1. INTRODUCTION

SAHYOG FINCAP Private Limited ("the Company" or "SFPL") is a registered **Non- Banking Financial Company (NBFC)** holding a valid Certificate of Registration from the **Reserve Bank of India (RBI)** under Registration No. **B-1100074** dated **29 November 1994**. It is currently classified as an **NBFC–Investment and Credit Company (NBFC-ICC)**.

The Company is engaged in providing finance for a range of products, including:

- Commercial Vehicles
- Cars
- Tractors
- Construction Equipment
- Three-wheelers and Two-wheelers
- Business Loans to the MSME segment (Secured and Unsecured)
- Loan Against Property (LAP)

2. REGULATORY REQUIREMENT

Reserve Bank of India (RBI) advised NBFCs to ensure that a proper policy framework on 'Know Your Customer' and Anti-Money Laundering measures with the approval of the Board shall be formulated and put in place in accordance with the provisions of the Master Direction - Know Your Customer (KYC) Direction, 2016 issued by RBI on February 25, 2016 and Prevention of Money-Laundering Act, 2002 read with Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, which is to be read along with the extant Directions/circulars/guidelines issued by the RBI in this regard or any other applicable law in force (**"RBI Guidelines"**).

3. ABOUT THE POLICY

The Know Your Customer ("KYC") and Anti Money Laundering ("AML") Policy ("Policy") is to prevent the Company from being used intentionally or unintentionally by criminal elements for committing financial frauds, transferring or deposits of funds derived from criminal activity or for financing terrorism and also to know / understand its customers and their financial dealings better which in turn help them manage their risks prudently.

The policy is also to put in place customer identification procedures for opening of accounts and monitoring transactions in the accounts for detection of transactions of suspicious nature by conducting the Customer Due Diligence (CDD) and further report about such suspicious transactions to Financial Intelligence Unit-India [FIU-IND] in terms of the recommendations made by Financial Action Task Force (FATF).

4. **OBJECT AND SCOPE OF THE POLICY** To lay down explicit criteria for acceptance of customers.
   1. To establish procedures to verify the bona-fide identification of individuals / non individuals before becoming an account holder/customer.
   2. To establish processes and procedures to monitor high value transactions and / or transactions of suspicious nature in accounts.
   3. To enable the Company to know / understand the customers and their financial dealings better, which in turn would help the Company to manage risks prudently.
   4. To develop measures for conducting due diligence.
   5. In respect of customers and reporting of such transactions.
   6. To comply with applicable laws and regulatory guidelines.
   7. To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.
   8. To prevent criminal elements from using the Company for money laundering activities.

5. **DEFINITIONS**

(i) **"Beneficial Owner" ('BO')** in relation to a customer is a person or an entity who is to be considered a beneficiary of the financial transaction entered in to with the Company by the customer. A list of persons who are to be considered as such BOs in relation to a customer is given below: -

Type of Customer	Persons to be considered Beneficial Owners(BOs)
Public/Private Limited Companies	a) A natural person having, whether alone or together, or through one or more juridical person, ownership of or entitlement to more than ten percent of shares or capital or profits of the Company; or b) A natural person having, whether alone or together, or through one or more juridical person, right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements; or c) Where none of the above is been identified–a natural person who holds the position of senior managing official.
Partnership Firm	a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than ten percent of capital or profits of the partnership or who exercises control through other means; or b) Where the above is not been identified–a natural person who holds the position of senior managing official

Unincorporated association of persons or body of individuals	a) A natural person having, whether alone or together, or through one or more juridical person, ownership of/ entitlement to more than fifteen percent of property or capital or profits of such association or body of individuals; or b) Where the above is not been identified–a natural person who holds the position of senior managing official.
Trust/Foundation	a) The Author of the trust; or b) The Trustees of the trust; or c) The Beneficiaries of the trust with ten percent or more interest in the trust; or d) A natural person exercising ultimate effective control over the trust through a chain of control or ownership.
Exemption from identification of BO: It is not necessary to identify and verify the identity of any shareholder or beneficial owner of an entity where the customer or the owner of the controlling interest is:- (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) is a subsidiary of such listed entities.	

(ii) **"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.

(iii) **"Customer Due Diligence (CDD)"** means identifying and verifying the customer and the Beneficial Owner using reliable and independent sources of identification. The CDD shall be include identify and verification of the customer's identity, information on the purpose and intended nature of the business relationship, where applicable, nature of the customer's business, ownership and control, identity of the beneficial owner of the customer.

Further the Company may obtain KYC Identifier with explicit customer consent to download KYC records from CKYCR, for the purpose of CDD.

(iv) **"Central KYC Records Registry" (CKYCR)** means the Company, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

(v) **"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.

(vi) **"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.

(vii) **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.

(viii) **"KYC Templates"** means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

(ix) **"Officially valid document"**(OVD) means the passport, the driving license, proof of possession of Aadhaar number, the Voter's Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address. Provided that: -

a) Where the customer submits his/her proof of possession of Aadhaar number as an OVD, he/she 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 current address within a period of three months of submitting the documents specified at 'b' above.

d) (as and when applicable) 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.

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

(xi) "**Principal Officer**" means an officer at the management level nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.

(xii) **"Reporting Entity"** for the purpose of this Policy would mean the Company, SFPL Financier Private Limited.

(xiii) **"Senior Management"** as defined in Nomination and Remuneration Policy of the Company.

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

a. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence regardless of the value involved; or
b. appears to be made in circumstances of unusual or unjustified complexity; or
c. appears to not have economic rationale or bona-fide purpose; or
d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

(xv) **"Video based Customer Identification Process (V-CIP) "**is an alternate method of customer identification with facial recognition and customer due diligence by an authorized official of the RE by undertaking seamless, secure, live, informed-consent based audio-visual interaction with the customer to obtain identification information required for CDD purpose, and to ascertain the veracity of the information furnished by the customer through independent verification and maintaining audit trail of the process. Such processes complying with prescribed standards and procedures shall be treated on par with face-to-face CIP for the purpose of this Master Direction.

(xvi) **"Wire transfer" related definitions:**

"Wire transfer" related definitions: for the purpose of this Policy, Wire Transfer and its related definitions would have the same meaning as assigned to it under the RBI's Guidelines on 'Know Your Customer' and Anti-Money Laundering Measures, as amended from time to time.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the RBI Guidelines and other regulations made there under, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

6. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT:

a) The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering & terrorist financing risk and shall properly document the risk assessment.

b) Further, the periodicity of risk assessment exercise shall be annual.

c) The outcome of the exercise shall be put up with the Risk Management Committee.

The Company shall apply a Risk Based Approach (RBA) and implement a CDD programme, having regard to the ML/TF risks identified by the Company and the size of business for mitigation and management of the identified risk and establish controls and procedures in this regard which shall be monitored regularly and enhance them if necessary.

7. KNOW YOUR CUSTOMER STANDARDS

The KYC policy of the Company have the following four elements:

(i) Customer Acceptance Policy (CAP)
(ii) Risk Management
(iii) Customer Identification Procedures(CIP); and
(iv) Monitoring of Transactions

(i) Customer Acceptance Policy (CAP)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the Company. The branches shall accept customer strictly in accordance with the said policy:

1. The Company will have an elaborate standard for obtaining comprehensive information regarding new customers at the initial stage and that of existing customers over a predetermined period, thereby establishing the bona fides of customers opening credit accounts with the Company.

2. The Company will lay down / spell clearly the document requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the guidelines issued by RBI

from time to time i.e. nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status, etc. The Company shall perform the due diligence procedure of customers on Unique Customer Identification Code (UCIC) level in order to avoid the repetition of due diligence, in case any existing customer desires to open another loan account or avail any other product or service from the Company as far as identification of the Customer is concerned. If the existing customers wish to open another account with the Company, after closure of its existing account, then the Company shall perform the due diligence only after expiry of at least six months from the date of closure of account.

3. The Company shall assign a Unique Customer Identification Code (UCIC) to each customer at the time of on boarding, following the completion of Know Your Customer (KYC) procedures as prescribed by the Reserve Bank of India (RBI). This shall include verification of identity, address, and risk categorization based on prescribed parameters. The Company shall establish a robust mechanism to prevent the duplication of UCICs and shall ensure that the same UCIC is used across all products and services availed by the particular customer.

4. Further, during the on boarding process of potential customers, their respective KYC details shall cross-verify automatically against the existing customer database. If a potential match is identified, the system flags the existing record under de duplication ("dedupe"). A new UCIC shall be generated only if no matching KYC details are found in the current database. Furthermore, the Company conducts periodic audits and system validations to further strengthen the effectiveness of the de-duplication mechanism.

5. The Company shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer account opening either due to non- cooperation of the customer or non-reliability of the documents/information furnished by the customer.

6. Any additional information, if required by the Company, other than those already specified in the KYC policy, shall require explicit consent of the customer.

7. The Company will not open accounts in the name of anonymous / fictitious / benami persons.

8. The Company will ensure that circumstance in which a customer is permitted to act on behalf of another person / entity will be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is

opened by an intermediary in the fiduciary capacity.

9. The Company will ensure that before opening a credit account there are adequate checks to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities like individual terrorist or terrorist organizations.

10. No account is opened where the identity of the customer matches with any person or entity, whose name appears in the sanctions lists circulated by RBI/FIU-IND.

11. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.

12. Where Goods and Services Tax (GST) details are obtained, the same shall be verified from the search/verification facility of the issuing authority.

13. Due Diligence Procedure of customers should be followed for all the joint account holders, while opening a joint account.

14. Where an equivalent e-document is obtained from the customer, Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000.

15. The Company shall not deny the financial facility to general public, especially those, who are financially or socially disadvantaged, however the company should comply its Loan & Credit Policy and other relevant policies of the company. If the Company is suspicious of money laundering or terrorist financing, and reasonably believes that performing the Customer Due Diligence (CDD) process will tip-off the customer, it shall not pursue the CDD process, and instead file a suspicious transaction report (STR) to FIU-IND.

16. ACustomercanactonbehalfofanotherentityonlyinthefollowingcircumstances:

Another entity	Conditions on Customer
Company	If he / she is a director of the Company or authorized signatory by Board of Directors
Trust	If he / she is a trustee
Partnership Firm	If he / she is a partner

(ii) Risk Management

1. The Board of Directors ("Board") of the Company shall ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It shall cover proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility would be explicitly allocated within the Company for ensuring that the Company's policies and procedures are implemented effectively. The Company shall, in consultation with their Board, devise procedures for creating Risk Profiles and principles for risk categorization of their existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

2. The Company has an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements shall have different focuses for front line 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.

3. The Company shall prepare a profile for each new customer based on risk categorization. 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, geographical risk covering customers as well as transactions, type of services offered, delivery channel used for delivery of services, types of transaction undertaken - cash, cheque/monetaryinstruments,wiretransfers,forextransactionsetc.Thenatureand extentof due diligence shall depend on the risk perceived by the Company.

4. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, shall be categorized as low risk. In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer, are to be met. Customers that are likely to pose a higher than average risk to the Company may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds, his client profile, geographical risk, type of services offered, delivery channel used for delivery of services, types of transaction undertaken - cash, cheque / monetary instruments, wire transfers, for ex transactions etc. The Company may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear.

5. The various information so collected from different category of customers for the purpose of risk categorization and related to perceived risk shall be on non-intrusive basis, notwithstanding the need for availability of minimum required information to meet the regulatory requirements.

6. Examples of customers requiring Lower due diligence may include:-

   i. Salaried employees with well-defined salary structures;
   ii. People working with government owned companies, regulators and statutory bodies, etc.;
   iii. People belonging to lower economic strata of the society whose accounts show small balances and low turnover;
   iv. People working with Public Sector Units;
   v. People working with reputed Public Limited Companies and Multinational Companies.

7. Examples of customers requiring medium due diligence may include:-

   i. Salaried applicant with variable income / unstructured income receiving Salary in cheque;
   ii. Salaried applicant working with Private Limited Companies related to travel agents, telemarketers, internet café and International direct dialing (IDD) call service.
   iii. Companies having close family shareholding or beneficial ownership.

8. Examples of customers requiring higher due diligence may include:-

   i. non-resident customers,
   ii. high networth individuals,
   iii. trusts, charities, NGOs and organizations receiving donations,
   iv. firms with 'sleeping partners',
   v. politically exposed persons (PEPs) of foreign origin,
   vi. non-face to face customers, and
   vii. those with dubious reputation as per public information available, etc.
   viii. Individuals and entities listed or identified in – various United Nations' Security Council Resolutions(UNSCRs)suchasUN1267,scheduletotheorderundersection51Aoft he Unlawful Activities (Prevention) Act, 1967, in watch lists issued by Interpol and other similar international organizations, regulators, FIU and other competent authorities as high-risk etc.
   ix. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and

unexplained movement of accounts to different institutions, etc.

x. Gambling / gaming including "junket operators" arranging gambling tours.

xi. Jewelers and Bullion Dealers.

Note: Company shall treat the risk categorization and reasons for risk categorization of customers as confidential.

9. Adoption of the customer acceptance policy and its implementation shall not become too restrictive and the Company will strive not to inconvenience the general public, especially those who are financially or socially disadvantaged.

10. The Company shall maintain Money Laundering/Terrorist Financing risks that may arise in relation to the development of new business practices or processes including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing services or practices.

11. Accordingly, the Company shall undertake risk assessments prior to the launch or use of such, practices, services and technologies; and take appropriate measures to manage and mitigate the risks.

(iii) Customer Identification Procedure(CIP)

Identification is an act of establishing who a person is in the context of KYC, it means establishing who a person purports to be and will involve identifying the customer and verifying his/her identities by using reliable and independent source documents, data or information. For this purpose, the Company will obtain sufficient information necessary to establish to its satisfaction the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of relationship. The Company shall perform the CDD either on its own or can rely on the CDD conducted by any third party, subject to obtain the record or information from the third party or CKYCR on immediately basis and being ultimate responsible for the identity of the Customer.

Being satisfied means that the Company must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such a risk-based approach is considered necessary to avoid disproportionate costs to Company and a burdensome regime for the customers.

Identity is verified for:

i. The named account holder

ii. beneficial owners

iii. signatories to an account and

iv. Intermediate parties.

1 **Accounts of Individuals**

In case of customers that are natural person, the Company will obtain sufficient identification data to verify (a) the identity of customer (b) his/her address/location and (c) his/her recent photograph. The Company may also undertake V-CIP to carry out CDD in case of new customer on-boarding for individual customers, proprietor in case of proprietorship firm, and shall adhere to the standards as prescribed under PML Act/ RBI guidelines/KYC Policy. The true identity and bona fides of the existing customers and new potential customers opening credit accounts with the Company and obtaining basic background information would be of paramount importance.

2 **Other than individual accounts**

For customers that are legal person or entities, the Company will (a) verify the legal status of the legal person / entity through proper and relevant documents, (b) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person, (c) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. The Company may also undertake V-CIP to carry out CDD in case of new customer on- boarding for authorized signatories and Beneficial Owners (BOs) in case of Legal Entity (LE) customers and shall adhere to the standards as prescribed under PML Act/ RBI guidelines/KYC Policy.

3 **Accounts of Companies and firms**

Branches need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with the Company. Branches should 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. These requirements may be moderated according to the risk perception e.g. in the case of a public Company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.

4 **Accounts of Politically Exposed Persons (PEPs) resident outside India**

Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations, important political party officials, etc. Branches should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain.

Branches should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The branches should seek prior approval from their concerned Credit Heads for opening anaccount in the name of PEP and if an existing customer or his/her beneficial owner subsequently becomes a PEP.

5 Accounts of proprietary concerns

The Company may undertake V-CIP to carryout CDD of a proprietorship firm, by obtaining the equivalent e-document of the activity proofs with respect to the proprietorship firm, as mentioned in clause 28 and clause 29 of RBI Guidelines, apart from undertaking CDD of the proprietor and shall adhere to the standards as prescribed under PML Act/ RBI Guidelines/KYC Policy. The Company should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/license issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority / Department. The Company may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, the 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 and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

6 Obtaining Guarantor on credit facilities

The Company generally insists on "Guarantee" by a known person (who becomes guarantor to a particular credit facility). Obtaining Guarantee from a known person is a process of ascertaining the identity of a person and his acceptability for establishing business relationship and verifying the true identity of the intending customer before opening a credit account. Further,

Guarantor also acts as an introducer of the customer to the Company for the credit facilities.

7 **Liabilities of the Guarantor**

Guarantor is legally responsible to the Company for the repayment of the credit facilities by the customer and is expected to be in a position to identify / trace the account holder in case of need.

8 **Procedure for providing Guarantee**

The Guarantor will be required to sign on the agreement entered into with the Customer at various places provided in the loan agreement form.

The Guarantor will be normally required to visit the Company's branch for signing the agreement. However, this need not be compulsory.

9 **Closure of accounts**

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer, the Company will consider closing the account or terminating the banking / business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions will be taken at a reasonably senior level.

Further process / Illustrative Customer identification procedure is defined in **Annexure A**

(iv) **Monitoring of Transactions**

a) Ongoing due diligence:

Ongoing monitoring is an essential element of effective KYC procedures. The Company can effectively control and reduce their risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity attached with the client. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Company may adopt appropriate innovations including artificial intelligence and machine learning (AI & ML) to support effective monitoring.

The permanent correct address shall meant he address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other

document accepted by the Company for verification of the address of the customer. In case utility bill is not in the name of the customer but is close relative:wife, son, daughter and parents etc. who live with their husband, father/mother and son, the Company shall obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) is a relative and is staying with him/her. The Company shall use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, the Company shall keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

Review of risk categorization of customers shall be carried out at a periodicity of not less than once in six months. The Company shall also introduce a system of periodical updation of customer identification data (including photograph/s) after the account is opened. The periodicity of such updation shall not be less than once in ten years in case of low risk category customers, not be less than once in five years in case of medium risk category customers and not less than once in twoyearsincaseofhighriskcategoriesinthefollowingmanner.TheCompanyshallensure that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high-risk. The Company shall also ensure monitoring in case of high-risk accounts.

1. INDIVIDUAL CUSTOMERS	
a) No change in KYC information	A self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc.

b) Change in address	A self-declaration of the new address shall be obtained from the customer through customer's email-id registered with the Company, customer's mobile number registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter etc. The Company may obtain a copy of OVD or deemed OVD or the equivalente-documents thereof, for the purpose of proof of address, declared by the customer at the time of updation / periodic updation.
c) Accounts of customers who were minor at the time of opening account on their becoming major	A fresh photograph shall be obtained from the customer on their becoming a major and it shall be ensured that CDD documents as per the current CDD standards are available with the Company. The Company may also carry out fresh KYC of such customers, wherever required.
d) Accounts opened using Aadhaar OTP based e-KYC, in non-face-to-face mode	Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. The Company shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud. The specific conditions stipulated for opening of an account using Aadhar OTP in non-face-to-face mode under RBI guidelines are not applicable for updation / periodic updation of KYC.
2. **CUSTOMERS OTHER THAN INDIVIDUALS (LEGAL ENTITY)**	
a) No change in KYC information	A self-declaration shall be obtained from the Legal Entity (LE) customer through its email id registered with the Company, ATMs, digital channels (such as online banking / internet banking, mobile application of Company), letter from an official authorized by the LE in this regard, board resolution etc. The Company shall ensure that Beneficial Ownership (BO) information available with them is accurate and up-to-date.

b) Change in KYC information	The Company shall undertake the KYC process equivalent to that applicable for on-boarding a new LE customer.
3. ADDITIONAL MEASURES	a) The Company shall ensure that the KYC documents of the customer as per the current CDD standards are available with them. Further, if the validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, Company shall undertake the KYC process equivalent to that applicable for on-boarding a new customer.

	b) Customer's PAN details, if available with the Company, is verified from the database of the issuing authority at the time of periodic updation of KYC. c) An acknowledgment is provided to the customer mentioning the date of receipt of the relevant document(s), including self-declaration from the customer, for carrying out updation / periodic updation. Further, it shall be ensured that the information / documents obtained from the customers at the time of updation / periodic updation of KYC are promptly updated in the records / database of the Company and an intimation, mentioning the date of updation of KYC details,is provided to the customer.
	d) In order to ensure customer convenience, Company may consider making available the facility of updation/periodic updation of KYC at any branch, in terms of their internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated. e) The Company shall adopt a risk based approach with respect to periodic updation of KYC.
4. OBLIGATIONS OF CUSTOMERS:	The Customers are required to submit the updated KYC Documents to the Company, in case of any updation in the KYC already submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary, within a period of 30 days from such update in order to comply with the PML Rules.

b) **Enhanced due diligence (non-face to face customer on boarding)**

The Company needs to apply enhanced due diligence measures in case of customers on boarding through non-face-to-face method. Presently, the Company onboard the customers through physical verification, and it shall comply with the respective provisions of RBI KYC & AML Master Direction as and when Company starts the procedure of on boarding the customers through non- face-to-face mode or V-CIP.

8. CDD PROCEDURE AND SHARING KYC INFORMATION WITH CENTRAL KYC RECORDS REGISTRY (CKYCR)

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR), the Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as required by the KYC templates prepared for 'individuals' and 'Legal Entities'("LE") as the case may be.

The Company shall, for the purpose of establishing an account-based relationship, updation / periodic updation or for verification of identity of a customer, 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 Company 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.

9. WIRE TRANSFER

Wire transfer refers to any transaction carried out on behalf of an originator through a financial institution by electronic means with a view to making an amount of funds available to a beneficiary at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person. The Company shall follow the responsibilities, procedure and other obligations applicable to the Company laid down in the rules for wire transfer occurring either domestic or cross border of RBI KYC & AML Master Direction.

10. APPOINTMENT OF DESIGNATED DIRECTOR

Mr DEV SINGH, Managing Director and Chief Executive Officer of the Company, has been appointed as Designated Director to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and Rules.

The Company shall submit the name, designation, address and contact details of the Designated Director to the FIU-IND and Reserve Bank of India **(RBI)**, whenever there is any change.

11. APPOINTMENT OF PRINCIPAL OFFICER

Mr. BIJAY KETAN DAS, Executive Director has been appointed as Principal Officer of the Company, who shall be responsible for ensuring compliance, monitoring transactions, sharing and reporting information as required under PML Act/ KYC Policy.

The Company shall submit the name, designation, address and contact details of the Principal Officer to the FIU-IND and Reserve Bank of India **(RBI)**, whenever there is any change.

12. COMPLIANCEOFKYCPOLICY

a) SAHYOG FINCAP to ensure compliance with KYC Policy through:
   (i) Senior Management, as defined in Nomination & Remuneration Policy of the Company, for the purpose of KYC compliance.
   (ii) Allocation of responsibility for effective implementation of policies and procedures at Head Office/ Regional Office/ Zonal Office / Branch Office level.
   (iii) All Head Office Departments to ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
   (iv) Independent evaluation of the compliance functions of the Company's policies and procedures, including legal and regulatory requirements be done by Internal auditor and Secretarial Auditor appointed by the Company;
   (v) Internal auditor shall verify the compliance with KYC / AML policies and procedures and submit audit notes and compliance report to the Audit Committee on quarterly basis.

b) The Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

13. MAINTENANCE OF RECORDS OF TRANSACTIONS/ INFORMATION TO BE PRESERVED/ MAINTENANCE AND PRESERVATION OF RECORDS/ CASH AND SUSPICIOUS TRANSACTIONS REPORTING TO FINANCIAL INTELLIGENCE UNIT-INDIA (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking/Financial companies in regard to preservation and reporting of customer information.

(i) Maintenance of records of transactions

The Company shall maintain the proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

a) all cash transactions of the value of more than Rupees ten Lakh or its equivalent in foreign currency;
b) all series of cash transactions integrally connected to each other which have been valued below Rupees ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh or its equivalent in foreign currency;
c) all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency;
d) 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 transaction;
e) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules;
f) all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India; and
g) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

(ii) Information to be preserved

The Company will maintain all necessary information in respect of transactions referred to in PML Rule 3 to permit reconstruction of individual transaction, including the following information:

a) the nature of the transactions;
b) the amount of the transaction and the currency in which it was denominated;
c) the date on which the transaction was conducted; and
d) the parties to the transaction

(iii) Maintenance and Preservation of Records

The Company will maintain the records containing information of all transactions including the records of transactions detailed in PML Rule 3. The Company should also 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.

Further, in terms of PML Amendment Act 2012 notified on February 15, 2013, the Company should maintain for at least five years from the date of transaction between the Company and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

The Company should ensure that records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during the course of business relationship, are properly preserved for at least five

years after the business relationship is ended as required under Rule 10 of the Rules. The identification records and transaction data should be made available to the competent authorities upon request.

The Company should ensure that if its customer is a non-profit organization, it shall be registered on the DARPAN Portal of NITI Aayog. If it's not registered, then Company shall take appropriate steps to register the same and maintain such registration records for a period of five years after the business relationship between the customer and the Company has ended or the account has been closed, whichever is later.

(iv) Reporting to Financial Intelligence Unit–India:-

There are following below mentioned reporting which are filed with FIU-ID at FINGATE:

Snap shot of various Transactions Reporting Formats to Financial Intelligence Unit–India					
Sl.	**Report**	**Description**	**Amount**	**Frequency & Due Date**	**Formats**
1	**Cash Transaction Reports(CTR)**	All cash transactions of the value of more than rupees ten lakhs or its equivalent in Foreign currency.	Rs. 10,00,000/-	Event Based and 15th day of the succeeding month	As Prescribed from time to time.
		All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month			
2	**Counterfeit Currency Reports(CCR)**	All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions			
3	**Non-Profit Organization Transaction Report(NTR)**	All transactions involving receipts by non-profit organizations of value more than Rs. Ten lakhs or, its equivalent in foreign currency			
4	**Cross Border Wire Transfer Reports (CBWTR)**	All cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.	Rs. 5,00,000/-		
5	**Report on sale/purchase of**	All purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the	Rs. 50,00,000/-	Event Based and 15th day of the month	

	immovable	reporting entity*, as the case may be.		succeeding the quarter.	

	property (IPR)			
6	**Suspicious Transaction Reports(STR)**	(i) All suspicious transactions whether or not made in cash; (ii) Any receipt(s) of money in cash from any single customer in a month exceeding INR 7,00,000/- (Indian Rupees Seven Lakhs only); and (iii) If any customer has been identified of submitting forged/ manipulated documents (KYC or otherwise) during the loan appraisal process (iv) Any receipt(s) of money in cash from any single customer in a quarter exceeding INR 15,00,000/- (Indian Rupees Fifteen Lakhs only) (v) Mortgage Backed Loans if loan account is: a) pre-closed within a period of 12 months of its origination, and b) the pre-closure amount is exceeding ₹20,00,000/- (vi) Pre-closure of any loan account other than Mortgage backed loan within a period of 6 months of its origination where repayment is made in cash exceeding ₹ 49,000. vii) If any loan account is partial pre-closed during the financial year for an amount more than Rs. 1,99,000 or more and such amount is more than 20% of the outstanding principal balance.		Event Based and Not later than seven working days on being satisfied that the transaction is suspicious.

In terms of the PMLA rules, the Company will report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address and portal

Address	Portal
Director, FIU-IND, Financial Intelligence Unit-India, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi-110021	http://fiuindia.gov.in/

The above guidelines do not require the Company to report NIL transactions.

14. COMBATING FINANCING OF TERRORISM

In terms of PMLA Rules, suspicious transactions shall include inter alia transactions which give rise to areas on able ground of suspicion that these may involve financing of the activities relating to terrorism. The Company, therefore, shall develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit–India (FIU-IND) on priority.

As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is circulated by Reserve Bank, the Company shall ensure to update the consolidated list of individuals and entities as circulated by Reserve Bank. The Company shall, before opening any new account, ensure that the name/s of the proposed customer does not appear on the list. Further, the Company shall scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in thelist. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall be immediately be intimated to RBI and FIU-IND.KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the financial channels. Adequate screening mechanism shall be put in place by the Company as an integral part of recruitment/hiring process of personnel. The Company shall follow the procedures laid down for the freezing of assets and provisions relevant to the procedure for Implementation of the Weapons of Mass Destruction (WMD) and their Delivery Systems as prescribed in the RBI KYC & AML Master Direction.

15. CUSTOMER EDUCATION / EMPLOYEE'S TRAINING / EMPLOYEE'S HIRING

a) Customer Education

The Company recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose.

The front desk staffs need to be specially trained to handle such situations while dealing with customers.

b) Employees' Training

The Company must have an ongoing employee training programme so that the members of the staff are adequately trained in KYC procedures. Training requirements 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.

There should be open communication, high-integrity, proper understanding of subject matter amongst the Company's staff dealing with KYC/AML matters.

16. VALIDITY

The Policy shall be valid till next review by Committee members and/or Board of Directors, as applicable.

17. REVIEW

The Company's CEO and CFO have been entrusted with the responsibility of enforcement of this policy. They are hereby given absolute power to jointly or severely, make necessary changes, amendments or additions or removals for the operational aspects of the policy within the overall spirit and guidance from time to time for reasons like technology or process upgradation, regulatory changes, maintaining competitive edge or responding to changes in market or risk environment, etc. This is required to ensure full operational freedom to the senior management and make the management team more adaptive to rapid changing external environment. All changes so made shall be noted to the policy approving authority during the next policy review.

The CEO and CFO can decide on delegation of authority and can design / redesign MIS systems and reporting as they see fit to improve the responsibility and accountability within the team hierarchy.

Annexure-A

Illustrative Customer identification procedure

Types of customers: features to be verified.	Illustrative Documents to be obtained

Accounts of individuals: -Legal name and any other names used -Correct permanent address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v) Job Card issued by NREGA duly signed by an officer of the State Government (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number (vii) Identity card (subject to the bank's satisfaction) (viii) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (ix) Aadhar Card including e-Aadhar. (i) Telephone bill (ii) Bank account statement (iii) letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Aadhar Card including e-Aadhar (vii) Letter from employer (subject to satisfaction of the Company) (any one document which provides customer information to the satisfaction of the Company will suffice).
Accounts of partnership firms • Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners.	(i) Registration certificate, if registered (ii) Partnership deed (iii) PAN of the Partnership Firm (iv) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (v) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (vi) Telephone bill in the name of firm/partners (vii) the names of all the partners; and (viii) address of the registered office, and the principal place of its business, if it is different.
Accounts of companies • Name of the Company • Principal place of business • Mailing address of the Company • Telephone / Fax Number.	(i) Certificate of Incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill. (vi) the names of the relevant persons holding senior management position; and (vii) the registered office and the principal place of its business, if it is different.

Accounts of trusts & foundations • Names of trustees, settlers, protector, beneficiaries and signatories. • Names and addresses of the founder, the managers/ directors and the beneficiaries. Telephone/fax numbers • Names of beneficial owners	(i) Certificate of registration, if registered (ii) Trust Deed (iii) PAN or Form 60 of the Trust (iv) Power of Attorney granted to transact business on its behalf (v) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses. (iv) Resolution of the managing body of the foundation/ association. (v) Telephone bill (vi) the names of the beneficiaries, trustees, settlor and authors of the trust (vii) the address of the registered office of the trust; and (viii) list of trustees and documents, for those discharging role as trustee and authorized to transact on behalf of the trust (ix) satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.
Accounts of Proprietorship Concerns • Proof of the name, address and activity of the concern	(i) Registration certificate (in the case of a registered concern) including Udyam Registration Certificate (URC) issued by Government. (ii) Certificate/license issued by the Municipal authorities under Shop & Establishment Act, (iii) Sales and income tax returns (iv) CST/VAT certificate / GST Certificate (v) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities (vi) License issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration / licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department, etc. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of the bank account etc. (vii) The 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 in the name of the proprietary concern. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.
Account of a Juridical Person such as societies, universities and local bodies like village panchayats, etc., or who purports to act on behalf of such juridical person or individual or trust	(i) Document showing name of the person authorised to act on behalf of the entity (ii) Documents, as specified in Section 16, of the person holding an attorney to transaction its behalf and (iii) Such documents as may be required by the RE to establish the legal existence of suchan entity / juridical person.

For SAHYOG FINCAP Private Limited

MR. DEV SINGH
MD & CEO

MR. BIJAY KETAN DAS
Executive Director