KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY LAUNDERING (AML) POLICY

LOGIX CORPORATE SOLUTIONS PRIVATE LIMITED

1. Introduction

Logix Corporate Solutions Private Limited ("the Company") is a Non-Banking Financial Company – Investment and Credit Company (NBFC-ICC), registered with the Reserve Bank of India ("RBI") vide Certificate of Registration No. [CoR Number], and classified as a Base Layer NBFC (NBFC-BL) under the RBI's Scale Based Regulatory framework. The Company does not accept public deposits.

This Policy sets out the Company's framework for Know Your Customer ("KYC") norms, Customer Due Diligence ("CDD") measures, and Anti-Money Laundering / Combating the Financing of Terrorism ("AML/CFT") controls, applicable to every customer with whom the Company establishes an account-based or lending relationship.

As per the RBI Master Direction - Know Your Customer (KYC) Direction, 2016 dated February 25, 2016 and updated from time to time wherein Non-Banking Finance Companies (NBFCs) are advised to follow certain customer identification procedures while undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions., Logix Corporate Solutions Private Limited has framed this Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy. This Policy shall come into force with effect from the date of its approval by the Board of Directors and shall remain in force until amended or replaced.

This Policy has been framed in accordance with the Reserve Bank of India (Know Your Customer (KYC)) Direction, 2016, dated February 25, 2016 (as amended from time to time), the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 (PML Rules), and other applicable laws, regulations, circulars, notifications and guidelines issued by the Reserve Bank of India from time to time.

2. Objective

Objective of RBI guidelines is to prevent banks and other financial institutions from being used as a channel for Money Laundering (ML)/ Terrorist Financing (TF) and to ensure the integrity and stability of the financial system. The guidelines also mandates making reasonable efforts to determine the true identity and beneficial ownership of accounts, source of funds, the nature of customer’s business, reasonableness of operations in the account in relation to the customer’s business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

3. Definitions

i. **"Authorised Representative"** means a person other than an Advocate duly appointed and authorised in writing to represent a complainant in the proceedings before the Ombudsman.

ii. **Beneficial Owner (BO)**

Beneficial Owner (BO) means the natural person(s) who ultimately owns, controls, or exercises effective control over the customer or on whose behalf a transaction is conducted.

a) **Company:** The BO is the natural person(s) having more than 10% ownership or entitlement to shares, capital or profits, or exercising control through management rights, shareholding, voting agreements, shareholders' agreements, or the right to appoint the majority of directors.

b) **Partnership Firm:** The BO is the natural person(s) having more than 10% ownership or entitlement to the capital or profits of the partnership or exercising control over its management or policy decisions.

c) **Unincorporated Association/Body of Individuals (including societies):** The BO is the natural person(s) having more than 15% ownership or entitlement to the property, capital or profits. Where no such natural person is identified, the Senior Managing Official shall be treated as the Beneficial Owner.

d) **Trust:** The BO shall include the author of the trust, trustee(s), beneficiaries having 10% or more interest, and any other natural person exercising ultimate effective control over the trust through ownership or control.

iii. **"Board"** means Board of Directors of the Company.

iv. **"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.

v. **"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. 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. 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.

vi. **"Company"** means Logix Corporate Solutions Private Limited.

vii. **"Director"** means individual Director or any of the Directors on the Board of the Company.

viii. **"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.

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

x. **"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.

xi. Officially Valid Document (OVD) means a Passport, Driving Licence, Proof of Possession of Aadhaar Number, Voter Identity Card, NREGA Job Card, or National Population Register (NPR) Letter containing the customer's name and address. Where Aadhaar is submitted as an OVD, it shall be in the form issued by the Unique Identification Authority of India (UIDAI).

Where an OVD does not contain the current address, the Company may accept such alternative documents as permitted under applicable RBI guidelines, subject to submission of an updated OVD within the prescribed period. For foreign nationals, documents issued by the foreign Government or the Foreign Embassy/Mission in India may be accepted as proof of address. An OVD shall remain valid despite a subsequent change in the customer's name, provided the change is supported by valid documentary evidence in accordance with applicable law.

xii. **"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).

xiii. "RBI" means Reserve Bank of India.

a. "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:
b. 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
c. appears to be made in circumstances of unusual or unjustified complexity; or
d. appears to not have economic rationale or bona-fide purpose; or
e. 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.

xiv. "Regulated Entities" (REs) means

a. 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'
b. All India Financial Institutions (AIFIs)
c. All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs)
d. Asset Reconstruction Companies (ARCs)
e. All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)
f. All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xv. **"Small Account"** means a savings account which is opened in terms of sub-rule (5) of rule 9 of the PML Rules, 2005. Details of the operation of a small account and controls to be exercised for such account.

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

- **a.** opening of an account;
- **b.** deposit, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- **c.** 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.

xvii. **Other Definitions:**

Unless the context otherwise requires, the following terms shall have the meanings assigned below:

i. **Common Reporting Standards (CRS):** The international reporting standards for automatic exchange of financial account information under the Convention on Mutual Administrative Assistance in Tax Matters.

ii. **Correspondent Banking:** Banking services provided by one bank to another bank, including cash management, international wire transfers, cheque clearing, payable-through accounts, and foreign exchange services.

iii. **Customer:** A person engaged in a financial transaction or activity with the Company, including a person on whose behalf such transaction or activity is undertaken.

iv. **Walk-in Customer:** A person who does not have an account-based relationship with the Company but undertakes transactions with it.

v. **Customer Due Diligence (CDD):** The process of identifying and verifying the customer and the beneficial owner using reliable and independent sources, including understanding the nature of the business relationship and ownership/control, wherever applicable.

vi. **Customer Identification:** The process of undertaking Customer Due Diligence (CDD).

vii. **KYC Templates:** Standard templates prescribed for capturing and reporting customer KYC information to the Central KYC Records Registry (CKYCR).

Unless otherwise defined in this Policy, all terms shall have the meanings assigned to them under the Banking Regulation Act, 1949, Reserve Bank of India Act, 1934, Prevention of Money Laundering Act, 2002, PML Rules, 2005, Aadhaar Act, 2016, and other applicable laws, rules, regulations, or statutory amendments.

4. Scope

REs' policy framework should seek to ensure compliance with PML Act/Rules, including regulatory instructions in this regard and should provide a bulwark against threats arising from money laundering, terrorist financing, proliferation financing and other related risks. While ensuring compliance of the legal/regulatory requirements as above, REs may also consider adoption of best international practices taking into account the FATF standards and FATF guidance notes, for managing risks better.

The KYC policy shall include following four key elements:
(a) Customer Acceptance Policy;
(b) Risk Management;
(c) Customer Identification Procedures (CIP); and
(d) Monitoring of Transactions.

5. Designation of Principal Officer

The Board of Directors shall designate a Principal Officer, at a senior management level, who shall be responsible for: (a) monitoring and reporting all transactions and sharing information as required under the PML Act, PML Rules, and this Policy; (b) filing of Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), and any other report required by FIU-IND; (c) maintaining close liaison with law enforcement agencies, banks, and other institutions involved in the fight against money laundering and terrorist financing; and (d) ensuring overall compliance with the Master Direction and this Policy.

The Principal Officer shall have timely access to customer identification data, CDD information, transaction records, and other relevant information. The name, designation, and contact details of the Principal Officer shall be communicated to FIU-IND and the Reserve Bank of India, and shall be updated in this Policy whenever there is a change.

6. Compliance of KYC policy

a) REs shall ensure compliance with KYC Policy through:
- **i.** Specifying as to who constitute 'Senior Management' for the purpose of KYC compliance.
- **ii.** Allocation of responsibility for effective implementation of policies and procedures.

iii. Independent evaluation of the compliance functions of REs' policies and procedures, including legal and regulatory requirements.
iv. Concurrent/internal audit system to verify the compliance with KYC/AML policies and procedures.
v. Submission of quarterly audit notes and compliance to the Audit Committee.

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

7. Customer Acceptance Policy

The Company shall establish customer relationships only after completing the prescribed Customer Due Diligence (CDD) in accordance with the applicable RBI KYC Directions, the Prevention of Money Laundering Act, 2002, and the rules made thereunder. No account or business relationship shall be established in the name of an anonymous, fictitious or benami person, or where the Company is unable to complete the required CDD due to non-cooperation of the customer or unreliable information/documents. Where appropriate, the Company shall file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit – India (FIU-IND) in accordance with the applicable regulatory requirements.

The Company shall obtain all mandatory KYC information at the time of onboarding and during periodic KYC updation, apply CDD at the Unique Customer Identification Code (UCIC) level, verify PAN, GSTIN (where applicable), and equivalent electronic documents, and screen customers against applicable sanctions lists. The Company shall also ensure that CDD is conducted for all joint account holders and for customers acting on behalf of another person or entity, in accordance with applicable laws and internal procedures.

The Customer Acceptance Policy shall be implemented in a fair and non-discriminatory manner and shall not result in denial of financial services to eligible customers, particularly financially or socially disadvantaged persons, including Persons with Disabilities (PwDs). Any additional information beyond the prescribed KYC requirements shall be obtained only with the customer's explicit consent, and any rejection of customer onboarding or KYC updation shall be based on valid reasons, duly recorded by the authorised officer.

8. Risk Management

The Company shall ensure the following:

a. Customers shall be categorised as Low Risk, Medium Risk and High Risk based on the assessment and risk perception of the Company.

b. The Company shall lay down broad principles for the risk categorisation of customers.

c. Risk categorisation shall be undertaken based on parameters such as the customer's identity, social and financial status, nature of business activity, information relating to the customer's business and location, geographical risk relating to customers as well as transactions, type of products and services offered, delivery channels used for providing products and services, and the types of transactions undertaken, including cash, cheque/monetary instruments, wire transfers and foreign exchange transactions. While considering the customer's identity, the ability to confirm identity documents through online or other services provided by the issuing authorities may also be taken into account.

d. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be disclosed to the customer.

Provided that the information collected from different categories of customers relating to the perceived risk is non-intrusive and is specified in this Policy.

The Company may also use the Financial Action Task Force (FATF) Public Statements, reports and guidance notes on KYC/AML issued by the Indian Banks' Association (IBA), and guidance issued by other relevant agencies for the purpose of risk assessment.

9. Customer Identification Procedure (CIP)

The Company shall undertake the Customer Identification Procedure (CIP) at the commencement of an account-based relationship, while carrying out occasional or specified transactions, international money transfer operations for non-account holders, or whenever there is doubt regarding the authenticity or adequacy of the customer's identification data. CIP shall also be carried out for walk-in customers, customers undertaking specified transactions or services offered by the Company, and where the Company has reason to believe that a customer is intentionally structuring transactions to avoid regulatory requirements. The Company shall not insist upon customer introduction for opening an account.

The Company may rely on the Customer Due Diligence (CDD) carried out by a regulated third party or through the Central KYC Records Registry (CKYCR), provided that the CDD records and identification documents are obtained without delay, the third party is regulated and compliant with the applicable provisions of the Prevention of Money Laundering Act, 2002 and the rules made thereunder, and is not based in a high-risk jurisdiction.

Notwithstanding such reliance, the ultimate responsibility for carrying out Customer Due Diligence (CDD), including Enhanced Due Diligence (EDD) wherever applicable, shall always remain with the Company.

10. Customer Due Diligence (CDD) Procedure – Individuals

The Company shall undertake Customer Due Diligence (CDD) while establishing an account-based relationship with an individual and while identifying any beneficial owner, authorised signatory or power of attorney holder of a legal entity. The Company shall obtain the prescribed KYC documents, including Aadhaar (where permitted), Officially Valid Document (OVD), KYC Identifier, PAN/Form 60, and such other information as may be required under its risk-based approach. Aadhaar, Digital KYC and equivalent electronic documents shall be verified in accordance with applicable RBI guidelines.

Where customer onboarding is undertaken through non-face-to-face modes, including Aadhaar OTP-based e-KYC or Video-based Customer Identification Process (V-CIP), the Company shall comply with the applicable RBI requirements relating to customer consent, authentication, identity verification, security, monitoring and record maintenance. Where simplified account opening is permitted under RBI guidelines, the Company shall comply with the prescribed conditions, complete full CDD within the stipulated timeline, and apply enhanced monitoring wherever required. KYC completed at any branch or office of the Company shall be valid across all branches/offices, subject to periodic KYC updation.

11. CDD Measures for Sole Proprietary Firms

For opening an account in the name of a sole proprietary firm, the Company shall carry out the CDD of the proprietor in accordance with this Policy. The Company shall obtain documentary evidence of the firm's existence and business activity, such as Government registration, GST registration, tax returns, statutory licences, IEC, professional certificates, or utility bills in the name of the firm. Normally, any two such documents (or equivalent e-documents) shall be obtained. However, where two documents are not available, the Company may accept one document, subject to satisfactory contact point verification and collection of additional information or documents to independently establish the existence and address of the proprietary concern.

12. CDD Measures for Legal Entities

Companies

For opening an account of a company, certified copies of the following documents (or equivalent e-documents) shall be obtained:

a. Certificate of Incorporation;
b. Memorandum and Articles of Association;
c. Permanent Account Number of the company;

d. a Board resolution and power of attorney granted to managers, officers or employees to transact on the company's behalf, together with CDD documents (as per Section 9) of such persons;
e. the names of persons holding senior management positions; and
f. the registered office and principal place of business, if different.

Partnership Firms

For opening an account of a partnership firm, certified copies of the following shall be obtained: registration certificate; partnership deed; PAN of the firm; CDD documents (as per Section 9) of the beneficial owner(s) and any person holding a power of attorney to transact on the firm's behalf; the names of all partners; and the address of the registered office and principal place of business, if different.

Trusts

For opening an account of a trust, certified copies of the following shall be obtained: registration certificate; trust deed; PAN or Form No. 60 of the trust; CDD documents of the beneficial owner(s) and any authorised signatory; the names of the beneficiaries, trustees, settlor/author and protector (if any); and the address of the registered office. Trustees shall be required to disclose their status to the Company at the time of commencement of the relationship or when carrying out any specified transaction.

Unincorporated Associations / Bodies of Individuals

For opening an account of an unincorporated association or body of individuals (which shall be deemed to include unregistered trusts, unregistered partnership firms, and societies), the Company shall obtain: a resolution of the managing body; PAN or Form No. 60 of the association; power of attorney to transact on its behalf; CDD documents of the beneficial owner(s) and authorised signatories; and such other information as may be required to collectively establish the association's legal existence.

Other Juridical Persons

For a customer that is a juridical person not specifically covered above (e.g., societies, universities, local bodies/panchayats), the Company shall obtain documentation identifying the person authorised to act on the entity's behalf, CDD documents of such person, and such documents as may be required to establish the entity's legal existence.

13. Identification of Beneficial Owner

For opening an account of a legal person that is not a natural person, the Company shall identify the beneficial owner(s), as defined in Section 3 of this Policy, and take all reasonable steps to verify their identity, using reliable and independent documentation, data or information, keeping in view the following:

a. where the customer, or the owner of the controlling interest, is an entity listed on a stock exchange in India, or is resident in a jurisdiction notified by the Central Government and listed on a stock exchange in such jurisdiction, or is a subsidiary of such a listed entity, it shall not be necessary to identify and verify the identity of any shareholder or beneficial owner of that entity;

b. in the case of trust, nominee or fiduciary accounts, the Company shall determine whether the customer is acting on behalf of another person as trustee, nominee or intermediary, and shall obtain satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they act, together with details of the nature of the trust or arrangement.

14. On-going Due Diligence

The Company shall undertake ongoing due diligence to ensure that customer transactions are consistent with the customer's profile, business, risk category and source of funds. The Company shall monitor unusual, complex or suspicious transactions, account activity inconsistent with the customer's profile, threshold-based transactions and unusual third-party transactions using a risk-based approach. The Company may leverage appropriate technology, including Artificial Intelligence (AI) and Machine Learning (ML), for effective transaction monitoring and shall review customer risk categorisation at least once every six months.

The Company shall carry out periodic KYC updation on a risk-based basis to ensure that Customer Due Diligence (CDD) records remain accurate and current, in accordance with RBI-prescribed timelines. Depending on the nature of changes, the Company may obtain self-declarations, updated KYC documents, fresh photographs or conduct fresh CDD, as applicable. Customers shall promptly inform the Company of any changes in their KYC information, and the Company shall update and verify KYC records, issue acknowledgements, send appropriate reminders for KYC compliance, and take regulatory action, including operational restrictions where required, in accordance with applicable RBI guidelines.

15. Enhanced and Simplified Due Diligence Procedure

The Company shall apply Enhanced Due Diligence (EDD) for customers onboarded through non-face-to-face channels in accordance with applicable RBI guidelines. Wherever available, Video-based Customer Identification Process (V-CIP) shall be the preferred mode of remote onboarding. The Company shall independently verify the customer's address, verify PAN from the issuing authority, ensure the first transaction/disbursement is routed through an

existing KYC-compliant bank account, and subject such customers to enhanced monitoring and appropriate risk classification until their identity is fully verified. The Company shall also implement suitable controls for registered mobile number changes in accordance with its Board-approved policy.

The Company may establish relationships with Politically Exposed Persons (PEPs) only after applying enhanced due diligence, including identification of PEP status, verification of source of funds/wealth, approval from Senior Management, and enhanced ongoing monitoring. These requirements shall also apply to the family members and close associates of PEPs. Where accounts are opened through professional intermediaries, the Company shall identify the underlying customer(s) and beneficial owner(s), may rely on CDD performed by regulated intermediaries where permitted, and shall retain ultimate responsibility for compliance with KYC/CDD requirements.

The simplified due diligence provisions prescribed under the RBI Master Direction for categories such as Self-Help Groups (SHGs), Foreign Portfolio Investors (FPIs), and foreign students' NRO accounts are generally not applicable to the Company's business as a Non-Deposit Taking NBFC-ICC and shall be adopted only if they become applicable to the Company's business model.

16. Record Management

The Company shall maintain records of all customer transactions and Customer Due Diligence (CDD) documents in accordance with the Prevention of Money Laundering Act, 2002 (PMLA) and the rules made thereunder. Transaction records shall be preserved for at least five years from the date of the transaction, while customer identification and KYC records shall be retained for at least five years after the business relationship ends. Such records shall be maintained in physical or electronic form.

The Company shall ensure that transaction records contain sufficient details to enable reconstruction of individual transactions and are readily retrievable for submission to competent authorities whenever required. Where the customer is a Non-Profit Organisation (NPO), the Company shall verify its registration on the DARPAN Portal of NITI Aayog, wherever applicable, and retain the related records for five years after the termination of the business relationship.

17. Reporting Requirements to Financial Intelligence Unit – India (FIU-IND)

The Company shall furnish to the Director, FIU-IND, the information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005, in the manner and format (including Cash

Transaction Reports and Suspicious Transaction Reports) prescribed by FIU-IND from time to time, using the electronic reporting utilities placed on the FIU-IND website (www.fiuindia.gov.in) where the Company has not adopted its own technological tools for report generation.

A delay of each day in reporting a transaction, or in rectifying a mis-represented transaction beyond the prescribed timeline, shall constitute a separate violation. The Company shall not restrict operations in an account merely on the basis of an STR having been filed in respect of it.

The Company, its Directors, officers and employees shall maintain strict confidentiality regarding the fact of record maintenance under Rule 3 and the furnishing of information to the Director, FIU-IND, save that such confidentiality shall not preclude the sharing of analysis of unusual transactions/activities as contemplated under this Policy.

The Company shall deploy software capable of generating alerts where transactions are inconsistent with the customer's risk categorisation and updated profile, as part of effective identification and reporting of suspicious transactions.

18. Obligations under International Agreements – Sanctions Screening

Unlawful Activities (Prevention) Act, 1967 (UAPA)

In terms of Section 51A of the UAPA, 1967, the Company shall ensure it does not maintain any account in the name of individuals/entities appearing on the UNSC's "ISIL (Da'esh) & Al-Qaida Sanctions List" or "Taliban Sanctions List", or in the Schedules to the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007. These lists shall be verified on a daily basis, and any account resembling a listed individual/entity shall be reported to FIU-IND and to the Ministry of Home Affairs. Where an order to freeze assets is received under Section 51A, the Company shall comply without delay in accordance with the procedure prescribed in the UAPA Order dated February 2, 2021 (Annex II to the Master Direction).

Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 (WMD Act)

The Company shall ensure meticulous compliance with the procedure prescribed under Section 12A of the WMD Act, 2005 (Annex III to the Master Direction), including running a check against the designated list at the time of onboarding and on a periodic basis, declining to carry out any transaction where particulars match the designated list, and immediately reporting any match to the Central Nodal Officer designated under the Act (with a copy to the RBI), together with full particulars of the funds/assets involved.

UNSCR 1718 (DPRK) and Other Sanctions Lists

The Company shall verify the 'UNSCR 1718 Sanctions List of Designated Individuals and Entities' on a daily basis and ensure compliance with the Implementation of Security Council Resolution on Democratic People's Republic of Korea Order, 2017, as well as other applicable UNSC Resolutions and the First and Fourth Schedules to the UAPA, as amended from time to time.

FATF High-Risk and Non-Cooperative Jurisdictions

The Company shall take into account FATF Statements circulated by the RBI identifying jurisdictions that do not, or insufficiently, apply FATF Recommendations, and shall apply enhanced due diligence — proportionate to the risk — to any business relationship or transaction connected with such jurisdictions, examining and retaining written findings on the background and purpose of such transactions for production to the RBI or other authorities on request. This does not preclude the Company from engaging in legitimate business with persons connected to such jurisdictions.

19. Other Instructions

Secrecy Obligations and Sharing of Information

The Company shall maintain the confidentiality of customer information and shall not disclose or use such information for cross-selling or any other purpose without the customer's consent, except where disclosure is required by law, in the public interest, to protect the Company's legitimate interests, or with the customer's express or implied consent. The Company shall upload and update customer KYC records with the Central KYC Records Registry (CKYCR) within the prescribed timelines, communicate the KYC Identifier to customers, and retrieve KYC records from CKYCR wherever available to avoid duplication of documentation.

Unique Customer Identification Code (UCIC) and Technology

The Company shall allot a Unique Customer Identification Code (UCIC) to customers and apply Customer Due Diligence (CDD) at the UCIC level to avoid repeated KYC for existing customers. Before introducing any new products, services or delivery channels, the Company shall assess and mitigate Money Laundering/Terrorist Financing (ML/TF) risks through an appropriate risk-based approach.

Employee Training and Third-Party Products

The Company shall maintain a Know Your Employee (KYE) framework, conduct periodic KYC/AML/CFT training for employees, and ensure that relevant staff possess adequate knowledge of regulatory requirements. Where the Company distributes third-party financial products, it shall comply with the applicable KYC, AML/CFT, record-keeping and transaction monitoring requirements prescribed under the applicable RBI and PMLA guidelines.

20. Repeal and Savings

This Policy shall be reviewed and placed before the Board of Directors (or a committee of the Board to which the power has been delegated) at least once every year, or earlier if warranted by a change in the Master Direction, the PML Act/Rules, or the Company's risk assessment. Any prior KYC/AML policy of the Company stands superseded to the extent of inconsistency with this Policy from the effective date stated in Section 1. Approvals, acknowledgements and actions taken under the superseded policy shall be deemed to have been taken under this Policy, and shall continue to be valid and binding unless expressly revised.

21. Annexures

The following shall be maintained as annexures to this Policy and updated independently of the main body as operational or regulatory requirements evolve:

a. Annexure I — List of Officially Valid Documents (OVDs) and deemed OVDs for proof of identity/address, as prescribed under Section 3(ix) of this Policy.
b. Annexure II — Risk Categorisation Matrix (criteria and scoring for Low/Medium/High risk classification, as referenced in Section 7).
c. Annexure III — Formats for Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR), as prescribed by FIU-IND.
d. Annexure IV — Name, designation, and contact details of the Principal Officer and escalation matrix for KYC/AML exceptions.
e. Annexure V — List of sanctions/watch-lists to be screened (UNSC 1267/1988/1718 lists, UAPA Schedules, WMD Act designated list), with the frequency of screening.