PREVENTION OF MONEY LAUNDERING / AML-CFT POLICY

Business-model note: The Company provides investment advice only. This policy is drafted for a SEBI-registered Investment Adviser whose present business model is advisory-only, does not receive or hold client securities or client investment monies, does not handle cash, and currently onboards only individual clients. It is deliberately written to retain conditional controls for activities that are legally relevant but presently outside the firm's business model. Such provisions become operative immediately if the business model changes.

Contents

1. Purpose, Scope and Regulatory Basis

1.1 The purpose of this Policy is to establish the framework by which SPT Investment Advisory Services Private Limited, a SEBI registered Investment Adviser (the "Company" / "IA") prevents, detects, assesses, escalates, records and reports risks relating to money laundering (ML), terrorist financing (TF) and, where applicable, proliferation financing (PF).

1.2 The Policy is intended to ensure compliance with the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), as amended from time to time, applicable SEBI regulations/circulars/master circulars, directions issued by FIU-IND, UAPA requirements, Section 12A of the WMD Act and other applicable governmental directions.

1.3 This Policy shall be read with the Company's KYC, client onboarding, compliance, record retention, information security and business continuity procedures. Where a later law, rule, SEBI circular, FIU-IND direction or binding

governmental order imposes a higher or different requirement, the later requirement shall prevail to the extent of inconsistency.

1.4 This Policy applies to the Board / senior management, Designated Director, Principal Officer, compliance personnel, advisory personnel, onboarding personnel and all employees/consultants/agents who handle client information or client relationships, to the extent applicable.

Regulatory instrument	Relevance to this Policy
PMLA, 2002 and amendments	Statutory obligations of reporting entities, CDD, records, confidentiality and reporting
PML Rules, 2005 and amendments	Record types, KYC/identity, beneficial ownership and FIU reporting procedures
SEBI Master Circular No. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated 06-Jun-2024	Current consolidated AML/CFT obligations for SEBI-registered intermediaries
SEBI Master Circular for Investment Advisers dated 06-Feb-2026, paragraph 18	IA-specific incorporation of AML/CFT obligations
SEBI Circular SEBI/HO/MIRSD/DOP/CIR/P/2019/113 dated 15-Oct-2019	Predecessor AML framework; substantive controls retained where relevant and now read with current consolidated requirements
SEBI Master Circular on KYC norms, as amended	KYC/KRA requirements and client identification framework
UAPA, Section 51A and Government directions	Sanctions/designated person screening and freezing/blocking obligations
WMD Act, Section 12A and Government order dated 30-Jan-2023, as amended	Targeted financial sanctions relating to proliferation financing
FIU-IND directions / FINnet 2.0 requirements	Registration, reporting formats, timelines and operational filing requirements

2. Business Model and Applicability

2.1 The Company currently provides investment advice only and does not act as a stock broker, depository participant, portfolio manager, fund manager, trustee or custodian. The Company does not receive, hold, control, transfer or disburse client investment funds or securities in connection with advisory services.

2.2 The Company does not accept or handle cash from clients. Client fees are accepted through permitted banking/electronic channels. The Company shall not use the absence of client-fund handling as a basis to dispense with mandatory AML/CFT, CDD, screening, recordkeeping or reporting requirements.

2.3 The Company currently onboards only individual clients. It does not presently onboard companies, LLPs, partnership firms, trusts, HUFs, societies, Section 8 companies, NGOs, non-profit organisations or other juridical/non-individual clients.

2.4 Provisions dealing with beneficial ownership of juridical persons/arrangements, trustees/settlor/protector, NPO/DARPAN registration, entity structures and similar matters are retained in this Policy because they form part of the applicable SEBI AML framework. They are marked “conditional” where they do not presently apply to the Company. They shall become mandatory before onboarding any such client category.

2.5 If the Company begins to receive/hold client funds or securities, permit cash, offer a new product/service, use a new delivery mechanism/technology with material AML/CFT implications, onboard non-individual clients, or materially change its client/geographic profile, the Principal Officer shall undertake and document an AML/CFT risk assessment before implementation and shall recommend policy changes to senior management/Board.

3. Definitions and Abbreviations

Term	Meaning / Policy treatment
AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
PF	Proliferation Financing
CDD	Client Due Diligence
CIP	Client Identification Procedure
EDD	Enhanced Due Diligence
FIU-IND	Financial Intelligence Unit - India
KRA	KYC Registration Agency
KYC	Know Your Client
ML/TF	Money Laundering / Terrorist Financing
PEP	Politically Exposed Person, as defined under applicable PML Rules
Principal Officer	Management-level officer designated to coordinate AML/CFT reporting and compliance
Designated Director	Person designated under PML Rules to ensure overall compliance under Chapter IV of PMLA and PML Rules
STR	Suspicious Transaction Report
CTR	Cash Transaction Report
NTR	Non-Profit Organisation Transaction Report
BO	Beneficial Owner

Term	Meaning / Policy treatment
CSC	Client of Special Category / equivalent higher-risk category

4. Governance and Responsibility

4.1 Board / Senior Management

- Approve this Policy and material amendments.
- Ensure adequate resources, systems and authority for AML/CFT compliance.
- Receive periodic AML/CFT reporting from the Principal Officer and ensure material weaknesses are remedied.
- Approve continuation or rejection of high-risk relationships where escalation is required under this Policy.
- Ensure the person reviewing the effectiveness of AML/CFT policies is independent of the person who originally framed them, to the extent practicable and commensurate with the Company's size.

4.2 Designated Director

The Company shall designate the Designated Director in accordance with PML Rules. The Designated Director shall ordinarily be the Managing Director or a whole-time Director duly authorised by the Board, subject to the current statutory framework. The Designated Director shall have overall responsibility for compliance with PMLA Rules and shall ensure appropriate governance, escalation and corrective action.

4.3 Principal Officer

The Company shall appoint a management-level Principal Officer with sufficient seniority, competence, independence and access to senior management/Board. The Principal Officer shall be the central reference point for identification, assessment and reporting of potentially suspicious activity, FIU-IND reporting, AML/CFT controls, regulatory correspondence and maintenance of AML/CFT evidence.

The Company shall communicate the name, designation, address and email/contact details of the Principal Officer and Designated Director to FIU-IND in the prescribed manner and promptly update FIU-IND when such details change.

4.4 Employees / Business Functions

- Onboarding staff shall not activate a client relationship until mandatory CDD and screening requirements are complete.
- Advisory personnel shall escalate unusual, inconsistent or suspicious information to the Principal Officer promptly.
- Finance personnel shall ensure permitted payment channels and alert on unusual/third-party fee payments.
- IT/operations shall maintain access controls, audit trails and retrieval capability for AML/KYC records.

5. Risk-Based AML/CFT Framework

5.1 The Company shall apply a documented risk-based approach (RBA), proportionate to the nature, size and complexity of its business. Risk shall be assessed at client, geographic, service, payment and activity levels.

5.2 Risk factors shall include, as relevant: client identity and transparency; residency/geography; PEP status; sanctions exposure; occupation/business; source of wealth/funds where relevant; complexity of the relationship; non-face-to-face onboarding; adverse media/reputation; unusual payment arrangements; inconsistencies in information; high-risk jurisdictions; and any other indicator identified through law, SEBI/FIU-IND guidance or internal experience.

5.3 The Company shall classify clients as Low, Medium or High Risk, with a CSC/PEP/high-risk overlay where applicable. Risk classification shall not replace mandatory CDD.

5.4 The Company shall document its enterprise-level ML/TF risk assessment and update it at least annually and whenever material changes occur. New products, practices, delivery mechanisms or technologies shall undergo AML/CFT risk assessment before launch or material use.

6. Client Acceptance Policy

6.1 No anonymous, fictitious-name or unverifiable client shall be accepted.

6.2 No client relationship shall commence unless the Company can complete required CDD and screening. If satisfactory identification cannot be obtained, the relationship shall be rejected or, where an existing relationship is involved, terminated/closed in accordance with law and applicable directions; the Principal Officer shall assess whether an STR is required.

6.3 The Company shall not knowingly accept a client whose stated or observed circumstances present an unacceptable ML/TF/sanctions risk, including persons on applicable designated/sanctions lists, subject to the applicable legal process for name-match validation and freezing/blocking.

6.4 The Company shall not accept third-party fee payments as a routine practice. Any exception shall be documented, the payer's relationship with the client established, and the risk assessed and approved by the Principal Officer or an authorised senior officer. Payments from unrelated or unexplained third parties shall be rejected/refunded only after considering applicable legal directions and STR/suspicion implications; the Company shall not take any action that could prejudice an investigation or result in tipping-off.

6.5 Current business-model restriction: only individual clients are eligible for onboarding. Non-individual categories shall be rejected unless the Board/management first approves the business-model change and the KYC/beneficial ownership framework is upgraded.

7. Client Identification and CDD

7.1 The Company shall identify and verify the client using reliable and independent documents/data/information and shall obtain information regarding the purpose and intended nature of the relationship.

7.2 CDD shall be completed at onboarding and revisited when there is a material change, doubt regarding adequacy/veracity of information, suspicion of ML/TF, or another regulatory trigger.

7.3 KYC shall be conducted in accordance with applicable SEBI KYC requirements, KRA rules, PML Rules and permitted digital/video verification processes. The Company shall not rely on a lower-risk classification to omit mandatory minimum KYC requirements.

7.4 The Company shall obtain and maintain, as applicable for an individual: name; photograph; date of birth; residential/correspondence address; PAN or other legally required identifier; OVD/identity evidence; contact details; tax residency/FATCA/CRS information where applicable; occupation/source information as appropriate to risk; bank/payment details where required for fee collection; and declarations/consents required by applicable law.

7.5 Where a person acts on behalf of another, the Company shall verify the authority of the representative and identify/verify both the client and relevant beneficial owner/person on whose behalf the relationship is being established.

7.6 Ongoing due diligence shall compare the client's known profile and expected activity against actual information available to the Company, including changes in occupation, residency, PEP status, sanctions exposure, source information or material inconsistencies.

7.7 KYC records shall be kept current, particularly for high-risk clients. The Company shall act on KRA updates, client communications and other reliable information indicating a material KYC change.

8. Enhanced Due Diligence and High-Risk Clients

8.1 EDD shall apply where a client is high risk or falls within the applicable CSC categories, including non-resident clients, high-net-worth clients, trusts/charities/NGOs/NPOs, companies with close family ownership, PEPs and related persons, clients connected with high-risk jurisdictions, non-face-to-face clients (except permissible video-based customer identification treated as face-to-face under the SEBI AML circular), and clients with dubious reputation or other material risk indicators.

8.2 EDD may include enhanced identity verification, additional address/contact verification, source of funds/wealth information, corroboration through independent sources, detailed purpose of relationship, adverse-media review, senior management approval, increased frequency of KYC review and enhanced ongoing monitoring.

8.3 A high-risk designation shall not automatically result in rejection unless the risk is unacceptable or cannot be mitigated. Conversely, a low-risk designation shall not prevent escalation where suspicion or new risk information arises.

8.4 High-risk clients shall be reviewed at least annually and sooner when trigger events occur, unless a more frequent review is warranted by the Principal Officer.

9. Politically Exposed Persons (PEPs)

9.1 The Company shall have systems to identify whether a client, prospective client or beneficial owner is a PEP. Identification shall use client declarations, reliable public sources and/or appropriate commercial databases.

9.2 Establishing or continuing a relationship with a PEP requires senior management approval. If an existing client subsequently becomes a PEP, approval shall be obtained to continue the relationship.

9.3 Reasonable measures shall be taken to establish source of funds and source of wealth of PEPs and relevant beneficial owners. Enhanced ongoing monitoring shall be applied.

9.4 Applicable enhanced measures shall also be considered for family members and close relatives/associates of PEPs in accordance with the PML Rules and SEBI AML requirements.

10. Beneficial Ownership and Non-Individual Clients

10.1 Conditional applicability: The Company presently does not onboard non-individual clients. Nevertheless, if such clients are introduced, the Company shall identify the natural person(s) who ultimately own or control the client, or the person on whose behalf the relationship is conducted, and verify such person(s) in accordance with applicable PML Rules/SEBI requirements.

10.2 For companies, the Company shall apply the applicable controlling-ownership/control tests and identify the senior managing official where no natural person is otherwise identified. For partnerships/unincorporated associations, trusts and other legal arrangements, the Company shall apply the applicable statutory beneficial ownership tests and identify relevant controllers/settlor/trustee/beneficiaries/protector or equivalent persons as required.

10.3 Where the client or controlling owner is an applicable listed entity/subsidiary for which beneficial-owner identification exemptions are legally available, the Company shall apply the exemption strictly in accordance with the current PML Rules and SEBI directions and retain evidence supporting its conclusion.

10.4 NPO/DARPAN requirement: If the Company ever onboards a non-profit organisation falling within the applicable definition, it shall comply with the requirement to register/verify the client on the NITI Aayog DARPAN Portal where mandated and retain evidence as prescribed.

11. Sanctions, UAPA and WMD Act Screening

11.1 The Company shall screen clients, relevant beneficial owners, authorised persons and, where appropriate, connected parties against applicable sanctions/designated-person lists, including United Nations Security Council lists and Indian lists/directions issued under UAPA, PMLA-related government measures and Section 12A of the WMD Act.

11.2 Screening shall occur before onboarding and periodically thereafter. The Company shall maintain the designated lists in electronic or otherwise retrievable form and use appropriate name-matching controls capable of identifying reasonable matches.

11.3 A potential name match shall be escalated immediately for validation. The Company shall not disclose the existence of a STR or screening escalation to the client or other unauthorised person.

11.4 Where a true match or applicable designated account is identified, the Company shall follow the then-current Government/SEBI/UAPA/WMD directions for freezing/blocking, reporting, communication to nodal authorities and prohibition on making funds, financial assets, economic resources or related services available to designated persons, to the extent applicable to an IA.

11.5 The Company shall comply with updated directions/corrigenda and the current contact/nodal-officer framework rather than relying on static contact details embedded in this Policy.

12. Transaction and Activity Monitoring

12.1 Because the Company does not handle client investment funds or securities, it does not operate a client-money or securities-account transaction-monitoring platform. Monitoring shall nevertheless be applied to activities and information available to the Company, including client onboarding, advisory instructions/communications where relevant, fee payments, attempted payments, third-party payment requests, material changes in client circumstances, and information indicating that a client's proposed investment activity may involve proceeds of crime or TF/PF.

12.2 The Company shall pay particular attention to complex, unusually large or unusual activities that appear to have no clear economic or lawful purpose, unexplained changes in activity, inconsistent client information, unusual payment routes, and activity involving high-risk jurisdictions or sanctioned/designated persons.

12.3 Alerts and exceptions shall be investigated proportionately. The investigation record shall include the facts considered, information sought, analysis, conclusion, escalation and action taken.

12.4 The compliance function shall undertake periodic sample-based review of client files/activity to assess whether the AML/CFT controls are operating effectively and whether potentially suspicious activity is being identified and escalated.

13. Suspicious Transaction Identification and Reporting

13.1 A suspicious transaction includes a transaction or attempted transaction, whether or not made in cash, that falls within the applicable PML Rules definition, including activity that gives rise to reasonable grounds of suspicion of unlawful/proceeds-of-crime-related activity or lack of economic/legal rationale.

13.2 Illustrative red flags include: difficulty verifying identity; non-cooperation; unexplained source of funds/wealth; substantial unexplained increase in activity; unusual overseas flows; attempted payments or instructions involving unrelated third parties; high-risk jurisdiction exposure; contradictory information; use of nominees/intermediaries without clear rationale; multiple attempts to circumvent controls; adverse information relating to criminality; and activity inconsistent with the known client profile.

13.3 Employees shall immediately escalate a suspicion to the Principal Officer. The Principal Officer shall assess the facts, obtain further information where appropriate and record reasons for the conclusion.

13.4 Where the Principal Officer is satisfied that an activity is suspicious, the STR shall be furnished to FIU-IND within the statutory timeline, presently within 7 days of arriving at the conclusion that the transaction/series is suspicious, in the prescribed manner and format.

13.5 No minimum monetary threshold is a prerequisite for STR filing where there are reasonable grounds to believe that activity involves proceeds of crime or otherwise meets the statutory definition.

13.6 The Company shall maintain confidentiality before, during and after filing. No employee shall disclose to a client or any unauthorised person that an STR or related information has been or may be filed (tipping-off).

13.7 The Company shall not automatically freeze or restrict ordinary operations solely because an STR has been filed, unless otherwise required by law, competent authority or sanctions/freeze directions. Any action shall be determined by the Principal Officer in consultation with appropriate senior management/legal authorities, as necessary.

14. Cash, Client Money and Third-Party Payments

14.1 Cash policy: The Company does not accept or disburse cash in connection with client relationships or client fees. Any attempted cash payment shall be declined and documented. If circumstances create a statutory reporting obligation or suspicion, the Principal Officer shall assess and report as required.

14.2 Client money/securities: The Company does not receive, hold, transfer or control client investment funds or securities. Accordingly, operational controls relevant solely to custody, client-money ledgers, demat credits/debits or settlement of client funds are presently not applicable to the Company's advisory business.

14.3 This business-model limitation does not remove the Company from PMLA reporting-entity obligations or from monitoring advisory relationships for suspicious activity.

14.4 Payments to the Company shall ordinarily be received from an account held in the client's own name through banking/electronic channels. Any deviation shall be treated as a risk trigger and documented.

15. Record Keeping and Retention

15.1 The Company shall maintain records sufficient to reconstruct relevant transactions/activities and to demonstrate compliance with CDD, risk assessment, monitoring, escalation, reporting and sanctions-screening obligations.

15.2 Records shall include, as applicable: client identification documents; KYC/KRA data; beneficial ownership evidence where relevant; risk classification; PEP/sanctions screening results; onboarding approvals; client communications; fee/payment records; unusual-activity investigations; STR/other FIU reporting evidence; management approvals; policy approvals; training records; audit/testing records; and regulatory correspondence.

15.3 Transaction records required under the PML Rules shall be maintained for the applicable statutory period, currently five years from the date of the transaction between the client and the reporting entity, or such longer period as applicable law/rules/SEBI directions require.

15.4 Identity records, account files and business correspondence shall be retained for five years after the business relationship has ended or the account has been closed, whichever is later, or for such longer period as required by law.

15.5 Records connected with an ongoing investigation, STR, regulatory inspection or legal proceeding shall be retained until the matter is formally closed and the applicable retention period has expired.

15.6 Records shall be securely stored, access-controlled, readily retrievable, tamper-evident to the extent practicable and capable of being produced to SEBI, FIU-IND or other competent authority when lawfully requested.

16. Confidentiality and Tipping-Off

16.1 The Company, its Directors, officers and employees shall maintain confidentiality regarding information maintained/furnished under PMLA, subject to lawful information-sharing requirements.

16.2 No employee shall discuss STRs, FIU communications, internal suspicion assessments, sanctions investigations or other sensitive AML escalations with the concerned client or unauthorised colleagues.

16.3 Internal escalation shall be on a strict need-to-know basis. Information sharing within a group, where applicable, shall be undertaken only in accordance with law and appropriate confidentiality controls.

17. Reliance on Third Parties / KYC Utilities

17.1 The Company may rely on a regulated third party/KRA/other permitted service provider for identification, identity verification and beneficial-owner determination only where permitted by the PML Rules and SEBI directions.

17.2 Any such reliance shall satisfy the applicable statutory conditions, including availability of CDD information/documents without delay, adequate assurance regarding the third party's regulation/supervision and CDD/record-keeping controls, absence of prohibited high-risk-jurisdiction concerns, and the Company's continuing ultimate responsibility for CDD and EDD.

17.3 Outsourcing or KYC utility use shall not transfer the Company's regulatory accountability. Contracts and operating procedures shall ensure audit/access rights and prompt retrieval of records.

18. Employee Screening, Training and Awareness

18.1 Employees handling client information or client relationships shall receive AML/CFT training appropriate to their roles. Training shall cover PMLA/PML Rules, KYC/CDD, risk indicators, sanctions screening, PEPs, escalation, STR confidentiality, tipping-off and record retention.

18.2 Training shall be provided at induction and periodically thereafter, and when material regulatory/process changes occur. Attendance and training material/evidence shall be retained.

18.3 The Company may conduct role-based employee screening and conflict/reputation checks proportionate to risk, especially for personnel with access to client records or compliance functions.

19. Internal Controls, Testing and Audit

19.1 The Company shall maintain documented internal controls over AML/CFT processes, including onboarding checklists, screening evidence, risk classification, approval workflows, exception handling, escalation and reporting.

19.2 The effectiveness of the AML/CFT framework shall be independently tested periodically and at least as required by applicable SEBI audit/inspection requirements. Testing shall cover file completeness, risk classification, KYC updates, screening, unusual-activity identification, reporting, confidentiality and retention.

19.3 The reviewer shall be independent of the person who framed the policy/process to the extent practicable. Material deficiencies shall have documented remediation owners and target dates.

19.4 The Company shall cooperate fully with SEBI/IAASB/other competent authorities during inspections and provide AML/CFT records promptly when lawfully required.

20. Regulatory Reporting and FINnet/FIU-IND

20.1 The Company shall register and maintain its reporting-entity profile on FINnet 2.0/FIU-IND as required and ensure that the Principal Officer and Designated Director details are current.

20.2 The Principal Officer is responsible for ensuring timely filing of applicable FIU-IND reports, including STRs and, where applicable, CTRs and NTRs, in the prescribed formats and within prescribed timelines.

20.3 Current operational timelines shall be monitored from the latest FIU-IND instructions. As reflected in the SEBI AML Master Circular, CTR and NTR reports are generally due by the 15th of the succeeding month where applicable, while STRs are due within 7 days of reaching the conclusion that the activity is suspicious.

20.4 Given the Company's current no-cash and individual-only business model, CTR and NTR filings will ordinarily be not applicable. This is an applicability conclusion, not an exemption from the underlying rules; it shall be reassessed whenever the client/service profile changes.

20.5 No NIL STR/CTR/NTR report shall be filed unless required by a later FIU-IND direction. The Principal Officer shall nevertheless maintain evidence of the periodic applicability assessment.

21. Breach Management and Escalation

21.1 Any failure to complete mandatory KYC, screening, risk assessment or recordkeeping shall be treated as a compliance exception and escalated to the Principal Officer.

21.2 Material or repeated breaches shall be reported to senior management/Designated Director and tracked to closure. Employee misconduct may be addressed under the Company's disciplinary framework.

21.3 No employee shall suppress or delay escalation of a genuine AML/CFT concern because the transaction value is small, the client is longstanding, or the Company does not handle client funds.

21.4 The Company shall maintain a confidential AML/CFT incident log covering material exceptions, investigations, STR decisions, sanctions hits, regulatory requests and remediation actions.

22. Review, Approval and Change Management

22.1 This Policy shall be reviewed at least annually and sooner upon any material change in law, SEBI/FIU-IND directions, PML Rules, business activities, client profile, payment methods, technology, delivery mechanism or sanctions framework.

22.2 The Principal Officer shall maintain a regulatory change log and identify changes requiring revisions to this Policy, client forms, onboarding controls, training or monitoring.

22.3 Material amendments shall be approved by the appropriate governing authority and communicated to relevant employees.

22.4 The Policy shall be available to relevant employees and maintained as a controlled document with version history.

Annexure A - Client Risk Scoring Matrix

The following is the Company's baseline scoring framework. The Principal Officer may apply a higher risk rating where qualitative facts justify escalation.

Risk Factor	Low	Medium	High / EDD
Client type	Individual with transparent profile	Complex individual profile / material ambiguity	PEP; high-risk/sanctions concern; unexplained nominee/agent involvement
Residency / geography	India / low-risk geography	Cross-border exposure	FATF high-risk / sanctioned or high-concern jurisdiction
PEP status	No PEP indicators	Potential/uncertain match pending validation	Confirmed PEP / family member / close associate
Identity transparency	KYC complete and consistent	Minor discrepancies resolved	Identity unverifiable, contradictory or suspected false
Payment profile	Electronic payment from client's own account	Occasional justified third-party payment	Unrelated third-party / unusual overseas / cash attempt
Reputation	No adverse information	Limited adverse information resolved	Credible adverse criminal/regulatory information
Activity profile	Consistent with stated profile	Some unusual but explainable activity	Complex/unusual activity with no apparent lawful purpose
Overall treatment	Standard CDD; periodic refresh	Enhanced review as needed	EDD, senior approval and enhanced monitoring

Annexure B - Indicative AML/CFT Red Flags

- Client repeatedly resists or delays providing KYC information or documentary evidence.
- Identity, address, occupation, tax residency or other information is inconsistent across documents or sources.
- Client requests use of an unrelated third party to pay fees or otherwise introduces unexplained payment relationships.
- Client information indicates unexplained wealth or source of funds inconsistent with the stated profile.
- Client is associated with a sanctioned/designated person or a close/repeated false-positive match is not satisfactorily resolved.
- Client or related person is a PEP and cannot provide satisfactory source-of-wealth/source-of-funds information.
- Unusual cross-border payment/activity or involvement of a high-risk jurisdiction without a clear commercial/personal rationale.
- Client seeks to structure or split activity to avoid a control, threshold or review.
- Client attempts to terminate the relationship or alter payment arrangements immediately after compliance questions.

- Adverse media or credible law-enforcement/regulatory information suggests fraud, corruption, terrorist financing, organised crime, tax crime or other predicate activity.
- An individual appears to be acting for another person without a coherent or documented reason.
- Information suggests the advisory relationship may be being used to facilitate movement, concealment or layering of proceeds of crime.

This list is illustrative and not exhaustive. Context, intent, surrounding facts and reasonable grounds of suspicion determine whether escalation/STR is required.

Annexure C - Compliance Calendar

Frequency	Control / Action	Responsible
At onboarding	KYC/CDD; sanctions screening; PEP screening; risk classification; approval	Onboarding / Compliance
Ongoing	Escalate unusual information/activity; update KYC on trigger events	All relevant staff
Monthly	Assess FIU reporting applicability; CTR/NTR if applicable; retain evidence	Principal Officer
At least annually	Enterprise ML/TF risk assessment; high-risk client review; policy review; training refresh	Principal Officer / Management
At least annually / as required	Independent AML/KYC control testing / compliance audit	Compliance / Independent Reviewer
On regulatory change	Update policy, forms, systems, training and controls	Principal Officer
On new product/technology/service	Pre-implementation ML/TF risk assessment	Principal Officer / Management
On PEP/ sanctions trigger	Immediate enhanced review and senior escalation	Principal Officer

Annexure D - Mandatory Records / Evidence Checklist

- Completed KYC/CDD records and supporting documents.
- KRA/KYC status and update evidence, where applicable.
- Client risk assessment and rationale / overrides.
- PEP and sanctions screening results and match-resolution evidence.
- EDD records for high-risk relationships.
- Authority documents for representatives, where applicable.
- Fee/payment records and evidence supporting any third-party payment exception.
- Internal suspicious-activity alerts, investigation notes and Principal Officer decisions.
- FIU-IND / FINnet submissions, acknowledgements and correspondence.
- Board/senior management approvals and AML/CFT reporting to management.
- Employee training attendance and materials.
- Independent testing/audit reports and remediation evidence.
- AML/CFT incidents, breaches and corrective-action records.
- Policy versions, review evidence and regulatory change log.

Annexure E - Regulatory References

1. Prevention of Money Laundering Act, 2002, as amended.

2. Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended.

3. SEBI Master Circular No. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06, 2024 - Guidelines on AML Standards and CFT / obligations of Securities Market Intermediaries under PMLA and Rules.

4. SEBI Master Circular for Investment Advisers dated February 06, 2026, reference HO/38/12/11(2)2026-MIRSD-POD/I/4300/2026, paragraph 18 - AML/CFT requirements.

5. SEBI Master Circular No. SEBI/HO/MIRSD/DOP/CIR/P/2019/113 dated October 15, 2019 - predecessor AML/CFT framework, considered as historical/legacy guidance to the extent superseded by the 2024 consolidated AML Master Circular.

6. SEBI Master Circular on KYC norms for the securities market, as amended from time to time.

7. Unlawful Activities (Prevention) Act, 1967, Section 51A and applicable Government of India orders/corrigenda.

8. Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, Section 12A and applicable Government directions.

9. FIU-IND FINnet 2.0 reporting instructions, manuals, formats and directions, as updated from time to time.

10. FATF statements and risk information, to the extent relevant and incorporated through applicable SEBI/Government directions.