upstox

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) Policy

VERSION 1.1

Document Details

Title: AML CFT Policy	Document Owner: Compliance
Document Author(s): Devyanti Rana	Version: 1
Classification: Internal	Release Date: 31-Jul-2026

Version Details

Sr No.	Version	Description	Modified By	Reviewed By	Approved By	Approval Date
1	1	Initial release of the AML CFT Policy governing GIFT City operations	Devyanti Rana	Meghana Mahadkar	Board of Directors	31/07/2026

Content

Preamble

Upstox Securities Private Limited ("the Entity") operates in the International Financial Services Centre (IFSC) through a Separate Business Unit (SBU) established at GIFT IFSC and is duly registered as a Broker-Dealer with the International Financial Services Centres Authority (IFSCA) under registration number CMI2026BDK1028, and separately holds trading membership of India INX . The Entity is also an IFSCA registered Global Access Provider under registration number [●] in its role as a GAP, shall be facilitating access to global markets for resident Indian individual clients in accordance with applicable regulatory requirements including the IFSCA Regulatory Framework for Global Access in the IFSC (circular dated 12 August 2025).

Given the cross-border nature of operations and the risks associated with international financial systems, the Entity acknowledges its responsibility to prevent misuse of its platform for money laundering, terrorist financing, and proliferation financing. This Policy is formulated in accordance with the IFSCA (Anti-Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022, as amended by circulars dated 13 October 2023, 5 June 2025 and 2 January 2026 (the "AML/CFT/KYC Guidelines"), read with the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the IFSCA (Capital Market Intermediaries) Regulations, 2025, the IFSCA Regulatory Framework for Global Access in the IFSC (circular dated 12 August 2025), and applicable circulars and directions issued by regulatory authorities.

This Policy establishes a comprehensive framework comprising governance, customer due diligence, transaction monitoring, reporting mechanisms, and internal controls designed to manage AML/CFT risks effectively.

Objective

The objective of this Policy is to implement a robust AML/CFT framework that enables the Entity to prevent, detect, and report money laundering and terrorist financing activities. The Policy aims to ensure that all customer relationships are established after proper due diligence, that transactions are monitored on an ongoing basis, and that suspicious activities are identified and reported in a timely manner.

The Policy further ensures that AML/CFT risks are assessed using a risk-based approach, records are maintained as per regulatory requirements, and employees are adequately trained to identify financial crime risks.

Scope and applicability

This Policy applies to all resident Indian individual clients onboarded by the IFSC SBU and covers

the entire lifecycle of the client relationship, including onboarding, trading activities, fund transfers, and ongoing monitoring.

The Policy shall apply to:

- All employees, officers, and directors of the Entity
- All business units involved in onboarding and operations
- All third-party service providers and intermediaries involved in AML functions

The Policy shall govern all modes of interaction with clients, including digital, physical, and intermediary-based channels.

Governance Framework

The Board of Directors shall have overall responsibility for the approval and oversight of this Policy. The Board shall periodically review the AML/CFT risk exposure and ensure that appropriate controls are in place.

Senior Management shall be responsible for implementation of the Policy and for ensuring that AML/CFT controls are effectively integrated into business operations.

A Designated Director of the Entity will be responsible for ensuring overall compliance with the obligations imposed under Chapter IV of the Prevention of Money-Laundering Act, 2002 and the rules made thereunder.

The Entity shall designate a Principal Officer who shall be responsible for monitoring compliance with AML/CFT requirements, reporting suspicious transactions to FIU-IND, and liaising with regulatory authorities.

The Designated Director and the Principal Officer shall at all times be different individuals. The names and contact details of the Designated Director and the Principal Officer, and any change thereto, shall be communicated to FIU-IND and IFSCA within 7 (seven) days of appointment or change. Both the Designated Director and the Principal Officer shall complete, and continuously maintain, the NISM-IFSCA-01 Certification Course on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) in the IFSC, in accordance with Clauses 8.2 and 8.4 of Chapter VIII of the AML/CFT/KYC Guidelines and IFSCA circular dated 17 November 2025.

The Compliance Function shall conduct customer due diligence, review transaction alerts, investigate red flags, maintain records, and ensure regulatory reporting. All employees shall promptly report any suspicious or unusual activity observed during the course of their duties.

Risk-Based Approach

The Entity shall adopt a risk-based approach to AML/CFT compliance, whereby the level of due diligence, monitoring, and control measures applied to a client shall be commensurate with the level of risk associated with such client.

At the time of onboarding and on an ongoing basis, the Entity shall undertake a structured assessment of each client's risk profile. This assessment shall consider key factors including the client's background and occupation, source of funds, geographic exposure, reputation including adverse media, mode of interaction, and expected transaction behaviour.

Based on this assessment, clients shall be categorised into **Low, Medium, or High risk**, and the extent of due diligence and monitoring shall be aligned accordingly. Higher-risk clients shall be subject to enhanced due diligence and more intensive monitoring, while lower-risk clients shall be subject to proportionate controls.

The risk categorisation shall not be static and shall be subject to periodic review. The Entity shall reassess and update the risk classification of clients in case of any material change in their profile, transaction patterns, or external risk indicators. Where elevated risk is identified at any stage, appropriate escalation and enhanced controls shall be applied without delay.

The overall risk assessment methodology, including scoring and classification criteria, shall be documented and reviewed periodically to ensure continued effectiveness and alignment with regulatory expectations.

Customer Due Diligence (CDD)

The Entity shall undertake Customer Due Diligence prior to establishing any business relationship. This shall include identification and verification of the customer using reliable, independent, and digitally verifiable sources.

The Entity shall onboard clients through electronic means in accordance with applicable regulatory requirements, including use of CKYCR records, e-KYC, and other permitted digital KYC processes. Non face-to-face onboarding shall be supported by appropriate verification controls to ensure authenticity of customer identity.

The Entity may use Video-based Customer Identification Process (V-CIP) or other regulator-permitted digital verification mechanisms, wherever applicable, to strengthen identity verification in a non face-to-face environment.

Documents to be obtained and verified shall include:

- Permanent Account Number (PAN)
- Aadhaar or Officially Valid Document (OVD), such as:

– Passport
– Driving Licence
– Voter ID
• Proof of current address (where required)
• Bank account details in the client's own name
• Recent photograph

Verification shall be carried out through a combination of database checks, document validation, and electronic verification mechanisms such as CKYCR retrieval, OTP-based confirmation, or other permissible digital authentication methods.

In addition to document verification, the Entity shall obtain and assess the following information:

• Purpose and intended nature of the relationship
• Expected level and type of trading activity
• Occupation and source of income
• Financial profile, including income or net worth range

The Entity shall ensure that the identity of the customer is verified prior to onboarding and shall not establish or maintain anonymous or fictitious accounts under any circumstances.

Reliance on Existing KYC Records within Financial Group

In case of resident Indian individual clients who have an existing relationship with the Entity or any other entity within the Financial Group in India, the Entity may rely on the KYC / CDD records previously obtained, in accordance with applicable regulatory provisions relating to third-party reliance.

Such reliance shall be subject to the following conditions:

• Explicit consent shall be obtained from the client for use and sharing of KYC records
• The Entity shall obtain or have access to the complete KYC / CDD records from the group entity without delay
• The Entity shall satisfy itself that the group entity is regulated and compliant with AML/CFT requirements
• The Entity shall confirm that there is no material change in the client's identity, profile, or KYC information

• Additional due diligence measures shall be undertaken, wherever required, to comply with applicable IFSC regulations

Notwithstanding such reliance, the Entity shall remain ultimately responsible for customer due diligence, including identification, verification, and application of enhanced due diligence, wherever applicable. Any deficiencies or gaps identified shall be rectified prior to activation of the client account.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence shall be applied in respect of clients assessed as high risk, including Politically Exposed Persons (PEPs), clients associated with high-risk jurisdictions, or clients identified through adverse media or unusual behaviour.
Enhanced Due Diligence shall also be applied in cases where reliance is placed on existing KYC records and any inconsistencies, gaps, or elevated risk indicators are identified
In the context of non face-to-face onboarding, the Entity shall apply additional safeguards to mitigate impersonation and identity risks.

Enhanced Due Diligence measures shall include:

• Collection of additional documentation to establish identity and financial standing
• Verification of source of funds and source of wealth through:
    - Bank statements
    - Income tax returns
    - Financial declarations
• Independent verification through public databases, adverse media screening, and regulatory sources
•Additional authentication measures, including video-based interaction or equivalent verification methods, wherever applicable
• Prior approval from Senior Management before onboarding
• Enhanced monitoring of transactions and more frequent review of client profile

The Entity shall ensure that higher-risk clients are subject to increased scrutiny both at onboarding and throughout the lifecycle of the relationship.

Ongoing Monitoring and Transaction Surveillance

The Entity shall conduct ongoing monitoring of client transactions to ensure that such transactions are consistent with the client's profile and declared source of funds.

Given the introducing broker model, transaction monitoring shall be carried out based on:

- Internal client and transaction data
- Reports and information received from the overseas broker
- Alerts generated through automated systems such as TrackWizz

Transactions that appear unusual, complex, or inconsistent with the client's profile shall be subject to detailed scrutiny. The Entity may obtain additional information from the overseas broker where required to assess the nature of such transactions.

Client-level AML/CFT risk assessment is conducted using a risk-based scoring methodology that evaluates client characteristics, geographic exposure, products, transaction behaviour and delivery channels.

Reliance on Overseas Broker

The Entity facilitates access to global markets through an overseas broker who undertakes execution of trades. The Entity shall rely on such overseas broker for execution and for obtaining transaction-related information required for monitoring.

Prior to entering into such arrangement, the Entity shall conduct due diligence of the overseas broker, including assessment of its regulatory status, licensing, and AML/CFT framework.

The Entity shall ensure that appropriate arrangements are in place to enable access to transaction data required for AML compliance.

Notwithstanding such reliance, the Entity shall retain ultimate responsibility for all AML/CFT obligations. Reliance on the overseas broker shall not dilute or transfer the Entity's responsibilities relating to customer due diligence, monitoring, and reporting of suspicious transactions.

Sanctions Screening

Screening and Identification of High-Risk Clients

The Entity shall implement a robust screening and risk identification framework to detect and prevent onboarding or continuation of relationships with individuals who may pose elevated risks of money laundering, terrorist financing, or other financial crimes.

Screening shall be carried out at the time of onboarding and on an ongoing basis, thereafter, including periodic re-screening and event-based reviews upon any material change in client profile or risk indicators.

The screening process shall include the following key components:

Sanctions Screening

The Entity shall screen all clients against applicable sanctions and watchlists, including:

• United Nations Security Council (UNSC) sanctions list, including terrorism and proliferation financing lists
• Lists notified under the Unlawful Activities (Prevention) Act, 1967 (UAPA)
•Any other lists, notifications, or directions issued by competent authorities, including Government of India and IFSCA

Politically Exposed Persons (PEPs)

The Entity shall identify whether a client qualifies as a Politically Exposed Person (PEP) or is a relative or close associate of a PEP. PEPs shall be considered as high-risk clients and shall be subject to enhanced due diligence, including additional verification and senior management approval prior to onboarding.

Adverse Media Screening

The Entity shall conduct screening for adverse media or negative information relating to clients using reliable public sources and databases. Clients linked to criminal activity, fraud, corruption, or other financial misconduct shall be subject to enhanced scrutiny and risk assessment.

Geographic Risk Assessment

The Entity shall assess geographic exposure of clients, including country of residence, nationality, or source of funds. Clients associated with jurisdictions identified as high-risk, sanctioned, or subject to increased monitoring by FATF or other authorities shall be treated as higher risk and subject to enhanced due diligence.

Behavioural and Interaction Risk

The Entity shall consider client behaviour during onboarding and subsequent interactions, including reluctance to provide information, inconsistencies in details, or unusual transaction patterns, as indicators of elevated risk.

Screening shall be conducted using automated tools such as TrackWizz to ensure timely identification of matches and risk indicators.

In the event of a potential or confirmed match with any sanctions list, PEP database, or adverse media input, the Entity shall conduct a detailed review to determine the nature and extent of the risk. Where required, appropriate actions shall be taken, including:

- Restriction or freezing of the account, where mandated
- Escalation to the Principal Officer
- Enhanced due diligence and monitoring
- Reporting to regulatory authorities, including FIU-IND, where applicable

The Entity shall maintain proper documentation of all screening results and actions taken and shall always ensure confidentiality of such information. No information relating to screening or reporting shall be disclosed to the client.

Suspicious Transaction Reporting (STR)

All relevant personnel of the Entity shall promptly report any unusual or suspicious activity to the Compliance Function without delay. The Compliance Function shall review the matter and escalate it to the Principal Officer for final determination.

The Principal Officer shall determine whether the transaction is suspicious, based on available information including data received from the overseas broker.

STR Filing Requirements:

- STR shall be filed with FIU-IND
- Timeline: within **7 working days** of determination

All STR-related information shall be treated as confidential, and no tipping-off shall be permitted.

Record Keeping

The Entity shall maintain complete, accurate, and up-to-date records of customer identification, transaction data, and Suspicious Transaction Reports (STRs) in accordance with applicable regulatory requirements.

Records shall include:

- Customer identification and KYC documentation

• Account files and business correspondence
• Transaction records
• STRs and related documentation

Such records shall be retained for a minimum period of eight (8) years for electronic records (in accordance with the IFSCA (Capital Market Intermediaries) Regulations, 2025) from the date of closure of the account or completion of the transaction, whichever is later, or such longer period as may be required under applicable law..

The Entity may utilise third-party systems or service providers for the purpose of storage, maintenance, and retrieval of records. However, the ownership, control, and responsibility for such records shall always remain with the Entity.

The Entity shall ensure that appropriate safeguards are in place, including data security measures, access controls, and audit trails, to maintain the integrity, confidentiality, and availability of records stored through such third-party systems.

Periodic KYC Updation

The Entity shall adopt a **risk-based approach** for periodic updation of Customer Due Diligence (CDD) information, in accordance with applicable regulatory requirements.

1. Standard Periodicity

The periodic updation of KYC / CDD shall be carried out from the date of account opening or last KYC updation, based on the risk categorisation of the client, as follows:

- High-Risk Clients: At least once every one (1) year
- Medium-Risk Clients: At least once every three (3) years
- Low-Risk Clients: At least once every five (5) years

2.Existing Resident Indian Clients (Financial Group Relationship)

In case of resident Indian clients having an existing relationship with the Financial Group in India, including clients onboarded in the IFSC unit based on prior domestic onboarding, the periodicity shall be:

- High-Risk Clients: At least once every two (2) years
- Medium-Risk Clients: At least once every eight (8) years
- Low-Risk Clients: At least once every ten (10) years
- Provided that, where the risk categorisation assigned by the Entity differs from that of another Financial Group entity, the stricter periodicity shall apply.

3. Trigger-Based Updation

Notwithstanding the above periodicity, the Entity shall update KYC / CDD records without delay upon occurrence of any trigger event, including:

- Change in address or contact details
- Change in occupation, employment status, or source of income
- Significant or unusual change in transaction behaviour
- Adverse media reports or regulatory alerts
- Identification or suspicion of suspicious activity

The framework for periodic updation shall be documented as part of this Policy and shall be approved by the Board of Directors.

Employee Accountability

All employees shall comply with AML/CFT requirements and promptly report suspicious activities. Failure to comply with these obligations shall be treated as a serious breach and may result in disciplinary action.

AML/CFT Training

The Entity shall conduct periodic training programs for all employees to ensure awareness of AML/CFT obligations, identification of suspicious transactions, escalation procedures, and regulatory requirements.

Such training shall be tailored to employee roles and conducted at regular intervals.

Use of Technology

The Entity shall utilise appropriate systems and tools to support AML/CFT compliance.
TrackWizz shall be used for:

- Sanctions screening
- Transaction monitoring
- Alert generation

All alerts generated by the system shall be reviewed by the Compliance Function.

Confidentiality

All information collected, generated, or maintained under this Policy, including customer identification data, due diligence records, transaction details, and Suspicious Transaction

Reports (STRs), shall be treated as strictly confidential.
Such information shall be accessed only by authorised personnel on a need-to-know basis and shall not be disclosed to any third party except where required under applicable laws, regulatory requirements, or by competent authorities.
The Entity shall ensure that appropriate safeguards are in place to protect the confidentiality and integrity of such information, including secure storage, controlled access, and audit trails.
No employee, officer, or representative of the Entity shall disclose to any client or third party that a Suspicious Transaction Report has been filed or that any investigation or analysis is being undertaken in relation to such client, in accordance with the prohibition on tipping-off under applicable law.

Review and Amendment

This Policy shall be reviewed at least on an annual basis or earlier, if required, to reflect changes in regulatory requirements, business operations, or risk environment. Any material amendments to this Policy shall be subject to approval by the Board of Directors.

Effective Implementation

The Entity shall ensure that adequate systems, processes, and internal controls are put in place to operationalise this, Policy. Compliance with this Policy shall be monitored on an ongoing basis through internal controls, system-driven checks, and periodic audits.
This Policy shall remain in force unless modified, amended, or replaced in accordance with the provisions set out herein.