
**ANTI-MONEY LAUNDERING & COUNTERING FINANCING OF TERRORISM
(AML/CFT) AND KNOW YOUR CUSTOMER & CUSTOMER DUE DILIGENCE
(KYC/CDD) POLICY**

(Version 1.2)

CONTENTS

- 1) Glossary
- 2) About Intermarket Securities Limited
- 3) Back Ground
- 4) Goals and Objectives
- 5) Scope
- 6) REGULATORY OVERSIGHT & COMPLIANCE RISK
- 7) AML/CFT & KYC/CDD Policies and procedures
 - a) Customer Identification
 - b) Risk assessment of customer
 - c) Circumstances where Enhanced Due Diligence is required
 - d) On-going due Diligence
 - e) Circumstances where simplified Due Diligence can be adopted
 - f) Compliance function
 - g) Data retention
 - h) Training and employee screening
- 8) Monitoring and Reporting of Suspicious Transactions
- 9) Non Compliance
- 10) Record Retention
- 11) Accountability and Responsibility
- 12) Internal Audit

ANNEXURES

- A) ML/TF WARNING SIGNS/ RED FLAGS
- B) LIST OF REQUIRED DOCUMENTS FROM DIFFERENT TYPES OF CUSTOMERS
- C) RISK ASSESSMENT OF CUSTOMER

1. GLOSSARY

AML	Anti-Money Laundering
AOF	Account Opening Form
BOD	Board of Directors
CCO	Chief Compliance Officer
CDD	Customer Due Diligence
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism
CIF	Customer Information File
CNIC	Computerized National Identity Card
CTR	Cash Transaction Report
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FMU	Financial Monitoring Unit
IMS	Intermarket Securities Limited
ML	Money Laundering
MSB	Money Service Business
NADRA	National Database and Registration Authority
NICOP	National Identity Card for Overseas Pakistanis
OFAC	Office of the Foreign Assets Control
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Person
PEPs	Politically Exposed Persons
POC	Pakistan Origin Card
PSX	Pakistan Stock Exchange
RMA	Relationship Management Application
RO	Money Laundering Reporting Officer
SBP	State Bank of Pakistan
SDD	Simple Due Diligence
SECP	Securities and Exchange Commission of Pakistan
SNIC	Smart National Identity Card
STR	Suspicious Transaction Report
TF	Terrorist Financing
UN	United Nations
UNSC	United Nations Security Council
NACTA	National Counter Terrorism Authority
NRA	National Risk Assessment

2. ABOUT INTERMARKET SECURITIES LIMITED

“Intermarket Securities Limited (IMS), the flagship of the Intermarket Group, came into its current corporate structure post the acquisition of ING Barings Pakistan operations in the early 2000s. IMS is a full-service brokerage platform offering trade execution/settlement, investment banking & advisory as well as equities & economic research. IMS has one of the most accredited equity market teams in Pakistan providing best in class services to clients. Team members in equity research and investment banking have been individually and jointly recognized by Asia Money and CFA Society Pakistan while our Sales Desk has extensive experience in servicing both domestic and international institutional investors with relationships across global financial centers.

3. BACK GROUND

In the last few years, across the world regulations have been put in place to discourage money laundering and financing of illegal/criminal activities. Furthermore, under the United Nations umbrella, several international agreements have been signed by U.N. member states under which member states are bound to implement policies that discourage money laundering and monitor financial transaction that are suspicious and raise concern about money laundering. The Islamic Republic state of Pakistan is a signatory to such agreement and is a member of relevant bodies such as Financial Action Task Force (FATF). As such, Pakistan has to abide by the recommendations of FATF and other relevant bodies and implement appropriate policies and procedures. If Pakistani policies are not in line with such recommendations, the image of the country is tarnished. Not only this, but Pakistani businesses and institutions (e.g. financial institutions, importers & exporters, investors, etc) can face difficulties in transacting business internationally with negative economic consequences for the country.

Pakistan has enacted the ANTIMONEY LAUNDERING ACT 2010. Financial institutions and intermediaries are required to comply with the provisions of this Act. In the above context, Apex capital market regulator, the Securities and Exchange Commission of Pakistan (SECP) has provided comprehensive guidelines for Pakistan capital market institutions regarding how to develop and implement policies and procedures that will help discourage money laundering and also allow capital market institutions to monitor and remain alert regarding suspicious transactions and/or parties who may be attempting to launder money. In the case of the brokerage industry, SECP being its Apex regulator and the Pakistan Stock Exchange Limited being the frontline regulator of the brokerage industry, have formulated detailed set of guidelines for brokers to help them in developing KYC and CDD policies & procedures and implementing the same.

Now, this document has been prepared to follow the guidelines and instructions of Regulators and shall be implemented being a broker of PSX & PMEX.

IMS is committed to the highest standards of AML and CFT. The members of the Management Board and all employees are required to adhere to these standards to protect IMS and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes.”

IMS will adhere to all applicable laws and regulation in all countries where it conducts business or has business relationships to, but in case of any adherence local laws will always prevail.

IMS will examine its AML and CFT strategies, goals and objectives on an ongoing basis and for all these topics IMS has implemented clear rules and regulations which must be complied with all IMS staff.

4. GOALS & OBJECTIVES

The objective of this policy is to ensure that the products and services of the Intermarket Securities Limited (IMS) are not used to launder the proceeds of crime and that all of the IMS'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/CFT 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 IMS is fully complies with applicable anti-money laundering rules and regulations.

The IMS 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 at compliance@imsecurities.com.pk

5. SCOPE

This policy is applicable to the IMS's local as well as overseas operations (if any) including business of other Financial Institutions routed through IMS.

In overseas offices (if any), IMS shall ensure compliance with the Regulations of the host country on KYC, CDD AML/CFT or that of the SECP whichever are more exhaustive.

6. REGULATORY OVERSIGHT & COMPLIANCE RISK

In the case of the brokerage industry, SECP being its Apex regulator and the PSX being the frontline regulator of the brokerage industry in Pakistan, have formulated detailed set of guidelines for brokers to help them in developing AML/CFT & KYC/CDD policies & procedures and implementing the same.

IMS is bound to use SECP, PSX guidelines and International Regulatory guidelines/standards as applicable to formulate its own AML/CFT & KYC/CDD Policy. The consequence of contravening the Regulations or failing to comply with any provision of these regulation made shall be liable to pay such sum as provided in section 40 of

the Securities and Exchange Commission of Pakistan Act, 1997 (XLII of 1997), in addition to any penalty provided under AML Act..

Notwithstanding the statutory and regulatory penalties, increased vigilance by Management and staff will protect IMS from the following risks:

- Reputational
- Operational
- Legal
- Financial

Reputational risk:

The reputation of a business is usually at the core of its success. The ability to attract good employees, customers and business is dependent on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong AML/CFT & KYC/CDD policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational risk:

This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If AML/CFT & KYC/CDD policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound.

Legal risk:

If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.

Financial risk:

If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve money that the customer owes.

7. AML/CFT & KYC/CDD POLICIES AND PROCEDURES

KYC/CDD is closely associated with the fight against money-laundering "AML". Supervisors around the world are increasingly recognizing the importance of ensuring that their financial institutions have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, financial institutions can be exposed to reputational, operational, legal and financial risks.

Following key Areas has been covered:

- a) Customer Identification
- b) Politically Exposed Persons:
- c) Risk assessment of customer in light of National Risk Assessment (NRA)
- d) Circumstances where Enhanced Due Diligence is required
- e) On-going due Diligence
- f) Circumstances where simplified Due Diligence can be adopted
- g) Compliance function
- h) Data retention
- i) Training and employee screening

a) Customer Identification

“IMS” should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or may complete verification after the establishment of the business relationship, provided that-

- (i) this occurs as soon as reasonably practicable;
- (ii) this does not interrupt the normal conduct of business; and
- (iii) the ML/TF risks are effectively managed.

Customer identification is very important that will protect our company from being used by unscrupulous and/or criminal elements. In this respect minimum documents/information as prescribed by SECP must be obtained from customers at the time of opening of accounts. Further, any additional document/information may be obtained on case to case basis where considered necessary. The key point is that anonymous or obviously fictitious accounts should not be opened.

- In case a customer is acting on behalf of another person, then identity of that person shall be ascertained and relevant documents/information of that person need to be obtained also.
- For non-individual customers (e.g. companies, pension funds, government owned entities, non-profit organizations, foreign companies/organizations) additional care shall be taken to establish the ownership and control structure of such an organization and who (i.e. person(s)) actually owns the organization and who manages it. It shall be verified that the person who represents himself as authorized signatory with powers to open and operate the account is actually authorized by the organization.
- For individual customers, proper authorization shall be obtained from person authorized to act on behalf of the customer.
- It shall be ensured that accounts of Institutions/organizations/corporate bodies are not opened in the individual name(s) of employee(s)/official(s). Because of sensitive nature of public sector (government) entities and risk of potential conflict of interest, these accounts shall not be opened in the individual name of any employee/official. Any such account, which is to be operated by an officer of a govt. owned entity, is to be operated by an officer of the Federal/Provincial/Local Government in his/her official capacity, shall be opened only on production of a special resolution/authority from the concerned administrative department,

duly endorsed by the Ministry of Finance or Finance Department of the concerned Provincial or Local Government.

Explanation:- “Government entities” includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.

- Sufficient information shall be obtained and documented on the purpose and intended nature of account to be opened and a profile shall be developed based on results of customer identification and the risk assessment. Information regarding intended investment plan of the customer must also be obtained to the extent possible and should be documented.
- Sufficient information shall be obtained to determine the expected source of funding for the account, particularly whether the customer shall receiving/remitting funds in foreign currency.
- It must be ensured that all receipts and payments to the customers above the prescribed threshold (i.e. Rs. 25,000/-) are made through cross cheques, bank drafts, pay orders or other crossed banking instruments. For exceptional circumstances where it shall become necessary to accept cash from a customer, reporting of such instances with rationale should be made immediately to the exchanges.
- Physical presence of the customer at the time of opening of account is necessary. In case of off-shore customers or customers in cities where no branch exist, appropriate procedures must be applied to ensure the identification of customer through video conferencing (e.g Skype, IMO etc.). When obtaining confirmation in different jurisdictions, it must be considered whether that jurisdiction is following the FATF recommendations.
- “IMS” shall perform appropriate enhanced due diligence (EDD) measures with customers that are identified as high risk by the “IMS” or are notified as such by the Commission.

b) Politically Exposed Persons:

A Politically Exposed Person (PEP) is defined by the Financial Action Task Force (FATF) as an individual who is, or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering (ML) offences and related predicate offences, including corruption, bribery, and conducting activity related to terrorist financing (TF). The potential risks associated with PEPs justify the application of additional anti-money laundering/counter-terrorist financing (AML/CFT) preventative measures with respect to business relationships with PEPs.

Politically Exposed Persons Categories

The difference between foreign and domestic PEPs may be relevant for firms making specific risk assessments. To help clients gain a holistic view of potential risk. In the first instance PEPs are classified at a high level in the following categories:

Foreign PEPs

Individuals who are, or have been entrusted with prominent public functions by a foreign country, for example heads of state or government, senior politicians, senior government,

judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs

Individuals who are, or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

International organization PEPs

Persons who are, or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions i.e. directors, deputy directors, and members of the board or equivalent functions.

Family members

Individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.

Close associates

Individuals who are closely connected to a PEP, either socially or professionally.

How you will seek approval from senior management?

"IMS" shall obtain Senior Management approval to determine the nature and extend of EDD where the ML/TF risks are high. In assessing the ML/TF risk of a PEP, "IMS" shall consider factors such as whether the Customer who is a PEP:

- Is from a high risk country;
- Has prominent public function in sectors know to be exposed to corruption;
- Has business interests that can cause conflict of interests (with the position held).
- How you will take adequate measures to establish source of wealth and source of funds?
- "IMS" shall consider other red flags include (in addition to the Red Flags that they consider for other applicants):
- The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
- Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
- A PEP uses multiple bank accounts for no apparent commercial or other reason;
- The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.
- "IMS" shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:
- the level of (informal) influence that the individual could still exercise; and

- whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

c) Risk assessment of customer in light of National Risk Assessment (NRA)

Risk assessment must be performed of all the existing and prospective customers on the basis of information obtained regarding their Identity, nature of income, source of funding, geography

- Countries identified by credible sources as published follow-up reports by FATF as not having adequate AML/CFT systems
- Countries subject to sanctions, embargos or similar measures by United Nations
- Countries identified by credible sources as having significant levels of corruption or criminal activity
- Vulnerable Areas Highlighted in NRA 2019
- Pakistan Porous Border Areas

Based on the results of such assessment which include Terror Financing (TF) Threat and Crimes as mentioned in NRA and, categorize customers among high risk, medium risk and low risk customers.

Annexure C the sets out examples of factors should be considered when performing risk assessment. Where there is one or more "yes" responses, professional judgement must be exercised, with reference to the policies and procedures of the "IMS", as to the nature of customer due diligence to be carried out.

d) Enhanced Due Diligence

Once a customer has been categorized as HIGH RISK, it is necessary to have Enhanced Due Diligence (EDD) when dealing with such a customer. Activities and transactions of HIGH RISK customers shall be monitored and any unusual transactions shall be reported in suspicious transaction report.

- When dealing with high-risk customers, including Politically Exposed Persons (PEP's), senior management' approval shall be obtained to establish business relationships with such customers. The same shall also apply in case of an existing customer which will be classified as high-risk pursuant to these policies or which will be subsequently classified as a result of ongoing due diligence. Further, reasonable measures shall be taken to establish the source of wealth and source of funds.
- If it will be not possible to comply with the above requirements, account shall not be opened or business relationship shall be terminated, as the case may be and suspicious transaction report shall be submitted.

- Where “IMS” are not able to satisfactorily complete 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 and where CDD of an existing customer is found unsatisfactory, the relationship should be treated as high risk and reporting of suspicious transaction be considered in accordance with point 8;
- Where “IMS” forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it may not pursue the CDD process, and instead should file an STR in accordance with point 8.

e) On-Going Due Diligence & Monitoring

- 1) All business relations with customers shall be monitored on an ongoing basis to ensure that the transactions are consistent with the “IMS” knowledge of the customer, its business and risk profile and where appropriate, the sources of funds.
- 2) “IMS” shall obtain information and examine, as far as possible the background and purpose of all complex and unusual transactions, which have no apparent economic or visible lawful purpose and the background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required.
- 3) “IMS” shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers and the review period and procedures thereof should be defined by “IMS” in their AML/CFT policies, as per risk based approach.
- 4) In relation to sub-regulation (3), customers’ profiles should be revised keeping in view the spirit of Know Your Customer/CDD and basis of revision shall be documented and customers may be consulted, if necessary.
- 5) Where “IMS” files an STR on reasonable grounds for suspicion that existing business relations with a customer are connected with ML/TF and the “IMS” considers it appropriate to retain the customer-
 - i. the “IMS” shall substantiate and document the reasons for retaining the customer; and
 - ii. the customer’s business relations with the “IMS” shall be subject to proportionate risk mitigation measures, including enhanced ongoing monitoring.
- 6) “IMS” shall not form business relationship with entities/individuals that are:
 - j) proscribed under the United Nations Security Council Resolutions and adopted by the Government of Pakistan;
 - ii) proscribed under the Anti-Terrorism Act, 1997(XXVII of 1997); and
 - iii) associates/facilitators of persons mentioned in (a) and (b).
- 7) The “IMS” should monitor their relationships on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the “IMS” shall take immediate action as per law, including freezing the funds and assets of such proscribed entity/individual and reporting to the Commission.

f) Simplified Customer Due Diligence

CDD measures shall be simplified or reduced in the following circumstances:

- risk of money laundering or terrorist financing is lower
- information on the identity of the customer and the beneficial owner of a customer is publicly available
- adequate checks and controls exist

Following customers may be considered for simplified or reduced CDD:

- Financial institutions which are subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and are supervised for compliance with those controls
- Public companies that are subject to regulatory disclosure requirements
- Government administrations or enterprises

When opting for simplified or reduced due diligence, the FATF guidelines in this regard shall be consulted. Simplified CDD shall not be followed when there is an identified risk of money laundering or terrorist financing.

g) Compliance Function

- A compliance function shall be established with suitable human resource and MIS reporting capabilities, enabling it to effectively monitor the customers' transactions and make timely reports.
- The Head of Compliance function shall have skills and experience necessary for satisfactory performance of functions assigned. Head of Compliance shall be independent and report directly to the Board of Directors.
- The Compliance function shall ensure compliance with the requirements of these policies as well as other regulatory requirements applicable under the relevant legal framework. A record shall be maintained of all violation/ non-compliance identified and reported to the BoD and must be available for the inspection of SECP as and when required.

h) Data Retention

It shall be required to maintain the relevant documents obtained through the application of KYC/CDD/AML/CFT procedures, especially those pertaining to identification of the identity of a customer, account files and correspondence exchanged for a minimum period of five years after termination of the business relationship.

i) Training and Employee Screening

Appropriate on-going employee training program and knowledge refreshment shall be arranged to ensure that the employees understand their duties and are able to perform the same on a satisfactory level.

Staff shall be hired with extra care and all possible screening measures shall be taken including independent inquiries, information from previous employers/colleagues etc. Further, screening process shall be an on-going exercise and shall be applied consistently to ensure that employees, particularly those working at sensitive positions, meet and maintain high standards of integrity and professionalism.

Any information concerning customers and their transactions shall be provided to the exchanges, Financial Monitoring Unit or the Commission as and when required. All requirements of Anti Money Laundering and Countering financing of Terrorism Regulations, 2018 as applicable, including the requirement to file Suspicious Transaction Reports and any directives, circulars, guidelines issued in this regard by Federal Government, Financial Monitoring Unit and SECP shall be complied.

A checklist has been developed and annexed to these policies and procedures. Details of necessary documents, information and procedures required to be obtained/followed have been incorporated therein. Further, necessary documents/information required have also mentioned in relevant account opening forms and are not reproduced herein to avoid repetition.

All relevant laws/regulations/recommendations/guidelines/directives of relevant authorities (e.g. SECP, FATF etc.) are available separately.

8. MONITORING AND REPORTING OF SUSPICIOUS TRANSACTION / ACTIVITIES

The company is required to report to Financial Monitoring Unit when company receives a cash based transaction involving payment, receipt, or transfer of an amount exceeding the minimum threshold as specified by the National Executive Committee (NEC), hereinafter referred to as the NEC, "IMS" shall file a report of such transaction on prescribed format immediately but not later than seven working days, after the respective currency transaction.

The company manually monitors a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified in SECP's guidelines on Anti Money Laundering Regulations, 2018 as mentioned in Annexure A. Company will look at transactions, including deposits and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction for that customer. Company will report suspicious transaction reporting to Financial Monitoring Unit immediately but not later than seven working days after forming that suspicious in respect of that particular transaction was followed through or not.

9. NON COMPLIANCE

Failure to abide by the Policy set by "IMS" to prevent money laundering and terrorist financing will be treated as a disciplinary issue. Any deliberate breach will be viewed as severe misconduct. Such

cases will be referred to HR for onward initiation of disciplinary action that could lead to termination of employment and could also result in criminal prosecution and imprisonment for the concerned staff member.

10. RECORD RETENTION

It is a Policy of IMS:

- To retain identification and transaction documentation for the minimum period as required by applicable Laws and Regulations.
- To retain records of all suspicious activity reports made by Compliance department to Regulators for an indefinite period unless advised by the Regulator otherwise.
- To be in a position to retrieve, in a timely fashion, records that are required by law enforcement agencies as part of their investigations.

To keep records of KYC & CDD, AML/CFT training provided to the employees, nature of the training and the names of staff who received such training.

11. ACCOUNTABILITIES AND RESPONSIBILITIES

The Board is Responsible for:

- Ensuring that adequate systems and controls are in place to deter and recognize criminal activity, money laundering and terrorist financing.
- Seeking compliance reports including coverage of AML/CFT issues) on quarterly basis and taking necessary decisions required to protect IMS from use by criminals for ML & TF activities.
- The Oversight of the adequacy of systems and controls that are in place to deter and recognize criminal activity, money laundering and terrorist financing.

Management is Responsible for:

- Ensuring that AML/CDD/CFT policy is implemented in letter and spirit.

All Employees are Responsible for:

- Remaining vigilant to the possibility of money laundering / terrorist financing through use of IMS's products and services.
- Complying with all AML/CFT policies and procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Promptly reporting to CO where they have knowledge or grounds to suspect a criminal activity or where they have suspicion of money laundering or terrorist financing whether or not they are engaged in AML / CFT monitoring activities.
- Understanding IMS's Policy and Procedures on AML/CDD/CFT and to sign-off on the require Form.

- Employees who violate any of the Regulations or the IMS's AML/CDD/CFT policies and procedures will be subject to disciplinary action.

12. INTERNAL AUDIT

Internal Auditor of the IMS shall also review the compliance of the Anti-Money Laundering function of the Company to ensure that the AML Policy is being effectively implemented by the management of the IMS.

ANNEXURE – A

ML/TF Warning Signs/ Red Flags

1. Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
2. Customers who wish to deal on a large scale but are completely unknown to the broker;
3. Customers who wish to invest or settle using cash;
4. Customers who use a cheque that has been drawn on an account other than their own;
5. Customers who change the settlement details at the last moment;
6. Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
7. Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
8. Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
9. Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
10. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
11. Customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
12. Customer trades frequently, selling at a loss
13. Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
14. Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
15. Any transaction involving an undisclosed party;

16. Transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
17. Significant variation in the pattern of investment without reasonable or acceptable explanation
18. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
19. Transactions involve penny/microcap stocks.
20. Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
21. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
22. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
23. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
24. Customer conducts mirror trades.
25. Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

ANNEXURE – B

LIST OF REQUIRED DOCUMENTS FROM DIFFERENT TYPES OF CUSTOMERS

S No.	Type of Customer	Minimum Documents required for CDD
1.	Individuals	<p>A photocopy of any one of the following valid identity documents:</p> <ul style="list-style-type: none"> (i) Computerized National Identity Card (CNIC)/Smart National Identity Card (SNIC) issued by NADRA. (ii) National Identity Card for Overseas Pakistani (NICOP/SNICOP) issued by NADRA. (iii) Form-B/Juvenile card issued by NADRA to children under the age of 18 years. (iv) Pakistan Origin Card (POC) issued by NADRA. (v) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (vi) Valid Proof of Registration (POR) Card issued by NADRA (vii) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Joint Account	<ul style="list-style-type: none"> (i) A photocopy of any one of the documents mentioned at Serial No. I; (ii) In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them is individual customers of the RP.
3.	Sole proprietorship	<ul style="list-style-type: none"> (i) Photocopy of identity document as per Sr. No. 1 above of the proprietor. (ii) Attested copy of registration certificate for registered concerns. (iii) Sales tax registration or NTN, wherever applicable (iv) Account opening requisition on business letter head. (v) Registered/ Business address.
4.	Partnership	<ul style="list-style-type: none"> (i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Attested copy of 'Partnership Deed' (iii) Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form (iv) Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. (v) Registered/ Business address.

5.	Limited Liability Partnership (LLP)	<ul style="list-style-type: none"> (i) Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. (ii) Certified Copies of: <ul style="list-style-type: none"> (a) 'Limited Liability Partnership Deed/ Agreement. (b) LLP-Form-III having detail of partners/ designated partner in case of newly incorporated LLP. (c) LLP-Form-V regarding change in partners/ designated partner in case of already incorporated LLP. (iii) Authority letter signed by all partners, authorizing the person(s) to operate LLP account.
6.	Limited Companies/ Corporations	<ul style="list-style-type: none"> (i) Certified copies of: <ul style="list-style-type: none"> (a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; (b) Memorandum and Articles of Association; (ii) Certified copy of Latest 'Form-A/Form-B'. (iii) Incorporate Form II in case of newly incorporated company and Form A / Form C whichever is applicable; and Form 29 in already incorporated companies (iv) Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account; (v) Photocopies of identity documents as per Sr. No. 1 above of the beneficial owners.
7.	Branch Office or Liaison Office of Foreign Companies	<ul style="list-style-type: none"> (i) A copy of permission letter from relevant authority i-e Board of Investment. (ii) Photocopies of valid passports of all the signatories of account. (iii) List of directors on company letter head or prescribed format under relevant laws/regulations. (iv) Certified copies of <ul style="list-style-type: none"> a. Form II about particulars of directors, Principal Officer etc.in case of newly registered branch or liaison office of a foreign company b. Form III about change in directors, principal officers etc. in already registered foreign companies branch or liaison office of a foreign company (v) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account. (i) Branch/Liaison office address.

8.	Trust, Clubs, Societies and Associations etc.	<p>(i) Certified copies of:</p> <p>(a) Certificate of Registration/Instrument of Trust</p> <p>(b) By-laws/Rules & Regulations</p> <p>(ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</p> <p>(iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</p> <p>(iv) Registered address/ Business address where applicable.</p>
9.	NGOs/NPOs/Charities	<p>(i) Certified copies of:</p> <p>(a) Registration documents/certificate</p> <p>(b) By-laws/Rules & Regulations</p> <p>(ii) Resolution of the Governing Body/Board of Trustees/Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate the account.</p> <p>(iii) Photocopy of identity document as per Sr. No. 1 above of the authorized person(s) and of the members of Governing Body/Board of Trustees /Executive Committee, if it is ultimate governing body.</p> <p>(v) Any other documents as deemed necessary including its annual accounts/ financial statements or disclosures in any form which may help to ascertain the detail of its activities, sources and usage of funds in order to assess the risk profile of the prospective customer.</p> <p>(vi) Registered address/ Business address.</p>
10.	Agents	<p>(i) Certified copy of 'Power of Attorney' or 'Agency Agreement'.</p> <p>(ii) Photocopy of identity document as per Sr. No. 1 above of the agent and principal.</p> <p>(iii) The relevant documents/papers from Sr. No. 2 to 7, if agent or the principal is not a natural person.</p> <p>(iv) Registered/ Business address.</p>
11.	Executors and Administrators	<p>(i) Photocopy of identity document as per Sr. No. 1 above of the Executor/Administrator.</p> <p>(ii) A certified copy of Letter of Administration or Probate.</p> <p>(iii) Registered address/ Business address.</p>

12.	Minor Accounts	<p>(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate).</p> <p>(ii) Photocopy of identity document as per Sr. No. 1 above of the guardian of the minor.</p>
-----	----------------	--

Note:

- (i) For due diligence purposes, at the minimum following information shall also be obtained and recorded on KYC (Know Your Customer)/CDD form or account opening form:
 - (a) Full name as per identity document;
 - (b) Father/Spouse Name as per identity document;
 - (c) Mother Maiden Name;
 - (d) Identity document number along with date of issuance and expiry;
 - (e) Existing residential address (if different from CNIC);
 - (f) Contact telephone number(s) and e-mail (as applicable);
 - (g) Nationality-Resident/Non-Resident Status
 - (h) FATCA/CRS Declaration wherever required;
 - (i) Date of birth, place of birth;
 - (j) Incorporation or registration number (as applicable);
 - (k) Date of incorporation or registration of Legal Person/ Arrangement;
 - (l) Registered or business address (as necessary);
 - (m) Nature of business, geographies involved and expected type of counter-parties (as applicable);
 - (n) Type of account/financial transaction/financial service;
 - (o) Profession / Source of Earnings/ Income: Salary, Business, investment income;
 - (p) Purpose and intended nature of business relationship;
 - (q) Expected monthly turnover (amount and No. of transactions); and
 - (r) Normal or expected modes of transactions/ Delivery Channels.
- ii) The photocopies of identity documents shall be validated through NADRA verisys or Biometric Verification. The regulated person shall retain copy of NADRA Verisys or Biometric Verification (hard or digitally) as a proof of obtaining identity from customer.
- iii) In case of a salaried person, in addition to CNIC, a copy of his salary slip or service card or certificate or letter on letter head of the employer will be obtained.
- iv) In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account.
- v) For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.

- vi) The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.
- vii) The condition of obtaining photocopies of identity documents of directors of Limited Companies/Corporations is relaxed in case of Government/Semi Government entities, where regulated person should obtain photocopies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, regulated person shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.
- viii) Government entities accounts shall not be opened in the personal names of a government official. Any account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government.

Explanation:-

For the purposes of this regulation the expression "Government entities" includes a legal person owned or controlled by a Provincial or Federal Government under Federal, Provincial or local law.

Explanation:-

For the purpose of this Annexure I the expression "NADRA" means National Database and Registration Authority established under NADRA Act, (VIII of 2000).