FINDOC INVESTMART (IFSC) PRIVATE LIMITED

Regd. Office: [Unit No. 303, 3rd Floor, Signature Building, Block No. 13B, Zone 1, GIFT SEZ, Gandhinagar, Gujarat – 382355]
CIN: [U65999GJ2017PTC095984] | IFSCA Registration No.: [INZ000200735] | Email: [ifsccompliance@myfindoc.com]

Policy for Prevention of Money Laundering

Anti-Money Laundering, Counter-Terrorist Financing and Know Your Customer (AML / CFT / KYC) Policy

Document Title	PMLA Policy – Findoc Investmart (IFSC) Pvt Ltd
Policy Reference No.	FIIPL/POL/AML-CFT-KYC/01
Version	1.1
Approved by	Board of Directors / Governing Board
Date of Approval	01-JUN-2026
Effective Date	02-JUN-2026
Review Frequency	Annual, or earlier upon regulatory change
Document Owner	Compliance Officer

1. Introduction and Regulatory Background

This Anti-Money Laundering, Counter-Terrorist Financing and Know Your Customer Policy ("this Policy") sets out the framework adopted by **Findoc Investmart (IFSC) Private Limited** ("the Company"), a Broker Dealer and Clearing Member registered with the International Financial Services Centres Authority ("IFSCA") and operating from the GIFT City International Financial Services Centre ("IFSC"), to prevent, detect and report money laundering and terrorist-financing activity.

This Policy is framed in accordance with, and shall be read together with, the following instruments as amended from time to time:

- The Prevention of Money-Laundering Act, 2002 ("PMLA") and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 ("PML Rules");
- The IFSCA (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022 (IFSCA/2022-23/GN/GL001 dated 28 October 2022), as amended (including the amendments effective 31 October 2025 and the amendatory circular dated 2 January 2026) ("IFSCA AML Guidelines");
- The IFSCA (Capital Market Intermediaries) Regulations, 2025 and the Master Circular for Broker Dealers and Clearing Members issued thereunder;
- The Unlawful Activities (Prevention) Act, 1967 ("UAPA") and the Weapons of Mass Destruction Act, 2005, together with the sanctions / designated-list obligations notified thereunder; and
- Guidelines, advisories and circulars issued from time to time by IFSCA and the Financial Intelligence Unit – India ("FIU-IND").

Note: Wherever any provision of this Policy conflicts with the IFSCA AML Guidelines or the PMLA, the statutory / regulatory provision shall prevail, and this Policy shall be deemed amended accordingly.

2. Objective

The objectives of this Policy are to: (i) establish a risk-based framework for client onboarding, monitoring and reporting; (ii) ensure the Company is not used, intentionally or unintentionally, as a conduit for laundering proceeds of crime or for financing terrorism; (iii) enable timely identification and reporting of suspicious transactions to FIU-IND; (iv) define clear roles, responsibilities and accountability; and (v) embed a culture of AML/CFT awareness through training and screening of staff.

3. Scope and Applicability

This Policy applies to all directors, the Designated Director, the Principal Officer, Key Managerial Personnel, officers, employees (permanent, temporary and contractual) and authorised representatives of the Company, and to all business relationships and transactions, including client onboarding, dealing, clearing and settlement, fund and securities handling, and record-keeping.

4. Definitions

Term	Meaning
Money Laundering	The process of concealing the origin, ownership or destination of proceeds of crime so as to make them appear legitimate, including the activities described in Section 3 of the PMLA.
Beneficial Owner (BO)	The natural person who ultimately owns or controls a client and/or the natural person on whose behalf a transaction is conducted, determined as per the controlling-ownership-interest thresholds in the IFSCA AML Guidelines / PML Rules.
Customer Due Diligence (CDD)	Identifying and verifying the identity of a client and its beneficial owner using reliable, independent source documents, data or information, and understanding the purpose and intended nature of the business relationship.
Politically Exposed Person (PEP)	An individual entrusted with prominent public functions by a foreign country, including heads of state/government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials, and their family members and close associates.
Clients of Special Category (CSC)	Categories of client warranting heightened attention, including PEPs, non-resident clients, high-net-worth individuals, trusts/charities/NGOs/NPOs, companies with close family shareholding, clients from jurisdictions identified as deficient by FATF, and clients in non-face-to-face relationships.
Suspicious Transaction	A transaction (including an attempted transaction), whether or not made in cash, which gives rise to a reasonable ground of suspicion that it involves proceeds of crime, is complex or unusual without economic rationale, or relates to terrorism financing.

5. Governance and Designated Officers

The Board of Directors holds ultimate responsibility for AML/CFT compliance and approves this Policy. Senior management is responsible for its implementation. The Company shall appoint the following officers, who shall be based in the IFSC unit and shall be two different natural persons not shared with any group entity operating in the domestic tariff area:

Role	Key Responsibilities
Designated Director	Overall accountability for ensuring compliance with the obligations under the PMLA, PML Rules and IFSCA AML Guidelines; the person heading the IFSC unit may act as the Designated Director.
Principal Officer	Day-to-day implementation; review of alerts; determination and filing of STRs/CTRs and other prescribed reports with FIU-IND; liaison with IFSCA and FIU-IND; maintenance of records. The Principal Officer shall not be assigned development or internal-audit functions.

The names, designations and contact details of the Designated Director and Principal Officer shall be communicated to FIU-IND within seven (7) days of appointment or any change, and the Company shall register and report through the FIU-IND FIN Gate 2.0 portal (selecting “IFSC” as the reporting-entity type and “IFSCA” as the regulator).

6. Customer Identification Procedure (CIP)

No account shall be opened, and no business relationship established, on an anonymous or fictitious / benami basis, or where the Company is unable to complete CDD. At onboarding the Company shall:

- Obtain and verify identity and address proof of the client, its authorised signatories and beneficial owner(s) against reliable, independent source documents, data or information;
- For non-individual clients, obtain constitutional documents, ownership/control structure and identify the beneficial owner(s) as per the prescribed thresholds;
- Screen the client, authorised signatories and beneficial owners against the UNSC consolidated sanctions lists and the lists notified under UAPA / WMD Act, and against applicable PEP databases, before establishing the relationship;
- Where in-person presence is not feasible, undertake Video-based Customer Identification Process (V-CIP) in accordance with the controls in the IFSCA AML Guidelines; and
- Record the purpose and intended nature of the business relationship and obtain information to develop the client risk profile.

The Company may rely on KYC records held by a registered KYC Registration Agency (KRA) or undertaken by a third party, subject to the conditions in the IFSCA AML Guidelines, while retaining ultimate responsibility for CDD.

Customer Acceptance Policy

The Company shall establish and implement a Customer Acceptance Policy to ensure that no account or business relationship is established where:

- the customer is anonymous or fictitious;
- the customer refuses to provide satisfactory identity or beneficial ownership information;
- the Company is unable to complete Customer Due Diligence;
- the customer appears on any sanctions list issued by the United Nations Security Council, Government of India or any other authority recognised under applicable law;
- the customer is identified as a shell bank or is associated with a shell bank;
- the customer presents an unacceptable money laundering or terrorist financing risk which cannot be effectively mitigated.

The Company reserves the right to decline or terminate any business relationship where adequate due diligence cannot be completed or where continuation of the relationship would expose the Company to unacceptable regulatory or reputational risk.

7. Risk Categorisation

Each client shall be assigned a risk category – Low, Medium or High – based on factors including the client's identity, social/financial status, nature of business activity, country of residence/incorporation, products/services used and expected transaction pattern. The risk categorisation and the underlying reasons are confidential and shall not be disclosed to the client. CDD records shall be periodically reviewed and updated at the following minimum frequency:

Risk Category	Review / Update Periodicity	Diligence Level
High	At least once every year	Enhanced Due Diligence
Medium	At least once every three years	Standard, monitored
Low	At least once every five years	Simplified, where permitted

7A. Enterprise-Wide Risk Assessment

The Company shall establish, document and maintain an Enterprise-Wide Money Laundering, Terrorist Financing and Proliferation Financing Risk Assessment ("EWRA") in accordance with the IFSCA AML/CFT/KYC Guidelines. The assessment shall identify, evaluate and document the money laundering and terrorist financing risks arising from the Company's business activities, products and services, customer categories, geographical exposure, delivery channels, transaction patterns, distribution models and the use of technology.

The EWRA shall also evaluate the effectiveness of existing internal controls and determine the residual risks faced by the Company. The assessment shall be reviewed at least annually, or more frequently whenever there are material changes in business operations, products, customer profile, regulatory requirements or emerging ML/TF risks. The results of the assessment shall be approved by the Board of Directors and shall form the basis for the Company's risk-based approach towards customer due diligence and transaction monitoring.

8. Enhanced Due Diligence (EDD) and Clients of Special Category

EDD shall be applied to all High-risk clients, all PEPs and all CSCs, and in any structural scenario specified by the IFSCA AML Guidelines, irrespective of the computed risk score. EDD measures include: senior-management approval to establish or continue the relationship; establishing the source of funds and source of wealth; obtaining additional identification and ownership information; and more frequent and intensive ongoing monitoring. Relationships with shell entities and correspondent relationships with shell banks are prohibited.

9. Ongoing Monitoring and Alerts

The Company shall conduct ongoing monitoring of transactions to ensure they are consistent with the client’s profile, risk category and source of funds. A surveillance/alert mechanism shall generate alerts for, among other things: transactions inconsistent with the client’s known profile; unusually large or complex transactions without apparent economic rationale; rapid movement of funds; trades that may indicate market manipulation; and clients or counterparties matching sanctions/PEP screening. Each alert shall be examined, dispositioned and documented by the Compliance Officer (or delegate), with the audit trail retained.

10. Reporting Obligations

The Company shall furnish the following reports to FIU-IND through FINGate 2.0 within the prescribed timelines:

Report	Trigger / Threshold	Timeline
Suspicious Transaction Report (STR)	On formation of suspicion (including attempted transactions); no monetary threshold	Promptly, and in any case within the period prescribed under the PML Rules of arriving at the conclusion
Cash Transaction Report (CTR)	Cash transactions above the prescribed threshold (Rs. 10 lakh or foreign-currency equivalent), aggregated monthly	By the 15th of the succeeding month
Non-Profit Organisation Transaction Report (NTR)	Receipts by/on behalf of an NPO above the prescribed threshold (Rs. 10 lakh or equivalent)	By the 15th of the succeeding month
Cross-Border Wire Transfer Report (CBWTR)	Cross-border wire transfers above the prescribed threshold (Rs. 5 lakh or equivalent) where origin/destination is in India	By the 15th of the succeeding month

Prohibition on tipping-off: No director, officer or employee shall disclose to the client or any other person the fact that an STR or related information has been or is being furnished, or that an investigation is being or may be carried out (Section 12(2) PMLA). The filing of an STR shall not, by itself, be a ground to refuse or restrict a client's transaction.

11. Record Keeping and Retention

- Records of the identity of clients and beneficial owners, and account files and business correspondence, shall be retained for at least five (5) years from the date of cessation of the business relationship or closure of the account, whichever is later;
- Records of transactions (domestic and international) shall be retained for at least five (5) years from the date of the transaction;
- Records relating to STRs and other reports shall be retained for at least five (5) years from the date of the transaction or reporting; and
- Without prejudice to the above, AML compliance documentation shall additionally be maintained in electronic, readily retrievable form for the minimum period prescribed under the IFSCA (Capital Market Intermediaries) Regulations, 2025 (eight years).

Records shall be maintained in a manner that permits reconstruction of individual transactions and shall be made available to IFSCA, FIU-IND and other competent authorities on request.

12. Employee Screening, Hiring and Training

The Company shall apply appropriate screening procedures when hiring employees to ensure high standards of integrity. All relevant staff shall receive AML/CFT training at induction and periodically thereafter (at least annually), covering this Policy, red-flag indicators, the obligation to escalate, reporting procedures and the tipping-off prohibition. Training records shall be maintained.

13. Awareness Among Clients and Staff

The Company shall create awareness among clients regarding the rationale for CDD and information requests, and among staff regarding their individual obligations under this Policy. Communication of AML/CFT expectations shall form part of client onboarding documentation and internal communications, without compromising the confidentiality of risk categorisation or the tipping-off prohibition.

13A. Internal Reporting and Escalation

Every employee shall immediately report any unusual, suspicious or potentially suspicious activity to the Principal Officer through the prescribed internal reporting mechanism.

Employees shall not independently communicate with any law enforcement agency or regulatory authority regarding suspicious transactions unless specifically authorised by the Principal Officer.

The identity of employees reporting suspicious activities shall remain confidential and employees acting in good faith shall be protected against retaliation.

14. Review, Ownership and Approval

This Policy shall be reviewed by the Board at least annually, and earlier upon any change in applicable law or regulation. The Compliance Officer is the document owner and shall maintain version control. Deviations from this Policy are not permitted without prior written approval of the Board.