ANTI-MONEY LAUNDERING (AML) AND COUNTERING THE FINANCING OF TERRORISM (CFT) POLICY

(FOR REGISTERED INVESTMENT ADVISER – SEBI COMPLIANT)

This **Anti-Money Laundering (AML) & Combating Financing of Terrorism (CFT) Policy** has been formulated by **Finideas Advisors Private Limited**, a SEBI-registered Investment Advisor, in compliance with the Prevention of Money Laundering Act, 2002 (PMLA), the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules), and SEBI (Investment Advisors) Regulations, 2013 in addition to SEBI (Investment Advisors) Second Amendment, 2024 and other guidelines issued by SEBI from time to time. This AML & KYC Policy is framed in accordance with the SEBI Master Circular **SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 6,2024** and **SEBI/HO/MIRSD/MIRSD-PoD/P/CIR/2025/94 dated June 27,2025** on Guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT), issued under the Prevention of Money Laundering Act (PMLA), 2002 and the rules thereunder, as amended from time to time. The policy aims to prevent misuse of our services for money laundering or terrorist financing activities.

Regulatory Framework:

Under the PMLA, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, all SEBI-registered intermediaries (including brokers, asset managers, portfolio managers, investment advisers, depository participants, etc.) must:

- Follow prescribed client account opening and KYC procedures.
- Maintain records and report specified transactions to FIU-IND.
- Establish internal mechanisms for detecting and reporting suspicious transactions as per SEBI guidelines.
- Note that violations such as manipulative or deceptive practices, insider trading, or substantial acquisition of securities/control (Section 12A read with Section 24 of the SEBI Act) are treated as scheduled offences under PMLA.

Governance & Responsibilities:

ROLE	RESPONSIBILITIES
Designated Director	Ensures overall AML/CFT compliance, provides strategic oversight, and reports to the Board and regulators.
Principal Officer	Acts as the central point for suspicious transaction monitoring and reporting; files STRs/CTRs with FIU-IND; coordinates with SEBI and law enforcement.

Senior Management	Approves AML/CFT policies, allocates resources, and ensures regular review and updates of compliance measures.
Compliance Team	Implements policies, conducts monitoring and internal reviews, organizes staff training, and keeps procedures aligned with regulatory updates.
Employees	Perform KYC/CDD diligently, stay alert to unusual activities, escalate suspicious transactions, and maintain confidentiality (no tipping-off).

Each registered intermediary shall adopt written AML procedures covering the Client Due Diligence (CDD) process, specifically:

1. Client acceptance policy.
2. Client identification procedures.
3. Risk management framework.
4. Ongoing monitoring of transactions.

Client Due Diligence (CDD)

- Verify client identity using reliable, independent sources.
- Identify and verify **beneficial owners**:
  - **10%** ownership/control in companies/partnerships; **>15%** in associations; trustees, settlors, beneficiaries **(>10%)** in trusts.
- If none identified, treat senior managing official as beneficial owner.
  - **Exemption:** listed entities and their subsidiaries.
- Ensure authorization of persons acting on behalf of clients (e.g., trusts, companies).
- Understand client's nature of business, ownership, and control structure.
- Conduct on-going monitoring to ensure transactions match client profile and source of funds.
- Periodically update client/beneficial owner documents, especially for high-risk clients.
- Register NPO clients on NITI Aayog's DARPAN portal.
- If CDD may "tip off" the client, suspend the process and file an **STR (Suspicious Transaction Report)**.
- No account or transaction without CDD.

Client Acceptance Policy

- No anonymous, fictitious, or benami accounts.
- Classify clients as **Low/Medium/High risk** based on geography, business activity, turnover, payment methods, etc.
- Apply **Enhanced Due Diligence (EDD)** for **Clients of Special Category (CSC):**

  - NRIs, HNIs, Trusts, Charities, NGOs, entities with complex ownership, PEPs and their associates, clients from high-risk countries, non-face-to-face clients, and clients with dubious reputation.
- Collect additional documentation depending on client risk classification.
- Do not open accounts where CDD cannot be completed or information is non-genuine/non-cooperative. File STRs where required.
- Ensure clients/beneficial owners are not on prohibited or criminal lists.
- Define clear rules for accounts operated on behalf of others, including authority, limits, and responsibilities.
- Revisit the CDD process whenever ML/TF suspicion arises.

Client Identification Procedures (CIP)

- Apply CIP at account opening, during transactions, or when data is **doubtful.**
- Verify clients and beneficial owners with reliable documents.
- Identify **PEPs (Politically Exposed Persons),** get senior management approval, and verify their source of funds.
- Reject/ escalate cases where identity cannot be confirmed.
- **No exemptions** – **KYC/CDD is mandatory for all clients.**

Reliance on Third Parties

- Allowed only if the third party is regulated and not in a high-risk jurisdiction.
- Intermediary must have immediate access to client data.
- **Ultimate responsibility stays with the intermediary.**

Risk Management Framework (RMF)

Risk-Based Approach (RBA)

- Apply RBA for managing ML (Money Laundering)/TF (Terrorist Financing) risks with policies approved by senior management.
- Use **enhanced due diligence (EDD)** for high-risk clients; simplified due diligence for low-risk clients.
- **Low-risk treatment not allowed** where ML/TF suspicion exists.

Risk Assessment

- Assess risks based on client profile, geography, nature/volume of transactions, and payment methods.
- Document and update assessments **regularly**; make them available to regulators when required.
- Conduct risk assessments before **launching new products**, **services**, or **technologies.**
- Incorporate government/SEBI advisories and UN (United Nations) sanctions lists into risk assessments.

Monitoring of Transactions

- Monitor client activity against normal profile; **flag complex, large, or unusual transactions.**
- Keep records of reviews and share with regulators when required.
- Apply **risk-based monitoring**, including for existing clients.
- Report all suspicious transactions (including attempted/aborted) to the **Principal Officer**, who files STRs with FIU-IND.
- **Never inform clients of suspicion ("no tipping off").**
- Extra scrutiny and countermeasures apply to clients from high-risk countries.

Record Keeping & Retention

- Maintain details of all transactions (nature, amount, date, parties).
- Keep sufficient records to reconstruct transactions for investigation/prosecution.
- Preserve information on beneficial ownership, fund flows, transaction origin/destination, and authority/instructions.
- Ensure records are readily available to regulators and investigators.

Mandatory Records

- Cash transactions **> ₹10 lakh** (or equivalent in foreign currency).
- Series of connected cash transactions **aggregating > ₹10** lakh in a month.
- Transactions with **forged/counterfeit currency** or forged documents.
- All suspicious transactions (cash or non-cash, including demat/security accounts)

Retention Periods

- Transaction records: **5 years from the date of transaction**.
- Client identification, KYC files, business correspondence: **5 years after account closure/end of relationship**.
- Records linked to STRs/investigations: retained until the case is closed.

Freezing of Funds / Sanctions Compliance

- No accounts may be opened/maintained for individuals/entities on **UNSC, UAPA, WMD Act, or SEBI-designated lists**.
- Continuously screen clients and accounts against updated sanction lists (UN, MHA, SEBI, FATF).
- In case of a match:
  - Stop transactions immediately.
  - Inform the **Central Nodal Officer (CNO)**, SEBI, FIU-IND, and relevant authorities without delay.
  - File a **Suspicious Transaction Report (STR)**.
- Use technology-based tools for regular screening.

Reporting to FIU-IND

- **CTR**: Monthly cash transaction reports (due by **15th** of the following month).
- **STR:** Within **7** days of suspicion.
- **NTR:** Monthly reports of NPO transactions.
- Principal Officer is responsible for timely filing; confidentiality and "no tipping off" are mandatory.

Employees & Clients

- **Hiring:** Screen key staff for integrity and competence.
- **Training:** Ongoing AML/CFT training for all levels of staff (frontline, back-office, compliance, risk, new client onboarding).
- **Investor Education:** Provide brochures/literature to explain AML/CFT requirements, source-of-funds checks, and KYC needs.