/- at any point in time. (This is specific to SB/CA account)

(e) The total credit in all the accounts taken together shall not exceedRs.1,00,000/- in a year. (This is specific to SB/CA account)

(f) The customer shall be made aware that no further transactions will be permitted until the full KYC procedure is completed in case of Directions (d) and (e) above are breached by him.

(g) When the balance reaches Rs.40,000/- or the total credit in a yearreaches Rs.80,000/-, the customer shall be notified that appropriate documents for conducting the KYC must be submitted otherwise the operations in the account shall be stopped when the total balance in allthe accounts taken together exceeds the limits prescribed in direction (d) and (e) above. (This is specific to SB/CA account)

7.1.3. For establishing an account-based relationship, the authorized official to ascertain as to whether the customer already has a Customer ID with the Company. In case the customer has an existing Customer ID, the new account shall be opened with the same existing Customer ID.

7.1.4. KYC verification, once done by one branch or office of the Company, shall be valid for transfer of the account to any other branch or office, provided full KYC verification has already been done for the concerned account, and the same is not due for periodic updation.

7.2. Customer Due Diligence (CDD) Measures for Sole Proprietary firms

7.2.1. For opening an account in the name of a sole proprietary firm, CDD ofthe individual (proprietor) shall be carried out.

7.2.2. In addition to the above, any two of the following documents or the equivalent e-document thereof as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

(i) Registration certificate including Udhyam Registration Certificate issued by Government of India.
(ii) Certificate/ License issued by the municipal authorities under Shop and Establishment Act.
(iii) Sales and income tax returns.
(iv) CST/ VAT/ GST certificate (provisional/ final).
(v) Certificate/ registration document issued by Sales Tax/ Service Tax/Professional Tax authorities.
(vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/ License/ certificate of practice issued in the name ofthe proprietary concern by any professional body incorporated under a statute.
(vii) 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.
(viii) Utility bills such as electricity, water, and landline telephone bills.

7.2.3. In cases where the Company is satisfied that it is not possible to furnish two such documents, the Company may, at its discretion, accept only one of those documents as proof of business activity.

Provided the Company undertakes contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

7.3. CDD Measures for Legal Entities

7.3.1. Partnership Firm: For opening an account of a partnership firm, the 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 paragraph7, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

7.3.2. 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
(e) Documents, as specified in paragraph7 above, 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

7.3.3. Trust: For opening an account of a trust, certified copies of each of thefollowing 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 paragraph 7, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf

7.3.4. Unincorporated Bodies or Associations: For opening an account of an unincorporated association or a body of individuals, 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 ofindividuals;
(b) Permanent Account Number or Form No. 60 of the unincorporatedassociation or a body of individuals;
(c) Power of attorney granted to transact on its behalf;
(d) Documents, as specified in paragraph 7 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 bodyof individuals

Explanation:

i. Unregistered partnership firms/ trusts shall be included under the term 'Unincorporated associations.
ii. Term body of individuals include 'societies'

7.3.5. For opening an account of Hindu Undivided Family, certified copies of each of the following documents shall be obtained:

(a) Identification information, as mentioned under paragraph 7 in respect ofthe Karta and Major Coparceners,
(b) Declaration of HUF and its Karta,
(c) Recent Passport photographs duly self-attested by major co-parcenersalong with their names and addresses.
(d) The Permanent Account Number or the equivalent e-document thereofor Form No. 60 as defined in Income-tax Rules, 1962.

7.3.6. Juridical Person: For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents orthe equivalent e-documents thereof shall be obtained:

(a) Document showing name of the person authorized to act on behalf ofthe entity;

(b) Documents, as specified in paragraph 7 above, of the person holding an attorney to transact on its behalf; and

(c) Such other documents as may be specified by the Company in writingto establish the legal existence of such an entity/ juridical person.

7.4. 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 theyare acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

8. 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 understands 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.

9. Periodic Updation

The Company will conduct periodic updation of KYC documents at least once in every 2 years for high-risk customers, once in every 8 years for medium risk customers and once in every 10 years for low-risk customers in any of the following manner:

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

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

(iii) In case identification information available with Aadhaar does notcontain the current address, an OVD containing the current address may be obtained.

(iv) Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals except those who are categorized 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.

(v) In the case of Legal entities, the Company should review the documents sought at the time of opening of the account and obtain fresh certified copies.

(vi) The Company will not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that the 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.

(vii) The Company will provide acknowledgment with the date of havingperformed KYC updation.

(viii) The time limits prescribed above would apply from the date ofopening of the account/ last verification of KYC.

(ix) V-CIP can be used for periodic updation of KYC for existing customers

(x) Aadhaar OTP based e-KYC in non-face-to-face mode may be used for updation/ periodic updation provided the mobile number is same.

(xi) Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. REs shall ensure that the mobile number used for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.

(xii) The company shall download customers' KYC records online from CKYCR with customer's consent without requiring him/ her to submit the same records again, unless there is a change in records available with CKYCR.

(xiii) The company shall update customers' KYC information/ records based on the update notification received from CKYCR

(xiv) The company shall use Business Correspondent (BC) for Updation/ Periodic Updation of KYC.

(xv) The company shall send at least three advance notices and three reminders before and after the KYC due date.

10. Enhanced Due Diligence Procedure

10.1 Accounts of non-face-to-face customers**:** The Company will ensure the first payment is done through any of the KYC Compliant account through banking channels.

10.2 Accounts of Politically Exposed Persons (PEPs): If the Company decides to establish a business relationship with PEPs, it will ensure the following:

(a) sufficient information including information about the sources of funds of PEPs is

gathered;

(b) the identity of the person shall have been verified before accepting the PEP as a customer;

(c) the decision to open an account for a PEP is taken at a senior level in accordance with the Company's procedures;

(d) all such accounts will be classified as High Risk and will be subjectedto required due diligence and monitoring, as applicable;

(e) if it gets confirmed to the Company that an existing customer or the beneficial owner of an existing account has subsequently become a PEP, an approval from a senior official of the Company will be obtained to continue the business relationship;

(f) further, such existing accounts that get classified PEPs subsequentlywill be subjected to enhanced due diligence, as applicable.

(g) PEP onboarding requires prior approval from Senior Management and enhanced ongoing due diligence.

10.2.1 The above will also be applicable to accounts where a PEP is a beneficial owner.

11. 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) CDD of all the members of SHG may be undertaken at the time of credit linking of SHGs.

12. Record Management

(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

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

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

(b) The records should contain 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).

13. Reporting Requirement to Financial Intelligence Unit-India (Fiu-Ind)

13.1 In accordance with the requirements under the PMLA, 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 are 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 15thof the succeeding month.

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

13.2 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.

13.3 Employees shall refrain from informing the customer about the STR filing to avoid tipping-off, as per Section 12 of PMLA.

13.4 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.

14. Secrecy Obligations and Sharing of Information

14.1. 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. Where the interest of the Company requires disclosure, and
iv. Where the disclosure is made with the express or implied consent of the customer.

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

14.3. 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.

15. 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 and its subsequent updates.

16. 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.

17. Compliance with Section 51A of Unlawful Activities (Prevention) Act, 1967

The Company will ensure compliance with Section 51A of UAPA Act, 1967 by screening the prospective and existing account holders for UN Sanction List or any other list as per UAPA Act, 1967. 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. The Company shall conduct periodic rescreening of existing customers against updated sanction lists.

18. 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.

19. 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 4of 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 beundertaken only by:

i. debit to customers' account or against cheques; and
ii. obtaining and verifying the PAN given by the account based aswell as walk-in customers.

20. Potential Red Flags

Money laundering is a global problem, and many countries and organizations have enacted laws to combat it. Compliance with AML and anti-terrorism laws and regulations requires an awareness of possible 'Red Flags' or suspicious activities, which may arise in the course of conducting business. When 'Red Flags' are identified, an appropriate level of additional due diligence must be performed and additional approvals should be obtained.

Some of the indicative actions or situations when observed together or individually by any Associate should raise 'red flag' concerns (each, whether or not listed herein, a "Red Flag"):

1. Customers or suppliers who are connected to countries identified as non-cooperative by the FATF established by the G-7 Summit in 1987, and international organizations against money laundering;

2. Customers or suppliers who are reluctant to provide complete information and / or

provide insufficient, false, or suspicious information or who are unwilling to comply with the Company's norms as may be in force from time to time;

3. Customers or suppliers who appear to be acting as an agent for another company or individual, but decline or are reluctant to provide information regarding that company or individual;

4. Customers or suppliers who express concern about, or want to avoid, reporting or record-keeping requirements;

5. Payments of amounts in excess of Rs. 20,000/- (Indian Rupees Twenty Thousand) only made in cash or cash equivalents, such as money orders, traveller's cheques, internet currencies or prepaid cash cards. Acceptance of such amounts of cash or cash equivalents as a form of payment by the Company is strongly discouraged. Cash payments are commonly used by money launderers, and leave very little in the way of audit trails. Alternative methods of payment which provide a stronger audit trail should be offered. Particular care should be taken with regard to customers and suppliers who structure these payments to avoid the relevant government reporting requirements for cash and cash equivalent payments (for example by making multiple smaller payments or payments from multiple sources);

6. The purchase of products, or a larger volume purchase, appears to be inconsistent with a customer's normal ordering pattern, and in the absence of any legitimate business reason such as a special price promotion;

7. Complex deal structures or payment patterns that reflect no real business purpose or economic sense;

8. Requests for payment to be made or received through an unrelated country or to an unrelated third party;

9. Multiple partial payments from various parties on behalf of a single customer and/or multiple partial payments from various locations. Also included are "double endorsed" or "third party" cheques, where a customer endorses over to a company as payment for their invoice a cheque that was originally made out to the customer;

10. Customers or suppliers whose address is not a physical site;

11. Customers making funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose; or

12. Customers paying in one form of payment and then requesting a refund of the payment in another form e.g. paying by credit card and requesting a wire transfer or cash refund.

13. The institution will implement enhanced due diligence and ongoing monitoring to detect and prevent the use of accounts as money mule accounts.

14. Transactions through digital wallets will be monitored for suspicious activity for

enhanced due diligence and reporting as per regulatory requirements.

15. All crypto-related transactions will be subject to ongoing monitoring, and suspicious transactions will be reported in accordance with AML/CFT obligations.

21. Company Act 2013

Corporate fraud prevention policy, in adherence to the Companies Act 2013, encompasses various types of fraud and misconduct to maintain the highest ethical standards within the organization. Following outlines these types of fraud:

a) Types of Corporate Fraud

The company is committed to upholding the principles of integrity, transparency, and compliance with all relevant laws and regulations, including the Companies Act 2013. To this end, the following types of corporate fraud and misconduct are strictly prohibited:

i. Bribery and Corruption: Engaging in or facilitating bribery, kickbacks, or other corrupt practices to gain an unfair advantage or influence business decisions.

ii. Theft of Funds: Unauthorized appropriation or embezzlement of company funds or assets for personal gain.

iii. Skimming (Without Recording Transactions): Deliberate failure to record financial transactions to conceal funds or assets misappropriation.

iv. Financial Statements Fraud: Manipulating financial records, including income statements, balance sheets, and cash flow statements, to misrepresent the company's financial health or performance.

v. Tax Frauds: Engaging in tax evasion or fraudulent tax practices, including misreporting income, inflating expenses, or claiming false deductions.

vi. Money Laundering: Concealing the origins of illicitly obtained funds by engaging in transactions designed to make them appear legitimate.

vii. Regulatory Non-Compliance: Violating laws, regulations, or industry standards applicable to the company's operations, including but not limited to securities laws, environmental regulations, and consumer protection laws.

viii. Forgery and Falsification: Creating or altering documents, signatures, or records with the intent to deceive or commit fraud.

ix. Conflict of Interest: Failing to disclose conflicts of interest that may compromise the impartiality and objectivity of business decisions.

x. Insider Trading: Unauthorized buying or selling of company securities based on non-public, material information.

b) Reporting and Consequences

Employees, contractors, and stakeholders are encouraged to promptly report any suspected instances of corporate fraud or misconduct through established reporting channels. Whistleblowers will be protected from retaliation, and all reports will be treated with confidentiality and investigated thoroughly. Violations of this policy may result in disciplinary action, which can include termination of employment, civil or criminal legal action, or other remedies as deemed necessary by the company or authorities.

c) Prevention and Compliance

The company is dedicated to preventing corporate fraud through robust internal controls, regular audits, compliance training, and ongoing monitoring of business activities. Employees are expected to adhere to this policy, relevant laws, and ethical standards to ensure the organization's integrity and reputation are upheld.

22. Quoting of PAN

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of Income Tax Rule 114B as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

23. Customer Education

Seeking of certain KYC information from customers can sometimes lead to queries from the customer as to the motive and purpose of collecting such information. In this regard, the Company will take appropriate steps to educate customers on the objectives of the KYC measures.

24. Hiring Of Employees And Employee Training

(a) Adequate screening mechanism as an integral part of their personnel recruitment/hiring process shall be put in place.

(b) On-going employee training programme shall be put in place so that the members of staff are adequately trained in the KYC Policy. The focus of the training will be different for frontline staff, compliance staff, and staff dealing with new customers.

25. Designated Director, Principal Officer, and Senior Management, internal audit.

a) Designated Director

1. The Board shall designate either the Managing Director or any whole-time 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.

b) Principal Officer

1. The Board shall nominate an officer, not below the rank of Chief Manager as Principal Officer of the company.
2. The name, designation, and address of the Principal Officer shall be communicated to the FIU-IND.
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.

c) 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.

d) Internal Audit

1. Quarterly audit notes and compliance status shall be submitted to the Audit Committee.
2. The audit findings and compliance thereof will be put up before the Audit Committee of the Board till the closure of findings.

26. 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.

27. Use of Technology

The Company shall endeavor to use the latest available technology fordetermining and ensuring compliance with KYC norms.

28. No Outsourcing of Decision-making function

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

Anti-Corruption and Anti-Bribery Policy of IKF Group

1. Objective

It is the policy of the Company to conduct all of its business activities with honesty, integrity, and the highest possible ethical standards and vigorously enforce its business practice of not engaging in bribery or corruption.

2. Scope

This anti-bribery and anti-corruption policy (this "Policy") applies to all individuals of the IKF Group (both IKF Finance and IKF Home Finance) at all levels and grades, including directors, senior executives, officers, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, casual workers, volunteers, interns, agents, or any other person associated with the Company.

3. Policy Details

A "bribe" is defined as anything of value and includes, but is not limited to: cash, cash equivalents, gifts, inside information, sexual or other favors, corporate hospitality or entertainment, offering employment to a relative, payment or reimbursement of travel expenses, charitable donation or social contribution, political contributions, abuse of function and can pass directly or through a third party.

Corruption includes wrongdoing on the part of an authority or those in power through means that are illegitimate, immoral, or incompatible with ethical standards. Corruption often results from patronage and is associated with bribery.

Employees or members of their immediate families (spouse, mother, father, son, daughter, brother, sister or any of these step- or in-law relationships, whether established by blood or marriage including common law marriage) should not provide, solicit or accept any bribe to or from competitors, vendors, suppliers, customers, or others that do business or are trying to do business with IKF. All relationships with those with whom the Company deals should be cordial, but must be on an arm's length basis. Nothing should be accepted, nor should the employee have any outside involvement, that could impair, or give the appearance of impairing, an employee's ability to perform his/her duties or to exercise business judgments in a fair and unbiased manner.

4. Gifts & Hospitality

Providing gift or hospitality is acceptable provided with the intention to improve the image of the Company, better present its products and services, or establish cordial relations.

Corporate gifts, hospitality & entertainment

i. No Designated Person should accept or solicit any personal benefit including Anything of Value from anyone, unless specifically permitted under the ABAC Policy.

ii. Some core guidelines to be considered for giving Anything of Value:

- it should be reasonable, infrequent, of nominal value, appropriate and should not be given with the intent of obtaining Improper Advantage or expectation of any Quid pro quo,
- it should not be given if it could be tantamount to Bribe,
- it should not be given in cash or cash equivalent,
- it should not exceed cumulative market value of INR 5000/- ("Threshold Limit"),
- it should also preferably include IKF GROUP's logo or official branding as approved by marketing team,
- it should be delivered to an office and not sent to a home address,
- it should be provided openly and transparently,
- it should not be given outside the ordinary course of business to current or prospective customers, their employees or agents or any person with whom IKF GROUP or its business associates have a contractual relationship or intend to enter into a business/commercial arrangement,
- it should not be offered to politicians or political parties or Government Officials under any circumstances.

iii. For receiving Anything of Value:

- it should be given in good faith,
- it should be given without the expectation of Quid pro quo,
- it should not be given in cash or cash equivalent,
- it should not exceed the Threshold Limit,
- if it exceeds the Threshold Limit, it should be reported to the Compliance Officer and returned to the donor. If the return is not feasible, it should be deposited with the Compliance Officer, who may decide appropriately, including but not limited to the option of donating it to a designated charity,
- it should not be accepted outside the ordinary course of business by current or prospective customers, their employees or agents or any person with whom IKF GROUP or its business associates have a contractual relationship or intend to enter into a business/commercial arrangement,
- it should not be accepted from politicians or political parties or Government Officials under any circumstances.

5. What is not acceptable under this Policy?

i. accept an offer of a gift of any size from any Third Party which is in negotiation with, or is submitting a proposal with us;

ii. give, promise to give, or offer, any payment, gift, hospitality or advantage with the expectation or hope that a business advantage will be given or received or to reward a business advantage already given;

iii. give, promise to give, or offer, any payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure;

iv. accept or solicit any payment, advantage, gift or hospitality from a Third Party that you know or suspect is being offered with the expectation that it will obtain a business advantage for them;

v. threaten, or retaliate against, another employee who has refused to commit a bribery offence or who has raised concerns under this Policy; or

vi. engage in any activity that might lead to a breach of this Policy.

The points stated above are illustrative in nature and in no way intend to limit the applicability of this Policy.

6. Charitable Donations

As part of its corporate citizenship activities, the Company may support local charities or provide sponsorship only to make charitable donations that are legal and ethical under the laws and practices and within the corporate governance framework of the organization.

i. Charitable donations include donations of money or in-kind donations of goods or services by IKF GROUP, such as to schools or community organizations. At a minimum, all charitable contributions must be:

- Permitted under all applicable laws; and
- Properly documented.
- Employee or Company donations can be made to a legitimate, bonafide organization for causes such as education, health & sanitation, environment etc.
- CSR funds can be given to registered nonprofit organization with 80G certification for supporting women micro-entrepreneurs or any other cause as deemed fit by the CSR committee from time to time.
- Not exceeding the amount as approved by the finance team.

ii. A Designated Person, in their personal capacity, can make donations that are legal and allowed under applicable laws. However, it must be ensured that charitable contributions are not used as a scheme to conceal Bribes and should not interfere or in any way conflict with the official work of the Designated Person or with IKF GROUP in any manner.

7. Political Activities

We do not make contributions to political parties, political party officials or candidates for political office. Payment or use of corporate assets of any type as payment, directly or indirectly to any person, business, political organization, or public official for any unlawful or unauthorized purpose is prohibited. We should not make any political contribution on behalf of the Company and use any Company resources to assist a candidate or elected official in any campaign, or coerce or direct another employee to vote a certain way.

8. Sponsorship

Any sponsorship must be for genuine business or charitable objectives without any element of Quid pro quo. Any such sponsorship must be transparent, duly approved, properly documented, and duly reported. Sponsorships must not be given to political organizations or any political figures or public officials or their relatives. The Designated Persons, before undertaking any such sponsorship, must obtain prior written approval of the Head of Finance team and head of marketing, by providing

complete information including rationale, amount, and party of such sponsorship. The marketing team reserves the right to approve or deny sponsorship of any kind should it affect the brand negatively or not serving business priorities and/or business objectives.

9. Business Relationships

The Company expects all Third Parties doing business with the Company to approach issues of bribery and corruption in a manner that is consistent with the principles set out in this Policy. The Company requires all Third Parties to cooperate and ensure compliance with these standards, to continue the business relationship.

10. Record-keeping

Must ensure all expenses claims relating to hospitality, gifts or expenses incurred to Third Parties are submitted and specifically record the details for the expenditure in the format as provided in Schedule I. All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts will be kept "off-book" to facilitate or conceal improper payments and the same is ensured through effective monitoring and auditing mechanisms in place.

11. Protection

The Company encourage openness and will support anyone who raises genuine concerns in good faith under this Policy, even if they turn out to be mistaken. We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place or may take place in the future.

12. Reporting of non-compliance

1. Every employee has an affirmative responsibility to identify and promptly report activity that may violate this, Policy.

2. If any employee or any third party working for or on behalf of IKF GROUP may have engaged in conduct inconsistent with this Policy, please contact your supervisor and the Compliance Officers, immediately.

3. In case of reported violations under this ABAC policy, the Compliance Officers take appropriate steps in relation to investigation and conclusion of any complaints.

4. No personnel who, in good faith, reports a violation of the ABAC Policy shall suffer harassment, retaliation or adverse employment consequences and any person who retaliates against or harasses such a whistleblower, shall be faced with disciplinary action.

13. Reporting Of Concerns and Investigations

1. Every IKF Group Personnel is encouraged to raise concerns about any bribery issue or any

case of corrupt practice or any breach of this ABAC Policy or applicable ABAC law at the earliest. If they are unsure whether a particular act constitutes bribery or corruption or if they have any other queries, these should be raised with their respective reporting manager and the Compliance Officer at the following email address (xxx)

2. IKF Group Personnel may also raise concerns or queries through the 'Whistle-blower Policy'.

3. No personnel who in good faith, reports a violation of this ABAC Policy shall suffer any harassment, retaliation or adverse employment consequences.

4. For the reported concern(s) of potential or actual violation(s) of this ABAC policy, the Compliance Officer shall take appropriate steps such as:

    i. Enquiry or investigation of the reported concern for potential violation of this ABAC Policy shall be conducted by or with oversight of the Compliance Officer. The objective of such enquiry or investigation would be to determine the facts.

    ii. All investigations shall follow principles of natural justice and shall ensure that the relevant IKF Group Personnel are provided with an opportunity to make their case before the investigation team.

    iii. Experts with the right knowledge and skills may be appointed to investigate the reported concern.

    iv. The investigation process and the report should be kept confidential and shall be shared only with such persons who have a "need to know" under applicable law or Company's standard investigation process.

Corrective Action: If necessary, corrective actions shall be prescribed or suggested to appropriate managers, officers and employees for implementation.

Disciplinary Action: The Compliance Officer, after considering inputs from relevant stakeholders shall recommend appropriate disciplinary action, including but not limited to suspension and termination of service of such a defaulting Personnel. The Compliance Officer shall also recommend if the violation is potentially criminal in nature and should be notified to the relevant authorities under applicable law. In the event of criminal or regulatory proceedings, the Personnel shall co-operate with relevant authorities. Depending on the nature and scale of default the Compliance Officer may also recommend to the Board to commence civil and/or criminal proceedings against such Personnel in order to enforce remedies available to the Company under applicable laws.

14. Training

1. IKF Group provides appropriate training to its employees on prevalent anti- bribery & anti-corruption laws, their role and importance; to be in conformance with legal requirements and be in compliance thereof.

2. Training on this Policy shall form part of the induction process for new employees at all levels working in those areas that are seen as susceptible to ABAC risk. All existing

employees in such areas, at all levels, shall receive regular, relevant training on how to implement and adhere to this Policy. Such training will be conducted either online or in-person or a combination of both and will be administered by HR.

3. IKF GROUP may also extend training programs to third parties, if it is envisaged that the work profile allocated to them carries a significant risk as per this ABAC Policy. IKF GROUP's zero-tolerance approach to bribery and corruption shall be communicated to all agents, suppliers, contractors, and business partners at the commencement of the business relationship with them and thereafter, as appropriate, by the Compliance Officers.

15. Waiver and amendment of the Policy

The Company is committed to continuously reviewing and updating the policy and procedures based on the learning. The HR Team will monitor the effectiveness and review the implementation of this Policy, regularly considering its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible. Therefore, this document is subject to modification from time to time. Any amendment or waiver of any provision of this Policy must be approved in writing by the Company's Board of Directors. The Policy will be reviewed and audited from time to time which requires cooperation from all concerned.

Schedule I: Declaration for Corporate gifts, Business Entertainment and Hospitality

I understand that if I have been offered any gift, entertainment, or hospitality or if I am offering any entertainment or hospitality by/to a business partner/customer or any other entity doing or seeking to do business with IKF GROUP, it is my obligation to make this declaration.

1.	Whether the gift/entertainment/hospitality is being	□ Offered □ Received
2.	Description of gift/entertainment/hospitality	
3.	Date on which the gift was/is planned to be given/received	
4.	Name of the person and organization to whom the gift/hospitality/entertainment is given/received	
5.	Business relations (or potential relationship) of the person/organization with IKF GROUP	
6.	Purpose for which the gift/hospitality was given/received	
7.	I further declare that to the best of my knowledge these gifts or services have a value of approx.	[insert amount in figures, words and mention the currency of payment]
8.	Additional details of the Gift, Entertainment or Hospitality services are as follows	

The above details include the business justification for the gift/hospitality, the current location of the gift (in case of gifts received) and any other information IKF GROUP may require to make an assessment.
I have attached with this declaration any supporting documentation for:

1. The value of the gift/hospitality.
2. The purpose for which the gift or hospitality is exchanged
3. Business justification of the gift or hospitality services
4. Any other relevant documentation that IKF GROUP may require to make an assessment on this matter

I acknowledge that the information provided by me is true to the best of my knowledge.
Name: _____
Employee ID: _____
Department: _____
Designation: _____
Signature: _____

Place: _____ Date: _____

Suspicious Transaction Report (STR)

1. Purpose

The purpose of this policy is to ensure that IKF Finance Limited adheres to the guidelines for the filing of Suspicious Transaction Reports (STR) and the review of customer risk categorization as part of its commitment to KYC (Know Your Customer) and AML (Anti-Money Laundering) compliance.

2. Scope

This policy applies to all employees, officers, and directors of IKF Finance Limited. It specifically addresses the procedures for filing STRs and reviewing and updating the risk categorization of customers.

3. Policy Statement

IKF Finance Limited is committed to complying with all relevant KYC/AML regulations. The company will take all necessary steps to ensure that it:

- Files Suspicious Transaction Reports (STRs) as required.
- Regularly reviews and updates the risk categorization of its customers.

4. Responsibilities

- Audit Committee of the Board: The Audit Committee is responsible for overseeing the company's compliance with KYC/AML guidelines, ensuring that the adherence to these guidelines is regularly reviewed and documented in the meeting minutes.
- Risk Team: The Risk Team is responsible for drafting and preparing the compliance note regarding STR filing and risk categorization review and presenting it to the Audit Committee.
- Compliance Officer: The Compliance Officer is responsible for the implementation and enforcement of this policy, ensuring that STRs are filed promptly and the risk categorization of customers is reviewed regularly.
- Employees: All employees are required to report any suspicious activities to the Compliance Officer and assist in the risk categorization process as needed.

5. Procedures

5.1. Filing of Suspicious Transaction Reports (STRs)

- Monitor transactions for suspicious activities.
- File STRs with the relevant authorities as per regulatory requirements.
- Maintain records of all filed STRs for audit and review purposes.

5.2. Review of Risk Categorization

- Assign initial risk categories to customers based on their profiles and transaction behaviors.
- Conduct regular reviews of customer risk categorization to reflect any changes in profiles or activities.
- Document the process and findings of risk categorization reviews.

6. Review and Audit

- The Risk Team will prepare and present a draft note on STR filing and risk categorization review for the upcoming Audit Committee meeting.
- The Audit Committee will review the adherence to this policy at least quarterly.
- An annual audit of the STR filing and risk categorization processes will be conducted to ensure ongoing compliance and identify areas for improvement.

7. Training and Awareness

- Conduct regular training sessions for employees on KYC/AML compliance requirements, specifically focusing on STR filing and risk categorization.
- Ensure that all employees understand their roles and responsibilities under this policy.

8. Penalties for Non-Compliance

- Any employee found to be non-compliant with this policy may be subject to disciplinary action, including termination of employment.

- The company may also face regulatory penalties for non-compliance with KYC/AML guidelines.

****