KYC POLICY

Introduction

This policy is formulated to assist the management of Ismail Iqbal Securities to manage / counter the Compliance, Risk & provide a safe path for its growth & glory in the local market.

The Compliance Risk can be described as the risk of imposition of legal or regulatory sanctions, financial loss or loss to reputation of the entity arising out of its failure to comply with applicable laws of land /regulations governing financial institution, prudential regulations and circulars issued by the regulator i.e. Securities & Exchange Commission of Pakistan & Pakistan Stock Exchange Limited. Compliance with laws, rules and regulation helps IIS to maintain its reputation and meet the expectations of its stakeholders, customers, the markets and society as a whole.

In order to protect the IIS from Compliance Risk and to clearly disassociate from the increasing danger of organized activity and money laundering, IIS has developed a clearly laid down Policy for "KNOW YOUR CUSTOMER" (KYC) & Anti Money Laundering (AML). The main emphasize of the policy is to provide onsite guidelines against the opening of fictitious accounts and to protect the IIS from non compliance threats.

The policies, procedures and controls outlined in this KYC & AML Policy are minimum mandatory compliance requirements and have been designed to be a current document, subject to on-going revisions and updates.

OBJECTIVE

The purpose of this policy is to safeguard IIS against involvement in money laundering activities, terrorist financing and other illegal trades and to guide the employees in the effective and efficient discharge of their duties to ensure compliance with the rules and regulations.

RESPONSIBLITY

The Board of Directors is over-all responsible for development, adoption implementation, and regular monitoring of this policy statement. It is the responsibility of the employees pertinently of Marketing and Sales department to ensure that they are fully aware of the contents of this policy.

POLICY STATEMENT

IIS shall acquire due diligence information pertaining to the customers/clients and the legitimacy of their business/transactions so as to prevent from the potential risks. Due diligence shall be done to identify Company's Customers and ascertain their relevant information, as detailed as possible.

The Company shall verify that the customers are not on any Sanction List of known fraudsters, terrorists or money launderers from all over the world. Besides sanctions lists, there may be other lists of third party vendors that track links between individuals regarded as high-risk owing to negative reports in the media or in public record. The KYC policy does not merely require name matching with the sanction lists but also monitoring of transactions of the customers against their recorded profile and history in the account(s) and with peers.

Customers shall be identified using due diligence in order to prevent the identity theft/concealment, fraudulent transactions, money laundering, terrorist financing and other suspicious/illegitimate transactions/activities and do the legitimate and ethical business/financial transactions with the all the customers / clients whether newly introduced or otherwise.

PROCEDURES

Customer services and knows your customers

KYC Standards and anti-money laundering Measures would enable IISto understand its customers, the beneficial owners in case of non-individual entities, the principals behind customers who are acting as agents and their financial dealings. This will help to manage its risks prudently.

The main components of the internal control process are:

- Reputation and integrity of operations will be protected by reducing the likelihood of becoming a vehicle/means for or a victim of financial crime and suffering consequential reputation damage. For this purpose, all measures will be taken to perform an effective due diligence of the customer.

- Appropriate risk management and compliance methodologies shall be followed by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management.

- The employees shall take reasonable steps to be aware of any unusual transaction activity or activity that is disproportionate to the customer's known business.

- As a general rule, IIS shall not establish a business relationship until the identity of the potential customer is satisfactorily established. If a potential customer refuses to produce any of the requested information, the relationship shall not be established. Likewise, if the potential customer is not forthcoming with requested follow-up information, any relationship already begin shall be terminated.

KYC is based on five key elements

Following are the five crucial elements of the KYC process:

- Risk classification
- Minimum Information / Documents Required
- Verification of Documents
- On-going Monitoring Processes
- Reporting

Other Anti Money Laundering (AML) Measures are:

- Customer education and awareness
- Channel partner education and awareness
- Staff education and awareness

The procedures to address the five key elements of KYC process are explained in provided in the succeeding paragraphs.

RISK CLASSIFICATION

The level of Money Laundering (ML) risks that the Company is exposed to by an investor relationship depends on:

- Type of the customer and nature of business.
- Type of product / service availed by the customer
- Country where the Customer is domiciled.

Based on the above criteria, the customers may be classified into two Money laundering Risk levels viz., High Risk and Low Risk.

a). High Risk Customers

IIS will conduct enhanced due diligence when;

i. Dealing with high risk customers, business relationship or transaction including the following;

- Non-resident customers;
- Non-Legal persons or arrangement including non-governmental organizations (NGOs) / not for profit organizations (NFPs) and trusts / charities;
- Customers belonging to countries where CDD / KYC and anti-money laundering regulations are lax;
- Customers with links to offshore tax heavens;
- High Net-worth customers with no clearly identifiable source of income; and
- Customers dealing in high value items.

ii. There is a reason to believe that the customer has been refused by another financial institution.

iii. Dealing with politically exposed persons (including foreigners) or customers holding public or high profile positions. For politically exposed persons or holders of public or high profile positions, enhanced due diligence should include the following:

- Relationship should be established and / or maintained with approval of senior management including when an existing customer becomes holder of any public office or high profile position.

- Appropriate risk management evaluation will be made to determine whether a potential customer, existing customer or the beneficial owner, is a politically exposed person, holder of public office or the holder of high profile position. The sources of wealth / funds of such customers shall be monitored on regular basis.

iv. Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying Financial Action Task Force (FATF) recommendations.

b). Low Risk Customers

Where there are low risk and information on the identity of the customer and the beneficial ownership of a customer is publicly available, or where adequate checks and controls exist, IIS may apply simplified or reduced customer due diligence. This will be done in following cases:

Financial institutions provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements.

Public listed companies that are subject to regulatory disclosure requirements, Government administration / entities etc.

MINIMUM INFORMATION/DOCUMENTS

The Company shall obtain the following minimum information / set of documents from various types of customers / account holder(s) for examination and verification, at the time of opening account.

Type of Customers	Information/Documents
Individual / Sole Proprietorship	Name Father's Name Address Telephone Number Copy of CNIC or Passport Sources of Income Business Employment Proof
Partnership Account	Name of partnership and partners Father's Name of Partners Address Telephone Number Copies of CNIC of all partners Copies of latest Financials of Partners
Joint Stock Companies	Name of Company and its Directors Registered Address Telephone Number Copies of CNICs of all Directors Audited Accounts of the Company Memorandum and Articles of Association Board Resolution

Club Societies & Associations	Certified Copy of Certification of Registration Certified Copy of Bye Laws / Rules & Regulations Board / Governing body resolution Copy of Latest Financials of the Society / Association
Trusts	Copy of CNIC of all trustees Certified Copy of Trust Deed Trustee / Governing body resolution Copy of latest Financials of the trust
Executors & Administrators	Copy of CNIC of the Executors / Administrators Certified Copy of Letter of Administration

For all customers, IIS shall determine whether the customer is acting on behalf of another person, and shall then take reasonable steps to obtain sufficient identification data such as copy of CNIC, or other relevant document/information to verify the identity of the beneficiary.

For customers that are legal persons or for legal arrangements, IIS shall take reasonable measures to:

- Understand the ownership & control structure of the customer;
- Determine that the natural persons who ultimately own or control the customer. This includes those persons who exercise ultimate effective control over a legal person or arrangement.

Government accounts shall not be opened in the personal names of the government official(s). Any such account, which 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 Department of the concerned Government.

VERIFICATION OF DOCUMENTS

Verification is an integral part of KYC and due diligence measures for which IIS shall ensure that;

- Copies of CNIC wherever required are invariably verified. Before opening the account, the Company shall verify CNIC by utilizing online facility of NADRA. In case the Company does not have the online facility, then CNIC shall be verified from the Regional Office of NADRA.

In case the Company is not able to satisfactory complete required KYC and due diligence measures, account shall not be opened, business relationship shall not be established and business transaction shall not be carried out. Instead, reporting of suspicious transition is considered. Similarly, relationship with existing customer should be terminated and reporting of suspicious transaction be considered if the KYC and due diligence results are found unsatisfactory.

MONITORING

Customer due diligence (CDD) / Know your Customer (KYC) is not a one time exercise to be conducted at the time of formal relationship with customer / accountholder. This is an ongoing process and to this end IIS is required to;

- Monitor the accounts and transactions on regular basis.
- Update customer information and records, if any.
- Chalk out plan of imparting suitable training to the staff.
- Maintaining proper records of customer identification and to clearly indicate, in writing, if any exception is made in fulfilling the KYC due diligence measures.

The guidelines on policies and procedures are to be monitored by the management on an ongoing basis. Non-adherence to the guidelines and any doubt on customer transaction must be reported to the management without loss of time. To strengthen the monitoring and prevent the money laundering activities, an appropriate training to the employees shall be provided regularly and the policies and procedures shall be amended on a need basis. Any amendment, partly or wholly, shall remain the integral of this KYC.

REPORTING

In normal circumstances, it is not easy to identify money laundering related transactions. A common golden rule is **Know Your Customer**. Management must know its customer including the ultimate beneficial owner (if different from the apparent legal owner), its economic background and/or its normal activities. It is through the knowledge about our customer or other give-away signs that may lead to a gut-feeling that a money laundering activity may be taking place. Mere verifying and collecting the identity and documents of the customer does not amount to "Know Your Customer". The staff should use their diligence and prudence to judge the customer and his capabilities and should be alert if there are any unusual transactions, which are not typical and compatible to the customer's background. The staff should try to match the profile of customer with that of the transactions of the customer.

The staff should verify in detail the source of funds and the purpose of transactions to satisfy the genuineness of the transaction. Compliance is the responsibility of the every employee. Therefore, strict compliance is very much necessary with all laws and regulations.

All issues noticed for a new customer shall be reported at appropriate level in Marketing and Sales department, Head of Compliance and Chief Financial Officer by the employee who noticed or surfaced any reportable matter. Appropriate decisions will be taken for such customer after further investigation. In case of existing Customer such matters will be brought into the notice of Chief Executive Officer for decision making.

RECORD KEEPING & COMPLIANCE

IIS shall keep record regarding the identification data obtained through the customer's due diligence process (e.g. copies or record of official identification documents like passports, identity cards, driving licenses, or similar documents), account files, and business correspondence for at least five years after the business relationship is ended.

Management shall be responsible to issue and enforce in-house instructions to comply with the guidelines, including reporting of suspicious transactions and any other matters relating to the prevention of money laundering. In order to be effective in the prevention of money laundering and to disseminate new regulations/policies, trainings and regular refresher courses should be given to all employees. Although management may not be involved in the day-to-day procedures, it is important that they know and understand their statutory duties. Therefore, they should have at least some of general awareness training sessions.

CONFIDENTIALITY

This Policy is strictly confidential. No copies of this Policy may be printed, copied or in any way removed from the offices of the Company.

FUTURE AMENDMENTS

The management will review and may amend or otherwise modify this Policy Statement from time to time with the approval of Board of Directors. Such review will preferably be carried out every year and will take into account among others the revisions in applicable regulatory framework specifically.

APPROVAL FROM BOARD OF DIRECTORS

This policy has been approved by the Board of Directors on January 01, 2015 and access has been provided to the employees of IIS.

EFFECTIVE DATE

This policy shall become effective from the January 01, 2015.

TRADING POLICY

Whenever an order of any client has been executed by a Broker, confirmation of such execution shall be transmitted to the said client by the Broker. Including:

(a) Date on which order is executed;

(b) Name and number of securities;

(c) Nature of transaction (SPOT, Ready, Future, Leveraged Market, Debt Market and also whether bought or sold);

(d) Price;

(e) Commission rate and any other charges ;

(f) Applicable regulatory levies i.e. trade or transaction fee of the Exchange, CDC, NCCPL and SECP etc;
(g) Applicable statutory levies i.e. taxes and duties of federal and provincial government;

(h) Whether the order is executed for the Broker's own account or from the market.

{Rule 4(4) of Securities & Exchange Rules, 1971)}.

ANNEXURE-A

[TREC Holder Name]

[TREC Holder Address]

KNOW YOUR CUSTOMER (KYC)/APPLICATION FORM FOR
SAHULAT ACCOUNT/SIMPLIFIED KYC

Individual

(Please use BLOCK LETTERS to fill the form)

Note: This form is only for opening Sahulat Accounts for INDIVIDUALS who wish to undergo simplified KYC. Such accountholders may keep custody of securities worth Rs. 500,000 or less and shall not in a given day buy or sell securities worth more than Rs. 500,000, i.e. gross trading in a day cannot exceed Rs. 1 million while net trading may be Rs. 500,000 or less.

A. IDENTITY DETAILS OF APPLICANT

1. Full name of Applicant (As per CNIC/SNIC/NICOP/ARC/POC) Mr. / Mrs. / Ms.															
2. Father's / Husband's Name:															
3. a. Nationality:	b. Marital status: ☐ Single ☐ Married						c. Status: ☐ Resident ☐ Non-Resident								
4. a. CNIC/ SNIC/NICOP/ARC/POC No:															
b. Expiry date:															
5. Date of Birth:															

B. ADDRESS DETAILS OF APPLICANT

1.(a)Mailing Address:
(Address should be different from TREC holder business address except for employees of TREC holder)

		City/Town/Village:	Province/State:	Country:
(b) Tel. (Off.)*:	(c) Tel. (Res.)*:	(d) Mobile:	(e) Email*:	(f) Fax*:

2. (a)Permanent Address:
(if different from above or overseas address, mandatory for Non-Resident Applicant)

(b) Tel. (Off.)*:	(c) Tel. (Res.)*:	(d) Mobile (Applicant or Attorney):	(e) Fax*:	(f) Email (If any):

C. OTHER DETAILS

1. Gross Annual Income Details (please specify): ☐ Below Rs. 100,000 ☐ Rs. 100,001 - Rs. 250,000 ☐ Rs. 250,001 - Rs. 500,000 ☐ Rs. 500,001 - Rs. 1,000,000 ☐ Rs. 1,000,001 - Rs. 2,500,000 ☐ Above Rs 2,500,001

2. Source of Income:

3. Shareholder's Category: INDIVIDUAL

4. (a) Occupation: *[Please tick (✓) the appropriate box]*							
	Agriculturist	Business	Housewife	Household
	Retired Person	Student	Business Executive	Industrialist
	Professional	Service	Govt. /Public Sector	Others (Specify)

(b) Name of Employer / Business: (c) Job Title / Designation:

(d) Address of Employer / Business:

D. BANK DETAILS

Bank Name:	Account No.:
Branch Name:	Branch Address:

E. CUSTODY, CLEARING AND SETTLEMENT AGENT

Primary Service Provider ☐ National Custodial Service (NCCPL) ☐ Direct Settlement Service (CDC) ☐ Professional Clearing Member: *please specify*

Investors not wishing to use one of the Primary Service Providers must strike out the preceding field, sign here and choose one of the Other Service Providers.

Other Service Provider ☐ Securities broker (Trading & Self-Clearing) ☐ Securities Broker (Other Trading and Clearing): *please specify*

F. DECLARATION

I hereby confirm that all the information furnished above is true and correct to the best of my knowledge and belief and I undertake to inform you of any changes therein, immediately. In case any of the above information is found to be untrue or false or misleading or misrepresenting, I am aware that I may be held liable for it.

Signature of the Applicant **Date:** _____ (dd/mm/yyyy) **Signature of the Applicant as per CNIC/SNIC/NICOP/ARC/POC** *(Only applicable if Applicant signature is different)*

FOR OFFICE USE ONLY

Authorized Signatory **Date** **Seal/Stamp of the Authorized Intermediary**

* Optional

Enclosures

i. Copies of CNIC, SNIC, NICOP, ARC or POC.
ii. Power of attorney, where applicable, along with contact details of the attorney.