GROUP-WIDE POLICY ON KNOW YOUR CUSTOMER NORMS & ANTI-MONEY LAUNDERING MEASURES

(Group-Wide KYC & AML Policy)

V 15

Index

Sr. No.	Topic	Page No.
1	Introduction	7
2	Recommendation of Financial Action Task Force (FATF)	8
3	Role of FIU-IND	8
4	Objectives of the Policy	8
5	Applicability, Scope & Responsibility	9
6	Definition	10
7	Customer Due Diligence (CDD)	13
8	Enhance Due Diligence (CDD)	13
9	Beneficial Owner (BO) identification process	14
10	Customer Acceptance Policy (CAP)	15
11	Customer Identification Procedure (CIP)	16
12	Periodic-KYC Updation	18
13	Risk Management (RM)	19
14	Money Laundering (ML) & Terrorist Financing (TF) Risk Assessment	20
15	Periodic Review of Risk-Categorization	20
16	Monitoring of Transactions	21
17	Appointment of the Designated Director and the Principal Officer	21
18	Anti-Money Laundering (AML)	22
19	C-KYC & sharing KYC information with Central KYC Records Registry (CKYCR)	23
20	Reporting to Financial Intelligence Unit -India (FIU-India)	24
21	Combating Financing of Terrorism (CFT)	25
22	Reporting requirement under FATCA & CRS	26
23	Records Retention and Retrieval	26
24	Sharing of Information relating to suspicious transactions and others	27
25	Customer Education	27
26	Introduction of New Technology	28
27	Ownership & Authority	28
28	Review of Policy	28
29	Annexures	29

1.Introduction

IndoStar Capital Finance Limited (ICFL) is a non-banking finance company ("NBFC") registered with the Reserve Bank of India as a NBFC-ML primarily engaged in providing financing solutions to borrowers across categories.

The Company currently has two wholly owned subsidiaries: IndoStar Home Finance Private Limited ("IHFPL") which provides affordable housing finance and IndoStar Asset Advisory Private Limited ("IAAPL") which acts as an investment manager.

The Company operates mainly in four principal lines of business, namely retail financing, SME lending, corporate lending, M-Laps by the Company and housing finance by its subsidiary (IHFPL).

The Company along with Subsidiary Companies are the reporting entities under the Prevention of Money Laundering Act, 2002 & Rules 2005, RBI -Master Directions on Know Your Customers (KYC) Directions-2016 (as amended from time to time) and would be required to adhere to the guidelines that issued thereunder, from time to time to share information, maintain records, conduct enhanced due diligence etc. Such companies have been named in the title to this Group-wide KYC & AML Policy and as such would be required to adhere to the standards as set out in the Policy.

The Reserve Bank of India (RBI) has vide Know Your Customer (KYC) Direction, 2016 ("RBI Directions"), issued comprehensive guidelines with regard to Know Your Customer ("KYC") norms to be followed by Non-Banking Financial Companies ("NBFCs") and measures to be taken in regard to Anti Money Laundering ("AML") and Countering Financing of Terrorism ("CFT").

Accordingly, NBFCs are required to put in place a comprehensive policy framework on 'KYC norms and AML measures', duly approved by their Board of Directors. This policy document has been prepared in line with the RBI Directions, the Prevention of Money-Laundering Act, 2002 ("PMLA") and Rules made thereunder, and incorporates IndoStar Capital Finance Limited's ("IndoStar" or the "Company") approach towards matters related to KYC, AML and CFT issues.

The Board of Directors of IndoStar have adopted this policy on KYC norms & AML measures ("Policy") in accordance with the various directions, guidelines, circulars and notifications issued by the RBI, under the PMLA and Rules made thereunder, and it is to be read in conjunction with and shall stand auto-corrected with related operational guidelines issued or any changes/modifications which may be advised from time to time by the RBI and/or other regulators. Terms not defined in this Policy shall, unless contrary to the meaning thereof, have the meaning as assigned to them in the RBI Directions, PMLA and Rules made thereunder, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Aadhaar and Other Laws (Amendment) Act, 2019 and regulations made thereunder.

In terms of PMLA and Rules framed thereunder and the RBI Direction, every regulated entity, which is part of a group, shall implement group-wide programs against money laundering and terror financing, including group-wide policies for sharing information required for the purposes of client due diligence and money laundering and terror finance risk management. Accordingly, the Company shall permit sharing of information required for the purposes of client due diligence and money laundering and terror finance risk management amongst the IndoStar Group, and for including adequate safeguards on the confidentiality and use of information exchanged within the group, to the extent applicable, including safeguards to prevent tipping-off.

2.Recommendation of Financial Action Task Fork (FATF)

The Financial Action Task Force (FATF) is an inter-governmental body which sets standards, and develops and promotes policies to combat money laundering (ML) and terrorist financial (TF).

As per FATF Statement (Recommendation No. 18) which deals with Internal Controls and foreign branches and subsidiaries which states that all programs relating to anti-money laundering shall be made application to all branches and majority owned subsidiaries and measures relating to development of policies, internal training program & independent audit function to test the system shall commensurate with the size and nature of the business of such entities. Recommendation No 18 also provides for Implementing programs for policies and procedures to share information within the group for effective enforcement of Anti Money Laundering (AML) / Countering Finance of Terrorism (CFT) purpose.

3.Role of FIU-INDIA

Financial Intelligence unit – India (FIU-IND) was set by the government of India vide Office Memorandum dated 18th November 2004 as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

The main function of FIU-IND is to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities.

4. OBJECTIVES OF POLICY

The RBI Master Directions and PML Act & Rules aim at preventing NBFCs from being used, intentionally or unintentionally, by criminal elements as a channel for money laundering and terrorist financing, including committing financial frauds, transferring or deposits of funds derived from criminal activity**.**

The RBI Directions, the PLMA and Rules made thereunder also mandate making reasonable efforts to determine the true identity and beneficial ownership of Customers, source of funds, the nature of Customer's business, etc. which in turn helps the Company to manage its risks prudently.

The standards set out in this Group-wide KYC & AML Policy are minimum requirements based on applicable legal and regulatory requirements and applies to all the companies forming part of IndoStar Group. These standards are formulated to enable the IndoStar Group companies to formulate and adopt policies and processes to prevent their businesses from being misused for Money Laundering (ML) and Terrorist Financing (TF), in terms of the Prevention of Money Laundering Act, 2002, Rules 2005 framed there under and the guidelines issued by their respective regulators.

The basic standards to be adopted by IndoStar Group companies, relating to customer identification, acceptance, monitoring and reporting of transactions, sharing information with each other under the KYC norms & AML guidelines, are detailed as under.

- All the members involved in 'Group' (including ICFL and all its subsidiaries) shall obey with instructions/procedures laid in this document.
- All the subsidiaries shall lay down the 'policies and procedures' at their entity level for sharing information, conduct enhance due diligence and maintaining records within the group for AML/CFT purposes.
- Ensuring that only legitimate and bona-fide customers are accepted.
- Verifying the identity of customers (including beneficial owners, directors, related parties and etc.) using reliable and independent documentation.
- Establishing systems and processes to facilitate creation of brief profile of customers so as to understand their personal and financial background and assess their risk profile from a ML or TF perspective:
- Monitoring and reviewing customer accounts and transactions to prevent or detect transactions that may be suspicious from a ML and TF perspective;
- Implementing processes to facilitate de-duping data of persons who have been reported for alleged offences relating to money laundering or those as set out in Schedule to the PMLA, 2002 & Rules 2005 so as to effectively manage any risks that may be posed by customers attempting to misuse the financial services provided by ICFL Group Companies.
- Ensure that information relating to persons involved in money laundering or terrorism financing as reported in the press and/ or notified by UNSC, UPA, MHA and/or notified by any statutory/ regulatory authority, are shared, to enable group companies to monitor such customers with their own database.
- To formulate strategies for training and developing material for training and dissemination of information for effective administration, enforcement and compliance with KYC norms.
- To recommend steps to safeguard the interest of IndoStar Group companies, from any potential risks associated with ML and TF, from a regulatory/ reputation perspective.

5. APPLICABILITY, SCOPE AND RESPONSIBILITY

This Group-wide KYC & AML policy applies to all new and existing customer relationships and to all products and services offered by the IndoStar Group Companies. Whilst each group company is required to formulate and adopt a KYC & AML Policy in accordance with the guidelines issued by its regulator, they are required to ensure that the standards set out herein with regard to policy formulation, processes and controls, customer identification, customer acceptance, monitoring and reviewing transactions, risk profiling, reporting of cash/ suspicious transactions, staff training / recruitment and storage of documents etc., are adhered to and accounted for. The Group Company being a Non-Banking Financial Company-Middle Layer engaged in the lending business, some of the provisions as specified in the RBI Directions, PMLA and rules made thereunder may not be strictly applicable to the IndoStar Group.

The Management Committee of the Company shall ensure compliance with this Policy, the RBI Directions, PMLA and rules made thereunder, with the assistance of the Designated Director and the Principal Officer.

The Management Committee or the Company's Internal Audit Team shall play an important role in evaluating and ensuring adherence to the Policy and procedures. Internal Audit Team shall conduct audits to specifically check and verify the application and compliance of the Policy, the RBI Directions, PMLA and rules made thereunder and procedures for compliance with this Policy, the RBI Directions, PMLA and rules made

thereunder, including at the branch level and any lapse or short coming observed shall be brought to the notice of the Management Committee / Audit Committee. The Company's Internal Audit Team shall also provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements.

The Management Committee shall submit quarterly notes and compliance with respect to this Policy, to the Audit Committee of the Board.

The Group shall maintain secrecy regarding the Customer information which arises out of the contractual relationship between the Company and the respective Customer in accordance with the RBI Direction.

6. DEFINITION

6.1 Customer:

Customer means a person or entity 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.

6.2 Common Reporting Standards (CRS):

CRS means reporting standards set for implementation of multilateral agreement signed to automatically exchange information based on Article 6 of the Convention on Mutual Administrative Assistance in Tax Matters.

6.3 Beneficial Owner:

Beneficial Owner is a natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means and a person having ownership of more than 10% of the capital, control, shares or profits in the entity.

6.4 Central KYC Records Registry (CKYCR) means an entity defined under Rule 2(1) of the PML Rules 2005, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

6. 5 Customer Due Diligence (CDD):

Customer Due Diligence is a process to collect documents & information in order to identify and verify information about a customer and ongoing risk assessment and management to assist the Company to fulfil their legal and regulatory requirements and protect themselves from financial crime. It's generally shall perform based on the below steps;

6.6 On-going Due Diligence means regular monitoring of transactions in accounts to ensure that those are consistent with the Group's knowledge about the customers, customers' business and risk profile, the source of funds / wealth.

6.7 Designated Director:

Designated Director means a person designated by the Company to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include;

The Managing Director or a whole-time Director, approved by Board of Directors, of the Company

6.8 Deemed OVD

In case 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:

1) Utility Bill likes (Electricity, Telephone, Post-paid Mobile Bill, Piped gas, Water Bill) not more than 2 months old;
2) Property or Municipal Tax Receipt;
3) Pension or family Pension Payment Orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
4) Letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;

In case, customer furnishes the any one of the above deemed OVD as address proof, the customer needs to submit OVD for address proof **within the period of 3 months** and update in the system & record.
If customer/borrower temporarily shifts or relocates to any other location or city, the customer shall provide a valid '**Rent Agreement'** as correspondence/communication address and the declared address shall be verified by positive confirmation, i.e., by means such as field verification, address verification letter, contact point verification, deliverables, etc. The same has to be supported with the OVD of permanent address proof.

6.9 Digital Signature shall have the same meaning as assigned to it in clause (p) of sub-section (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).

6.10 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.

6.11 Internal Audit Team: means the audit team headed by Head – Internal Audit and the other employees of the Company reporting to Head – Internal Audit.

6.12 IndoStar Group: shall include the Company (i.e., a parent entity) and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes:

1) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or
2) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.

6.13 Officially Valid Document (OVD) means;

1) Passport,
2) Driving Licence,
3) Aadhaar Card or proof of possession of Aadhaar number,
4) Voter's Identity Card issued be Election Commission
5) NREGA issued Job Card duly signed by an officer of the State Government and
6) Letter issued by the National Population Register containing details of name and address.

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

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

6.16 Principal Officer: means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

6.17 Senior Management shall constitute Executive Vice Chairman, Chief Executive Officer, Chief Financial Officer and Chief Risk Officer.

6.18 Suspicious transaction: means a "transaction" as defined below, including an attempted transaction, whether or not made in cash, which, to a person acting in good faith:

1) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
2) appears to be made in circumstances of unusual or unjustified complexity; or
3) appears to not have economic rationale or bona-fide purpose; or
4) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

6.19 Transaction: means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes;

1) Opening of an account;
2) 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;
3) The use of a safety deposit box or any other form of safe deposit;
4) Entering into any fiduciary relationship;
5) Any payment made or received, in whole or in part, for any contractual or other legal obligation; or
6) Establishing or creating a legal person or legal arrangement.

7. Customer Due Diligence (CDD)

A. Customer Due Diligence

Every Group Company shall conduct Customer Due Diligence (CDD) at the time of onboarding customer and periodic KYC review by obtaining below mentioned documents and perform below mentioned checks;

a) The documents required for identification and verification of the Customers, an indicative list of which is set out in Annexure I below
b) CIBIL verification
c) Internal dedupe
d) Understand and verify the profile of the customer/business activity
e) Obtain customer's Beneficial Ownership structure in all non-individual cases and identify the Ultimate Beneficial Owner (UBO).

Note: Where (i) an individual customer; or (ii) proprietor of a sole proprietorship firm; or (iii) a Beneficial Owner, managers, officers or employees holding an attorney to transact on behalf of the partnership firm or the trust or an unincorporated association/ body of individuals or a company; or (iv) a person holding an attorney to transact on behalf of the juridical persons not specifically covered, submits proof of possession of Aadhaar Number containing his Aadhaar Number, it shall be ensured such person redacts or blacks-out his Aadhaar Number through appropriate means or it shall be ensured that a copy of masked Aadhaar card of such person is obtained.

B. Provided that where the customer has submitted,

- Aadhaar number, the Group shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.
- Further, in such a case, if customer wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a self-declaration to that effect to the IndoStar.
- Proof of possession of Aadhaar under above para where offline verification cannot be carried out, the IndoStar shall carry out offline verification.
- An equivalent e-document of any OVD, the IndoStar shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as per digital KYC process.

8. Enhanced Due Diligence (EDD)

Every Group Company shall conduct Enhance Due Diligence (EDD) on all its High-Risk customers and when found customer is considered to present a higher risk and required more investigation as per details given in Annexure II

The Group Companies shall collect additional information & documents from customers, screening to be performed diligently and further information to be collected from public domain or from regulatory filings, media reports, government databases, and specialized risk intelligence platforms, etc. In some high-risk jurisdictions, this information may not be digitized and available online.

Steps to be followed in Customer Enhanced Due Diligence:

- Obtaining additional identifying information.
- Reviewing Ultimate Beneficial Ownership
- Using adverse media screening.
- Conducting on-site visits (Field Verification Report).
- Satisfactory Bureau Check & Credit Rating checks (for non-individuals)
- Reviewing documentation and reporting.
- Adopting a Risk-Based Approach and etc.

9. Beneficial Owner (BO) Identification Process

Every Group Company should identify the 'Beneficial Owner (BO)' for all non-individual customers and have well-defined process in place to identify and verify the identity of BO & UBO and required KYC documents must be collected for CDD.

The necessary threshold limit should be followed while identifying ownership structure/details of the legal entity as given below;

For **Company**, the details of beneficial owners holding of **10%** ownership, control, shares, capital or profits in the company must be obtained.

Exempted: If Company's ownership structure is as given below;

(i) an entity listed on a stock exchange in India, or

(ii) an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or

(iii) a subsidiary of such listed entities;

Not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies covering in above 3 scenarios.

For **Partnership**, the details of beneficial owners holding of **10%** ownership, control, shares, capital or profits in the partnership firm must be obtained.

For **Trust**, the details of beneficial owners holding of **10%** ownership, control, management, shares, capital or profits in the trust must be obtained.
For **an unincorporated association or body of individuals**, the details of beneficial owners holding of **15%** ownership, property, control, major voting rights management, shares, capital or profits in the trust must be obtained.The Group companies shall need to obtained Beneficial Ownership Declaration from its all-non-individual customers as per format given in **Annexure – IV.**

10. Customer Acceptance Policy (CAP)

Every Group Company shall take into account the following factors whilst framing norms relating to CAP

- No transaction is initiated in anonymous or fictitious/ benami name(s).The Company shall obtain the documents and information for KYC purpose, **an indicative list of which is set out in Annexure I below**, for initiating or undertaking any transaction and for periodic updation and such documents and information shall be verified from the verification facilities of the issuing authority, wherever applicable. Further, if any additional information is required to be obtained from the Customer(s), which is not specified in this Policy, the Company shall obtain such additional information with explicit consent of such Customer(s).

- Necessary checks or suitable systems are put in place before initiating a new transaction so as to ensure that the identity of the Customer does not match with any person or entity, whose name appears in the sanctions list indicated in the RBI Directions or any person with a known criminal background or with banned entities such as individual terrorists or terrorist organizations etc. The Company shall allocate a Unique Customer Identification Code (UCIC) to each Customer and shall ensure not to issue dual UCIC to any single Customer.

- The Company shall obtain the information, details and documents of the Customer which is relevant to the business and risk category and shall not intrusive.
- The Company shall not initiate a transaction or terminate an existing transaction where the Company is unable to apply appropriate Customer Due Diligence measures i.e., the Company is unable to verify the identity and/or obtain documents required as per the risk categorisation either due to non-cooperation of the Customer or non-reliability of the documents/data/information furnished to the Company.
- The Company shall consider filing a suspicious transaction report ("STR"), if necessary, when it is unable to comply with the relevant Customer Due Diligence measures in relation to the Customer. It shall be necessary to have suitable built-in safeguards to avoid harassment of the Customer.
- Decision to terminate a transaction shall be taken by the principal nodal officer of the Company (appointed under the Reserve Bank – Integrated Ombudsman Scheme, 2021, as amended or modified or supplemented from time to time), after giving due notice to the Customer explaining the reasons for such a decision.
- For the purpose of risk categorisation of Customer, Company shall obtain the relevant information from the Customer at the time of transaction.

  The decision to open an account for / enter into transactions with - Politically Exposed Person (PEP) shall be taken at a senior level i.e., Principal Officer.

  Adoption of Customer Acceptance Policy and its implementation shall not become too restrictive and shall not result in denial of financial services to general public, especially to those, who are financially or socially disadvantaged.
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- The Company shall ensure that in case of Customers who are non-profit organizations, the details of such Customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal. The Company shall also maintain such registration records for a period of 5 (five) years after the business relationship between the Customer and the Company has ended.

11 Customer Identification Procedure (CIP)

Customer identification is carried out to verify identity of the Customer by using reliable and independent source of documents, data or information to ensure that the Customer is not a fictitious person. Company shall conduct CIP in the following cases: (i) at the time of commencement of a relationship with the Customer; (ii) when there is a doubt about the authenticity or adequacy of the Customer identification data it has obtained; (iii) selling third party products as agents, selling their own products. Every Group Company shall take into account the following factors whilst framing norms relating to CIP and implementation of it;

- The Group shall carry out customer identification and Customer Due Diligence procedure before initiating or undertaking any transaction. In case the Customer transacts in joint name, customer identification and Customer Due Diligence procedure shall be carried out for all individuals / entities involved.

- The Company shall prepare a profile for each Customer based on risk categorization and allot a unique customer identification code to such Customer. The Customer profile may contain information relating to Customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the Company. However, while preparing Customer profile, the Company shall take care to seek only such information from the Customer which is relevant to the risk category and is not intrusive.
- The Customer profile shall be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes without the express permission of the Customer. Further, if an existing KYC compliant Customer desires to initiate another transaction with the Company, the Company may fetch information from the already existing profile of the said Customer and may not conduct fresh Customer Due Diligence exercise.
- During the course of interacting with a potential Customer or at the time of customer identification and Customer Due Diligence procedure, if the Company forms a suspicion of money laundering or terrorist financing, and the Company reasonably believes that performing the Customer Due Diligence process will tip-off the Customer, it shall not pursue the Customer Due Diligence process, and instead file an STR with Financial Intelligence Unit-India ("FIU-IND").

The Company shall obtain sufficient information necessary for identification and due diligence to establish, to its satisfaction, the identity of each Customer including the identity of the Beneficial Owner and authorized signatory acting on behalf of any non-natural person, whether regular or occasional, and the purpose of the intended nature of business relationship. Besides risk perception, the nature of information/ documents required would also depend on the type of Customer (individual, corporate, etc.). The illustrative list of such information/documents to be obtained from Customer for identification and due diligence is provided at Annexure – I.

The Company shall capture / obtain the KYC information, with explicit consent from the Customer, for submitting with the Central KYC Records Registry ("CKYCR") in the prescribed KYC templates for individuals and legal entities, in prescribed format and for downloading of records from CKYCR.

The Company may, for purpose of verifying the identity of Customers, to its satisfaction, rely on Customer Due Diligence done by a third party, subject to conditions mentioned in the RBI Directions, PMLA and rules made thereunder.

The verification of the documents must be done by an authorized officer of the IndoStar Group.

All KYC documents accepted physically as part of CIP, must be self-attested [Original Seen and Verified (OSV)] by the customer and counter signed by the concerned officer of the ICFL Group Company with his employee identification on such documents.

Decision making functions of determining compliance with KYC norms shall not be outsourced.

The Group will perform appropriate, specific and where necessary, enhanced due diligence on its Customers that is reasonably designed to know and verify the true identity of its Customers and to detect and report instances of criminal activity, including money laundering or terrorist financing.

The procedures, documentation, type of information obtained and levels of KYC due diligence to be performed

will be based on the level of risk associated with the relationship (products, services, business processes, geographic locations, etc.) between the Company and the Customer and the risk profile of the Customer. Customers / Beneficial Owners who are Politically Exposed Persons shall be subjected to enhanced due diligence in accordance with conditions mentioned in the RBI Directions, PMLA and rules made thereunder.

The Company shall take all reasonable measures to ascertain and verify the true identity of all Customers who transact with the Company. Each business process may design and implement specific due diligence standards and procedures that are appropriate given the nature of the respective businesses, customers and the associated risks.

The submission of Aadhaar is mandatory only when the customer is desirous of receiving any benefit or subsidy under any scheme notified under Section 7 of the Aadhaar Act or as per the Notification, Circular, Guidelines, as issued by RBI and UIDAI from time to time, otherwise Aadhaar is not mandatory and the Company shall not to insist for the same. However, the individual, if so desires, may provide the same out of volition. The customer, at their option, shall submit one of the OVDs.

In case, customer providing other OVD as address proof instead of Aadhar Card or possession of Aadhaar (like address updated Passport Copy, Driving Licence, Voter ID and etc.) should be accepted as valid address proof and updated in the record.

Only in case customer unable to provide updated OVDs for address proof, the Group Companies should obtain deemed OVDs (not older than 2 months) as specified above in para 2.12 and follow the required procedure as mentioned therein.

The Aadhaar Number of all the customers **must be masked** appropriately as per guidelines given in Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

12. Periodic Updation

Each Group Company shall conduct Customer Identification and Customer Due Diligence documents shall be updated periodically, in order to ensure that the information or data collected under Customer Due Diligence is kept up to date and relevant, particularly where there is high risk. Such periodic updation shall be carried out at least once at following time intervals and manner:

1) Low Risk Customers: 10 years
2) Medium Risk Customers: 8 years
3) High Risk Customers: 2 years

- The time limits prescribed above would apply from the date of initiation of transaction / last KYC verification.

- The Company shall advise the Customers that in order to comply with the PMLA and the rules framed thereunder, in case of any update in the documents submitted by the Customer at the time of establishment of business relationship and thereafter, as necessary; the Customers shall submit to the Company, the update of such documents. This shall be done within 30 (thirty) days of the update to

the documents for the purpose of updating the records at Company's end.

- Save as otherwise provided in this Policy, the instructions or procedure for customer identification and Customer Due Diligence shall mutatis mutandis apply in case of Periodic Updation.
- In case of no change in KYC information but the 'Group Company' doesn't have updated information & documents or not as per the CDD standards or in case of validity of documents available with the 'Group Company' has expired at the time of periodic updation of KYC, the 'Group Company' shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.
- PAN details of the Legal Entity customers must be verified with the issuing authority at the time of periodic updation of KYC.
- The 'Group Company' shall immediately update in their system & record of information, details & documents obtained during periodic updation of KYC.
- At any situation customers are not insisted for periodic KYC updation and shall provide alternate options to submit updated KYC details like online updation, nearest branch visit and etc.

For Individual Customers:

In case no change in KYC information:

A self-declaration from the customer shall be obtained through customer's registered e-mail ID and registered mobile number.

In case of Change in Address:

A self-declaration of the new address shall be obtained from the customer through registered e-mail ID and registered mobile number available with the Company and the declared address shall be verified through positive confirmation within two months, by field verification, address verification letter, deliverables, etc.

In case the current address is different from the address in Aadhaar, shall not require positive confirmation but shall ensure that **mobile number for Aadhaar authentication is same as the registered mobile number available with the Company, in order to prevent frauds**.

For Non-Individual Customers:

In case no change in KYC information:

A self-declaration from the customer shall be obtained from Legal Entity (LE) through its registered e-mail ID and registered mobile number available with the Company, letter from an official authorized by the LE, Board Resolution copy and etc. Further, Group shall ensure during this process that Beneficial Ownership (BO) information available with them is accurate and shall update the same, if required, to keep it as up-to-date as possible.

In case of Change in KYC information:

a) The 'Group' shall undertake the entire KYC process equivalent to that applicable for on-boarding a new Legal Entity or non-individual customer.
b) Acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation/ periodic updation and an intimation, mentioning the date of updation of KYC details, is provided to the customer.

13. Risk Management

Every Group Company (IndoStar) - shall classify its Customers into various risk categories (i.e., low, medium and high risk), and based on the assessment and risk perception, decide on customer identification and Customer Due Diligence procedure to be followed. The illustrative list of such risk categorisation is provided at **Annexure** – II. In case of identification of any such risk by IndoStar Group, it shall promptly intimate the details to the board of directors of the other entities belonging to the IndoStar Group, which shall take immediate action, including by reporting the same to regulatory authorities.

Parameters of risk perception shall be clearly defined in terms of the Customer's identity, nature of business activity, information about the Customer's business and location of Customer and his clients, geographical risk covering Customers as well as transactions, type of product/services offered, delivery channels used for product/ services, mode of payments (cash, cheque/ monetary instruments, wire transfers, forex transactions etc.), volume of turnover, social and financial status, ability to confirm identity documents through online or other services offered by issuing authorities etc. to enable categorization of Customers into low, medium and high risk.

The 'Group' shall devise procedures for creating risk profiles of their existing and new customers and apply various AML measures issued under PML Act & Rules and by RBI through Master Directions – Know Your Customers (KYC) Direction-2016 (amended from time to time).Documentation requirements and other information to be collected in respect of different categories of Customers will depend on perceived risk and keeping in mind the requirements of PMLA and rules framed thereunder and guidelines issued by RBI from time to time. An illustrative list of documents and information required to be collected and checks to be performed by the Company in respect to Customers belonging to high-risk categories is set out in **Annexure III** below.

Provisions with regard to Wire transfer shall be complied with as and when applicable by the Group.

14. Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment

To ensure effective implementation of KYC guidelines. The implementation procedure covers allocation of responsibilities, proper management oversight, systems and controls, segregation of duties, training and other related matters. The Company & every Group Company shall carry out money laundering and terrorist financing risk assessment exercise periodically **(at least once in a year)** to identify, assess and take effective measures to mitigate its money laundering ("ML") and terrorist financing ("TF") risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc.

The assessment process should consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While assessing the ML/TF risk, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share from time to time.

The Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment shall be placed before Board or Audit Committee and the Board or Audit Committee shall be reviewed at least 'once in a year'. The Group shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risks and should have Board approved policies, controls and procedures in this regard. The Company shall implement the Customer Due Diligence programme, having regard to the ML/TF risks identified and the size of business. Further, the Company shall monitor the implementation of the controls and enhance them if necessary.

15. Periodic Review of Risk-Categorization

Each Group Company shall conduct periodic 'Review on Risk-Categorization', at least **'once in six months'** by considering the parameters such as customer profile, geographic location, products, services, distribution channels. administration and local jurisdiction, with specific attention to complex and unusually large transactions which have no apparent economic or visible lawful purpose.

Each Group Company shall prescribe procedures to periodically review profile of existing customers against lists of prohibited individuals and entities issued by the United Nations or any other regulatory/statutory authorities. Such due diligence must be conducted based on the risk categorization of customers, inter alia detailed as under:

- The 'Group' shall conduct review of risk-categorization by performing enhance due diligence in case of receipt of any updated document/information from customer or receipt of information about Customer from any other source or from public or by regulators, FIU-India, Law Enforcement Agency, Enforcement Department or any other legal agencies.
- Each Group Company shall ensure to upgrade and downgrade the new residual risk of their Customers based on the review of risk-categorization. Also, needs to update the number of cases where risk-rating is unchanged.
- The Group shall include other parameters while conducting Periodic Risk-Categorization like customer geographical location, nationality, products, delivery channels, transaction mode, CTR & STR Filed during the review period and etc.

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

16. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Each Group Company should undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the Customers, Customers' business and risk profile, the source of funds/ wealth. If required and viable for the Company for ongoing due diligence, the Company may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

The Group shall understand the customer profile diligently based on it they can monitor the risk involved therein. However, the extent of monitoring will depend on the risk categorisation of the Customer. However, the extent of monitoring will depend on the risk categorisation of the Customer. High-risk Customers have to be subjected to intensified monitoring in accordance with RBI Directions.

The Group Companies should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Further, in the case of high-risk customers and/ or customers undertaking unusually large transactions/ customers exhibiting unusual patterns which have no apparent economic or visible lawful purpose, any transaction proposed to be undertaken by such customer shall require the prior approval of the Management Committee for such transaction to be processed.

The Group shall put in place an appropriate system / mechanism to throw alerts when the transactions are inconsistent with risk categorization and updated profile of Customers.

The Group should ensure that a record of transactions with Customers is preserved, maintained and reported as required in terms of Section 12 of the PMLA and Para 46 of the RBI Directions. It may also be ensured that transactions of suspicious nature and/or any other type of transaction notified under the PMLA, is reported to the appropriate law enforcement authority, in the prescribed form and within the stipulated time frame.

17. Appointment of Designated Director and Principal Officer

To ensure effective implementation of this Policy, the Board of Directors shall appoint / designate Managing Director / Whole-Time Director, duly authorized by the Board of Directors of the Company, as the Designated Director who shall be responsible for ensuring overall compliance as required under this Policy, the RBI Directions, PMLA and the rules made thereunder.

The Principal Officer, who shall be an officer at the management level nominated by the Board of Directors and responsible for ensuring compliance, monitoring transactions, and sharing and reporting information and furnishing / reporting all transactions as required under the law/regulations, including PMLA and rules framed thereunder.

In no case the Principal Officer shall be appointed as the Designated Director.

The name of the Designated Director and the Principal Officer so designated and other information (including the designation, address and contact details) shall be intimated to the Director, FIU-IND and to RBI.

18. Anti-Money Laundering (AML)

Anti-Money Laundering (AML) refers to the collection of laws, law enforcement, processes, policies, and regulations that prevent illegally obtained money from entering the financial system by criminals, money launders, terrorist financing and through other illegal activities, etc.

Preamble

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified there under came into force with effect from July 1, 2005. Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act.

Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the “Offence of money laundering” as under:

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering”

Money launders use the financial system for cleansing ‘dirty money’ obtained from criminal activities with the

objective of hiding/disguising its source. The process of money laundering involves creating a series of financial transactions so as to hide the origin and true nature of these funds.

For the purpose of this document, the term 'money laundering' would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

Obligations under Prevention of Money Laundering [PML] Act 2002

Section 12 of PML Act 2002 places certain obligations on every financial institution and intermediary which include:

(i) Maintaining a record of prescribed transactions
(ii) Furnishing information of prescribed transactions to the specified Authority
(iii) Verifying and maintaining records of the identity of its clients
(iv) Preserving records in respect of (i), (ii), (iii) above for a period of 10 years from the date of cessation of transactions with the clients.

Stages of Money Laundering:

There are three stages of money laundering introducing laundered funds into the financial system:

1) **Placement.**

The placement stage marks the beginning of the money laundering process (a.k.a. the money laundering stages), where dirty money is introduced into the financial system. This stage is considered the most vulnerable for criminals, as they must find ways to deposit large amounts of cash without raising suspicion, like Depositing cash in smaller amounts to avoid detection.

2) **Layering.**

Layering is the second stage of the money laundering stages in which criminals engage in a series of transactions to create confusion and distance the funds from their criminal origin. This can involve, transferring money between multiple bank accounts, often in different locations and jurisdictions.

The objective of layering is to create a complex web of financial transactions that makes it extremely difficult for law enforcement to trace the source of the illicit funds. Criminals can further shield themselves from detection and prepare to reinfuse their laundered funds into the legitimate economy after successfully traversing the layering stage.

3) **Integration.**

Integration is the final stage of the money laundering process, in which the laundered money is reintroduced into the legitimate financial system, often through investments in real estate, luxury assets, or business ventures. At this point, the funds appear to have been acquired from legitimate sources, making it difficult for authorities to distinguish between legal and illegal assets.

19. C-KYC and sharing KYC information with Central KYC Records Registry (CKYCR)

As per amendment made on November 06th, 2024 to RBI Master Direction on Know Your Customer (KYC) Direction 2016.

The Group shall implement the CKYC process and shall collect 14 digits of CKYC number from the customer, shall upload/download and update the customer details in CKYCR portal and also adhere to the below measures. The Group shall retrieve the KYC records online from the CKYCR and download the records with explicit consent.

In terms of provision of Rule 9(1A) of the PML Rules, the Group shall capture customer's KYC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer.

The Group shall upload KYC records pertaining to accounts of LEs opened on or after April 1, 2021, with CKYCR in terms of the provisions of the Rules ibid. The KYC records have to be uploaded as per the LE Template released by CERSAI.

Once KYC Identifier is generated by CKYCR, Group shall ensure that the same is communicated to the individual/LE as the case may be.

In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Group shall upload/update the KYC data pertaining to accounts of individual customers and LEs opened prior to the above-mentioned dates as per above points, at the time of periodic updation as specified in paragraph 38 of this Master Direction, or earlier, when the updated KYC information is obtained/received from the customer. Also, whenever the Group obtains additional or updated information from any customer as per clause (j) below in this paragraph or Rule 9 (1C) of the PML Rules, the Group shall within seven days or within such period as may be notified by the Central Government, furnish the updated information to CKYCR, which shall update the KYC records of the existing customer in CKYCR.

CKYCR shall thereafter inform electronically all the reporting entities who have dealt with the concerned customer regarding updation of KYC record of the said customer. Once CKYCR informs the Group regarding an update in the KYC record of an existing customer, the Group shall retrieve the updated KYC records from CKYCR and update the KYC record maintained by the Group.

Group shall ensure that during periodic updation, the customers are migrated to the current CDD standard.

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

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

20. Reporting to Financial Intelligence Unit – India (FIU-India)

In terms of PMLA Rules, each Group Company is required to report to the FIU-IND, details of their respective customers transactions, documents, information, reporting of records, including with respect to cash transactions and suspicious transactions, counterfeit currency reports as per Rule 3 of the PML (Maintenance of Records) Rules 2005 as required in terms of the PML Act 2002 and under Chapter VIII of RBI-Master Direction of KYC Directions 2016 (amended from time to time), the rules made thereunder shall be furnished to the Director, FIU-IND, in the prescribed formats and within prescribed time frame under the PML Act 2002 and the Rules 2005 made thereunder.

Director, FIU-IND
Financial Intelligence Unit-India
6th Floor, Hotel Samrat
Chanakyapuri
New Delhi – 110 021
Website – http://fiuindia.gov.in

The Group Companies and its directors, officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the Director, FIU-IND is confidential. However, such confidentiality requirement shall not inhibit sharing of information under paragraph 4(b) of RBI Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Group shall not put any restriction on operations in the accounts merely on the basis of the STR filed.

21. Combating Financing of Terrorism (CFT)

Each Group Company shall ensure that in terms of the Unlawful Activities (Prevention) Act, 1967 and amendments thereto (UAPA), the name of the Customer does not appear in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council. The Company shall also refer to the lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time. The aforementioned lists, i.e., UNSC Sanctions Lists and lists as available in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as amended from time to time, shall be verified on daily basis and any modifications to the lists in terms of additions, deletions or other changes shall be taken into account by the Company for meticulous compliance.

Details of accounts resembling any of the individuals / entities in the lists shall be reported to the Director, FIU-IND and shall be advised to the Ministry of Home Affairs.

The Group Companies shall ensure meticulous compliance with the "Procedure for Implementation of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005" laid down in terms of Section 12A of the WMD Act, 2005 vide Order dated September 1, 2023, by the Ministry of Finance, Government of India (as set out in Annex III and paragraph 52 of the RBI Direction).

The Group Companies shall verify every day, the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities', as available at https://www.mea.gov.in/Implementation-of-UNSC-Sanctions-DPRK.htm, to take into account any modifications to the list in terms of additions, deletions or other changes and also ensure compliance with the 'Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017', as amended from time to time by the Central Government. Additionally, the Company shall also take into account – (a) other UNSCRs and (b) lists in the first schedule and the fourth schedule of UAPA, 1967 and any amendments to the same for compliance with the Government orders on implementation of Section 51A of the UAPA and section 12A of the WMD Act.

The Group Companies shall consider the Financial Action Task Force ("FATF") Statements circulated by the Reserve Bank of India from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations.

The Group Companies shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF. Special attention shall be given to business relationships and transactions with individuals (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

FIU-India Reporting Details

Cash Transaction	**Time Period Within which to be reported**	**Report Type**
Cash Transaction of the value in excess of Rs. 10 lakhs or its equivalent in foreign currency during a month.	Within the 15th day of the succeeding of the month.	Cash Transaction Report (CTR)
All series of cash Transaction integrally connected to each other which have been valued below Rs. 10 lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value exceeds Rs. 10 lakhs.	Within the 15th day of the succeeding of the month.	Cash Transaction Report (CTR)
Suspicious Transaction	**Time period within which to be reported**	**Report Type**
All suspicious transactions whether or not made in cash and by way of as mentioned in Rule 3 D of the PML Rules 2005.	Not later than 7 working days on being satisfied or identified by Principal Office that the transaction is suspicious.	Suspicious Transactions Report (STR)
Forged or Counterfeited Currency Report (CCR)	**Time period within which to be reported**	**Report**
All cash transactions where forged or Counterfeited Currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transaction.	Within the 15th day of the succeeding of the month.	Counterfeited Currency Report (CCR)

22. Reporting Requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

The Designated Director and the Principal Officer shall ensure compliance with the requirements under the FATCA and CRS.

The Company shall register itself as Reporting Financial Institution and shall submit online reports with the Income Tax Department.

23. Records Retention and Retrieval

In terms of the KYC & AML guidelines, every Group Company is required to maintain and preserve all the necessary information in respect of transactions as per Rule (3) of the PML Rules 2005 as given below:

i) the nature of the transaction,
ii) the amount of the transaction & currency in which it was denominated
iii) the date of the transaction occurred
iv) the parties involved in the transaction.

The Company (IndoStar Capital Finance Ltd) has in place a policy on record retention duly approved by the Board and as may be amended from time to time and advise to all its subsidiary to have a Board approved record and retention policy in place.

The Group Companies shall take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

24. Sharing of Information relating to suspicious transactions and others

Every IndoStar Group Company shall endeavour to **share information amongst the group companies relating to transactions, accounts, customer details that are deemed to be suspicious or barred from a ML or TF perspective** in such manner and with such safeguards as may be decided by this Committee.

Every IndoStar Group Company shall take effective steps to ensure that such information is treated in **strict confidence** and used only for the purpose of detection of transactions relating to ML and/ or TF, as contemplated under the KYC & AML guidelines. As failure to maintain secrecy of such transaction could lead to tipping of and this would be violation of KYC & AML guidelines

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

The Group Companies has an on-going employee training programme so that the members of the staff are adequately trained in KYC/AML/CFT policy. Training requirements shall have different focuses for frontline staff, compliance staff and staff dealing with new Customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently. Proper staffing of the audit function with

persons adequately trained and well-versed in KYC/AML/CFT policies of the Group, regulation and related issues shall be ensured.

The Group Companies shall put in place an adequate screening mechanism, including Know Your Employee / Staff policy, as an integral part of their personnel recruitment/hiring process.

25. Customer Education

The Group Companies shall prepare specific literature/pamphlets etc. so as to educate the Customer of the objectives of the KYC & AML programme. The Group Companies on an on-going basis educates the front desk staff, the branch staff and the new joinees on the elements of KYC & AML through various training programmes and e-mails to *inter alia* handle issues arising from lack of customer education.

26. Introduction of New Technologies

The Group Companies shall pay special attention to any Money Laundering and Terrorist Financing risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms and from new or developing technologies for both new and existing products, in the implementation of the Policy and shall ensure that appropriate KYC procedures issued from time to time are duly applied before introducing new products / services / technologies.

27. Ownership & Authority

The IndoStar Capital Finance Limited (ICFL) – parent company will hold the ownership, modification, changes in guidelines in line with FATF, PML Act & Rules and RBI guidelines issued from time to time. The IndoStar Group Companies (Parent Company and all its subsidiary) are responsible for implementation and adhere to the guidelines or compliances provided therein.

Every IndoStar Group Company shall appoint a 'Principal Office' in accordance with the applicable KYC & AML guidelines. The Principal Officer shall be responsible for monitoring, reviewing the standards as set out in this Group-Wide KYC and AML Policy and reporting compliance to the Board/Audit Committee.

The Principal Officer shall endeavor to attend all meetings of AML Committee of Principal Officer – IndoStar Group Companies, so as to ensure matters as set out in its terms of reference are reviewed.

Each IndoStar Group Company shall ensure that this Group-wide KYC & AML Policy is periodically reviewed & the revised policy is adopted by its Board of Directors, as recommended by FATF and guidelines issued by RBI.

28. Review of Policy

This 'Group Policy' shall be reviewed as and when required, considered necessary modifications by the Board and as per amendments received by Reserve Bank of India as & when or otherwise at least '**once in a year**'.

Prepared By	Approved By
Ms. Rashmita Prajapati	**Mr. Vinodkumar Panicker**
(Chief Compliance Officer)	**(Principal Officer)**

Annexure – I

Customer Identification

Customer Type and features to be verified	Documents / Information
Individuals - Legal name / any other name used - Correct Permanent and Current Address - Nature of business & financial status	- A certified copy of the following documents to be obtained for verifying identity and address of an individual, including an individual who is a Beneficial Owner, authorized signatory or the power of attorney holder related to any legal entity: • PAN or Form 60 **(Mandatory)** • proof of possession of Aadhaar Number • passport • driving licence. • Voter's Identity Card issued by the Election Commission of India. • job card issued by NREGA duly signed by an officer of the State Government. • Letter issued by the National Population Register containing details of name, address. - In case the abovementioned documents do not contain the updated/ current address, pending updation of current address on such documents, a certified copy of any of the following documents to be obtained, which will be valid only for 3 months from the time of submitting the same, prior to expiry of which, the Customer shall submit the abovementioned documents with updated/ current address: • utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); • property or municipal tax receipt; • pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; • letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation. • registered lease deed; • bank account statement (not more than 6 months old); • post-paid mobile bill (not more than 6 months old); • notarized rent agreement along with copy of the landlord's address proof (e.g., electricity, telephone, post-paid mobile phone, piped gas, water bill). - Documents with respect to nature of business and financial status as may prescribed by Management Committee from time to time. - Salary Slip (latest 3 months) - Recent Photograph.

Customer Type and features to be verified	Documents / Information
	- KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry. - In case where the co-applicant's Aadhaar is not updated with the current address, in such cases the Group shall in addition to the co-applicant's Aadhaar, shall collect the spouse's Aadhar Card (with current address), an undertaking letter along with relationship proof. - Such other documents as may be prescribed from time to time. In this Annexure I, obtaining a certified copy by the customer shall mean comparing the copy of the document so produced by the Customer with the original and recording the same on the copy by person authorized by the Company. **The use of Aadhaar, proof of possession of Aadhaar etc., shall be in accordance with the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016, the Aadhaar and Other Law (Amendment) Act, 2019 and the regulations made thereunder and the RBI Directions.**
Sole Proprietorship - Legal Name of the Sole Proprietor - Correct address / place of business of the proprietor and firm - Business / activity of the firm - Contact Point Verification	Documents to be obtained from Proprietor: - Documents as same *to be obtained from "Individual Customers"* Documents to be obtained from the Proprietary Firm: Any two of the following documents as a proof of business/ activity in the name of the proprietary firm: • Udyam Registration certificate. • Certificate/licence issued by the municipal authorities under Shop and Establishment Act. • Sales and income tax returns. • CST/VAT/GST certificate (provisional / final). • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. • IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT/ Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. • 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. • Utility bills such as electricity, water, and landline telephone bills, etc. Where the Company is satisfied that it is not possible to furnish any 2 (two) of the abovementioned documents, the Company may, at its

Customer Type and features to be verified	Documents / Information
	discretion, accept only one of those documents as proof of business/ activity; provided that the Company undertakes contact point verification and such other information and clarification has been collected which would be required to establish the existence of such firm, and the Company shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern. - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - Such other documents as may be prescribed from time to time
Partnership - Legal name - Address - Names of all partners and their addresses - Ultimate Beneficial Owners - Telephone numbers of the firm and partners	Documents to be obtained from Beneficial Owner, managers, officers or employees holding an attorney to transact on behalf of the partnership firm: - Documents to be obtained from *"Individual Customers"* Certified copies of each of the following documents to be obtained from the partnership firm: - Registration certificate. - Partnership deed. - Permanent Account Number of the partnership firm. - The names of all the partners. - Address of the registered office, and the principal place of its business, if it is different. - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry. - Such other documents as may be prescribed from time to time. - Utility Bill on the name of firm.
Trust - Legal Name & address of the Trust - Names of trustees, settlers, beneficiaries - Telephone/fax numbers	Documents to be obtained from Beneficial Owner, managers, officers or employees holding an attorney to transact on behalf of the Trust: - Documents to be obtained from *"Individual Customers"* Certified copies of each of the following documents to be obtained from the trust: - Registration certificate. - Trust deed. - Permanent Account Number or Form No.60 of the trust. - The names of the beneficiaries, trustees, settlor, protector, if any and - authors of the trust. - The address of the registered office of the trust. - List of trustees, settlor, protector or any authors of the trust and documents (*Please refer to documents to be obtained from "Individual Customers*), for those discharging the role as trustee and authorized to transact on behalf of the trust. - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry. - Such other documents as may be prescribed from time to time.

Customer Type and features to be verified	Documents / Information
	- Address proof of Registered Office of the Trust
Unincorporated association or body of individuals (includes unregistered trust / partnership firms and societies) - Business / activity - Legal existence - Principal place of business - Ultimate Beneficial Owner - Contact Point Verification	Documents to be obtained from Beneficial Owner, managers, officers or employees holding an attorney to transact on behalf of the unincorporated association / body of individuals: - *Documents to be obtained from "Individual Customers"* Certified copies of each of the following documents to be obtained from unincorporated association or body of individuals: - Resolution of the managing body of such association or body of individuals. - Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals. - Power of attorney granted to transact on its behalf. - Documents/ such information as may be required to collectively establish the legal existence of the association / body of individuals. - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry - Such other documents as may be prescribed from time to time
Companies - Name of the company, directors & promoters - Principal place of business - Ultimate Beneficial Owners - Mailing address of the company - Telephone/Fax Number	Documents to be obtained from Beneficial Owner, managers, officers or employees holding an attorney to transact on behalf of the company: - Documents *to be obtained from "Individual Customers"* Certified copies of each of the following documents to be obtained from companies: - Certificate of incorporation. - Memorandum and Articles of Association. - Permanent Account Number of the company. - A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on behalf of the company. - The names of the relevant persons holding senior management position. - The registered office and the principal place of its business, if it is different. - KYC Template / information as prescribed by the Reserve Bank of India for uploading data with Central KYC Record Registry. - Such other documents as may be prescribed from time to time.
Juridical persons not specifically covered in the earlier sections, such as societies, universities and local bodies like village panchayats or who purports to act on behalf of such	A certified copy of each of the following documents shall be obtained and verified: - Document showing name of the person authorized to act on behalf of the entity; - Documents to be obtained of the person holding an attorney to transact on its behalf– (*Please refer to documents to be obtained from "Individual Customers"*).

Customer Type and features to be verified	Documents / Information
juridical person or individual or trust - Legal existence - Contact Point Verification - Identity of Person purporting to act on behalf on its behalf	- Such documents as may be required by the Company to establish the legal existence of such an entity/ juridical person. - KYC Template / information as prescribed by the RBI for uploading data with Central KYC Record Registry. - Such other documents as may be prescribed from time to time.

In terms of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, equivalent e-document of the abovementioned documents can be obtained for the purpose of KYC in compliance with the said rules.

Annexure – II

Risk Categorisation of Customers

Customers whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile, may be categorized as low risk. Customers that are likely to pose a higher-than-average risk of money-laundering should be categorized as Medium or High-Risk Customers, depending on Customer's background, nature and location of activity, country of origin, sources of funds, client profile, etc.

Low Risk (Grade A) ***Illustrative examples of Low-Risk Customers:***
Listed companies or their majority owned subsidiaries in India
Entities that are regulated by any Indian financial sector regulator like SEBI, RBI or IRDA.
Government departments & Government owned companies, regulators, statutory bodies and juridical bodies created under a law in force in India
Individuals / entities like salaried or self-employed individuals, professionals, proprietary firms, partnership firms, people belong to low-income group, Hindu Undivided Family (HUF), Trusts, private / public limited companies, with clear sources of funds verifiable through documents like IT Returns, statutory filings, documents registered / filed with statutory authorities, etc. (other than as mentioned in Grade B below)
Individual entities, proprietary firms, partnership firms, Hindu undivided family having Income below taxable limits /not filed ITRs whereas income source is being identified basis business experience, repayment tracks/ CIBIL history.
Medium Risk (Grade B) ***Illustrative examples of Medium Risk Customers:***
Entities belonging to business groups where at least two major entities are companies listed in India
Entities belonging to business group where at least one major entity is regulated by an Indian financial sector regulator like SEBI, RBI or IRDA. However, if the regulated entity is a stock broker or an insurance broker, this sub-rule cannot be applied
Entities whose loan has been purchased from, or is assigned to us by a listed NBFC
Entities that have a credit rating of AA or higher from 2 or more SEBI approved Indian rating agencies
Entities like proprietary firms, partnership firms, Hindu undivided family, trusts, private / public limited companies, with clear sources of funds verifiable through documents like IT Returns, statutory filings, documents registered / filed with statutory authorities, etc., with transaction size of more than INR 50 crore.
Trusts, charities, NGOs and other organizations receiving donations
Entities / Individuals engaged in / deriving income from activities related to Real Estate sector.
Non-profit organizations, non-government organizations not promoted by the United Nations or its agencies
Non-banking finance companies
Micro finance institutions
Foreign currency exchange dealers
Chit funds
Association of persons/ body of individuals/ artificial judicial person
Entities / individuals engaged in / deriving income from activities related to Stock Market activities (individual and franchisees of brokers)
Customers engaged into the business (with annual turnover of less than or equal to INR 100 crores) of bullion, gold, silver, diamond, gems/ precious stones, jewelry)
High Risk (Grade C) ***Illustrative examples of High-Risk Customers:***
Entities that cannot be covered under KYC Grade A or B, as per specified criteria.
Non-residents / Foreign Nationals

High Net Worth Individuals i.e., individuals with net worth of more than INR 10 crore
Firms with 'sleeping partners'
Politically Exposed Persons of foreign origin or connected Customer / Beneficial Owner/ Directors/ Related Parties/Key Managerial Persons
Multi-level Marketing Companies
Customers in jurisdictions that do not or insufficiently apply the FATF Recommendations
Customers with dubious reputation as per public information
Cooperative banks
Credit societies
Companies incorporated overseas
Customers engaged into the business (with annual turnover of more than INR 100 crores) of bullion, gold, silver, diamond, gems, precious stones, jewelry)

- The grade assigned to a Customer must be clearly indicated in the relevant Credit Memo and the intensity of due diligence for each Customer will depend on its risk category.

- KYC grading guidelines mentioned above are indicative. In case of ambiguity on classification, the next higher KYC grade must be applied. For instance, a real estate company that is listed on Stock Exchange would be covered under KYC Grade A, by virtue of being listed. However, since its primary business is real estate, KYC Grade B would be applicable.

Annexure - III

- In the case of high-risk Customers and/ or Customers undertaking unusually large transactions/ customers exhibiting unusual patterns which have no apparent economic or visible lawful purpose:

- it shall be mandatory that manager/ officer of the branch visits the Customer's premises and place of business to conduct physical verification and to ascertain the real existence of the business/ unit and to ascertain if its scale of operations commensurate with its turnover and transactions undertaken.

- further, in case of high-risk Customers, it shall be mandatory that the Customers and/ or the authorized officer(s) of the Customers (as applicable) personally visits the concerned branch of the Company (including at the time of periodic updation) and personally deposit the requisite customer identification documents with the manager of such branch.

- it shall be mandatory that manager/ officer of the branch to collect additional information and documentation regarding the purpose of the transaction and end-use of the amounts, source of income/ funds and review of income/ financial statements and banking statements.

- more than 1 (one) document (as set out in Annexure I above) shall be required to be obtained from the Customer for verification/ cross checking depending on the risk perception of the Company and such documents and information shall be verified from the verification facilities of the issuing authority, where ever applicable.

- information such as Customer's background, nature and location of activity and/ or business, country of origin, and his/ her/ its client profile etc. should be obtained.

- in case of high-risk Customers having multiple addresses and/ or multiple places of business, suitable documents shall be obtained from such Customers to verify all such addresses and/ or places of business.

- In order to prevent frauds, alternate mobile numbers shall not be linked post customer due diligence with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening.

- all such accounts and Customers shall be subject to enhanced monitoring on an on-going basis. In addition to above and depending upon facts and circumstances, the Company shall obtain from the respective Customers, such information and documents, as deemed necessary by the management of the Company, for the purpose of monitoring of such account and the Customer.

- it shall be imperative, in cases of companies, firms, body of individuals and other juridical persons, to examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management and due diligence should be undertaken on any guarantors, security providers, if applicable.

- There exists the possibility that trust accounts can be used to circumvent the customer identification procedures. The Company shall obtain satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf such trust is acting, as also obtain details of the nature of the trust or other arrangements in place. While entering into relationship with a trust, the Company shall take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any

person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers / directors and the beneficiaries, if defined.

- In the event that the Company relies on the Customer due diligence done by an intermediary, the Company should satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements in line with the conditions mentioned in the RBI Directions, PMLA and rules made thereunder.

- The Company should gather sufficient information on Politically Exposed Persons of foreign origin or connected Customer/ Beneficial Owner intending to establish a relationship with the Company and check all the information available on the person in the public domain. The Company should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

Annexure - IV

DECLARATION OF BENEFICIAL OWNERSHIP

[Applicable to Company, Partnership Firm, Unincorporated Association or Body of Individuals and Trusts. Not applicable for listed companies & their subsidiaries and registered charities]

Name of the Customer: _____
Registered Address: _____
_____

The Customer as stated above hereby confirms and declares that as on date, the following natural person(s) exercise control or ultimately have a controlling ownership interest i.e., having ownership/entitlement of more than 10% in case of Company, partnership firm and trust and more than 15% in case of unincorporated association or body of individuals of capital/profits/property or have controlling interest through voting rights, agreement, arrangement etc.

Sl. No.	Full Name of Beneficial owner/controlling natural person(s)	DIN/ Nature of relation with applicant entity	Nationality	KYC Documents		Controlling Ownership Interest/ Profit Share (%)
				Document Type	Document Type	

I/We certify that the facts stated above are true and correct. I/we acknowledge and confirm that IndoStar Group shall be entitled to rely on my/our declaration above on the identity(ies) of and information relating to the Beneficial Owners of the account. I/we undertake to inform the company in writing; should there be any changes to the ownership/shareholding structure in the future.

For and on behalf of (name of the entity): _____

Signature of the Authorized Official(s): _____

Full Name of the Authorized official (s): _____

Designation / Position: _____

Date: __ __ / __ __ / __ __ __ __ Place: _____

Annexure - V

DECLARATION OF ADDRESS CHANGE
[Applicable to all types of customers and related parties]

To
IndoStar Capital Finance Limited

I am Mr./Mrs. _____
hereby declare that my Address as per Aadhaar is _____
_____
_____
_____
I hereby declare that; I am residing at (Correspondence Address) _____
_____
_____
Nearest landmark _____
Since last _____ Months _____ Years.

I hereby submitting Registered Rent Agreement or any other deemed OVD for current address proof.

Please consider the above Correspondence address for communication purpose. I will update the given correspondence address in my OVD and ensure to submit to the Company (IndoStar Capital Finance Limited) within 90 days from loan disbursement for their record purpose and completing KYC requirements.

Aadhaar copy is attached.

Yours faithfully,

Signature:

Name: _____

LAN or Customer ID _____

Annexure - VI

DECLARATION OF MOBILE NUMBER CHANGE
[Applicable to all types of customers and related parties]

To
IndoStar Capital Finance Limited

Date:

I am Mr./Mrs. _____
hereby declare that my new mobile number as per attached proof is _____

Name of account holder	
Mobile Number	
Email ID (If available)	

I have herewith attached the post-paid mobile number proof or other proof for the evidence of above-mentioned mobile number confirmation.

Yours faithfully,

Signature:

Name: _____

LAN or Customer ID _____