Protium

KNOW YOUR CUSTOMER (KYC), ANTI-MONEY LAUNDERING (AML), COMBATTING FINANCING OF TERRORISM (CFT) AND CUSTOMER ACEPTANCE POLICY (CAP*)*

Created By	Compliance Team
Reviewed by	Business/Operations/
Review Period	Mr. Amit Gupta
Approved by Board of Directors	Annual
Version	05.05.2026
Formation	Version 8

Sr. No.	Version	Revision Summary	Approving Authority	Effective Date
1	Version 1	Created	Board of Directors	06.01.2020
2	Version 2	Structured as per regulation	Board of Directors	04.10.2021
3	Version 3	Structured as per regulation	Board of Directors	27.09.2022
4	Version 4	Structured as per regulation	Board of Directors	20.07.2023
5	Version 5	Structured as per regulation	Board of Directors	28.10.2023
6	Version 6	Policy name updated and structure realigned to meet regulatory requirements	Board of Directors	18.10.2024
7	Version 7	Annual review with minor changes	Board of Directors	14.08.2025
8	Version 8	Annual review with minor changes	Board of Directors	05.05.2026

Contents

1. INTRODUCTION AND BACKGROUND

Protium Finance Limited (hereinafter referred to as 'the Company' or 'Protium'), is a Non-Banking Financial Company Investment and Credit Company categorized as Middle Layer ("NBFC ICC ML"). The Company provides both secured and unsecured loans to consumers and educational institutions, and also extends secured and unsecured loans to Micro, Small, and Medium Enterprises (MSMEs) across India.

Under the provisions of the Prevention of Money-Laundering Act, 2002 ("PMLA") and the Prevention of Money- Laundering (Maintenance of Records) Rules, 2005 ("PML Rules"), as notified and further amended from time to time, regulated entities like banks and NBFCs are required to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise. They are also required to monitor these transactions closely. Additionally, these entities are required to take steps to ensure implementing the provisions of the aforementioned Act, Rules and Ordinance, including operational instructions issued in pursuance of such amendment(s).

Further, as per Para 4 (a) of the 'Reserve Bank of India (Non-Banking Financial Companies - Know Your Customer (KYC)) Directions, 2025 ' ("RBI KYC Directions"), the Company being an NBFC is required to have a Know Your Customer Policy approved by their respective Board of Directors ("Board").

Accordingly, the Company has adopted this KYC/AML/CFT and CAP Policy ('the Policy') in line with the requirements of the RBI's Master Direction (Non-Banking Financial Companies - Know Your Customer (KYC)) Direction, 2025, as updated from time to time. This policy has been duly approved by the Board of Directors of the Company.

This Policy framework shall seek to ensure compliance with PMLA and PML Rules, including regulatory instructions in this regard. It shall provide a bulwark to the Company against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, the Company shall also endeavor to adopt the relevant best practices taking into account the standards and guidance notes issued by the Financial Action Task Force ("FATF"), for managing risks better. The Company shall apply enhanced due diligence measures, which are effective and proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

The Company shall ensure Compliance with the provisions of Foreign Contribution (Regulation) Act, 2010. Further, the Company shall ensure meticulous compliance with any instructions / communications on the matter issued from time to time by the RBI based on advice received from the Ministry of Home Affairs, Government of India.

2. OBJECTIVE AND SCOPE OF THE POLICY

With the above background, the following are the objectives of the Policy:

a) To ringfence the Company's business activities/ products/ services from being used as a channel for Money Laundering("ML")/ Terrorist Financing("TF').
b) To establish a framework for implementing appropriate Anti- Money Laundering ("AML") procedures and controls in the business operations of the Company.
c) To ensure compliance with the applicable laws and regulations, from time to time.
d) To protect the Company's reputation.
e) able the Company to know / understand its customer and their financial dealings better, which in turn helps to manage its risks prudently.

f) establish a proper Customer Due Diligence ("CDD") process before on-boarding Customers.

g) comply with all the legal and regulatory obligations in respect of KYC, AML and CFT measures.

3. APPLICABILITY

The Policy shall be applicable to the Company including all its branches, its customers and all the products and services offered by it and all the other relevant stakeholders of the Company. This Policy also apply to any third parties relied upon or used by the Company to perform any of the requirements prescribed under the RBI KYC Directions. This Policy shall also be made applicable to the other group entities of the Company for the purpose of discharging obligations of the Company or such entities under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002 (15 of 2003), wherever applicable. This version of the Policy shall supersede all existing/ previous versions of the Policy.

4. DEFINITION OF THE TERMS USED IN THIS POLICY:

The terms herein shall bear the meanings assigned to them below:

a. Terms bearing meaning assigned in terms of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005:

i. **"Aadhaar Act"** means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

ii. "**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).

iii. "**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.

iv. "**Authentication**", in the context of Aadhaar authentication, means the process as defined under subsection (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

v. **Beneficial Owner** (BO) –

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

Explanation- For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 10 percent of the shares or capital or profits of the company.

2. "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.

b. Where the **customer is a partnership firm**, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 percent of capital or profits of the partnership or who exercises control through other means.

Explanation "control" shall include the right to control the management or policy decision.

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

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

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

vi. "**Board**" shall mean the Board of Directors of the Company.

vii. "**Certified Copy**" - Obtaining a certified copy by the RE 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 authorized officer of the RE as per the provisions contained in the Act.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy, certified by any one of the following, may be obtained:

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

viii. "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.

ix. "Designated Director" means a person designated by the RE to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the Rules and shall include:

a. the Managing Director or a whole-time Director, duly authorized by the Board of Directors, if the RE is a company,

b. the Managing Partner, if the RE is a partnership firm,

c. the Proprietor, if the RE is a proprietorship concern,

d. the Managing Trustee, if the RE is a trust,

e. a person or individual, as the case may be, who controls and manages the affairs of the RE, if the RE is an unincorporated association or a body of individuals, and

f. a person who holds the position of senior management or equivalent designated as a 'Designated Director' in respect of Cooperative Banks and Regional Rural Banks.

Explanation - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.

x. "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the Act.

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

xii. "FIU-IND" or "FIU" shall mean Financial Intelligence Unit.

xiii. "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.

xiv. "Group" – The term "group" shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act,1961 (43 of 1961).

xv. "Group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes,- (i) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or (ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.
"**Know Your Client (KYC) Identifier**" means the unique number or code assigned to a customer by the Central KYC Records Registry.

xvi. "Non-profit organisations" (NPO) means any entity or organisation, constituted for religious or

charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under Section 8 of the Companies Act, 2013 (18 of 2013).

xvii. "**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 proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.

b) where the OVD furnished by the customer does not have updated address, the following documents or the equivalent e-documents thereof shall be deemed to be OVDs for the limited purpose of proof of address:-

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

ii. property or Municipal tax receipt;

iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with such employers allotting official accommodation;

c) the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above

d) where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

xviii. "**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).

xix. "**Person**" has the same meaning assigned in the Act and includes:

a) an individual,

b) a Hindu undivided family,

c) a company,

d) a firm,

e) an association of persons or a body of individuals, whether incorporated or not,

f) every artificial juridical person, not falling within any one of the above persons (a to e), and

g) any agency, office or branch owned or controlled by any of the above persons (a to f).

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

xxi. "**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.

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

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

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.

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

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

a) opening of an account;

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

c) the use of a safety deposit box or any other form of safe deposit;

d) entering into any fiduciary relationship;

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

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

Terms bearing meaning assigned in this Policy, unless the context otherwise requires, shall bear the meanings assigned to them below:

i. "**Customer**" means a person who is engaged in a financial transaction or activity with a Regulated Entity (RE) and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

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

iii. "**Customer Due Diligence** (CDD)" means identifying and verifying the customer and the beneficial owner using reliable and independent sources of identification.

iv. Explanation – The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include:

v. Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

vi. Taking reasonable steps to understand the nature of the customer's business, and its ownership and control;

vii. Determining whether a customer is acting on behalf of a beneficial owner, and identifying the beneficial owner and taking all steps to verify the identity of the beneficial owner, using reliable and independent sources of identification.

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

ix. "**FATCA**" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

x. "KYC" means KYC is a process by which a Regulated Entity (RE), including a bank, obtains information on identity and address of the customer, nature of business and financial status of a customer and, verifies the same. This process helps to ensure that an RE is aware of the customer it is dealing with, and the services provided by the RE are not misused for Money Laundering/ Terrorist Financing/ Proliferation Financing (ML/TF/PF) purposes.

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

xii. "**Non-face-to-face customers**" means customers who open accounts without visiting the branch/offices of the REs or meeting the officials of REs.

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

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

xv. "**Regulated Entities**" (REs) means –

xvi. all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs) /State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

xvii. All India Financial Institutions (AIFIs)

xviii. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)

xix. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

xx. All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xxi. "**Risk Management Committee**" or "RMC" shall mean the committee constituted by the Board of Directors

xxii. **"Senior Management"** shall mean the employees designated as "Partners" excluding Board of Directors and including key managerial personnel as per Companies Act or such other person as may be specified. The Committee would review the definition annually depending on the organization structure of the Company.

xxiii. "**Unique Customer Identification Code"** or "UCIC" or "Customer Identification File/ Form" or "CIF" shall mean a unique code provided by the Company to each of the customers while entering into an account-based relationship with a customer in order to maintain identification records at the customer level.

xxiv. "**UIDAI"** means 'Unique Identification Authority of India'.

xxv. "**Video based Customer Identification Process** (V-CIP)": an alternate method of customer identification with facial recognition and customer due diligence by an authorised 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.

5. POLICY GOVERNANCE

a. Key Responsibilities of the Board of Directors/ Board:

i. To review and approve the Policy as and when required as per the RBI KYC Directions

ii. To consider and approve appointment of the Designated Director and the Principal Officer, as and when required.

iii. To delegate any authority for review, approval and implementation of the Policy.

b. Key responsibilities of the Risk Management Committee ("RMC")

To review the Money Laundering and Terrorist Financing Risk Assessment conducted by the Company and provide appropriate guidance to the Company for managing the money laundering and terrorist financing risk.

c. Key Responsibilities of the Senior Management:

I. To ensure implementation of the KYC and AML Policy and related procedures.
II. To ensure that decision-making functions of determining compliance with KYC norms are not outsourced.

d. Designated Director and Key Responsibilities:

I. The Company shall appoint the Managing Director or a whole-time Director designated by the Board of Directors of the Company to ensure overall compliance with the obligations prescribed by the PMLA and the PML Rules. The name, designation, address and contact details of the Designated Director shall be communicated to the FIU as well as the RBI.
II. The Designated Director shall ensure overall compliance with the obligations prescribed by the PMLA, the PML Rules and RBI KYC Directions. The Designated Director shall consider, review and approve various procedures which may be proposed for the implementation of this Policy.

e. Principal Officer and Key Responsibilities:

The Company shall designate one of its officials as the Principal Officer of the Company, who shall be responsible for overseeing implementation of the KYC and AML Policy and related procedures. The Principal Officer should have knowledge, sufficient independence, authority, time and resources to manage and mitigate the AML risks of the business.

Key Responsibilities of the Principal Officer ("PO") shall be as under:

I. The PO shall recommend suitable amendments to the Policy based on the latest applicable requirements under the PMLA, the PML Rules and RBI KYC Directions, as and when required
II. To consider, review and recommend various procedures which may be necessary for implementation of the Policy.
III. PO, with the assistance of relevant functions, shall put in place relevant procedures required for implementation of this Policy.
IV. To ensure implementation of the Company's KYC and AML policy and monitoring of the same
V. To ensure reporting of transactions to the FIU-IND and/ or the RBI and sharing of the information as required under the applicable laws/ regulations.
VI. To ensure submission of periodical reports to the Board/ senior management of the Company.
VII. Co-ordination with the HR function in organizing training of employees to make them aware of the KYC and AML requirements, from time to time.
VIII. The name, designation, address and contact details of the Principal Officer shall be communicated to the FIU as well as to the RBI.

a. Responsibilities of the Employees of the Company

The employees of the Company, while delivering their official responsibilities, shall be required to comply with this KYC and AML Policy and other procedures defined by the Company for implementation of the Policy.

b. Responsibilities of the Company's Agents and their authorized representatives

The Company's agents or persons authorized by it, for its business, shall be required to ensure adherence with the Company's KYC and AML Policy. In this regard, as per the regulatory requirements, the Company shall be responsible for consequences of any violation by the persons authorised by the Company including agents etc. who are operating on its behalf. Further, all information and books of accounts of persons authorized by the Company including agents etc., so far as they relate to business of the Company, shall be made available to the RBI or any of the Company authorised representative for audit/ inspection to verify the compliance

with the Policy.

6. KEY ELEMENTS OF THE POLICY

(i) Customer Acceptance Policy ("CAP")

(ii) Customer Identification Procedures ("CIP").

(iii) Customer Due Diligence ("CDD")

(iv) Risk Management

(v) Monitoring of transactions.

6.1 CUSTOMER ACCEPTANCE POLICY ("CAP")

The Customer Acceptance Policy lays down explicit criteria for acceptance of customers. The Policy ensures that the following procedures shall be followed in relation to customer who approaches for availing financial facilities with the Company.

(a) Company shall not open any account(s), or no transactions shall be executed in anonymous, fictitious or benami' name(s) or on behalf of other persons whose identity has not been disclosed or cannot be verified.

(b) No transaction shall be undertaken where the Company is unable to apply appropriate CDD measures as set out in this Policy, either due to non-cooperation of the customer or non –reliability of the documents/ information furnished by the customer. 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

(c) In order to avoid fictitious and fraudulent applications of the customers, and to achieve a reasonable degree of satisfaction as to the identity of the customer, the Company shall conduct appropriate basic customer due diligence. Further, it shall not undertake transaction or account-based relationship without following the CDD measures.

(d) CDD procedure shall be followed by the Company for all the co-borrowers and guarantors wherever applicable.

(e) All mandatory information sought at the time of CDD of a new customer or at the time of periodic updation, shall be specified by the Company in this Policy. Any other additional information not specified in this Policy shall be obtained with the explicit consent of the customer.

(f) For initial KYC purposes and during the periodic updation, all mandatory information shall be sought by the Company.

(g) The Company shall define the process for accepting a third person to act on behalf of another person/ entity/ customer as a mandate holder or authority holder of the actual beneficiary, based on the legal and regulatory requirements.

(h) The Company shall ensure that necessary checks are carried out before creating/ opening a new loan account to ensure 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. Full details of accounts/ customers bearing resemblance with any of the individuals/ entities in the list shall be reviewed and reported if found suspicious or matching with any entry in the sanction list.

An illustrative list is as below and shall be always driven by the latest update released by the Authority from time to time-

- ISIL (Da'esh) &Al-Qaida Sanctions List (UNSCR 1267)
- ISIL (Da'esh) &Al-Qaida Sanctions List (UNSCR 1989)
- ISIL (Da'esh) &Al-Qaida Sanctions List (UNSCR 2253)
- Taliban Sanctions List [UNSCR 1988 (2011)]
- Designated List under 12A(1) of the Act
- UNSCR 1718 Sanctions list
- Other UNSCRs
- Lists in the 1st and 4th schedule of UAPA, 1967
- Individual Terrorists Under UAPA
- UNSC 2231 Sanctions Committee Designated List
- Nations Security Council Consolidated List
- The List established and maintained pursuant to Security Council res. 1718 (2006)
- Updates to UNSCR 1718 Sanctions Committee on DPRK
- Urgent Updates For Implementation Of Section 51a of UAPA 1967
- Updates of Designation of Individuals U/s 35(1)(a) of the Unlawful Activities (Prevention) Act, 1967
- The List established and maintained pursuant to Security Council res. 2231 (2015)

Further, the Company shall take into consideration those individuals/entities whose names appear in the sanctions lists including United Nations Security Council Resolutions ('UNSCRs'), and also to those individuals/entities from jurisdictions that do not or insufficiently apply the Financial Action Task Force (FATF) Recommendations as per the FATF statements circulated by the RBI.

(i) A Unique Customer Identification Code ("UCIC") or Customer Identification File/ Form ("CIF") shall be allotted while entering into new relationships with customers. However, the Company shall not issue UCIC to occasional customers such as purchasers of third-party products.

(j) The Company shall conduct due diligence at the UCIC/ CIF level. Thus, if an existing KYC compliant customer desires to open another account with the Company, there shall be no need for a fresh CDD exercise.

(k) The nature and extent of due diligence to be conducted, at the time of initiation of business relationship, would depend upon risk category of the customer and involve collection/ verification of information by using reliable independent documents, data or information. This may include information relating to the customer's identity, social/ financial status, nature of business activity, information about his clients' business and their location, etc.

(l) The Company, while preparing customer profile, shall ensure that it obtains only such information from the customer which is relevant to the risk category and is not intrusive, and is in conformity with the guidelines issued. The customer profile shall be treated as a confidential document and details contained therein shall not be divulged for cross selling or any other purposes without the customer's consent.

(m) The purpose of commencing the relationship/opening of accounts shall be established and the beneficiary of the relationship/ account shall also be identified.

(n) The information collected from the customer shall be kept confidential.

(o) Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider terminating the business relationship. However, the decision to close an existing account shall be taken at the Principal Officer or departmental head level after giving due notice to the customer explaining the reasons for such a decision.

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

(q) Where Goods and Services Tax ("GST") details are available, the GST number shall be verified from the search/verification facility of the issuing authority.

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

(s) ere the Company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file a Suspicious Transaction Report ("STR") with the FIU.

(t) Parameters of risk perception in terms of monitoring Suspicious Transactions shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc.

(u) Customer shall be categorized as low, medium, and high risk, based on their risk perception assessed as per the principles laid out by the Company for risk-categorisation.

(v) Appropriate Enhanced Due Diligence ("EDD") measures shall be adopted for customers with a high-risk profile from a money laundering perspective. Further, in respect of unusual or suspicious transactions/applications or when the customer moves from a low risk to a high- risk profile, appropriate EDD measures shall be adopted.

(w) The account shall be monitored and when there is suspicion of ML/TF activities or other high-risk scenarios, the identity of the customer shall be established as per Customer Due Diligence Procedure.

(x) Records or the information of the customers due diligence carried out through the records of CKYCR shall be obtained by the Company within 2 days from the Central KYC Records Registry.

(y) Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.

The Company shall factor the above aspects while formulating the KYC/AML procedures for various customers/ products. However, while defining the KYC/CDD procedures, the Company shall ensure that its procedures does not become too restrictive or pose significant difficulties in availing its services by deserving general public, especially the financially and socially disadvantaged sections of society including the Persons with Disabilities (PwDs). No application for onboarding or periodic updation of KYC shall be rejected without application of mind. Reason(s) of rejection shall be duly recorded by the officer concerned

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

6.2 CUSTOMER IDENTIFICATION PROCEDURES ("CIP")

Customer identification means identifying the customer and verifying his/ her identity by using reliable, independent source documents, data, or information of individual as well as corporate. The Company shall endeavor to obtain sufficient information necessary to assess not only the identity of each proposed customer, but also the purpose of the proposed nature of relationship. The Company shall adopt the customer identification procedure to be carried out at different stages in accordance with the applicable provisions of

the Act, Rules and the RBI KYC Directions.

Accordingly, the Company shall undertake identification of customers in the following circumstances:

a. Commencement of an account-based relationship with a customer, or while carrying out occasional transaction(s) of an amount equal to or exceeding ₹50,000, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations.
b. Whenever there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
c. Whenever selling third party products as agents, selling their own products, payment with respect to any other product for more than ₹50,000/-.
d. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds ₹50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
e. When the Company has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of ₹50,000/-
f. The Company shall ensure that introduction is not to be sought while opening accounts.

The Company may rely upon CDD done by a third party subject to the following condition:"

a) Records or the information of the customers due diligence carried out by the third party is obtained by the Company immediately from the third party or from the Central KYC Records Registry.
b) Adequate steps are taken by the 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.

6.3 CUSTOMER DUE DILIGENCE PROCEDURES

The Company shall obtain certified Officially Valid Documents ("**OVD**" or "**KYC documents**") in accordance with the regulatory requirements to verify the customer's identity, beneficial owner and location along with such other documents pertaining to the nature of business or financial status as may be specified by the Company.

6.3.1 ***Customer Due Diligence Procedure if an Individual is the Customer***

The provisions of this paragraph shall be applicable to an individual who himself/ herself is a customer or is a beneficial owner or an authorized signatory/ power of attorney holder on behalf of a legal entity who is proposed to be a customer of the Company. For Customer Due Diligence ("CDD") of an individual, the Company shall carry-out the following activities:

a. Photograph and OVDs to be obtained- One recent photograph of the customer to obtained.

b. **Permanent Account Number ("PAN") -** PAN or the equivalent e-document thereof shall be obtained. If PAN has not been obtained by the customer, then Form No. 60 as defined in Income-tax Rules, 1962 shall be taken.

c. **OVDs to be obtained**- In addition to the above, certified copy of one of the OVDs or the equivalent e-document thereof or one of the following shall be taken for verification of the identity and the address:

- The Company shall, to verify the identity of individual obtain a certified copy of the proof of possession of Aadhaar number or any other OVD, along with a recent photograph of the individual where an equivalent e-document is not submitted.
- Here, the copy of the proof of possession of Aadhaar or OVD, as the case may be, is compared with the original documents in the possession of the individual and is stamped as certified copy by the authorised official of the Company.
- All documents provided by the customer (for applicant/co-applicant/beneficiary owner/proprietor) should be sighted in original and verified by the "Authorised Offcial" of the Company who is authorized to do OSV and signed with OSV remarks. OSV shall be mandatory for all the KYC documents and documents for which original can be produced for verification.

- Aadhaar Number:
  v' If customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act; *or*
  v' If customer decides to submit his Aadhaar number voluntarily to the Company, provided the Company notified under first proviso to sub-section (1) of section 11A of the PMLA for e-KYC authentication facility provided by the UIDAI; ***or***
- Proof of Possession of Aadhaar number where offline verification can be carried out; ***or***
- 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; ***or***
- The KYC Identifier with an explicit consent to download records from CKYCR. Where a customer, for the purposes of establishing an account-based relationship, submits a KYC Identifier to the Company or retrieve the KYC Identifier, if available, with an 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:
  v' there is change in the information of the customer vis-à-vis that existing in the records of CKYCR; *or*
  v' the current address of the customer is required to be verified; *or*
  v' the respective credit approving authority of 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 customer; *or*
  v' the validity period of documents downloaded from the CKYCR has lapsed.
  v' the KYC records / information retrieved from the CKYCR is incomplete or is not as per the prevailing applicable KYC norms.
- Detailed use of the CKYCR Registry is mentioned hereinbelow in para 6.3.7 of this Policy.

d. **Documents relating to business and financial status**- 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 prescribed by the Company from time to time.

If the Customer's line of business is such wherein a specific license/certificate/approval is required from

the govt. authorities, then, in addition to the valid KYC documents collected from the customer, the Company may collect relevant documents.

e. **Other requirements to be complied with respect to various KYC documents**

- Aadhaar number may specifically be obtained in the following scenarios:

✓ If customer is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar Act; ***or***

✓ If customer decides to submit his Aadhaar number voluntarily to the Company, provided the Company notified under first proviso to sub-section (1) of section 11A of the PMLA for e-KYC authentication facility provided by the UIDAI.

- Authentication using e-KYC authentication facility provided by the UIDAI- As and when the Company is authorized to conduct authorization through e-KYC authentication facility provided by the UIDAI, it may conduct such authorization and use the e-KYC facility in accordance with the conditions prescribed under the Aadhaar Act or the RBI KYC Directions. Further, in such a case, if a customer wants to provide a current address, different from the address as per the identity information available in Central Identities Data Repository of the UIDAI, he shall provide a self-declaration to that effect to the Company.
- If the customer submits his Aadhaar number, the Company will ensure such customer to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under Section 7 of the Aadhaar Act.
- The use of Aadhaar, proof of possession of Aadhaar etc. shall be in accordance with the Aadhaar Act and other applicable regulations/ rules.
- In case proof of possession of the Aadhaar has been submitted by a customer, the Company shall carry out offline verification wherever possible.
- Where a customer has submitted an equivalent e-document of any OVD, the Company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under the Digital KYC Process as specified in the paragraph 6.3.5 below.

Where a customer submits any OVD or proof of possession of Aadhaar number and its offline verification of such OVD/ proof of possession of Aadhaar cannot be carried out, the Company shall have option to carry out verification through Digital KYC Process as specified in the paragraph 6.3.5 below.

6.3.2 *Customer Due Diligence Procedure if a non-individual is the Customer*

For customers that are legal persons or entities, the Company shall:

- verify the legal status of the legal person/ entity through charter documents and tax registration etc.
- 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 through authentic documents and
- understand the ownership and control structure of the customer and determine who are the natural persons ultimately controlling the legal person.

The list of documents to be collected and verified depending upon their nature is specified in below table:

Types of entity	Type of document to be collected and verified
Sole Proprietary firms	In addition to performing CDD applicable in case of an Individual at Para 6.3.1. and 6.3.6 of this Policy (for the proprietor) any two of the following documents must be obtained as a proof of business/ activity in the name of the proprietary firm: i. Registration certificate including Udyam Registration Certificate (URC) issued by the Government ii. Certificate/license issued by the municipal authorities under Shop and Establishment Act iii. Sales and income tax returns iv. CST/VAT/ GST certificate (provisional/final) v. Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities vi. IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or License/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute vii. Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. viii. Utility bills such as electricity, water, landline telephone bills, etc. Provided, in cases where the Company is satisfied that it is not possible to furnish two such documents as mentioned above, it may accept only one of those documents as proof of business/ activity, subject to contact point verification and collection of such other information and clarification as would be required to establish the existence of such firm. Further, it should be satisfied that the business activity has been verified from the address of the proprietary concern
Corporate (Public Limited/ Private Limited Company)	Certified copies of each of the following documents or the equivalent e-documents of the Company shall be obtained: i. Certificate of Incorporation ii. Updated Memorandum and Articles of Association iii. PAN of the Company iv. A resolution from the Board of Directors and power of attorney granted to its managers, officers, or employees to apply, open, and operate the loan on its behalf v. Documents specified above in Para 6.3.1 and 6.3.6 of this Policy for individuals relating to beneficial owner, the managers, officers, or employees, as the case may be, holding an attorney to transact on the company's behalf 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.
Partnership Firms	Certified copies of each of the following documents or the equivalent e-documents of the Firm shall be obtained: i. Registration Certificate ii. Partnership Deed iii. PAN of the Partnership Firm iv. Documents, as specified in para 6.3.1 and 6.3.6 of this Policy, relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf v. The names of all the partners; and

	vi. Address of the registered office, and the principal place of business, if it is different
Trust	Certified copies of each of the following documents or the equivalent e-documents of the Trust shall be obtained: i. Registration certificate ii. Trust deed iii. Permanent Account Number or Form No.60 of the trust iv. Documents, as specified in para 6.3.1 and 6.3.6 of this Policy, relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf v. the names of the beneficiaries, trustees, settlor, and authors of the trust vi. the address of the registered office of the trust; and vii. list of trustees and documents, as specified in para 6.3.1 of this Policy, for those discharging the role as trustee and authorized to transact on behalf of then trust.
Unincorporated association or a body of individuals & Unregistered trust/ partnership firms/ societies	Certified copies of each of the following documents or the equivalent e-documents of the unincorporated association or a body of Individuals shall be obtained: i. Resolution of the managing body of such association or body of individuals ii. Permanent Account Number or Form No. 60 of the unincorporated association or a body of individuals iii. Power of attorney granted to transact on its behalf iv. Documents, as specified in para 6.3.1 and 6.3.6 of this Policy, relating to beneficial owner, managers, officers, or employees, as the case may be, holding an attorney to transact on its behalf; and v. Such information as may be required by the RE to collectively establish the legal existence of such an association or body of individuals.
Customer who is a juridical person (not specifically covered in the earlier sections)	For opening account of a customer who is a juridical person (not specifically covered in the earlier part) 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, certified copies of the following documents or the equivalent e-documents thereof shall be obtained and verified: i. Document showing name of the person authorised to act on behalf of the entity. ii. Documents, as specified in para 6.3.1of this Policy, of the person holding an attorney to transact on its behalf. iii. Such documents as may be required by the Company to establish the legal existence of such an entity/juridical person.

Note:

- The Company shall collect the necessary documents and information in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by the RBI from time to time.
- The first 8 digits of the Aadhaar number need to be blackout before accepting Aadhar from customer.
- In case of trust, the Company will ensure that trustees disclose their status at the time of commencement of an account-based relationship or when carrying out transactions as specified in the KYC Master Direction.

6.3.3 *Identification of Beneficial Owner*

For opening an account of a Legal Person who is not a natural person, the Company would take reasonable measures to identify the beneficial owners and thereafter verify the beneficial owner(s) in terms of Rule 9(3) of the PML Rules, keeping in view the below:

Type of Entity	Criteria for Identification of Beneficial Owner
Company	Individual (natural person) who has the ownership of/entitlement to more than 10% of share or capital or profits of the Company.
Partnership Firm	Individual/partner (natural person) who has the ownership of/entitlement to more than10% of the capital or profits of the Firm.
Unincorporated Association or Body of individual	Individual (natural person) who has the ownership of/entitlement to more than 15% of the property or capital or profits of the association
Trust	Individual (natural person) who is the setter of the trust, the trustee, the protector, 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

a) 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.

b) 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.

6.3.4 *Accounts opened using the Aadhaar OTP based e-KYC, in Non-Face-to-Face Mode*

Accounts opened using OTP based e-KYC authentication, in non-face-to-face mode, shall be subject to the following conditions:

a. There must be specific consent from the customer for authentication through OTP;
b. Only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed Rs.60,000/- in a year;
c. As a risk-mitigating measure for such accounts, the Company shall ensure that transaction alerts, OTP, etc., are sent only to the mobile number of the customer registered with Aadhaar.
d. Change in the mobile number used for opening of the account through the Aadhaar OTP shall be permitted

subject to the following due diligence by the Company:

(i) The request for change in the mobile number may be considered only after the customer completes the CDD as per Paragraph 6.3.1 above or V-CIP as per Paragraph 6.3.6 below; *or*

(ii) The customer logs into the customer portal or mobile app of the Company and places request for change in the mobile number. Once such a request is placed through the customer portal or mobile app of the Company, existing mobile number and new mobile number shall be verified through separate OTPs.

e. Accounts opened using OTP based e-KYC shall not be allowed for more than one year unless identification is carried-out either as per preceding paragraphs at Paragraph 6.3.1 above or as per Paragraph 6.3.6 (V-CIP) below. If Aadhaar details are used under V-CIP, the process shall be followed in its entirety including fresh Aadhaar OTP authentication;

f. If the CDD procedure as mentioned above is not completed within a year, no further debits shall be allowed;

g. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other RE. Further, while uploading KYC information to CKYCR, the Company shall clearly indicate that such accounts are opened using OTP based e-KYC; and

h. The Company shall not open new accounts by way of e-KYC if, based on the KYC information available in the CKYCR, another RE has already opened an account of the customers with OTP based e-KYC procedure in non-face-to-face mode.

i. The Company shall have a strict monitoring procedure including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

6.3.5 ***Digital KYC Process***

a. If the Company plans to implement Digital KYC Process, the Company shall develop an application for Digital KYC process which would be made available at customer touch points for undertaking KYC of its customers and the KYC process shall be undertaken only through this authenticated application of the Company.

b. The access of the Application shall be controlled by the Company, and it shall ensure that the same is not used by any unauthorized persons. The Application should be accessed only through login-id and password, or Live OTP or Time OTP controlled mechanism given by the Company to its authorized officials.

c. The customer, for the purpose of KYC, will be required to visit the location of the authorized official of the Company or vice-versa. The original OVD should be in the possession of the customer.

d. For this process, it shall be ensured that the Live photograph of the customer is taken by its authorized official and the same photograph is embedded in the Customer Application Form ("**CAF**"). Further, the system application of the Company should put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by the Company) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.

e. The Application of the Company shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is captured. The background behind the customer while capturing live photograph should be of white color and no other person should come into the frame while capturing the live photograph of the customer.

f. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), should be captured vertically from above and water-

marking in readable form as mentioned above should be done. No skew or tilt in the mobile device should be there while capturing the live photograph of the original documents.

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

h. Thereafter, all the entries in the CAF should be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address may be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.

Once the above-mentioned process is completed, a One Time Password (OTP) message containing t he text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/ her own mobile number, then the mobile number of his/ her family/ relatives/ known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the Company shall not be used for customer signature. It shall be checked that the mobile number used in customer signature should not be the mobile number of the authorized officer.

j. The authorized officer should provide a declaration about the capturing of the live photograph of the customer and the original document. For this purpose, the authorized official will be required to verify authenticity with a One Time Password (OTP) which will be sent to his mobile number registered with the Company. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.

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

l. The authorized officer of the Company shall check and verify that:

i. information available in the picture of document is matching with the information entered by authorized officer in CAF;

ii. live photograph of the customer matches with the photo available in the document.; *and*

iii. all of the necessary details in CAF including mandatory field are filled properly.

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

6.3.6 ***Video based Customer Identification Process (V-CIP)***

- The Company may undertake V- CIP to carry- out:
  a. In case of onboarding of new customers, CDD applicable to individual customers, proprietor in case of proprietorship firm, authorised signatories, and the BOs in case of a customer which is a legal entity.
  b. Conversion of existing accounts opened in non-face to face mode using Aadhaar OTP based e-KYC authentication mentioned above.
  c. Updation/ Periodic updation of KYC for customers, as applicable from time to time.

- If the Company opts to undertake V-CIP, it shall adhere to the following minimum standards:

I. V-CIP Infrastructure

a. The Company shall comply with the applicable directions prescribed by the RBI on minimum baseline cyber security and resilience framework.

b. The technology infrastructure shall be housed in own premises of the Company, unless cloud deployment model is used, and the V-CIP connection and interaction should necessarily originate from its own secured network domain. Any technology related outsourcing for the process shall be compliant with the applicable RBI directions/ guidelines.

a) If cloud deployment model is used, it shall be ensured that the ownership of data in such model rests with the Company only and all the data including video recording is transferred to the Company's exclusively owned/ leased server(s) including cloud server, if any, immediately after the V-CIP process is completed and no data shall be retained by the cloud service provider or third-party technology provider assisting the V-CIP of the Company.

b) The Company shall ensure end-to-end encryption of data between customer device and the hosting point of the V-CIP application, as per appropriate encryption standards. The customer's consent should be recorded in an auditable and alteration-proof manner.

c) The V-CIP infrastructure/ application should be capable of preventing connection from IP addresses outside India or from spoofed IP addresses.

d) The video recordings should contain the live GPS co-ordinates (geo-tagging) of the customer undertaking the V-CIP and date-time stamp. The quality of the live video in the V-CIP should be adequate to allow identification of the customer beyond doubt.

e) The application should have components with face liveness/ spoof detection as well as face matching technology with high degree of accuracy, even though the ultimate responsibility of any customer identification rests with the Company.

f) Appropriate artificial intelligence (AI) technology can be used to ensure that the V-CIP is robust.

g) Based on experience of detected/ attempted/ 'near-miss' cases of forged identity, the technology infrastructure including application software as well as workflows shall be regularly upgraded. Any detected case of forged identity through V-CIP shall be reported as a cyber event under extant regulatory guidelines.

h) The V-CIP infrastructure shall undergo necessary tests such as Vulnerability Assessment, Penetration testing and a Security Audit to ensure its robustness and end-to-end encryption capabilities. Any critical gap reported under this process shall be mitigated before rolling out its implementation. Such tests should be conducted by the empanelled auditors of Indian Computer Emergency Response Team (CERT-In) and shall be conducted periodically, in conformity with the applicable regulatory guidelines.

i) The V-CIP application software and relevant APIs/ webservices should also undergo appropriate testing of functional, performance, maintenance strength before being used in a live environment. Only after closure of any critical gap found during such tests, the application should be rolled out. Such tests shall also be carried out periodically in conformity with internal policy and applicable regulatory guidelines.

II. V-CIP Procedure

a) The Company shall adhere to these V-CIP procedures and shall have a clear workflow in this regard. The V-CIP process shall be operated only by officials of the Company specially trained for this purpose. The official should be capable of carrying out liveliness check and detect any other

fraudulent manipulation or suspicious conduct of the customer and act upon it. The liveness check shall not result in exclusion of person with special needs.

b) Disruption of any sort including pausing of video, reconnecting calls, etc., should not result in creation of multiple video files. If pause or disruption does not lead to the creation of multiple files, then the Company may not initiate a fresh session. However, in case of call drop / disconnection, a fresh session initiated.

c) The sequence and/or type of questions, including those indicating the liveness of the interaction, during video interactions shall be varied in order to establish that the interactions are real-time and not pre- recorded.

a) Any prompting, observed at end of customer shall lead to rejection of the account opening process.

b) The fact of the V-CIP customer being an existing or new customer, or if it relates to a case rejected earlier or if the name appearing in some negative list should be factored in at an appropriate stage of workflow.

c) The authorised official of the Company performing the V-CIP shall record audio- video as well as capture photograph of the customer present for identification and obtain the identification information using any one of the following:

d) OTP based Aadhaar e-KYC authentication.

e) Offline Verification of Aadhaar for identification.

f) KYC records downloaded from CKYCR, as prescribed, using the KYC identifier.

g) Equivalent e-document of OVDs including documents issued through Digilocker.

h) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, it shall be ensured that the XML file or QR code generation date is not older than three working days from the date of carrying out V-CIP. Accordingly, the Company shall also ensure that the video process of the V-CIP is undertaken within 3 working days of downloading/ obtaining the identification information through CKYCR/ Aadhaar authentication/ equivalent e-document, if in the rare cases, the entire process cannot be completed at one go or seamlessly. The Company shall ensure that no incremental risk is added due to this.

i) The Company shall capture a clear image of the PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker.

j) Use of printed copy of equivalent e-document including e-PAN shall not be considered valid for the V-CIP.

k) The authorised official of the Company shall ensure that photograph of the customer in the Aadhaar/OVD and PAN/e -PAN matches with the customer undertaking the V-CIP and the identification details in Aadhaar/OVD and PAN/e- PAN shall match with the details provided by the customer.

l) All accounts opened through V-CIP shall be made operational only after being subject to concurrent audit, to ensure the integrity of the process and its acceptability of the outcome.

III. V-CIP Records and Data Management

a. The entire data and recordings of V-CIP shall be stored in a system located in India. The Company shall ensure that the video recording is stored in a safe and secure manner and bears the date and time stamp that affords easy historical data search.

b. For V- CIP also, the Company shall comply with extant regulatory requirements relating to record management.

c. The activity log along with the credentials of the official performing the V-CIP shall be preserved.

6.3.7 *CDD Procedure and sharing of KYC Information with Central KYC Records Registry (CKYCR)*

a. Government of India has Authorised the Central Registry of Securitisation Asset reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette notification No. S.O 3183 (E) date November 26, 2015
b. In terms of the provision of Rule 9(1A) of PML Rules, the Company shall capture customer's K YC records and upload onto CKYCR within 10 days of commencement of an account-based relationship with the customer. This shall be applicable to customers whose data is not already uploaded on the CKCYR and the KYC Identifier is not available.
c. The Company will capture the KYC information/ details as per the KYC templates and share the same with the CKYCR in the manner as prescribed in the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.
d. The Company shall capture the KYC information for sharing with the CKYCR in the manner mentioned in the Rules, as per the KYC templates prepared for 'Individuals' and 'Legal Entities' (LEs), as the case may be.
e. Once KYC Identifier is generated by CKYCR, the Company shall ensure that the same is communicated to the individual/ LE, as the case may be.
f. Where a customer for the purpose of establishing an account-based relationship, updation/periodic updation or for verification of identity submits a KYC identifier to Company or retrieve the KYC Identifier, if available, with an 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 –
    - There is change in KYC information of the customers as existing in the records of CKYCR.
    - The current address of the customer is required to be verified.
    - 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.
    - the validity period of documents downloaded from CKYCR has lapsed.the KYC records / information retrieved from the CKYCR is incomplete or is not as per the prevailing applicable KYC norms.
g. In order to ensure that all KYC records are incrementally uploaded on to CKYCR, the Company shall upload/update the KYC data pertaining to accounts of individual customers and LEs at the time of scheduled periodic updation, specified in this Policy as per the risk categorization of a customer, or earlier, if any updated KYC information is obtained/received from the customer.
h. The Company shall ensure that during periodic updation, the customers are migrated to the on-going CDD standard of the Company.
i. Where an additional or updated information is received from the customer at the time of establishing an account based relationship, periodic updation, or updation initiated by customer, the Company shall furnish the updated information to the CKYCR within 7 days or within such period as may be notified by the Central Government. The CKYCR shall thereafter electronically notify all other REs who have dealt with the concerned customer of the updated information.
j. When the Company receives any communication from the CKYCR of any updated information of their existing customers, it shall retrieve the updated KYC records from the CKYCR and replicate the update in its records promptly.

6.3.8 *On-going Due Diligence and Monitoring of Transactions*

a. Ongoing monitoring is an essential element of the Policy. The Company shall undertake on-going due diligence of customers to ensure that their transactions are consistent with its knowledge about its customers, customers' business/ employment and risk profile, and source of funds.
b. 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, or transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer.
c. The extent of monitoring shall be aligned with the risk category of the customer.
d. Periodic review of risk categorization of account will be carried out at least once in six months.
e. For ongoing due diligence, the Company shall consider adopting appropriate technological means/ support that may be required for effective monitoring commensurate with the money laundering risk perceived for the business undertaken by the Company.

6.3.9 *Validity of KYC Due Diligence once done by the Company*

KYC verification if done once by one branch/ office of the Company shall be valid for its any other branch/ office, provided complete KYC verification has already been done for the concerned account and the same is not due for periodic updation.

6.3.10 *Enhanced Due Diligence Procedures*

i. Enhanced Due Diligence for Higher Risk Customers

For its medium and high-risk customers, the Company, an addition to the CDD, shall conduct risk-based Enhanced Due Diligence ("EDD"). Such EDD should assist the Company in the following:

- Determining whether the customer appears to be engaged in legitimate business activities and has legitimate sources of funds; and
- Anticipating the customer's usual and expected activity so that suspicious activity can be detected.

Any business relationship with a high risk or medium risk customers as per the Annexure 1 of this Policy shall require approval from an appropriate authority. Further, any suspicious triggers relating to higher risk customer's transactions shall be reviewed more rigorously. For higher risk customers, the EDD procedures shall include collecting additional information and documentation regarding the following:

- Purpose of the account/ end-use.
- Source of income/ funds.
- Review of income/ financial statements and banking statements.
- Diligence regarding the customer's workplace/ business and business operations.
- Proximity of the customer's residence, place of employment, or place of business.
- Due diligence of the individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors, if any.

Further, as part of the EDD procedures, the Company shall follow a system of periodic updation of KYC information for various categories of the customers as prescribed in this Policy.

EDD is an ongoing process, and the Company should take measures to ensure that information is updated as

required and that appropriate risk-based monitoring occurs to ensure that any suspicious activity is escalated, analyzed and reported, as prescribed in the Policy.

ii. Accounts of Non-Face-to-Face Customers (other than Aadhaar OTP based on-boarding done as per Paragraph 6.3.4 above)

Non-face-to-face onboarding facilitates the Company to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this paragraph includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. The Company shall adhere to the following EDD measures for non-face-to-face customer onboarding (other than Aadhaar OTP based on- boarding done in terms with the Paragraph 6.3.4 above):

a. If the Company has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. Such V-CIP shall be treated on par with face- to-face CIP for the purpose of the RBI KYC Directions.

b. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. For any change in the mobile used for accounting opening, the following process shall be adopted for due diligence:

   - The request for change in the mobile number may be considered only after the customer completes the CDD as per Paragraph 6.3.1 or V-CIP as per Paragraph 6.3.6 of this Policy; or

   - The customer may log-in through customer portal or mobile app of the Company and place request for change in the mobile number. Once such a request is placed through the customer portal or mobile app of the Company, the existing mobile number and new mobile number shall be verified through separate OTP.

c. Apart from obtaining the current address proof, the Company shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.

d. PAN of the customer shall be verified from the verification facility of the issuing authority.

e. The Company shall ensure that the first transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.

f. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

g. Such non-face-to-face modes for the purpose of this paragraph include use of digital channels such as the Central KYC Records Registry ("CKYCR"). The Regulated Entity ("RE") that has last uploaded or updated the customer's KYC records in the CKYCR shall be responsible for verifying the identity and / or address of the customer, as applicable. Accordingly, the Company, while downloading and relying upon such KYC records from CKYCR, shall not be required to re-verify the authenticity of the customer's

identity and / or address, provided that the KYC records downloaded from CKYCR are current and compliant with the provisions of the Prevention of Money Laundering Act, 2002 and the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Act / PML Rules") and the applicable RBI KYC Directions. Notwithstanding the foregoing, the Company shall remain responsible for all other aspects of the Customer Due Diligence ("CDD") procedure and compliance with the provisions of these Directions, including ongoing due diligence and transaction monitoring, except for the verification of identity and / or address of the customer to the extent reliance is placed on current and compliant CKYCR records.

iii. Accounts of Politically Exposed Persons (PEPs)

a. The Company, while establishing a relationship with PEPs (whether customer or beneficial owner) apart from performing normal customer due diligence, shall ensure the following:

b. The Company shall have in place appropriate risk management systems to determine whether the customer or the beneficial owner is a PEP;

c. Reasonable measures are taken by the Company for establishing the source of funds / wealth

d. The identity of the person shall have been verified before accepting the PEP as a customer.

e. Any lending/business relationship with a PEP shall be established only with the approval of an official from the Senior Management.

f. All such accounts are subjected to enhanced monitoring on an on-going basis.

g. In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, senior management's approval shall be obtained to continue the business relationship. All PEP accounts would be classified as high-risk accounts and will be subject to enhanced monitoring on an on-going basis.

The above will also be applicable to accounts where a PEP is the beneficial owner or to the account of a family members or close associates of a PEP.

6.3.11 Reliance on Customer Due Diligence done by a Third Party

For verifying the identity of customers at the time of commencement of an account-based relationship, the Company may also rely on customer due diligence done by a third party, only if the following conditions are met:

- 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 Act.
- Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the CKYCR.
- 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.

- The third party shall not be based in a country or jurisdiction assessed as high risk.
- The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the Company.

6.4 Freezing of Assets

The Company shall Freeze Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of Master Direction), is strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA.

Freezing of Assets under Section 51A of UAPA, 1967: The procedure laid down in the UAPA Order dated February 2, 2021 (Annex II of this Master Direction), is strictly followed and meticulous compliance with the Order issued by the Government shall be ensured. The list of Nodal Officers for UAPA is available on the website of MHA

If an order to freeze assets under Section 12A is received by the REs from the CNO, REs shall, without delay, take necessary action to comply with the Order

The process of unfreezing of funds, etc., shall be observed as per paragraph 7 of the Order. Accordingly, copy of application received from an individual/entity regarding unfreezing shall be forwarded by RE along with full details of the asset frozen, as given by the applicant, to the CNO by email, FAX and by post, within two working days.

6.5 RISK MANAGEMENT

6.5.1 Risk Categorisation of customers

For Risk Management, Protium shall have a risk based approach which includes the following:

- The Company will categorise its customers under Low, Medium or High-risk categories, based on the assessment, profiling and the money laundering risk perceived by it in accordance with the provisions of the RBI KYC Directions.
- The risk categorisation shall be done based on type of credit exposure, the customer's background, nature, location and type of occupation/ employment/ business, purpose of loan, sources of funds, mode of repayment etc. However, while conducting such assessment, the Company shall ensure that various other information/ details collected from different categories of customers relating to the perceived risk, are non-intrusive.

The Company shall adopt the risk categorisation as per the grid provided in the **Annexure 1** enclosed with the Policy. The RMC shall have authority to review and revise the grid provided in the **Annexure 1.** The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer.

The nature and extent of due diligence will depend on the risk perceived by Protium. However, while preparing customer profile Protium should take care to seek only such information from the customer which is relevant to the risk category and is not intrusive and is in conformity with the guidelines issued by RBI in this regard. Any other information from the customer will be sought separately with his/her consent.

Customer Risk in this context refers to the money laundering and terrorist funding risk associated with a particular customer from Protium's perspective. This risk categorisation is based on AML/KYC risk perceptions associated with customer profile and not the level of credit risk.

Explanation: FATF Public Statement, the reports and guidance notes on KYC/AML issued by the Indian Banks Association (IBA), guidance note circulated to all cooperative banks by the RBI etc., may also be used in risk assessment

6.5.2 Probable Match with Negative List

The Company shall monitor the following instances and review those from a money laundering risk perspective:

a. Probable match of a customer's identity with the details provided in the UN Sanctioned Terrorist List or any of the negative lists prescribed by the RBI.
b. Negative/ Adverse media report against any customer.
c. Any material complaint or alert received against a customer of the Company.
d. Query or information received from a Law Enforcement Agency regarding a customer of the Company.

6.5.3 Periodic Review of Risk Categorisation

The Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures wherever required as per the regulatory requirements. The Company will put in place a system of periodical review of risk categorization of accounts. The Company will carry such review of risk categorization of customers at a periodicity of not less than once in six months. In case of higher risk perception on a customer, the Company shall assess the need for applying enhanced due diligence measures for such customer.

6.5.4 Money Laundering ("ML") And Terrorist Financing (TF") Risk Assessment

The Company shall carry out the ML and the TF risk assessment for mitigation of AML risks at least Yearly covering the following aspects:

a. Identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, products, services, transactions or delivery channels, etc.
b. 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 also take cognizance of the overall sector- specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.
c. The risk assessment shall be commensurate to the nature, size, geographical presence, complexity of activities of the Company and should be properly documented.
d. The outcome of the exercise shall be put up to the Risk Management Committee of the Company ("RMC") and should be available to competent Authorities and self-regulating bodies.
e. The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the risks (identified on their own or through national risk assessment) and should have Board approved policies, controls and procedures in this regard and shall monitor the implementation of the controls and enhance them if necessary. The Company shall implement a CDD programme, having regard to the ML/TF risks identified and the size of business. Further, company shall monitor the implementation of the controls and enhance them if necessary.

6.5.5 Updation/ Periodic Updation of KYC

The Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. The Company will conduct periodic updation of KYC documents 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. For updation of KYC documents, the Company, shall ensure compliance with the following:

i. Individual Customers

a. **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. The customer may provide such self-declaration through letter or through his/ her email-id/ mobile number registered with the Company or through the Company's digital channels, if available, such as customer portal/ mobile application of the Company etc.
b. **Change in address**: In case of a change in address of the customer, a self-declaration of new address shall be obtained from the customer. The customer may provide such self-declaration through letter or through his/ her email-id/ mobile number registered with the Company or through the Company's digital channels, if available, such as customer portal/ mobile application of the Company etc. Thereafter, the Company shall get the declared address verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc. However, due to its inability to conduct contact point verification/ address verification or any reason as per the discretion of any Senior Management official or the Principal Officer, the Company may obtain a copy of OVD or deemed OVD or the equivalent e- documents thereof, for the purpose of proof of address, declared by the customer at the time of periodic updation.

Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Paragraph 6.3.4 of this Policy are not applicable in case of updation / periodic updation of KYC through 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. However, 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.

ii. Non- Individual Customers

a. **No change in KYC information:** In case of no change in the KYC information of the non- individual customer, a declaration/ letter from an official authorized by such customer along with a copy of the board resolution etc., as applicable, shall be taken. The customer may provide such declaration through letter or through its email-id/ mobile number registered with the Company or through the Company's digital channels, if available, e.g., customer portal/ mobile application of the Company etc.
b. **Beneficial Ownership ("BO") information:** The Company shall take steps to keep BO information available with them accurate and updated, as far as possible.
c. **Change in KYC information:** In case of change in KYC information, the Company shall undertake the KYC process equivalent to that applicable for on boarding a new non- individual customer.

6.5.6 In addition to the above, the Company shall take the following measures:

a. KYC updation shall be applicable even if there is no change in customer information but the documents available with the Company are not as per the current CDD standards. Further, in case the

validity of the CDD documents available with the Company has expired at the time of periodic updation of KYC, the Company shall undertake the KYC process equivalent to that applicable for on boarding a new customer.

b. The customer's PAN details, if available with the Company, will be verified from the database of the issuing authority at the time of periodic updation of KYC.
c. 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.
d. Further, the Company would ensure 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.
e. In order to ensure customer convenience, the facility of updation/periodic updation of KYC may be made available at any branch or through any of the online/ digital/ electronic channels of the Company, subject to compliance with the RBI KYC Directions.
f. The Company shall advise its customers that in order to comply with the PML Rules, in case of any update in the documents submitted by the customer at the time of establishment of business relationship / account-based relationship and thereafter, as necessary; the customers shall submit to the Company the update of such documents, within 30 days of the update to such documents.
g. The Company shall intimate customers in advance about KYC updates and provide at least three reminders before the due date, including one by letter, using available communication channels. If the customer does not comply, three post-due date reminders (again including one letter) shall be sent. These communications shall include clear KYC update instructions, escalation options, and potential consequences for non-compliance.
h. All intimation/reminder records shall be maintained in the Company's system for audit purposes.

6.4.7 Internal Control System

a. The Company's internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC & AML policy and procedures. The compliance function under the guidance of Compliance Head / officer will provide an independent evaluation of the Company's policy and procedure, including legal and regulatory requirements.
b. The Company will ensure that its audit function is staffed adequately with individuals who are well-versed in such policies and procedures or hire the services of a reputed Company engaged in providing quality services in the said field.
c. Internal Auditors will specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard will be put up before the Audit Committee of the Board at quarterly intervals. Any gaps identified by the auditors need to be rectified under the supervision of the Business head or Compliance Head / officer.

6.4.8 Measures to be adopted while dealing with jurisdictions that do not or insufficiently apply the FATF Recommendations

a. Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account.

b. The Company shall consider FATF statements issued by the RBI and other publicly available information to identify countries that do not, or insufficiently, comply with FATF Recommendations. For such countries, REs are required to apply enhanced due diligence measures that are effective and proportionate to the associated risks, in relation to both individuals and entities (including financial institutions).
c. Special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

   Explanation: The processes referred to in (i) & (ii) above do not preclude the Company from having legitimate trade and business transactions with the countries and jurisdictions mentioned in the FATF statement.
d. The background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations shall be examined, and written findings together with all documents shall be retained and shall be made available to Reserve Bank/other relevant authorities, on request.

6.6 MONITORING OF TRANSACTIONS

The Company shall undertake an on-going due diligence/ monitoring of transactions of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business, and risk profile; and the source of funds shall be undertaken on an on-going basis.

The Company shall monitor the transactions undertaken by its customers including the following types of transactions:

a. Cash repayments above certain thresholds.
b. Large and complex transactions and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
c. Frequent prepayments above some thresholds which are not consistent with the Customer's repayment capacity.
d. Frequent cash repayments.
e. Early loan closure within very short time-period of availing the loan.
f. Any unusual pattern in the operations of the accounts which seems inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose, shall be closely monitored
g. Transactions which exceed the thresholds prescribed for specific categories of accounts.

The extent of monitoring shall be aligned with the risk category of the customer. Further, High risk accounts shall be subjected to more intensified monitoring.

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

For ongoing due diligence, Protium may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

Reporting Requirements to Financial Intelligence Unit-India (FIU-IND):

a. In terms of the Rules, the Company is required to report information relating to cash and suspicious transactions electronically to FIU India. The Company needs to comply with such reporting requirement by utilising the formats stipulated in the Master Directions and as prescribed by FIU-IND.
b. For the following transactions, the Company shall file the Cash Transaction Report ("CTR") which for a month should reach to the FIU-IND by 15th day of the succeeding month:
   - all cash transactions of the value of more than ₹10 Lakh; or
   - all series of cash transactions integrally connected to each other which have been valued below ₹10 Lakh where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds ₹10 Lakh.
c. The Suspicious Transaction Report (STR) shall be submitted within 7 working days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature.
d. In this regard, the Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.
d. The Company shall keep in mind that any delay in furnishing of information would result into a violation of the requirement stipulated in the Rules.
e. The Principal Officer will be responsible for timely submission of STR to FIU-IND. No Nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.
f. Details of accounts resembling any of the individuals / entities in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC) shall be reported to FIU-IND apart from advising Ministry of Home Affairs as required under Unlawful Activities Prevention Act, 1967 ('UAPA') notification dated February 2, 2021.
g. The Company shall not put any restrictions on operations in the accounts merely based on the STR filed.
h. In addition to the above, all such cash transactions identified where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transactions, if any, shall also be reported by the Company to FIU-IND as Counterfeit Currency Report by 15th day of the succeeding month.

The Company, its Directors, Officers, and all employees shall ensure that the fact of maintenance of records referred to in rule 3 of the PML (Maintenance of Records) Rules, 2005 and furnishing of the information to the director is confidential and its Directors, Officers and employees (permanent and temporary) will be prohibited from disclosing ('tipping off') the fact that an STR or related information is being reported or provided to the FIU- IND. However, such confidentiality requirement shall not inhibit sharing of information under section 4(b) of Master Direction of any analysis of transactions and activities which appear unusual, if any such analysis has been done.

This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be the duty of all employees involved to ensure that there is no tipping off to the customer at any level.

Reporting requirement under Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standards (CRS)

The Company adheres to the provisions of the Income Tax Rules 114F, 114G and 114H, as applicable. It shall determine whether they are a reporting financial institution and shall follow the steps for complying with the reporting requirements.

7. RECORD MANAGEMENT

The following steps shall be taken regarding maintenance, preservation and reporting of customer information, with reference to provisions of PML Act and Rules.

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. maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following:
   i. the nature of the transactions.
   ii. the amount of the transaction and the currency in which it was denominated.
   iii. the date on which the transaction was conducted; and
   iv. the parties to the transaction.
c. preserve the records pertaining to the identification of the customers and their addresses obtained while opening the account and during the course of business relationship, for at least five years after the business relationship is ended;
d. make available swiftly, the identification records and transaction data to the competent authorities upon request;
e. introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005);
f. 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.
g. The records of identity and address of their customer, and records in respect of transactions referred to in Rule 3 shall be maintained in hard or soft copy.
h. The Company shall ensure that in case of customers who are non-profit organisations, the details of such customers are registered on the DARPAN Portal of NITI Aayog. If the same are not registered, the Company shall register the details on the DARPAN Portal and also maintain such registration records for a period of five years after the business relationship between the customer and Company has ended or the account has been closed, whichever is later.

Explanation. – For the purpose of this Section, the expressions "records pertaining to the identification", “identification records,” etc., shall include updated records of the identification data, account files, business correspondence and results of any analysis undertaken.

8. OTHER INSTRUCTIONS

8.1. *Selling Third Party Products*

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

a. The identity and address of the walk-in customer shall be verified for the transactions as required under the CIP prescribed above.
b. Transaction details of sale of third-party products and related records shall be maintained.

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

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

e. Instruction at 'd' above shall also apply to sale of REs' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for rupees fifty thousand and above.

f. Monitoring of transactions for any suspicious activity will be done.

8.2. *Quoting of PAN*

In accordance with the Income Tax Rule 114B, for cash collection of ₹50,000/- and more than in a single day, the Company shall ensure the following:

a. If the borrower's PAN is not updated in system, PAN of the customer along with a copy of the PAN Card shall be required to be collected for cash receipt of ₹50,000/- or more. Further, the PAN shall be updated in the Company's system.

b. If any borrower is not having PAN, then Form 60 duly signed by the borrower along with a valid identity proof shall be collected for cash receipt of ₹50,000/- and more.

8.3. *Hiring of Employees and Employee Training*

8.3.1. Hiring of Employees

The Company shall put in place an adequate screening mechanism as an integral part of its personnel recruitment/ hiring process.

The Company shall endeavour to ensure that the staff dealing with/ being deployed for KYC/ AML/ CFT matters have the following:

i. high integrity and ethical standards;
ii. good understanding of extant KYC/ AML/ CFT standards;
iii. effective communication skills; and
iv. ability to keep up with the changing KYC/ AML/ CFT landscape, nationally and internationally.

The Company shall also strive to develop an environment which fosters open communication and high integrity amongst the staff. Any inefficient or suspicious behavior of employees shall be dealt with suitably. It shall be ensured that there is no tipping off to the customer at any level.

8.3.2. Employees' training

The Company shall organise employee training programmes so that the members of staff are adequately trained in the KYC/AML /CFT procedures and fully understand the rationale behind the KYC/AML policies and implement them consistently.

All necessary circulars, guidelines, notifications issued by the RBI or government authority in connection with KYC / AML procedures will be communicated to all relevant members of the Company by the Compliance Officer. Relevant members of the Company shall include frontline staff, back-office staff, senior staff, risk management staff and staff dealing with new clients.

The training shall include all frontline staff, operations staff and staff dealing with new customers. The front desk staff shall be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policy of Ambium, regulation and related issues shall be ensured by the compliance officer.

8.4. *Customer Education*

The implementation of KYC procedures requires the Company to demand certain information from customers, which may be of personal nature, or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Company's front line staff will therefore personally discuss this with customers and if required, the Company may also prepare specific literature/ pamphlets, etc. to educate the customer on the objectives of the KYC program.

8.5. *Secrecy Obligations and Sharing of Information*

a. The Company officials shall maintain confidentiality of information as provided under Section 45NB of the RBI Act 1934.
b. The Company shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the Company and customer.
c. Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.
d. While considering the requests for data/information from Government and other agencies, the Company shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the transactions.
e. The exceptions to the said rule shall be as under:
    i. Where disclosure is under compulsion of law
    ii. Where there is a duty to the public to disclose,
    iii. The interest of the Company requires disclosure; and
    iv. Where the disclosure is made with the express or implied consent of the customer.

8.6. *Introduction of New Technologies*

The Company shall identify and assess the ML/ TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Further, the Company shall ensure:

a. to undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
b. adoption of a risk-based approach to manage and mitigate the risks through appropriate EDD measures and transaction monitoring, etc.

9. REVIEW OF THE POLICY

The Board of Directors shall review this Policy annually or on a need-basis i.e., in the event of change in regulatory framework or for business or operational need (whichever is earlier). Such updates / changes to the Policy will be communicated to the relevant staff /personnel (both in-house or outsourced) and relevant stakeholders across the Company.

Any deviations from this Policy can only be undertaken with the approval of the Board, unless specified otherwise in this Policy.

Annexure 1

RISK CATEGORIZATION TABLE

Risk Categorization at the time of onboarding		
High Risk	**Medium Risk**	**Low Risk**
a. Non-Resident Indians for the authorized business transactions, if any b. Foreign citizens for the authorized business transactions, if any c. Cooperative banks d. Credit Societies e. Companies Incorporated overseas. f. Charitable Originations (Non Education) g. Trusts (Non-Education) h. Society (Non-Education) i. NGOs (excluding UN promoted NGOs) j. Local/ domestic foreign Politically Exposed Persons (PEPs) and their relatives. k. Customers engaged into the following businesses (with Annual Turnover > 100 Cr.) Bullion, Gold, Silver, Diamond, Gems/ Precious Stones, Jewellery l. Non face to face	a. NBFCs b. Micro Finance Institutions (MFI) c. HUF d. Trusts (Education less than 5 years) e. Society (Education less than 5 years) f. Foreign Currency Exchange Dealers g. Chit Funds h. Association of Persons (AOP)/Body of Individuals (BOI)/ Artificial Judicial Person (AJP) i. Customers engaged into the following: ▪ Real Estate (Individual & Nonindividual) ▪ Stock Market (Individual & Franchisees of brokers) (j) Customers engaged into the following businesses (with Annual turnover <= 100 Cr.): Bullion, Gold, Silver, Diamond, Gems/ precious stones, Jewellery	a. Individual Resident (other than specified in High risk). b. Sole proprietorship entity c. Partnership d. Unlisted Public Limited Companies e. Limited Liability Partnership (LLP) f. Private Limited company g. Domestic Listed companies. h. Government depts. &local bodies i. Central or State Government owned companies j. Regulatory & Statutory bodies k. Society (Education more than 5 years) l. Trusts (Education more than 5 years) m. Corporate Financial Intermediaries regulated/ governed/ controlled by RBI/ IRDA/ SEBI/ PFRDA example- ▪ Insurance companies ▪ Mutual funds ▪ Security firms registered with the SEBI. ▪ Banks (excluding coop. bank) n. Other customers not covered in high and medium