



OXYZO FINANCIAL SERVICES LIMITED
(FORMERLY KNOWN AS OXYZO FINANCIAL SERVICES PRIVATE LIMITED)

(COMPANY OR OXYZO)

ANTI MONEY LAUNDERING (AML) & KNOW YOUR CUSTOMER (KYC) POLICY

REVIEW & APPROVING AUTHORITY

Authority	Designation
Prepared By	Credit Operations Department
Reviewed and Approved By	Compliance Department & Risk Management Department
Approved By	Board of Directors

VERSION HISTORY

Version	Issue Date	Brief Description
1.0	30-11-2017	Created
2.0	16-09-2019	Updated
3.0	29-06-2020	In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time by GOI and Latest Master Direction - Know Your Customer (KYC) Direction, 2016 - dated May 10, 2021
4.0	05-04-2021	1. Amendment in CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) as per notification dated December 18, 2020. 2. Amendment as per UAPA notification dated February 02, 2021 and notified by RBI Master Direction March 23, 2021
5.0	24-05-2021	1. Definition of Video based Customer Identification Process (V-CIP) 2. Cosmetic changes under CDD section

6.0	09-11-2023	1. Revision in definition of Beneficial Owner 2. Updation in Politically Exposed person 3. Periodic updation of KYC 4. Other Misc changes
7.1	15.04.2024	Reviewed by Operational Committee
7.2	28.05.2024	Approved by Board of Directors
7.3	07.09.2024	Amended version approved by Board of Directors
8.0	07.04.2025	Amended as per Notification dated 06 th November 2024 and Included the process of filing STR.
8.1	28.05.2025	Reviewed and approved by Board of Directors
9.0	30.07.2026	Alignment of the Policy with the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 dated November 28, 2025 (the “KYC Directions, 2025”), which repealed and replaced the Master Direction – Know Your Customer (KYC) Direction, 2016, read with the Amendment Directions dated December 29, 2025. Extension of the periodic KYC updation timeline for low-risk individual customers to one year from the date of falling due or June 30, 2026, whichever is later, with such accounts subject to regular monitoring – RBI (KYC) (Amendment) Directions, 2025 dated June 12, 2025. Introduction of the advance intimation and reminder regime for periodic updation of KYC (three advance intimations and three reminders, including at least one by letter each), with prescribed content and audit trail, and intimation to the customer on completion of updation. Extension of CDD to occasional transactions of ₹50,000 and above, whether single or in a series of connected transactions, and to international money transfers; inclusion of Persons with Disabilities within financially or socially disadvantaged customers; and recording of reasons for rejection of any onboarding or KYC updation application – RBI (KYC) (2nd Amendment) Directions, 2025 dated August 14, 2025. Allocation of responsibility for verification of customer identity and/or address between the Regulated Entity last uploading/updating records on CKYCR and the NBFC downloading and relying on such records – Amendment Directions dated December 29, 2025.
9.1	12.08.2026	Reviewed and approved by Board of Directors

Disclaimer: This document is confidential in nature and supersedes all policy on Anti Money Laundering (AML) and Know Your Customer (KYC) in the Company and should be read in conjunction with the most recent policies and procedures documented and held on file.

1. **PREAMBLE:**

The Reserve Bank of India (RBI) has issued comprehensive 'Know Your Customer' (KYC) Guidelines to all Non-Banking Financial Companies (NBFCs) in the context of the recommendations made by the Financial Action Task Force (FATF) and Anti Money Laundering (AML) standards and Combating Financing of Terrorism (CFT) policies as these being used as the International Benchmark for framing the stated policies by the regulatory authorities. In view of the same, OXYZO Financial Services Limited (Formerly known as OXYZO Financial Services Private Limited) ("Company") has adopted the said KYC guidelines with suitable modifications depending on the activity undertaken by it. The Company has ensured that a proper policy framework on KYC and AML measures are formulated in line with the prescribed RBI guidelines and duly approved by the Board of Directors.

2. **DEFINITIONS:**

- i. **"Aadhaar number"** shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);
- ii. **"Act" and "Rules"** means the Prevention of Money Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.
- iii. **"Authentication"**, in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- iv. **"Certified Copy"** - Obtaining a certified copy by the Company shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the RE as per the provisions contained in the Act.
- v. **"Central KYC Records Registry" (CKYCR)** means an entity defined under Rule 2(1) of the Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
- vi. **"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 Rules and shall include those persons as defined Companies Act, 2013 (the Managing Director or a whole-time Director duly authorised by the Board)
- vii. **"Digital KYC"** The Company shall undertake Digital KYC only through its own authenticated application. The application shall capture a live photograph of the customer along with the original Officially Valid Document (OVD) or proof of possession of Aadhaar, affix a legible watermark containing the CAF number, GPS coordinates, date and time stamp, and the authorised official's name and unique employee code, record the customer's signature through OTP validation on the customer's registered mobile number along with the authorised official's declaration, perform all prescribed verification checks, and digitally sign the Customer Application Form (CAF) upon successful completion of the Digital KYC process.
- viii. **"Digital Signature"** shall have the same meaning as assigned to it in clause (p) of subsection (1) of section (2) of the Information Technology Act, 2000 (21 of 2000).
- ix. **"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.

- x. **"Know Your Client (KYC) Identifier"** means the unique number or code assigned to a customer by the Central KYC Records Registry.
- xi. **"Officially Valid Document"** shall have the same meaning as defined in the the KYC Directions, 2025
- xii. **"Offline verification"** shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).
- xiii. **"Principal Officer"** means as Officer nominated by the Company, responsible for furnishing information as per rule 8 of the Rules.
- xiv. **"Video based Customer Identification Process (V-CIP)"**: Where the Company undertakes V-CIP, it shall comply with the minimum standards in paragraphs 26-27 of the KYC Directions, 2025, including hosting the technology infrastructure on its own secured network with data stored in India, end-to-end encryption and alteration-proof consent, prevention of connections from IP addresses outside India, geo-tagged and time-stamped recordings, face liveness / spoof detection and face-matching, a documented workflow / SOP operated only by specially trained officials, CERT-In empanelled security testing, and concurrent audit of all V-CIP accounts before they are made operational.
- xv. **"Commencement of Account Based Relationship"**: Pursuant to Rule 9(1A) of PML Rules read with the NBFC KYC Directions, 2025, the commencement of the account-based relationship with the customer will be the date when the transaction will be ready for disbursement post completion of due diligence process.

3. **OBJECTIVE, SCOPE AND APPLICATION OF THE POLICY:**

OBJECTIVE: The objective of KYC guidelines is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC procedures shall also enable the Company to know and understand its Customers and its financial dealings better which in turn will help it to manage its risks prudently.

Thus, the KYC policy has been framed by the Company for the following purposes:

- a) To prevent criminal elements from using Company for money laundering activities.
- b) To enable Company to know and understand its customers and their financial dealings better which, in turn, would help the Company to manage risks prudently.
- c) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- d) To comply with applicable laws and regulatory guidelines.
- e) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures. This KYC Policy is applicable to all branches/offices of the Company and is to be read in conjunction with related operational guidelines issued from time to time.
- f) To have a proper Customer Due Diligence (CDD) process before onboarding a client.
- g) To monitor/maintain records of all cash transactions of the value of more than Rs.10 lacs.
- h) To monitor and report suspicious transactions.
- i) To discourage and identify money laundering or terrorist financing activities.
- j) To take adequate and appropriate measures to follow the spirit of the PMLA.

SCOPE AND APPLICATION: The scope of this policy is to ensure explicit criteria are

laid off for acceptance, identification, monitoring, risk assessment and due diligence of customers as detailed below:

- a) To lay down explicit guidelines and criteria for identification/acceptance of customers.*
- b) To lay down processes around monitoring of transactions in an account.*
- c) To lay down processes and measures around risk assessment of client.*
- d) To lay down measures for conducting Customer Due Diligence (CDD)*

To ensure above scope find its logical end, Company has adopted Ten (10) Key Elements in this policy as under:

- I) Customer Acceptance Policy (CAP).*
- II) Customer Identification Procedures (CIP).*
- III) Monitoring of Transactions.*
- IV) Risk Management.*
- V) Customer Due Diligence.*
- VI) Training Programme.*
- VII) Internal Control Systems.*
- VIII) Record Keeping.*
- IX) Appointment of Principal Officer.*
- X) Reporting to FIU – India.*

a. CUSTOMER ACCEPTANCE POLICY (“CAP”):

- 1. The Company’s CAP lays down the criteria for acceptance of Customers. The guidelines in respect of Customer relationship in the Company broadly includes the following:*
 - a. No facility is to be provided to any person in anonymous or fictitious/benami name(s)/entity(ies).*
 - b. Accept Customers only after verifying their identity, as laid down in Customer Identification Procedures. Necessary checks before entering into any transaction with the Customer that the identity of the Customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc.*
 - c. No facility is to be provided to any person without following the CDD Procedure.*
 - d. Classify Customers into various risk categories and, based on risk perception, apply the acceptance criteria for each category of Customers. Also, a profile of each Customer will be prepared based on risk categorization, identifying Customers who require a very high level of monitoring.*
 - e. Documentation requirements and other information to be collected in respect of different categories of Customers depending on perceived risk and compliances with Prevention of Money Laundering Act, 2002 (PMLA) and RBI/ Company’s guidelines/instructions.*
 - f. Implementation of CAP should not become too restrictive and result in denial of the Company services to general public.*

- g. The Company shall ensure that its onboarding and KYC processes are accessible and inclusive for financially or socially disadvantaged persons, including Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without due application of mind, and the officer concerned shall duly record the reason(s) for any such rejection.*
- h. Suitable system is put in place to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists circulated by Reserve Bank of India.*
- i. Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of issuing authority. Where an equivalent e-document is obtained from the customer, the company shall verify the digital signature as per the provisions of the 2002 Information Technology Act, 2000 (21 of 2000).*
- j. PEPs – Politically Exposed Persons (PEP) who are or have been entrusted with prominent public functions by a foreign country (Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.) would be subjected to enhanced CDD and such accounts would be permitted at least at a level higher than what is otherwise permitted to approve the account. Close relative of PEP also would be treated at par with PEP. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval is obtained to continue the business relationship.*

Additional PEP controls: The Company shall have risk-management systems to determine whether a customer or beneficial owner is a PEP, shall take reasonable measures to establish the source of funds and source of wealth of PEPs, and shall obtain senior-management approval before opening a PEP account; all such accounts shall be subject to enhanced monitoring on an ongoing basis. These requirements apply equally to the family members and close associates of PEPs.

- 2. The Company shall prepare a profile for each new Customer during the credit appraisal based on risk categorization. The Customer profile shall contain the information relating to the Customer's identity, social and financial status and nature of employment or business activity. The nature and extent of due diligence will depend on the risk perceived by Company. At the time of credit appraisal of the Customer the details are recorded along with his profile based on the documents provided by the Customer and verified by Company either by itself or through third party sources. The documents collected will be as per the product norms as may be in practice. However, while preparing Customer profile, the Company shall seek only such information from the Customer which is relevant to the risk category and is not intrusive.*

The Customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or for any other purposes.

As per KYC policy, for acceptance and identification, Company's Customers shall be categorized based on perceived risk broadly into three categories – High risk, Medium Risk, Low Risk. None of the Customers will be exempted from Company's KYC procedure, irrespective of the status and relationship with

Company or its Promoters.

6. *The System should be in place to capture Customer classification from the Money Laundering perspective including flagging of negative profile customers, terrorist organizations as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) etc.*

ISIL(Da'esh) & Al-Qaeda Sanctions List"

<https://www.un.org/sc/suborg/sites/www.un.org.sc.suborg/files/1267.pdf>

Taliban Sanctions List"

<http://www.un.org/sc/committees/1988/list.shtml>

²*Details of accounts resembling any of the individuals/entities in the lists shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated February 02, 2021. In addition to the above, other UNSCRs circulated by the Reserve Bank in respect of any other jurisdictions/ entities from time to time shall also be taken note of. The Company shall follow the procedure laid down in the UAPA order February 02, 2021 and comply with the orders issued by Government from time to time.*

Daily verification of lists: *The Company shall verify the UNSC sanctions lists and the lists in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007 on a daily basis, and shall also verify daily the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities' (DPRK) and ensure compliance with the related Implementation Order, taking account of all additions, deletions and other changes. Obligations under the Weapons of Mass Destruction Act, 2005: The Company shall additionally ensure compliance with the requirements of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, read with the Government Order dated September 1, 2023 prescribing the procedure for its implementation. Accordingly, the Company shall screen its Customers against the list of designated individuals and entities notified under the said Act, shall not carry out any transaction or extend any facility in relation to any such designated individual or entity, and shall intimate full particulars of any such attempted transaction, without delay, to the Central Nodal Officer and the State Nodal Officer concerned, with a copy to the Reserve Bank of India.*

² Amended

Where an existing KYC-compliant Customer having a Unique Customer Identification Code (UCIC) with the Company seeks to avail of another product or facility, the Company shall not require the Customer to submit fresh proof of identity and/or proof of address, unless there is a change in the Customer's KYC information or the Company is required to undertake Enhanced Customer Due Diligence (ECDD) or any other due diligence in accordance with the applicable regulatory framework.

DEFINITION OF CUSTOMER:

For the purpose of Company's KYC policy, a 'Customer' means a Person as defined under Know Your Customer Guidelines issued by RBI (and any amendment from time to time by RBI) which are at present as under: -

- a) *A person or entity that has a business relationship with the Company.*
- b) *A Person who has a financial transaction or activity with the Company.*
- c) *A Person on whose behalf the person who is engaged in the transaction or activity, is acting.*

A "Person" shall have the meaning as defined under KYC Directions of RBI (and any

amendment from time to time by RBI) which at present is as follows:

'Person' shall include:

(i) an Individual.

(ii) a Hindu Undivided Family.

(iii) a Company.

(iv) a Firm.

(v) an association of persons or a body of individuals, whether incorporated or not;

(vi) every artificial juridical person, not falling within any one of the above person (i to v);

(vii) any agency, office or branch owned or controlled by any one of the above persons (i to vi).

b. Customer Identification Procedures ("CIP"):

1. Customer Identification means identifying the Customer and verifying his/her identity by using reliable, independent source documents, data or information. Company shall obtain sufficient information necessary to verify the identity of each new Customer along with brief details of its promoters and management, wherever applicable, whether regular or occasional and the purpose of the intended nature of business relationship as specified in Annexure I

2. Besides risk perception, the nature of information/documents required would also depend on the type of Customer (individual, corporate etc). For Customers that are natural persons, Company shall obtain sufficient identification data to verify the identity of the Customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the Company shall;

i) verify the legal status of the legal person/ entity through proper and relevant documents.

ii) 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.

3. Understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer identification requirements keeping in view the applicable provisions of Prevention of Money Laundering Act and Rules

An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure I. The Company will frame internal guidelines based on its experience of dealing with such persons/entities, normal prudence and the legal requirements.

The Company shall not insist upon Aadhaar for customer identification except where permitted or required under the Aadhaar Act, 2016, the Prevention of Money-laundering Act, 2002, the rules made thereunder, or any applicable law. Where Aadhaar-based authentication is undertaken, it shall be carried out only with the explicit consent of the customer and in accordance with the applicable legal and regulatory framework. The Company may use Aadhaar Face Authentication, where available and permitted, as one of the modes of Aadhaar authentication. Persons who avail the loan facility from the Company, the details of Customer Identification Procedure and documents required are listed in Annexure I.

The Company will formulate and implement a Customer Identification Programme to determine the true identity of its customers keeping the above in view. The Policy shall also

cover the Identification Procedure to be carried out at different stages, i.e. while establishing a relationship; carrying out a financial transaction or when there is a doubt about the authenticity/veracity or the adequacy of the previously obtained Customer Identification data.

4. The Company shall periodically update Customer Identification Data after the transaction is entered. A system of periodic review of risk categorization of transaction or business relationship with such periodicity being at least once in six months and need for applying enhanced due diligence measures shall be put in place.

5. For the purpose of verifying the identity of customers at the time of commencement of an account-based relationship, Company, may rely on customer due diligence done by a third party, subject to the following conditions:

(a) Records or the information of the customer due diligence carried out by the third party shall be obtained immediately from the third party or from the Central KYC Records Registry.

(b) Adequate steps are taken by Company to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.

(c) The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.

(d) The third party shall not be based in a country or jurisdiction assessed as high risk.

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

(f) The Company shall maintain a Board-approved policy prescribing a robust due diligence process for requests relating to change of the registered mobile number. In respect of accounts opened through the non-face-to-face mode, transactions shall be permitted only through the mobile number registered at the time of account opening. The Company shall not permit the linkage or substitution of any alternate or additional mobile number after completion of Customer Due Diligence (CDD), except where specifically required under applicable law or regulatory directions.

(g) Where Aadhaar e-KYC authentication cannot be completed due to injury, illness, infirmity, old age, or any other reason permitted under applicable law, the Company may undertake customer identification through the alternative process permitted under the applicable regulatory framework. All such cases shall be recorded in a centralised exception register/database containing the details of the customer, the reason for the exception, the alternative identification process adopted, the date of approval, and the name and employee code/designation of the authorising official. The exception register shall be subject to periodic review by the Internal Audit and Concurrent Audit functions and shall be made available to regulatory or supervisory authorities, including the Reserve Bank of India, upon request.

Beneficial Ownership (BO's)

In view of Rule 9 (1A) of the Prevention of Money Laundering Rules, 2005 every bank /FI as the case may be - shall identify the beneficial owner and take all reasonable steps to verify his identity.

The term "beneficial owner" has been defined as the natural person who ultimately owns or controls a client and/or the person on whose behalf the transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person.

In view of RBI's KYC Direction and Rule 9 (3) of the Prevention of Money Laundering Rules 2005:

i) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

a). "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.

b). "Control" shall include the 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 shareholders agreements or voting agreements.

ii). Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership.

iii). Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

iv). Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

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

Further, while undertaking customer identification, Company shall also be ensured that:

(1) Decision-making functions of determining compliance with KYC norms are not outsourced.

(2) Introduction is not sought while opening accounts.

(3) Optional/additional Officially Valid Document ("OVD") is obtained with the explicit consent of the borrower.

(4) Customers are required to furnish separate proof of address for permanent and current addresses, if these are different. In case the proof of address furnished by the customer is not the address where the customer is currently residing, the Company shall obtain a declaration from the customer of the local address on which all correspondence will be made by the Company.

(5) The local address for correspondence, for which their proof of address is not available, shall be verified through Contact point verification. 'Positive confirmation'.—

(6) In case it is observed that the address mentioned as per 'proof of address' has undergone a change, regulated entities shall ensure that updated proof of address is obtained within a period of three months.

Unique Customer Identification Code ("UCIC"/Customer ID): *he Company shall allot a Unique Customer Identification Code (UCIC)/Customer ID to every customer, including individual and legal entity customers, at the time of establishing a new relationship and shall also assign the same to existing customers, wherever not already allotted. The UCIC/Customer ID shall be used to uniquely identify each customer across all business relationships and products maintained with the Company, prevent duplication of customer records, and facilitate effective customer due diligence, monitoring, and regulatory compliance. The Company shall ensure that only one UCIC/Customer ID is assigned to each customer.*

UCIC Allocation and Customer Deduplication:

a) OXYZO shall assign a Unique Customer Identification Code (UCIC) to every customer at the time of onboarding, as per applicable regulatory requirements.

b) OXYZO system will proactively identify and consolidate multiple customer relationships under a single UCIC using key KYC identifiers such as PAN, OVD and other official documents.

c) To prevent the creation of duplicate customer records, automated deduplication checks leveraging rule-based logic and fuzzy matching algorithms are performed during customer onboarding or when a customer avails a new facility using the same information.

d) In cases where potential duplicate records are identified, they will be verified and following due diligence, merged based on a confirmed match with existing information.

e) All UCIC-related data shall be managed with strict data integrity, confidentiality, and security, in line with OXYZO's data protection and KYC policies.

f) In instances where an individual also operates a sole proprietorship, a separate UCIC may be created for the sole proprietorship/s only if the facility being availed is clearly for business purposes, supported by appropriate documentation of business income.

g) If the sole proprietorship does not maintain a clear distinction from the individual (e.g., no separate business financials), the individual's UCIC shall be used for both personal and business purposes, subject to internal risk assessment and documentation.

III.) MONITORING OF TRANSACTIONS

Ongoing monitoring is an essential element of effective KYC procedures. Monitoring of transactions and its extent will be conducted taking into consideration the risk profile and risk sensitivity of the transaction. Company shall make endeavours to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular/pattern of activity can be identified, Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. Company should pay particular attention to the transactions having high risk. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of Company. Higher risk transaction shall be subjected to intense monitoring. Company shall set key indicators for such transaction basis the background of the customer, country of origin, sources of funds, the type of transactions involved and other risk factors which shall determine the extent of monitoring. Company shall carry out the periodic review of High-risk categorization of transactions and the need for applying enhanced due diligence measures at a periodicity of not less than once in six months.

The extent of monitoring shall be aligned with the risk category of the customer.

iv.) RISK MANAGEMENT:

The Management of the Company under the supervision of the Board of Directors or the Loan and Credit Risk Committee, if any shall ensure that:

- a) an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation.*
- b) It will cover proper management oversight, systems and controls, segregation of duties, training, and other related matters.*
- c) Responsibility will be explicitly allocated within the Company for ensuring that the policies and procedures as applicable to Company are implemented effectively.*
- d) The Company shall devise procedures for creating Risk Profiles of their existing and new Customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction or business relationship.*

- e) Risk-Based Approach: The Company shall adopt a Risk-Based Approach for Customer Due Diligence (CDD) and shall categorise customers into Low, Medium and High Risk categories based on factors including the customer's identity, occupation, social and financial status, nature of business, source of funds, geographical location, products and services availed, delivery channels, transaction profile, and any other relevant risk indicators. The Company may also consider guidance, advisories and public statements issued by the Reserve Bank of India (RBI), the Financial Action Task Force (FATF) and other competent authorities while assessing customer risk. The customer's risk categorisation and the reasons thereof shall remain confidential and shall not be disclosed to the customer. The Company may collect such additional non-intrusive information as may be necessary for effective risk assessment and management.*

Money Laundering and Terrorist Financing Risk Assessment by Company

- (a) 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 and terrorist financing 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 preparing the internal risk assessment, the Company shall take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with REs from time to time.*

- (b) The risk assessment by the company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the RE.*

- (c) The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and should be available to competent authorities and self-regulating bodies.*

Four Key Elements: In accordance with Paragraph 6 of the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2025, this Policy is structured around the four key elements, namely: (i) Customer Acceptance Policy (CAP), (ii) Risk Management, (iii) Customer Identification Procedures (CIP), and (iv) Monitoring of Transactions. The additional provisions contained in this Policy shall be read as integral components supporting the effective implementation of these four key elements.

Annual Review of ML/TF Risk Assessment: The Company shall undertake a comprehensive assessment of its Money Laundering and Terrorist Financing (ML/TF) risks and review the assessment at least annually, or more frequently where warranted by changes in the Company's business activities, products, services, customer profile, delivery channels, or the regulatory environment. The Board of Directors, or a Committee duly authorised by the Board, shall approve the periodicity of such review based on the outcome of the risk assessment.

Group-wide Programme: As a member of a group, the Company shall implement group-wide programmes for combating money laundering and terrorist financing. Such programmes shall include group-wide policies and procedures for sharing information required for customer due diligence, ML/TF risk management, and compliance with applicable AML/CFT requirements, while ensuring appropriate safeguards to maintain the confidentiality, security, and permissible use of information exchanged, including measures to prevent tipping-off.

V.) CUSTOMER DUE DILIGENCE ("CDD"):

"Customer Due Diligence (CDD)" means identifying and verifying the customer and the Beneficial Owner using 'Officially Valid Documents' or 'Identification information as mentioned under section 15 of the RBI's Guidelines, as a 'proof of identity' and a 'proof of address' in the manner provided under this Policy read along with the manner prescribed under the RBI's Guidelines on "Know Your Customer" and Anti-Money Laundering Measures, as amended from time to time. If a customer wishes to open a new account or avail of additional services, no fresh Customer Due Diligence (CDD) procedure will be required. In addition to account-based relationships, the Company shall undertake CDD in respect of any occasional transaction of ₹50,000 and above, whether carried out as a single transaction or as several connected transactions, in terms of the Reserve Bank of India (Know Your Customer (KYC)) (2nd Amendment) Directions, 2025 dated August 14, 2025.

1. Simplified Due Diligence: This is the lowest level of due diligence that can be completed on a customer who does not always pose a high risk to the organization. The customers have less probability of being involved in money laundering or terrorist financing.

2. Enhanced Due Diligence or EDD is required when a customer is perceived to be at a higher risk to the company. A high-risk situation also occurs where there is an increased opportunity for money laundering or terrorist financing through the service or product you are providing. Examples of higher risk customers may include politically exposed people, customers with suspicion of terrorist activities, non-face to face account opening and customers located in high-risk locations.

3. Enhanced Due Diligence for Non-Face-to-Face Onboarding: Where a customer is onboarded through a non-face-to-face mode, other than accounts opened under Paragraph 25 of the RBI Master Direction on KYC, the Company shall offer V-CIP as the preferred mode of customer identification. The Company shall obtain and verify the customer's PAN, ensure that the first transaction is a credit received from the customer's own KYC-compliant bank account, verify the customer's current address through positive confirmation, classify such customer as High Risk, and subject the account to enhanced transaction monitoring until the customer's identity is verified through a face-to-face interaction or V-CIP, in accordance with the applicable regulatory requirements.

4. Updation/Periodic Updation of KYC

Company shall have a risk-based approach for periodic updation of KYC. However, periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation. Policy in this regard shall be documented as part of Company's internal KYC policy duly approved by the Board of Directors of Company or any committee of the Board to which power has been delegated.

The Company shall provide customers with the facility to undertake KYC updation or periodic

updatation at any of its branches and through such other channels as may be made available by the Company, in accordance with the applicable regulatory requirements.

In case no change in KYC information: In case of no change in the KYC information, a self-declaration from the customer in this regard shall be obtained through customer's email-id registered with the Company or from customer's mobile number registered with the Company, digital channels (such as online application of Company), On letter head, etc.

Advance intimation and reminders: Prior to the due date for periodic updatation of KYC, the Company shall give at least three advance intimations, including at least one intimation by letter, at appropriate intervals, through the communication options/channels available to it. Subsequent to the due date, the Company shall give at least three reminders, including at least one reminder by letter, at appropriate intervals, to customers who have still not complied with the requirement despite advance intimations. Each intimation and reminder shall, inter alia, contain easy-to-understand instructions for updating KYC, the escalation mechanism for seeking help and the consequences of failure to update KYC in time, and the issue of every such intimation/reminder shall be duly recorded in the Company's system against each customer for audit trail.

Change in Address: Where there is a change only in the customer's address and there is no change in any other Customer Due Diligence (CDD) information, the Company may obtain a self-declaration from the customer regarding the new address. The declared address shall be verified through positive confirmation within two months of receipt of the self-declaration by appropriate means, including an address verification letter, contact-point verification, delivery of communications or other suitable verification mechanisms, in accordance with the applicable regulatory requirements.

Minor becoming major: For customers for whom an account was opened while they were minors, the Company shall obtain fresh photographs on their becoming major and ensure that CDD documents as per current standards are available, carrying out fresh KYC wherever required.

Aadhaar OTP-based e-KYC for Updation: The Company may use Aadhaar OTP-based e-KYC in non-face-to-face mode for updation or periodic updatation of Customer Due Diligence (CDD) information. The restrictions applicable to accounts opened through Aadhaar OTP-based e-KYC under Paragraph 25 of the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2025 shall not apply to such updation or periodic updatation.

Updatation of KYC – Legal Entity Customers: In the case of customers other than individuals, where there is no change in the KYC information or the details of the Beneficial Owner(s), the Company shall obtain a self-declaration from the customer confirming the same and shall verify the accuracy of the Beneficial Ownership information maintained in its records. Where there is any change in the KYC information or the Beneficial Ownership details, the Company shall undertake the Customer Due Diligence (CDD) process applicable to onboarding a new legal entity customer, in accordance with the applicable regulatory requirements.

Updatation of Customer Documents: The Company shall advise its customers to promptly inform the Company of any change in the documents submitted at the time of establishing the business relationship or thereafter, as applicable. Customers shall submit the updated documents to the Company within **30 days** of such change to enable timely updatation of the Company's records in accordance with the applicable provisions of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 and the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2025.

PAN / Form 97 for Existing Customers: The Company shall obtain the Permanent Account Number (PAN) or Form 97, as applicable, from existing customers within the timeline prescribed under the applicable law. Where a customer fails to furnish PAN or Form 97

within the prescribed timeline, the Company may temporarily cease operations in the account after providing an accessible notice and a reasonable opportunity of being heard. The Company may, in accordance with its Board-approved policy, permit suitable relaxations for customers who are unable to comply due to old age, injury, illness or infirmity. Such accounts shall be subject to enhanced monitoring until the required information is furnished.

In view of CDD, RBI came up with detailed guidelines issued on Customer Due Diligence (CDD) for Non-banking Financial Companies by the Basel Committee on Banking Supervision. 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 is formulated and put in place. Accordingly, Company has in place Board approved Anti Money Laundering Policy and KYC Norms (the Policy). Based on the experience gained over the past years, the Policy is proposed to be reviewed and improved keeping in view the Master Circular on the subject issued by RBI on 1 July 2014, the revised guidelines vide circular no RBI/2014- 15/330 DNBR (PD).CC. No. 005 /03.10.42/2014-15 dated 1 Dec 2014 and the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Directions, 2025 dated November 28, 2025, which repealed and replaced the Master Direction – Know Your Customer (KYC) Direction, 2016, as amended from time to time including by the Reserve Bank of India (Non-Banking Financial Companies – Know Your Customer) Amendment Directions, 2025 dated December 29, 2025 (the "KYC Directions, 2025"), ('RBI's Guidelines') which is to be read along with the extant Directions issued by the RBI in this regard or any other applicable law in force. The Company shall further ensure compliance with the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, including operational instructions issued in pursuance of such amendment(s) and it shall not outsource decision-making functions of determining compliance with KYC norms.

Objectives for Enhanced Due Diligence in Company:

The Company shall adopt Enhanced Due Diligence (EDD) measures for customers identified as presenting a higher risk of money laundering, terrorist financing, proliferation financing, fraud, or other financial crime, in accordance with the risk-based approach prescribed under the applicable regulatory framework. The objectives of EDD shall include the following:

- a) To identify and apply enhanced due diligence measures to customers who, based on the Company's risk assessment, are classified as high risk and warrant enhanced scrutiny.**
- b) To ensure that high-risk customer relationships are established, continued and monitored only after appropriate due diligence, risk assessment, approvals and enhanced ongoing transaction monitoring, in accordance with the Company's internal policies.**
- c) To obtain additional information and documentation, where considered necessary, to establish the customer's identity, source of funds, source of wealth, nature of business, purpose of the relationship and expected account activity.**
- d) To decline the establishment of a business relationship, refuse to undertake a transaction, or discontinue an existing relationship where the Company is unable to satisfactorily complete the required Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD), or where the customer poses an unacceptable legal, regulatory or reputational risk.**
- e) To periodically review the risk categorisation of customers and determine**

whether enhanced due diligence measures should be continued, strengthened or modified based on the customer's risk profile and transactional behaviour.

- f) **To monitor the end use of funds, wherever applicable, in accordance with the Company's credit and monitoring policies, particularly for customers or transactions identified as presenting higher ML/TF risks, and to investigate or report unusual or suspicious transactions in accordance with applicable AML/CFT requirements.**

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR):

For the purpose of compliance of the provision of Rule 9(1A) of PML Rules as amended from time to time, Company shall capture customer's KYC information for sharing with the Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI) platform as authorised by Government of India vide Gazette Notification No. S.O. 3183(E) dated November 26, 2015 and shall act as Central KYC Records Registry (CKYCR). The Company shall upload the customer's KYC records on CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'individuals' and 'Legal Entities' as the case may be. Once the KYC identifier is generated by CKYCR, the company shall communicate the same to the individual/Legal Entity as the case may be.

The Company shall capture the customer's KYC records and upload the same to the Central KYC Records Registry (CKYCR) within 10 (ten) working days from the commencement of an account-based relationship with the customer or within such period as may be notified by the Central Government from time to time, in accordance with Rule 9(1A) of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

The Company shall ensure that the KYC records uploaded to CKYCR are accurate, complete and kept up to date. Where the Company is the Regulated Entity that has last uploaded or updated the customer's KYC records in CKYCR, it shall be responsible for verifying the identity and/or address of the customer, as applicable. Accordingly, where the Company downloads and relies on such records from CKYCR, it shall not be required to re-verify the authenticity of the customer's identity and/or address, provided the KYC records downloaded from CKYCR are current and compliant with the PML Act, 2002 / PML Rules, 2005. The Company shall, however, remain responsible for all aspects of the CDD procedure and the provisions of the KYC Directions, 2025, except verification of the identity and/or address of the customer.

CDD Procedure and sharing KYC information with Central KYC Records Registry (CKYCR) shall be undertaken as per Section 56 (Chapter X).

The Company shall perform the periodic updation of the customer's KYC records and upload/update the same on CKYCR portal as specified in the corresponding provisions of the KYC Directions, 2025 or earlier when the updated KYC information is obtained/received from the customer. During the periodic updation, the customers are migrated to the current CDD standard of the company. If a customer submits a KYC identifier at the time establishing new relationship with the company and shall give their explicit consent to download records from CKYCR, then the company shall retrieve the KYC records online from the CKYCR using the KYC identifier and the customer shall not be required to submit the same KYC records or information or any other additional identification documents or details, unless:

- (i) there is a change in the information of the customer as existing in the records of CKYCR.*
- (ii) the KYC record or information retrieved is incomplete or is not as per the current applicable KYC norms*
- (iii) the current address of the customer is required to be verified.*
- (iv) the validity period of downloaded documents has lapsed;*

- (v) *the company considers it necessary in order to verify the identity or address of the customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.*

Customer shall also provide Company with the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962 and such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company.

6. **Suspicion of Money Laundering or Terrorist Financing:** *Where the Company forms a suspicion that a customer or transaction may be associated with money laundering, terrorist financing or proliferation financing, and reasonably believes that undertaking or continuing the Customer Due Diligence (CDD) process may result in tipping-off the customer, the Company shall refrain from pursuing the CDD process to the extent necessary and shall consider filing a Suspicious Transaction Report (STR) with the Financial Intelligence Unit – India (FIU-IND) in accordance with the applicable provisions of the Prevention of Money-laundering Act, 2002, the Prevention of Money-laundering (Maintenance of Records) Rules, 2005, and the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2025.*
7. **Ongoing due diligence - transactions to be monitored:** *The Company shall necessarily monitor large and complex transactions (including RTGS) with unusual patterns and no apparent economic rationale, transactions exceeding thresholds prescribed for specific account categories, high account turnover inconsistent with the balance maintained, and deposits of third-party cheques / drafts followed by large cash withdrawals.*
8. **Money mules:** *The Company shall undertake diligence and meticulous monitoring to identify accounts operated as 'money mules' and file STRs with FIU-IND; failure to file an STR where an account is established to be that of a money mule shall be deemed non-compliance with the KYC Directions, 2025.*
9. **Client accounts opened by professional intermediaries:** *Where accounts are opened through professional intermediaries, the Company shall identify the clients and beneficial owners (including for sub-accounts), shall not open accounts of intermediaries bound by client-confidentiality that prohibits disclosure of client details, and shall retain ultimate responsibility for knowing the customer.*
10. **Quoting of PAN :** *PAN or Form No. 97, as applicable, shall be obtained and verified from customers while undertaking transactions specified under Rule 159 of the Income-tax Rules, 2026, as amended from time to time.*

Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS): *Company shall take necessary steps for complying with the reporting requirements and shall develop Information Technology framework to ensure compliance as applicable.*

VI.) Training Programme:

Company shall have an ongoing employee training programs so that the members of the staff are adequately trained in KYC/ AML/ CFT procedures. Training requirements shall have different focuses for front line staff, compliance staff and officer/ staff dealing with new Customers so that all those concerned fully understand the rationale behind the KYC Policies and implement them consistently.

VII.) Internal Control System:

The Company's Internal Audit and Compliance functions will evaluate and ensure adherence to the KYC Policies and procedures. As a general rule, the compliance function will provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The Company under the supervision of the Board shall ensure that the audit function is staffed adequately with skilled individuals. Internal Auditors will specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard.

VIII. Quarterly Audit Reporting: *The Company shall maintain a concurrent and/or internal audit system to periodically verify compliance with the applicable KYC/AML/CFT policies, procedures and regulatory requirements. The audit observations, together with the status of compliance and corrective actions taken, shall be submitted to the Audit Committee of the Board on a quarterly basis for its review and oversight.*

Further, the Company shall have an adequate screening mechanism in place as an integral part of their recruitment/ hiring process of personnel so as to ensure that person of criminal nature/ background do not get an access, to misuse the financial channe

IX Record Keeping:

1. Maintenance of records of transactions: *The Company shall maintain proper record of the transactions as required under Section 12 of the PMLA read with Rule 3 of the Prevention of Money Laundering Rules, 2005 (PML Rules) as mentioned below:*

- 1. All cash transactions of the value of more than Rupees Ten Lakhs (Rs. 10, 00, 000/-) or its equivalent in foreign currency, though by policy the Company neither accept cash deposits nor in foreign currency.*
- 2. All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakhs (Rs. 10,00,000/-) or its equivalent in foreign currency where such series of transactions have taken place within a month.*
- 3. All transactions involving receipts by non-profit organizations of Rupees ten lakhs or its equivalent in foreign currency.*
- 4. 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 has taken place, any such transactions.*
- 5. All suspicious transactions whether or not made in cash and in manner as mentioned in the PML Rules framed by the Government of India under PMLA. An Illustrative List of suspicious transaction pertaining to financial services is given in Annexure II.*

2. Records to contain the specified information *The Records referred to above in Rule 3 of PML Rules to contain 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.*
- d) the parties to the transaction.*

3. Maintenance and preservation of records *Section 12 of PML Act requires the Company to maintain records as under:*

- a) Maintain all necessary records of transactions between the Company and the Customer, both domestic and international, for at least five years from the date of transaction.*
- b) Preserve the records pertaining to the identification of the customers and their addresses obtained during the course of Business relationship, for at least five years*

after the business relationship is ended.

- c) Make available the identification records and transaction data to the competent authorities upon request.*
- d) The Company shall take appropriate steps to evolve a system for proper maintenance and preservation of information in a manner (in hard and/or soft copies) that allows data to be retrieved easily and quickly whenever required or as/when requested by the competent authorities.*
- e) Where a Customer is a non-profit organisation, the Company shall register the details of such Customer on the DARPAN Portal of NITI Aayog, if not already registered, and shall maintain such registration records for a period of five years after the business relationship with the Customer has ended or the account has been closed, whichever is later.*

X Appointment of Principal Officer:

To ensure effective implementation and coordination across different functions of policy company shall designate a senior employee as 'Principal Officer' (PO) who shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. PO shall maintain close liaison with enforcement agencies, NBFCs and any other institution which are involved in the fight against money laundering and CFT. Further, Designated Director shall be responsible to ensure overall compliance with the obligations imposed under Chapter IV of the PML Act and the Rules.

The Principal Officer shall be independent and report directly to the senior management or to the Board of Directors. Principal Officer is responsible for monitoring KYC/AML compliance at operational units, escalation of suspicious transactions reported by branches through STRs and sharing of information as required under the law. He will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The role and responsibilities of the Principal Officer include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made there under, as amended from time to time. The Principal Officer is responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by Non-Profit Organisations of value more than Rupees ten lakh or its equivalent in foreign currency to FIU-IND. The Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information. The Principal Officer under PMLA Act, 2002 shall be the competent authority for fixing the thresholds for generation of AML alerts and the periodicity of reviewing the alerts shall be at half yearly intervals or as and when required.

XI Reporting to Financial Intelligence Unit – India:

Reporting of Transactions

As per the provisions of the Prevention of Money Laundering Act (PMLA), 2002, and the associated Rules, the Principal Officer is mandated to report all cash transactions, suspicious transactions, and transactions involving counterfeit currency to the Financial Intelligence Unit - India (FIU-IND). Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:

- *Identity of Client*
- *Suspicious Background*
- *Multiple Accounts*
- *Activity in Accounts*
- *Nature of Transactions*

➤ *Value of Transactions*

The types of transactions and the procedures for reporting are outlined below:

Cash Transaction Reporting (CTR) Framework

OXYZO, as a policy, does not accept cash or postal orders from clients. However, individual cash transactions of Rs. 2 lakh and above by a single client will be reviewed for potential suspicious activity.

The following transactions are reportable to FIU-IND:

- 1. All individual cash transactions of Rs. 10 lakh or more (or equivalent in foreign currency).*
- 2. Series of interconnected cash transactions, each below Rs.10 lakh, which collectively exceed Rs. 10 lakh in a calendar month.*
- 3. Any cash transaction involving the use of forged or counterfeit currency or forgery of a valuable security.*

Note: For identifying interconnected transactions, all individual cash credits and debits in an account during a month must be considered separately. While filing the CTR, details of individual transactions below ₹50,000 need not be reported.

The CTR for each month must be submitted electronically to FIU-IND by the 15th of the following month.

Suspicious Transaction Reporting (STR) Framework

A suspicious transaction includes any attempted or completed transaction, whether or not involving cash, that meets any of the following criteria:

- Raises reasonable suspicion of involvement of proceeds of crime listed in the PMLA Schedule;*
- Appears unusually complex or lacks legitimate economic rationale;*
- Shows inconsistencies with the customer's known profile or transaction behaviour;*
- Indicates possible links to terrorist financing.*

All reporting shall be conducted exclusively through electronic means, with strict adherence to confidentiality protocols. A robust transaction monitoring system has been implemented to trigger alerts for transactions that deviate from the customer's assigned risk category, updated profile, or other defined risk parameters, thereby enabling timely identification and reporting of suspicious activities.

Technology Framework to Identify Suspicious Transactions

4. Due Diligence on Client and Group Entities

- Conduct comprehensive due diligence to identify the borrower's group entities, related parties and beneficial ownership structures.*
- Assess whether disbursed funds are subsequently transferred to group companies or related parties.*
- Investigate whether suppliers or counterparties exhibit characteristics of shell entities or appear to be under the indirect control or influence of the borrower or their affiliates.*

5. Tracing of Fund Flow Post-Disbursement

- *Monitor the flow of funds from the borrower's account post-term loan disbursement to detect unusual or circular routing of funds to group entities, vendors, or other affiliates.*
- *Evaluate whether such fund flows align with the stated purpose of the loan and report any inconsistencies as potential misuse or diversion of funds.*

6. Review During Loan Renewal or Revision

- *At the time of loan renewal or revision, review updated banking information to identify any **reverse transactions** or repayments made by suppliers to the borrower.*
- *Special attention must be paid to transactions involving funds previously disbursed under the loan to detect collusive or circular arrangements.*

7. GST Compliance Monitoring

- *The company may periodically verify the GST return filing status of both the borrower and their key suppliers.*
- *Identify non-filing, mismatch of data, or repeated compliance issues as red flags indicating potential fraud or operational risk.*

8. Document Integrity and Tampering Checks

- *Implement system-assisted checks to detect manipulation or tampering of documents such as invoices, purchase orders, and contracts.*
- *Flag and escalate any discrepancies or anomalies for further investigation.*

9. Sanctions and Political Exposure Screening

- *Continuously screen customers and their counterparties against updated global sanctions lists and politically exposed persons (PEPs) databases.*
- *Transactions or relationships involving such entities should be escalated for enhanced review and compliance evaluation.*

10. Business Profile Alignment

- *Validate that the declared nature of business of the borrower's suppliers aligns with the goods or services intended to be procured.*
- *Any significant divergence between declared and actual business activities shall be treated as a red flag and investigated accordingly.*

11. Transaction Pattern Analysis

- *Utilize transaction monitoring tools to identify payments that are unusually large or inconsistent with the borrower's historical transaction behavior, particularly following a term loan disbursement.*
- *Such anomalies should be evaluated in the context of possible fund diversion, fraud, or money laundering.*

Key guidelines related to STRs:

- *An STR shall be filed within 7 working days of concluding that a transaction is suspicious.*

- OXYZO shall take all reasonable steps to ensure timely review and escalation once a potential STR is identified.
- The Principal Officer shall document the rationale for the suspicion, in consultation with the Chief Risk Officer, Chief Credit Officer, and other relevant officials.
- The Principal Officer is responsible for submitting both CTRs and STRs in the format prescribed by FIU-IND, strictly through electronic means.
- Confidentiality shall be maintained at all levels. STRs shall not be disclosed to the customer or any unauthorized person (i.e., no tipping-off).
- OXYZO shall report all suspicious attempts, including incomplete or failed transactions, regardless of the transaction amount.
- STRs will be filed if there are reasonable grounds to believe that the transaction involves proceeds of crime, even if the transaction value is below thresholds mentioned in Part B of the PMLA Schedule.

An STR may also be filed where OXYZO is unable to complete CDD procedures due to customer non-cooperation or submission of unreliable documents/information.

The PO shall report information relating to cash and suspicious transactions, if detected, to the Director, Financial Intelligence Unit India (FIUIND) as advised in terms of the PML Rules, in the prescribed formats as designed and circulated by RBI on time to time basis:

The employees of Company shall maintain strict confidentiality of the fact of furnishing/reporting details of suspicious transactions.

GENERAL:

A). Customer Education:

Company shall educate Customers on the objectives of the KYC programme so that Customer understands and appreciates the motive and purpose of collecting such information. The Company shall prepare specific literature/ pamphlets, terms and conditions etc. so as to educate the Customer about the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with Customers.

B). Introduction of new technologies:

Company shall pay special attention to any money laundering threats that may arise from new or developing technologies including online transactions that may favor anonymity, and take measures, if need, to prevent their use in money laundering. Company shall ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode for any amount is affected by cheques and not against cash payment.

C). Applicability to Branches and Subsidiaries outside India:

This Policy shall also be applicable to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit as and when the Company opens overseas branches. Where the regulatory requirements of the host country and those applicable under Indian law differ, the Company shall apply the more stringent of the two standards, to the extent permitted by the laws of the host country. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought to the notice of RBI for guidance.

D). Termination of Financing/Business Relationship:

Where Company is unable to apply appropriate KYC measures due to non-furnishing of information and/or non-operation by the Customer, Company may terminate Financing/Business Relationship after issuing due notice to the Customer explaining the

reasons for taking such a decision. Such decision shall be taken with the approval of Board of Directors or any other person authorized for the purpose.

E). KYC for the Existing Customers:

While the KYC Policy will apply to all new Customers, the same would be applied to the existing Customers on the basis of materiality and risk. However, transactions with existing Customers would be continuously monitored for any unusual pattern in the operation of the accounts.

F). Updation in KYC Policy of Company:

Board of Directors shall make the necessary amendments/modifications in the KYC/ AML/ CFT Policy or such other related guidance notes of Company, to be in line with RBI or such other statutory authority's requirements/updates/ amendments from time to time.



ANNEXURE 1

Customer Identification Procedure Features to be verified and Documents that may be obtained from Customers.

<u>Sl.No.</u>	<u>Officially Valid Document (OVD)</u>	<u>Proof of Identity</u>	<u>Proof of Address*</u>
<u>1</u>	<u>Driving Licence</u>	<u>✓</u>	<u>✓</u>
<u>2</u>	<u>Valid Passport</u>	<u>✓</u>	<u>✓</u>
<u>3</u>	<u>Voter Identity Card issued by the Election Commission of India</u>	<u>✓</u>	<u>✓</u>
<u>4</u>	<u>Proof of possession of Aadhaar Number (where obtained in accordance with applicable law)</u>	<u>✓</u>	<u>✓</u>
<u>5</u>	<u>Job Card issued by NREGA, duly signed by an officer of the State Government</u>	<u>✓</u>	<u>✓</u>
<u>6</u>	<u>Letter bearing the name and address of the customer issued by the National Population Register containing details of name and address</u>	<u>✓</u>	<u>✓</u>

Photograph: In accordance with the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2025, the Company shall obtain a recent photograph or a live digitally captured photograph of every individual customer as part of the Customer Due Diligence (CDD) process. In the case of legal entity customers, the Company shall obtain the photograph(s) of the authorised signatory(ies), Beneficial Owner(s), and such other individual(s) as may be required under the applicable regulatory requirements.

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: -

1. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
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;

The customer shall submit OVD with current address within a period of three months of submitting the documents specified' above



Submitting 'Officially Valid Documents' - Change in name on account of marriage or otherwise: A document shall be deemed to an "officially valid document" even if there is a change in the name subsequent to its issuance, provided it is supported by a marriage certificate issued by the State Government or a Gazette notification or a Affidavit duly attested by Gazetted Officer, indicating such a change of name".

Accordingly a copy of marriage certificate issued by the State Government or Gazette notification or a Affidavit duly attested by Gazetted Officer, indicating change in name together with a certified copy of the 'officially valid document' (as indicated above) in the existing name of the person while establishing an account based relationship or while undergoing periodic updation exercise may be accepted [Simplified procedure" means the procedure for undertaking customer due diligence in respect of customers, who are rated as low risk by the Company and who do not possess any of the six officially valid documents, with the alternate documents as prescribed above]

'Certified copy of officially valid document' shall have the meaning assigned to it under the KYC Directions, 2025, as issued by RBI.

"Proof of possession of Aadhaar number" shall be submitted in such form as permitted under the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act (including the rules, regulations and notifications issued thereunder) and in compliance with the KYC Directions, 2025 issued by RBI.

"Beneficial Owners" shall mean such persons identified by the applicant in the application form in terms of Rule 9 (3) of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

Constitution	KYC DOCUMENT
Proprietorship	Any two of the following documents in the name of the proprietary concern needs to be obtained if the loan is in the name of Proprietorship Firm (Main Applicant) 1. Registration certificate including Udyam Registration Certificate (URC) issued by the Government 2. Certificate/licence issued by the municipal authorities under Shop and Establishment Act. 3. Sales and income tax returns. 4. CST/VAT/ GST certificate (provisional/final). 5. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. 6. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. 7. 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. 8. Utility bills such as electricity, water, landline telephone bills (should not be more than two months old) Other than the above mentioned, PAN of the Proprietor In cases where the REs is satisfied that it is not possible to furnish two such documents, REs may, at their discretion, accept



	only one of those documents as proof of business/activity. Provided REs undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.
Partnership Firm	The certified copies of each of the following documents shall be obtained: 1. Registration certificate 2. Partnership deed 3. Permanent Account Number of the partnership firm and 4. KYC of beneficial owner. 5. KYC of managers, officers or employees, as the case may be, holding a Power of attorney to transact on its behalf 6. the names of all the partners and address of the registered office, and 7. the principal place of its business, if it is different.
Trust	The certified copies of each of the following documents shall be obtained: 1. Registration certificate 2. Trust deed 3. Permanent Account Number or Form No.60 of the trust 4. KYC of beneficial owner 5. KYC of managers, officers or employees, as the case may be, holding a Power of attorney to transact on its behalf 6. the names of the beneficiaries, trustees, settlor and authors of the trust 7. the address of the registered office of the trust; and 8. list of trustees and documents, as specified in Section 16, for those discharging the role as trustee and authorised to transact on behalf of the trust.
AOP (Association of Persons) /Unincorporated Incorporations	The certified copies of each of the following documents shall be obtained: 1. Resolution of the managing body of such association or body of individuals 2. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals 3. Power of attorney granted to transact on its behalf 4. KYC of beneficial owner 5. KYC of managers, officers or employees, as the case may be, holding a Power of attorney to transact on its behalf 6. Such information as may be required by the Regulated Entity to collectively establish the legal existence of such an association or body of individuals.
Disclaimer: As a Risk Policy Company does not encourage working with AOP/Unincorporated corporations but defining KYC document as the case may arise during future course of business as a credit enhancement technique.	



 **Contact:** +91-7353013499
 **Email:** getsupport@oxyzo.in
 **Website:** www.oxyzo.in

Companies (Pvt Ltd /Ltd	<i>The certified copies of each of the following documents shall be obtained:</i> 1. Certificate of incorporation
------------------------------------	---

/OPC)	2. Memorandum and Articles of Association 3. Permanent Account Number of the company 4. A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf 5. Documents, relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf 6. the names of the relevant persons holding senior management position; and 7. the registered office and the principal place of its business, if it is different.
-------	--

Common Mandatory Documents:

1. Recent photograph of Applicant, Co- Applicant, Beneficial Owners or Authorized Persons holding an attorney to transact on behalf of the Applicant
2. GST Registration Certificate of the Entity
3. Certified copy of officially valid documents (OVD) as proof of identity and address of Authorized Persons and Co-Applicant
4. Copy of below mentioned documents of the individual who is a beneficial owner holder related to any legal entity:
 - a) the Aadhaar number where,
 - i. he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
 - ii. he decides to submit his Aadhaar number voluntarily to a bank or any RE notified under first proviso to sub-section (1) of section 11A of the PML Act; or
 - (aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
 - (ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any OVD or the equivalent e-document thereof containing the details of his identity and address; and
 - (b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
 - (c) such other documents including in respect of the nature of business and financial status of the customer, or the equivalent e-documents thereof as may be required by the Company

Where a customer submits proof of possession of Aadhaar number, the Company shall ensure that such customer redacts or blackout his Aadhaar number before submitting the same to the Company.

Note:

1. Photograph of the applicant s mandatory, however digitally captured photograph is acceptable.
2. The KYC documents/ Officially Valid documents can be verified by the employees/ representatives/ service providers of OXYZO.
5. KYCs of all beneficial owners shall be collected which means:
 - Ownership of more than 10% shares in a company
 - More than 10% of ownership in other forms of entities (LLP / Partnership firms etc).

Where the customer or the owner of the controlling interest is

- (i) an entity listed on a stock exchange in India, or
- (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or

- (iii) *it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.*

The identity of the Entity(ies)/Beneficial Owners may be confirmed through the use of identity documents via online services or other resources provided by issuing authorities, particularly in specific instances, as prescribed by RBI.

In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

ANNEXURE II

Suspicious Transaction Report:

The Prevention of Money laundering Act, 2002 and the Rules notified thereunder require every intermediary to furnish details of suspicious transactions whether or not made in cash. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith:-

- *gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or*
- *appears to be made in circumstances of unusual or unjustified complexity; or*
- *appears to have no economic rationale or bonafide purpose.*

Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:

- **Identity of Client**
- **Suspicious Background**
- **Multiple Accounts**
- **Activity in Accounts**
- **Nature of Transactions**
- **Value of Transactions**

Risk Mitigation Measures:

Our nature of lending and products majorly purchase financing wherein we pay to supplier account against purchase of Raw material and services which automatically ensures the end use of funds. In Business Loans we take End Use certificate from borrow. In addition to this we review followings: -

- *Supplier onboarding*
- *Market Feedback*
- *Supplier ledger and Bank statements*
- *Cross references*

Periodic risk monitoring through Bank statements and GST
