1. What is Money Laundering?

Money laundering involves the placement of illegally obtained money into legitimate financial systems so that monetary proceeds derived from criminal activities are transformed into funds with an apparently legal source.

Money laundering has many destructive consequences both for society as a whole and for those entities involved in money laundering activities.

With respect to society as whole, money laundering may provide resources for drug dealers, terrorists and other criminals to operate and expand their criminal activities.

With respect to entities, any involvement whether it be to instigate, assist, conceal, or ignore the source, nature, location, ownership or control of money laundering activities, can lead to both civil and criminal proceedings against both the individual and the entity involved .

2. Terrorist Financing

Terrorist financing refers to the processing of funds to sponsors involved in or those who facilitate terrorist activity. Terrorist individuals / groups / organization derive income from a variety of sources, often combining both lawful and unlawful funding, and where the agents involved do not always know the illegitimate end of that income.

3. Policy Statement

PIML is committed to fully comply with all applicable laws and regulations regarding Anti Money Laundering procedures. PIML has adopted and will enforce the provisions set forth in AML / CFT Regulations in order to prevent and detect money laundering, terrorist financing and other illegal activities.

If PIML, its personnel or premises are inadvertently used for money laundering or other illegal activities, PIML can be subject to potentially serious civil and/or criminal penalties. Therefore, it is imperative that every staff member including directors are familiar with and complies with the policy and procedures set forth in this document.

4. Goals & Objectives

The objective of this policy is to ensure that the products and services of the PIML are not used to launder the proceeds of crime and that all of the PIML's staff are aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing.

The document also provides a framework to comply with applicable laws, Regulatory guidelines specially related with detection and reporting of suspicious activities. Other objectives pursued by this policy are as follows:

- Promote a "Know Your Customer" policy as a cornerstone principle for the Brokerage firm's ethics and practices;
- Introduce a controlled environment where no business with a Customer is transacted until all essential information concerning the Customer has been obtained;
- Conduct self-assessments of compliance with AML policy and procedures;
- Introducing to the employees the stages of money laundering process and their individual duties;
- Establishing a review process which will be used to identify opportunities that might be used to launder money;
- Providing instructions regarding taking appropriate action once a suspicious activity or a money laundering activity is detected or suspected.

Adherence to this policy is absolutely fundamental for ensuring that the PIML is fully complied with applicable anti-money laundering rules and regulations.

The PIML is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and maintaining an effective AML Policy for its business.

In case of any clarification contact Compliance Department of PIML at sharifchaudry@gmail.com.

5. Scope

This policy is applicable to the PIML's operations including business. PIML shall ensure compliance with the Regulations on KYC, CDD AML / CFT or that of the SECP whichever are more exhaustive. Our coverage will include:

- Compliance of AML Act 2010.
- Compliance of SECP requirements on KYC, CDD AML / CFT.
- FATF Recommendations
- International Standards and guidelines, including Regulatory sanctions as applicable.

6. Internal Audit Function

To ensure that the PIML's policies and procedures are adhered to, PIML Board of Directors will act as internal audit function since the size of Brokerage house is small, having a small amount of clients. Compliance officer will update the board regarding all the information required to carry out Internal Audit tasks.

7. Compliance Officer

To ensure that the PIML's policies and procedures are adhered to, PIML shall designate Compliance Officer.

Responsibilities of the Compliance Officer include the following:

- Review of Account Opening Forms and sign off from Compliance perspective
- Coordination and monitoring of PIML's day-to-day compliance with applicable Anti Money Laundering Laws and Regulations and PIML's own AML / CFT Policy and Procedures;
- Conducting Employee training programs for appropriate personnel related to the PIML's AML / CFT policy and procedures and maintaining records evidencing such training;
- Receiving and reviewing any reports of suspicious activity from Employees;
- Determining whether any suspicious activity as reported by an Employee warrants reporting to senior management of the Firm;
- Coordination of enhanced due diligence procedures regarding Clients; and Responding to both internal and external inquiries regarding PIML's AML / CFT policy and procedures.

8. Employee Training

PIMLs should ensure that all appropriate staff, receive training on ML / TF prevention on a regular basis ensure that all staff fully understand the procedures and their importance, that they will be committing criminal offences if they contravene the provisions of the legislation.

Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements

PIML provide their staff training in the recognition and treatment of suspicious activities. Training should also be provided on the results of the PIML's risk assessments. Training should be structured to ensure compliance with all of the requirements of the applicable legislation.

Staff should be aware on the AML / CFT legislation and regulatory requirements, systems and policies.

All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.

All new employees should be trained on ML / TF know the legal requirement to report and of their legal obligations in this regard.

PIMLs shall consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML / CFT matters, read the PIML's AML / CFT manuals, policies and procedures, and understand the AML / CFT obligations under the relevant legislation.

Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers.

Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions.

All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account

Although Directors and Senior Managers may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML / CFT policies and procedures.

Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML / CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.

The CO should receive in-depth training on all aspects of the primary legislation, the Regulations, regulatory guidance and relevant internal policies. They should also receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

9. Employee Screening

PIMLs should maintain adequate policies and procedures to screen prospective and existing employees to ensure high ethical and professional standards when hiring. The extent of employee screening should be proportionate to the potential risk associated with ML / TF in relation to the business in general, and to the particular risks associated with the individual positions.

PIMLs shall ensure that their employees are competent and proper for the discharge of the responsibilities allocated to them. While determining whether an employee is fit and proper, the PIML may:

- Verify the references provided by the prospective employee at the time of recruitment
- Verify the employee's employment history, professional membership and qualifications
- Verify details of any regulatory actions or actions taken by a professional body
- Verify details of any criminal convictions; and
- Verify whether the employee has any connections with the sanctioned countries or parties.

10. Client Identification Procedures

PIML's AML / CFT policy and procedures are intended to ensure that, prior to accepting funds from Clients, all reasonable and practical measures are taken to confirm the Clients' identities.

PIML may take assistance from the bank or other financial institutions for completing client identification process. The assistance shall not relieve the PIML for identification process to be conducted by the

company. These Client Identification Procedures are based on the premise that the PIML will accept funds from a new and existing Client only after:

- PIML has confirmed the Client's identity and that the Client is acting as a principal and not for the benefit of any third party unless specific disclosure to that effect is made; or
- If the Client is acting on behalf of others, PIML has confirmed the identities of the underlying third parties.

11. Customer acceptance policies

At first the transaction from a customer is accepted, as per policy criteria set under the heading of Restricted Personal List.

After this the understanding of the customer's business and its activities help a lot to contribute to the company's overall reputational, concentration, operational and legal risk management through the detection of potentially harmful activities.

Restricted Personal List

The UNSC Sanctions Committee, maintains the consolidated list of individuals and entities subject to the sanctions covering assets freeze, travel ban and arms embargo set out in the UNSC Resolution 1267 (1999) and other subsequent resolutions, concerning ISIL (Daésh) / Al-Qaida and Taliban and their associated individuals.

Government of Pakistan publishes Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 in the official Gazettes to give effect to the decisions of the UNSC Sanctions Committee and implement UNSC sanction measures in Pakistan. The regularly updated consolidated lists is available at the UN sanctions committee's website, at following link;

www.un.org/sc/committees/1267/aq_sanctions_list.shtml

https://www.un.org/sc/suborg/en/sanctions/1988/materials

https://www.un.org/sc/suborg/en/sanctions/1718/materials

http://www.un.org/en/sc/2231/list.shtml

https://www.un.org/sc/suborg/en/sanctions/1718/prohibited-items

The Ministry of Interior issues Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997, to implement sanction measures under UNSCR 1373(2001), and the regularly updated consolidated list is available at the National Counter Terrorism Authority's website, at following link;

http://nacta.gov.pk/proscribed-organizations/

Where there is a true match or suspicion, PIMLs shall take steps that are required to comply with the sanctions obligations including freeze without delay and without prior notice, the funds or other assets of designated persons and entities and reporting to the Commission, if they discover a relationship that contravenes the UNSCR sanction or a proscription.

12. Client Identification Procedures for Individual Persons

For Identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on KYC / CDD form or account opening form:

- Full name as per Identity document of the Applicant

- Date of Birth, Gender, Marital status, Religion, Occupation, and Qualification
- Residential Status, Nationality, Country of Residence
- Details of Employer/Business
- CNIC/NICOP/SNIC/POC/Passport Number
- Existing Mailing and Permanent address
- Residential Telephone Number, Office Telephone Number, Fax Number, Mobile Number and Email address
- NTN and STN number
- Nature and Type of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining with other Broker(s)
- Source of Income, Gross Annual Income, Sources of Fund for Stock Market, Expected value of Investment
- Knowledge of stock Market and Investment experience
- Normal or expected mode of transaction

Client Identification Procedures for Joint Accounts:

In case of Joint account, the customer due diligence measures on all of the joint account holders shall be performed as if each of them were individual customers of the PIML. In order to confirm the identity of the Client, copies of the following documents will be obtained and retained for PIML's record:

- Duly filled and signed Account Opening Form (AOF) by Title and Joint Account Holder(s).
- Bank Verification on AOF from the bank where Title Account Holder is maintaining a bank account.
- Physical presence of Title and Joint Account Holder(s) at any of the PIML Office along with valid original ID document.
- Attested Copies of valid ID document of Title and Joint Account Holder(s).
- Attested Copies of valid ID document of witnesses.
- Local Mobile Number and/or email address.
- Copy of Zakat Declaration (CZ-50) duly attested by notary public as per the prescribed format for Zakat exemption (Optional).
- For Non-Muslims PIML, written request for Zakat non-applicability.
- Power of Attorney duly attested by Notary Public on prescribed format duly signed by all Account Holders (optional).
- Copy of NTN certificate, if NTN is provided in AOF.
- Copy of NICOP for non-resident Pakistanis, Passport for foreigners duly attested by Consulate office of Pakistan or Notary Public of respective country.
- Bank statement or utility bill; or other residential identifying information;
- Bank references.
- Proof of Employment/ Business
- If the account is opened by the officer of government, Special resolution / Authority from the Federal / Provincial / Local Government department duly authorized by the Ministry of Finance or Finance department of the concerned provincial or Local Government.

Client Identification Procedures for Corporations, Partnerships, Trusts and Other Legal Entities:

PIML shall take reasonable steps to ascertain satisfactory evidence of an entity Client's name and address, its authority to make the contemplated investment. For Identity and due diligence purposes, at the minimum following information shall be obtained, verified and recorded on KYC / CDD form or account opening form:



- Full name as per Identity document
- Company registration / Incorporation number
- Date and country of Incorporation
- Date of Business Commenced
- Residential Status
- Type of Business
- Name of parent Company
- Email, website and contact number
- Registered and mailing address
- NTN number and Sales Tax number
- Details of Contact Person and authorized person to operate the account
- Nature and Type of Account
- Details of Bank Account
- Details of Investor Account maintaining with CDC and Details of Sub Account maintaining with other Broker(s)
- Financial and General Information including Investment experience, Expected value of investment, recent change in ownership of the company, customer type,
- Normal or expected mode of transaction RASL will obtain the following documents, as appropriate under the circumstances
- Certified true copy of Board Resolution. (Specimen provided as per Annexure "A") / Power of Attorney*
- Certified true copies of Constitutive Documents of the Applicant (Memorandum & Articles of Association, Act / Charter / Statute / By-laws / Rules & Regulations, Certificate of Incorporation, Certificate of Commencement of Business, Prospectus for Modaraba, Relevant licenses and registration issued by Regulatory Bodies etc.)
- Certified copy of list of Directors / Trustee (if applicable)*
- List of authorized signatories.
- List of Nominated persons allowed placing orders.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Authorized Signatories.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Contact Person.
- Attested copies of C.N.I.C. / N.I.C.O.P / Passports of the Witnesses.
- Certified copy of N.T.N. Certificate. (If exempted please provide Exemption Certificate).
- Latest Audited Accounts of the Company.

Beneficial ownership

f a customer has authorized another person, than the additional documentation are required. These include:

- Attested copies of ID document of Authorized person
- Power of Attorney duly attested by Notary Public on prescribed format duly signed by all Account Holders with the following minimum information:
- Name of Authorized person and his/her Relationship
- CNIC / NICOP / Passport number
- Contact Details and email address
- Specimen Signature of the person authorized.
- Nature of business of beneficial owner

The authorized person is only allow to issue instruction for buy or sale of securities on behalf of client and all payments or receipt of funds must be made to or from the client own accounts and must include CNIC number clearly marked on all payment cheques.

13. Account Shall Not Open

Where CDD Measures are not completed, In case the PIML is not been able to satisfactorily completed required CDD measures, account shall not be opened or any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR.

Anonymous or Fictitious Account: PIML shall not open or maintain anonymous account or accounts in the name of factitious persons.

Government Accounts: Government Account shall not be opened in the personal names of the government officials.

Proscribed Individuals / Entities: PIML shall not provide services to Proscribed Individuals, Groups and Entities declared / listed by UNSC (United Nations Security Council) and / or by OFAC (Office of Foreign Asset Control – USA) OR those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

14. Risk Profiling Of Customers

All relationships shall be categorized with respect to their risk levels i.e. High, Medium and Low based on the risk profiling of customer (through KYC / CDD application and as guided in the operational Manual for making effective decision whether to perform Simplified Due Diligence (SDD) or Enhanced Due Diligence (EDD) both at the time of opening and ongoing monitoring of business relationship.

High-Risk Clients

The Compliance Officer will provide and will continuously update a list of the types of Clients that PIML considers to be of 'high risk,' such that enhanced due diligence procedures are warranted compared to the routine Client Identification Procedures. Following are the examples of Clients who pose a high money laundering risk:

- Non-resident customers;
- Legal persons or arrangements including non-governmental organizations; (NGOs)/ not for-profit organizations (NPOs) and trusts / charities;
- Customers belonging to countries where CDD/KYC and antimony laundering regulations are lax or if funds originate or go to those countries;
- Customers whose business or activities present a higher risk of money laundering such as cash based business;
- Customers with links to offshore tax havens;
- High net worth customers with no clearly identifiable source of income;
- There is reason to believe that the customer has been refused brokerage services by another brokerage house;
- Non-face-to face / on-line customers;
- Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations; and
- Politically Exposed Persons (PEPs) or customers holding public or high profile positions. Politically Exposed Persons (PEPs) these generally include individuals in prominent positions such as senior politicians, senior government, judicial or military officials; senior executives of State Corporations and their family members and close associates. These individuals present reputational risk and potential conflict of interest and extra caution is required when opening their brokerage account and monitoring their account activity. The above definition is not intended to cover middle ranking /

junior officials in above noted categories. However, prudence requires brokers to be careful while dealing with such customers

15. **Enhanced Client Identification Procedures for 'High Risk' Natural Persons Enhanced Client Identification**

Procedures for 'high risk' natural persons as Clients include, but are not limited to, the following:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means;
- Considering the source of the Client's wealth: including the economic activities that generated the Client's wealth, and the source of the particular funds intended to be used to make the investment;
- Reviewing generally available public information, such as media reports, to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists;
- Conducting a face-to-face meeting with the Client to discuss/confirm the account opening documents.

The enhanced due diligence procedures undertaken with respect to 'high risk' Clients must be thoroughly documented in writing, and any questions or concerns with regard to a 'high risk' Clients should be directed to the Compliance Officer.

16. **Enhanced Client Identification Procedures for 'High Risk' Corporations, Partnerships, Trusts and Other legal Entities Enhanced Client Identification**

Procedures for 'high risk' Corporations, partnerships and other legal entities include, but are not limited to, the following:

- Assessing the Client's business reputation through review of financial or professional references, generally available media reports or by other means;
- Reviewing recent changes in the ownership or senior management of the Client;
- Conducting a visit to the Client's place of business and conducting a face-to-face meeting with the Client to discuss/confirm the account application, the purpose of the account and the source of assets;
- Reviewing generally available public information to determine whether the Client has been the subject of any criminal or civil enforcement action based on violations of anti-money laundering laws or regulations or any criminal investigation, indictment, conviction or civil enforcement action relating to financing of terrorists.

17. **Payment Mechanism**

For amounts greater than PKR 25,000

The RASL shall accept from / pay to the Account Holder(s) through "A/C Payee Only" crossed cheque, bank drafts, pay orders or other crossed banking instruments in case if amounts exceeds Rs. 25,000/=.

Electronic transfer of funds through banks would be regarded as good as cheque. The RASL shall be responsible to provide the receipt to the Account Holder(s) in the name of Account Holder(s) duly signed by authorized agents / employee of the Broker and the Account Holder(s) shall be responsible to obtain the receipt thereof.

For amounts less than or equivalent to PKR 25,000.

In case of cash dealings, proper receipt will be taken and given to the Account Holder(s), specifically mentioning if payment is for margin or the purchase of securities. The PIML shall immediately deposit in its bank accounts all cash received in whole i.e. no payments shall be made from the cash received from clients.

Exceptional Circumstances

However, in exceptional Circumstances, where it becomes necessary for the PIML to accept cash in excess of Rs. 25,000/=, the RASL shall immediately report within one business day, such instances with justification thereof, to the Stock Exchange in accordance with the mechanism prescribed by the Exchange.

Copies of these payment instruments including cheques, pay orders, demand drafts and online instructions shall be kept in record for a minimum period of five years.

18. General Reporting Procedures

- The Compliance Officer on behalf of the organization is nominated to receive disclosures under this regulation.
- Anyone in the organization, to whom information comes in the course of the relevant business as a result of which he suspects that a person is engaged in money laundering, must disclose it to the Compliance Officer;
- Where a disclosure is made to the Compliance Officer, the officer must consider it in the light of any relevant information which is available to PIML and determine whether it gives rise to suspicion:
- Where the Compliance Officer determines in consultation with the Senior Management, the information must be disclosed to the Regulatory Authority after obtaining an independent legal advice.

19. **Reporting of Suspicious Transactions / Currency Transaction Report**

A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction must be considered unusual, and the RASL should put "on enquiry".

RASLs should also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

Where the enquiries conducted by the PIML do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML / CFT Compliance officer.

Activities which should require further enquiry may be recognizable as falling into one or more of the following categories:

- Any unusual financial activity of the customer in the context of the customer's own usual activities;
- Any unusual transaction in the course of some usual financial activity;
- Any unusually-linked transactions;
- Any unusual method of settlement;
- Any unusual or disadvantageous early redemption of an investment product;
- Any unwillingness to provide the information requested.

Reporting STR

If the PIML decides that a disclosure should be made, the law require the PIML to report PIML without delay to the FMU, in standard form as prescribed under AML Regulations 2015. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AMLRegulations2015.pdf.



PIML is required to report total number of STRs filed to the Commission (SECP) on bi-annual basis within seven days of close of each half year. The Compliance Officer should ensure prompt reporting in this regard.

Reporting CTR

PIML is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

PIML will maintain a register of all reports made to the FMU. Such registers should contain details of:

- The date of the report;
- The person who made the report;
- The person(s) to whom the report was forwarded; and
- Reference by which supporting evidence is identifiable.

20. **Record-Keeping Procedures**

As per guidelines provided by SECP:

PIML ensure that all information obtained in the context of KYC / CDD / EDD is recorded. This includes both;

- Recording the documents the PIML is provided with when verifying the identity of the customer or the beneficial owner, and
- Transcription into the PIML's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

PIML should maintain, for at least 5 years after termination, all necessary records on transactions to be able to comply swiftly with information requests from the competent authorities. Such records should be sufficient to permit the reconstruction of individual transactions, so as to provide, if necessary, evidence for prosecution of criminal activity.

Where there has been a report of a suspicious activity or the PIML is aware of a continuing investigation or litigation into ML / TF relating to a customer or a transaction, records relating to the transaction or the customer should be retained until confirmation is received that the matter has been concluded.

Records relating to **reporting by securities broker** will generally comprise:

- Monthly report prepared on reporting by securities broker under the Circular no.10/2017 of SECP.

Records relating to **verification of identity** will generally comprise:

- A description of the nature of all the evidence received relating to the identity of the verification subject; and
- The evidence itself or a copy of it or, if that is not readily available, information reasonably sufficient to obtain such a copy.

Records relating to **transactions** will generally comprise:

- Details of personal identity, including the names and addresses, of:
- The customer;
- The beneficial owner of the account or product; and
- Any counter-party

Details of **securities and investments** transacted including:

- The nature of such securities/investments;

- Valuation(s) and price(s);
- Memoranda of purchase and sale;
- Source(s) and volume of funds and securities;
- Destination(s) of funds and securities;
- Memoranda of instruction(s) and authority(ies);
- Book entries;
- Custody of title documentation;
- The nature of the transaction;
- The date of the transaction;
- The form (e.g. Cash, cheque) in which funds are offered and paid out.

21. Policy Review Period:

The AML / CFT Policy & Procedures will be reviewed on annual basis and updated as and when required.