PRUDENT BROKING SERVICES PRIVTE LIMITED
POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING
(as per the requirements of the PMLA Act 2002)

1. Company Policy

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

The purpose of this policy is to set out the prevention of money laundering commitments and obligations for Prudent Broking Services Private Limited (hereinafter referred to as 'Company')

This policy is based on the provision of the "Prevention of Money Laundering Act, 2002 and circular issued by SEBI and exchanges thereof".

This internal policy sets out and establishes governing principles, broad guidelines and standards to be adopted by the Companies in order to protect the Companies from being used by any person to launder money.

Policy objectives

To protect the Company from being used for money laundering

To follow thorough "Know Your Customer" (KYC) policies and procedures in the day-to-day business.

To take appropriate action, once suspicious activities is detected, and make report to designated authorities in accordance with applicable law / laid down procedures.

To comply with applicable laws as well as norms adopted internationally with reference to Money Laundering.

2. Principal Officer Designation and Duties

The Company has designated Mr. Munjal Mehta as the Principal Officer for its Anti-Money Laundering Program, with full responsibility for the Company's AML program is qualified by experience, knowledge and training. The duties of the Principal Officer will include monitoring the Company's compliance with AML obligations and overseeing communication and training for employees. The Principal Officer will also ensure that proper AML records are kept. When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND)

The Company has provided the FIU with contact information for the Principal Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The Company will promptly notify FIU of any change to this information.

3. Customer Identification and Verification

At the time of opening an account or executing any transaction with it, the Company will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status as under

Constitution of Client	**Proof of Identity**	**Proof of Address**	**Others**
Individual	1. PAN Card, driving license etc	2. Copy of Bank Statement, Ration card, letter by employee, driving license, etc	3. N.A.

Company	4. PAN Card 5. Certificate of incorporation 6. Memorandum and Articles of Association 7. Resolution of Board of Directors	8. As above	9. Proof of Identity of the Directors/Others authorized to trade on behalf of the Company
Partnership Firm	10. PAN Card 11. Registration certificate 12. Partnership deed	13. As above	14. Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Trust	15. PAN Card 16. Registration certificate 17. Trust deed	18. As above	19. Proof of Identity of the Trustees/ others authorized to trade on behalf of the trust
AOP/ BOI	20. PAN Card 21. Resolution of the managing body 22. Documents to	23. As above	24. Proof of Identity of the Persons authorized to trade on

	collectively establish the legal existence of such an AOP/ BOI		behalf of the AOP/ BOI

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our Company will not open the new account.

All PAN Cards received will be verified form the Income Tax/ NSDL website before the account is opened.

The Company will maintain records of all identification information for ten years after the account has been closed.

4. Maintenance of records

- all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;

- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;

- all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;

- all suspicious transactions whether or not made in cash. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith -
    - gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
    - appears to be made in circumstances of unusual or unjustified complexity; or
    - appears to have no economic rationale or bonafide purpose; or
    - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

The records shall contain the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction."

The records will be updated on daily basis, and in any case not later than 5 working days.

5. Monitoring Accounts For Suspicious Activity

The company will monitor through the automated means of Back Office Software *(specify how suspicious transaction activity would be monitored)* for unusual size, volume, pattern or type of transactions. For non automated monitoring, the following kinds of activities are to be mentioned as Red Flags and reported to the Principal Officer.

· The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the Company's AML policies (particularly concerning his or her identity, type of business and assets), or is

reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the Company's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs.10,00,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

When a member of the Company detects any red flag he or she will escalate the same to the Principal Officer for further investigation

Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:

Identity of Client

- False identification documents
- Identification documents which could not be verified within reasonable time
- Non-face to face client
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities

Suspicious Background

- Suspicious background or links with known criminals

Multiple Accounts

- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale
- Unexplained transfers between multiple accounts with no rationale

Activity in Accounts

- Unusual activity compared to past transactions
- Use of different accounts by client alternatively
- Sudden activity in dormant accounts
- Activity inconsistent with what would be expected from declared business
- Account used for circular trading

Nature of Transactions

- Unusual or unjustified complexity
- No economic rationale or bonafide purpose
- Source of funds are doubtful
- Appears to be case of insider trading
- Investment proceeds transferred to a third party
- Transactions reflect likely market manipulations
- Suspicious off market transactions

Value of Transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting
- Large sums being transferred from overseas for making payments
- Inconsistent with the clients apparent financial standing
- Inconsistency in the payment pattern by client
- Block deal which is not at market price or prices appear to be artificially inflated/deflated

Customer Due Diligence Check (CDD):

The Customer Due Diligence process is defined under 3 parameters:

a. Policy for acceptance of Clients
b. Client Identification Procedure
c. Suspicious Transaction Identification and Reporting

The main aspect for CDD is to obtain sufficient information from the client in order to identify who is the actual beneficial owner of the securities or on whose behalf transactions are conducted. To ensure that there are no accounts that are opened under fictitious names or there are no benami accounts. Also to verify the

customers identity using reliable independent source document, data or information. Conduct ongoing due diligence and scrutiny of the account / client to ensure that the transactions conducted are consistent with clients financial background / status, its activities and risk profile.

6. Reporting to FIU IND

For Cash Transaction Reporting

- All dealing in Cash that requiring reporting to the FIU IND will be done in the CTR format and in the matter and at intervals as prescribed by the FIU IND

For Suspicious Transactions Reporting

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND and the required deadlines. This will typically be in cases where we know, suspect, or have reason to suspect:

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any the transaction reporting requirement,
- the transaction is designed, whether through structuring or otherwise, to evade the any requirements of PMLA Act and Rules framed thereof
- the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- the transaction involves the use of the Company to facilitate criminal activity.

We will not base our decision on whether to file a STR solely on whether the transaction falls above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

All STRs will be reported quarterly to the Board of Directors, with a clear reminder of the need to maintain the confidentiality of the STRs

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PMLA Act and Rules thereof.

7. AML Record Keeping

a. STR Maintenance and Confidentiality

We will hold STRs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a STR. We will refuse any requests for STR information and immediately tell FIU IND of any such request we receive. We will segregate STR filings and copies of supporting documentation from other Company books and records to avoid disclosing STR filings. Our Principal Officer will handle all requests or other requests for STRs.

b. Responsibility for AML Records and SAR Filing

Principal Officer will be responsible to ensure that AML records are maintained properly and that STRs are filed as required

c. Records Required

As part of our AML program, our Company will create and maintain STRs and CTRs and relevant documentation on customer identity and verification. We will maintain STRs and their accompanying documentation for at least ten years.

8. Training Programs

We will develop ongoing employee training under the leadership of the Principal Officer. Our training will occur on at least an annual basis. It will be based on our Company's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the Company's compliance efforts and how to perform them; the Company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PMLA Act.

We will develop training in our Company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

9. Program to Test AML Program

a. Staffing

The testing of our AML program will be performed by the Statutory Auditors of the company

b. Evaluation and Reporting

After we have completed the testing, the Auditor staff will report its findings to the Board of Directors. We will address each of the resulting recommendations.

10. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors

11. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the Company's AML compliance program to the Principal Officer, unless the violations implicate the Principal/Compliance Officer, in which case the employee shall report to the Chairman of the Board, Mr./Ms. Such reports will be confidential, and the employee will suffer no retaliation for making them.

12. Board of Directors Approval

We have approved this AML program as reasonably designed to achieve and monitor our Company's ongoing compliance with the requirements of the PMLA and the implementing regulations under it.

Prudent Broking Services Private Limited
Principle Officer