Asad Mustafa Securities Private Limited.

KNOW YOUR CUSTOMER / CUSTOMER DUE DILIGENCE, ANTI-MONEY LAUNDERING, COUNTER FINANCING OF TERRORISM AND PROLIFERATION FINANCING

POLICY AND PROCEDURES

Version 16 October 2023

Updated Time to Time

Background

Money Laundering ("ML") and Terrorist Financing ("TF") are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF. An effective Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") regime requires financial institutions to adopt and effectively implement appropriate ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF.

SECP has issued detailed AML/CFT Guidelines in 2021 ("the Guidelines") based on updated National Risk Assessment ("NRA"), which complements the SECP AML/CFT Regulations. These Guidelines are applicable to all Regulated Persons ("RPs") as defined under the Regulations conducting relevant financial business and designed to assist RPs in complying with the Regulations. These Guidelines clarify and explain the general requirements of the legislation to help RPs in applying national AML/CFT measures, developing an effective AML/CFT risk assessment and compliance framework suitable to their business, and in particular, in detecting and reporting suspicious activities.

These Guidelines are based on Pakistan AML/CFT legislation and reflect, so far as applicable, the 40 Recommendations and guidance papers issued by the Financial Action Task Force ("FATF").

1. Introduction, Purpose and Scope

These policy and procedures are in line with requirements of Anti Money Laundering and Countering Financing of Terrorism Regulations, 2020 and the related Guidelines issued by the SECP.

This Policy and related procedures establishes the standards to which Asad Mustafa Securities (Pvt.) Limited ("the Company") should adhere to. This document will be used to create an understanding amongst employees concerning the risks of money laundering and terrorist financing. Accordingly, the Company is required to adopt risk-based approach to prevent the Company as a conduit for Money Laundering or Terrorist Financing activities.

2. Objective

(i) Understand the obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes.

(ii) Develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations.

(iii) Company's Board of Directors and senior management are engaged in the decision making on AML/CFT policies, procedures and control and takes ownership of the risk-based approach.

(iv) Awareness of the level of ML/TF risk the Company is exposed to and take a view on whether the Company is equipped to mitigate that risk effectively.

(v) Establish and maintain an effective AML/CFT compliance culture and adequately training its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations.

(vi) Establish written internal procedures so that, in the event of a suspicious activity being discovered, employees are aware of the reporting chain and the procedures to be followed.

(vii) Appoint a Compliance Officer ("CO") at the management level, who shall report directly to the Board of Directors ("Board") and shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit ("FMU").

(viii) Ensure that any suspicious transaction report must be made by employees to the CO.

(ix) Responsibility for ensuring that employees are aware of their reporting obligations and the procedure to follow when making a suspicious transaction report ("STR").

3. Definitions

Know your customer ("KYC") is the process of identifying and verifying the identity of its customers and ascertain relevant information required for doing business with them. KYC involves:

- Seeking evidence of identity and address from the customer and independently confirming that evidence at the start of a relationship with the Company and periodically updating the information as per customer risk classification; and
- Seeking information regarding the sources of income and nature of business etc. of the customer.

Customer Due Diligence ("CDD") information comprises the facts about a customer that should enable an organization to assess the extent to which the customer exposes it to a range of risks. These risks include money laundering, terrorist financing and having business relationship with a sanctioned individual/entity or designated terrorist under Pakistan's Anti-Terrorism law.

"Close Associate" of a PEP means— (i) an individual known to have joint beneficial ownership of a legal person or a legal arrangement or any other close business relations with a PEP; (ii) any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have been set up for the benefit of a PEP; (iii) an individual who is reasonably known to be closely connected with the PEP for any other reason, including socially or professionally.

"High Net Worth Individuals" (HNWIs) are defined as real persons or corporate entities with substantial financial resources. HNWIs, for the purposes of this definition, shall be categorized into two distinct groups based on their net worth. HNWIs shall be subject to Enhanced Due Diligence:

Individual High Net Worth Individuals (I-HNWIs):
I-HNWIs are natural persons who have a net worth exceeding PKR 75 million. Net worth, for the purpose of this definition, is calculated by considering the aggregate value of their tangible and intangible assets, including but not limited to real estate, investments, financial instruments, cash holdings, and any other assets of significant value.

Corporate High Net Worth Individuals (C-HNWIs):
C-HNWIs are corporate entities, including but not limited to companies, partnerships, and other legal entities, which have a net worth exceeding PKR 150 million. Net worth, for the purpose of this definition, is calculated by aggregating the total value of their assets, equity, and any other financial holdings, excluding liabilities.

"Politically Exposed Persons" or "PEPs" means an individual who is or has been entrusted with a prominent public function either domestically or by a foreign country, or in an international organization and includes but not limited to: (i) for foreign PEPs, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and political party officials; (ii) for domestic PEPs, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, political party officials; (iii) for international organization PEPs, members of senior management or individuals who have been entrusted with equivalent functions. Provided that middle ranking or more junior individuals in the above referred categories are not included in the definition of PEPs.

Money Laundering ("ML") is the involvement of any transaction or series of transactions seeking to conceal or disguise the nature or source of proceeds derived from illegal activities, including narcotics trade, human trafficking, terrorism, ransom, extortion money, organized crime, fraud, and other crimes.

Financing Terrorism ("TF") refers to activities that provide financing or financial support to individual terrorists or non-state actors.

"Professional Clearing Member" means E-Clear Limited, a Company licensed to provide professional clearing services.

Customer means any natural person, legal person or legal arrangement to whom financial services have been extended by a regulated person.

Beneficial Owner in relation to a customer of the Company means, the natural person who ultimately owns or control a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercise ultimate effective control over a person or a legal arrangement.

Legal Persons means entities other than natural persons whether incorporated or not or a legal arrangement that can establish a permanent customer relationship with a regulated person or otherwise own property and include companies, bodies corporate, foundations, Limited Liability partnership (LLP), partnerships, or associations and other relevantly similar entities.

FMU means Financial Monitoring Unit established under section 6 of the AML Act, 2010.

Regulated person means securities brokers, commodities brokers, Insurers, Takaful Operators, NBFCs and Modarabas.

4. Customer Identification

No account shall be opened in the name of person who fails to disclose his/her true identity or fails to provide valid identity document. To authenticate identity of new customer, legible and attested copy of CNIC / NICOP / Passport (in case of foreigner) shall be obtained before account opening. The photocopies of identity documents shall be validated through NADRA Verisys, identifying presence of any adverse remarks in the comments.

Source of income shall be essentially disclosed by the customer. In case source of customer's income is business /employment, name of the business / employer shall also be disclosed. In case of a salaried person an attested copy of his service card or salary slip or certificate or letter on letter head of the employer will be obtained.

All prospective customers must be seen face to face by the Company's Representative (CR).

For any new account opening form, the Professional Clearing Member engaged by the Company shall match the particulars of the customer from the UNSC Sanctions list from UNSC website under consolidated sanction list (https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list) and Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997 issued by Ministry of Interior obtained daily from National Counter Terrorism Authority's website (http://nacta.gov.pk/proscribed-organizations/) and if any matching name is found the account is being declined and reported to FMU simultaneously in the form of STR.

If a customer is acting on behalf of another person than the identity of that person will be ascertained and relevant documents of that person will also be obtained. These include CNIC/NICOP/Passport copy of person so acting on behalf of the original customer along with the signed authority letter of the customer and reason for appointment of such representative. CNIC of the representative is also verified through NADRA Verisys portal and screened against UNSC and terrorists databases as mentioned above. If, the CR founds that the person looks shaky and hesitant to provide the complete information, he/she will report to CO for further action. The CO will check the information and will report to FMU in case he finds something suspicious.

For non-individual customers (e.g. companies, association of persons, pension funds, government owned entities, non-profit organizations, foreign companies/ organizations) additional care must be taken to understand the customer's business, 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 should be ensured that the person who represents himself as authorized signatory with powers to open and operate the brokerage account should have the Authority Letter from company.

Accounts of Institutions / organizations / corporate bodies shall not be opened in the name of employee(s)/official(s).

5. Program and Systems to prevent ML and TF

(i) The Company will establish and maintain programs and systems to prevent, detect and report ML/TF. The systems will be appropriate to the size of the Company and the ML/TF risks to which it is exposed and will include:

a) Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;

b) Policies and procedures to undertake a Risk Based Approach ("RBA");

c) Internal policies, procedures and controls to combat ML/TF, including appropriate risk management arrangements;

d) Customer due diligence measures;

e) Record keeping procedures;

f) AML/CFT programs;

g) An audit function to test the AML/CFT system;

h) Screening procedures to ensure high standards when hiring employees; and

i) An appropriate employee-training program.

ii. It will be the responsibility of the senior management to ensure that appropriate systems are in place to prevent, detect and report ML/TF and the Company is in compliance with the applicable legislative and regulatory obligations.

6. The Three Lines of Defense

The Company will promote self-assessment culture at every level, making each function primarily accountable for its domain of responsibilities rather than dwelling on Compliance, Risk Management and Internal Audit to identify non-compliances, including ML/TF related non-compliance, in their reviews. To promote this Company will enforce three lines of defense concept;

- First Line: Although each unit will act as first line of defense for its own activities, the business units (e.g. front office, customer-facing staff/traders). Staff / the Professional Clearing Member will ensure that the Cheques are received and paid to the customer only within defined threshold.
- Second Line: This includes Compliance Department and the Professional Clearing Member is supposed to provide support for AML/CFT related compliances in the capacity of Company's second line of defense. Company will perform adequate screening of each employee and ensure their timely trainings as per training schedule, Compliance will review fulfillment of all KYC related requirements at the time of on-boarding of employees, review account closing and fund transfer processes at specified intervals, review of ongoing monitoring activities, provide support for continuous staff trainings, raising STRs and coordinating with all departments and regulatory bodies.
- Third Line: The Internal Audit function along with Board Audit Committee will act as the Company's final line of defense, which will ensure that first two lines of defense are performing their duties, including AML/CFT related compliances, as per Company's established policies and procedures, and these policies and procedures are aligned with country's regulatory framework.

i. In order to enable all employees in discharging their duties as first line of defense, policies and procedures will be clearly specified in writing and communicated to all employees. These will contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activities of the Company in compliance with the Regulations. These include internal procedures for detecting, monitoring and reporting suspicious transactions.

ii. As part of second line of defense, the CO must have the authority and ability to oversee the effectiveness of the Company's AML/CFT systems, compliance with applicable AML/CFT legislation and provide guidance in day-to-day operations of the AML/CFT policies and procedures.

iii. CO must be a person who is fit and proper to assume the role and who:

(1) has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
(2) reports directly and periodically to the Board on AML/CFT systems and controls;
(3) has access to all information necessary to perform the AML/CFT compliance function;
(4) ensures regular audits of the AML/CFT program;
(5) maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
(6) responds promptly to requests for information by the SECP/LEAs.
(7) maintains confidentiality of affairs unless under duty to disclose to competent authority by operation of any law.

iv. An independent Internal Audit function, the third line of defense, should periodically conduct AML/CFT audits and be proactive in following up their findings and recommendations. As a general rule, the processes used in auditing should be consistent with internal audit's broader audit mandate as approved by the Board, subject to any prescribed auditing requirements applicable to AML/CFT measures.

7. Risk Assessment and Applying a Risk Based Approach ("RBA")

i. The RBA enables the Company to ensure that AML/CFT measures are commensurate to the risks identified and allow resources to be allocated in the most efficient ways. RBA is applied keeping into consideration the Company's size, geographical coverage, structure and business activities and applied the RBA e.g. when notice receives from NACTA, a system-based sanction screening. As a part of the RBA, The Company:

1) Identify ML/TF risks relevant to it.

2) Assess ML/TF risks in relation to-
   a. Its customers (including beneficial owners, HNWI's etc);
   b. Country or geographic area in which its customers reside or operate and where the Company operates;
   c. Products, services and transactions that the Company offers; and
   d. Their delivery channels.

3) Design and implement policies, controls and procedures that are approved by its Board to manage and mitigate the ML/TF risks identified and assessed;

4) Monitor and evaluate the implementation of mitigating controls and improve systems where necessary;

5) Keep its risk assessments current through ongoing reviews and, when necessary, updates;

6) Implement and monitor procedures and updates to the RBA; and

7) Have appropriate mechanisms to provide risk assessment information to the Commission.

iii. Under the RBA, where there are higher risks, the Company takes enhanced measures to manage and mitigate those risks; and correspondingly, where the risks are lower, simplified measures are permitted. However, simplified measures are not permitted whenever there is a suspicion of ML/TF. In the case of some very high-risk

situations or situations which are outside the Company's risk tolerance, the Company may decide not to take or accept the customer, or to exit from the relationship. CO in such cases will consider need to raise an STR to FMU.

iv. In view of the fact that the nature of the TF differs from that of ML, the risk assessment must also include an analysis of the vulnerabilities of TF. Many of the CFT measures the Company has in place will overlap with its AML measures. These may cover, for example, risk assessment, CDD checks, transaction monitoring, escalation of suspicions and liaison relationships with the authorities.

v. The process of ML/TF risk assessment has four stages:

1) Identifying the area of the business operations susceptible to ML/TF
2) Conducting an analysis in order to assess the likelihood and impact of ML/TF;
3) Managing the risks; and
4) Regular monitoring and review of those risks.

a) Identification, Assessment and Understanding Risks

i. The first step in assessing ML/TF risk is to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the Company.

ii. In the second stage, the ML/TF risks that can be encountered by the Company need to be assessed, analyzed as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the Company from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories, their combination and the conclusion on the total risk level must be based on the relevant information available.

iii. For the analysis, the Company will identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but possible. In assessing the impact, the Company will, for instance, look at the financial damage by the crime itself or from regulatory sanctions or reputational damages that can be caused. The impact can vary from minor if that are only in short-term or there are low-cost consequences, to very major, when they are found to be very costly inducing long-term consequences that affect the proper functioning of the institution.

iv. Company will allow for the different situations that currently arise in its business or are likely to arise in the near future. For instance, risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF risks will often operate together and represent higher risks in combination. Potential ways to assess risk include but are not limited to:

1) How likely an event is;
2) Consequence of that event;
3) Vulnerability, threat and impact;
4) The effect of uncertainty on an event;

v. The assessment of risk will be informed, logical and clearly recorded. Further, the risk assessment should indicate how the Company arrived at this rating.

Risk Assessment (lower complexity)

Company will assess risk by only considering the likelihood of ML/TF activity. This assessment will involve considering each risk factor that have been identified, combined with business experience and information published by the Commission and international organizations such as the FATF. The likelihood rating will correspond to:

1) Unlikely - There is a small chance of ML/TF occurring in this area of the business;
2) Possible - There is a moderate chance of ML/TF occurring in this area of the business;
3) Almost Certain - There is a high chance of ML/TF occurring in this area of the business

Risk Assessment (moderate complexity)

Another way to determine the level of risk is to work out how likely the risk is going to happen and cross-reference that with the consequence of that risk.
Using likelihood ratings and consequence ratings can provide the Company with a more comprehensive understanding of the risk and a robust framework to help arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist the Company in applying the appropriate risk management measures as detailed in the program.

Cross-referencing possible with moderate risk results in a final inherent risk rating of moderate. The program should then address this moderate risk with appropriate control measures. Company will need to undertake this exercise with each of the identified risks.

Risk Assessment (higher complexity)

Company will further assess risk likelihood in terms of threat and vulnerability.

Determining the impact of ML/TF activity can be challenging but to focus AML/CFT resources in a more effective and targeted manner. When determining impact, Company can consider a number of factors, including:

1) Nature and size of your business (domestic and international);
2) Economic impact and financial repercussions;
3) Potential financial and reputational consequences;
4) Terrorism-related impacts;
5) Wider criminal activity and social harm;
6) Political impact;
7) Negative media.
8) Narcotics Trafficking
9) Corruption & Bribery
10) Smuggling (including in relation to customs and excise duties and taxes)
11) Tax Crimes
12) Illegal MVTS/Hawala/Hundi

13) Cash Smuggling
14) Terrorism including Terrorism Financing

Company will more weight to certain factors to provide a more nuanced understanding of your ML/TF risk.

In addition, Company may consider how its risks can compound across the various risk factors.

Applying the Risk Assessment

The risk assessment will assist in ranking and prioritizing risks and providing a framework to manage those risks. The risk assessment will enable the Company to prepare a comprehensive program. It will enable to meet relevant obligations under the regulations, including obligations to conduct CDD, monitor accounts and activities and report suspicious activity.

The assessment will help in determining suspicion and consequently assist in the decision to submit an STR to the FMU. The Company will submit an STR to the FMU if it thinks that activities or transactions are suspicious.

The Company will conduct ongoing CDD. The risk assessment will help target and prioritize the resources needed for ongoing CDD.

The Company will undertake account monitoring. The risk assessment will help to design the triggers, red flags and scenarios that can form part of account monitoring.

New and Developing Technologies and Products

New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. The risk assessment will consider whether the business is, or may be, exposed to customers involved in new and developing technologies and products. The program will detail the procedures, policies and controls that the Company will implement for this type of customer and technology.

Material Changes and Risk Assessment

The risk assessment will adapt when there is a material change in the nature and purpose of the business or relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.

Material change could include circumstances where the Company introduces new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when the Company starts using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, the Company will need to refresh its risk assessment.

vi. Compliance resources are accordingly allocated to the areas with higher Inherent Risk to bring the Residual Risk within tolerable band. This risk assessment is an ongoing process and is reviewed on an annual basis to factor in new and emerging risks due to business dynamics and changes in regulatory framework. This include changes in

risk levels as new products are offered, as new markets are entered, as high-risk customers open or close accounts, or as the products, services, policies, and procedures change. The Company also have appropriate mechanisms to provide risk assessment information to the Commission, if required. This is done through a specially designed document which is provided as Annexure 1 to these policy and procedures.

Examples of Risk Classification Factors
Below are some examples that can be helpful indicators of risk factors / indicators that may be considered while assessing the ML/TF risks for different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels. However, this list is not exhaustive and staff should use critical thinking in determining risk of ML/TF.

High-Risk Classification Factors

(1) Customer risk factors: Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

(a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the Company and the customer)
(b) Non-resident customers
(c) Politically Exposed Persons (PEPs) (d) Legal persons or arrangements
(e) Companies that have nominee shareholders
(f) Business that is cash-intensive.
(g) The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal person
(h) shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions
(i) trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets
(j) Requested/Applied quantum of business does not match with the profile/particulars of client
(k) Not-For-Profit organization ("NPOs") with association with political parties or religious groups
(l) Real estate dealers,
(m) Dealers in precious metal and stones, and
(n) Lawyers/notaries

Example Scenarios of Customer Types

Small and Medium Sized Enterprises:

Small and medium business enterprise customers usually entail domestic companies with simple ownership structures. Most of these businesses deal with cash and multiple persons that can act on its behalf. The likelihood that funds deposited are from an illegitimate source is HIGH, since it can't easily be identified and can have a major impact on a large number of SME customers. Thus, the risk assessment and risk rating result is HIGH.

International corporations:

International corporate customers have complex ownership structures with foreign beneficial ownership (often). Although there are only a few of those customers, it is often the case that most are located in offshore locations. The likelihood of Money Laundering is High because of the limited number of customers of this type and the beneficial ownership could be questionable, with two criteria that in this scenario result in a possible risk impact of moderate and a moderate risk assessment.

As an example, these descriptions can result in a table as depicted below:

Customer Type	Likelihood	Impact	Risk Analysis
Retail Customer/ Sole Proprietor	Moderate	Moderate	Moderate
High Net Worth Individuals	High	High	High
NGO/NPO	High	High	High
International Corporation	High	Moderate	Moderate
PEP	High	High	High
Company Listed on Stock Exchange	Low	Low	Low

Note: The above risk analysis is a general one for types or categories of customers. It is the starting point for the risk classification of an individual customer. Based on the circumstances of an individual customer, such as its background or information provided, the risk classification of an individual customer can be adjusted. Based on that individual risk classification, customer due diligence measures should be applied.

(2) Country or geographic risk factors: Country or geographical risk may arise because of the location of a customer, the origin of a destination of transactions of the customer, but also because of the business activities of the Company itself, its location and the location of its geographical units. Country or geographical risk, combined with other risk categories, provides useful information on potential exposure to ML/TF. The factors that may indicate a high risk are as follow:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems
(b) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations
(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity
(d) Countries or geographic areas identified by credible sources as providing funds or support for terrorist activities, or that have designated terrorist organizations operating within their country
(e) Entities and individuals from jurisdictions which are known tax heavens
(f) Countries which are hostile to national interest of Pakistan or with which diplomatic relations are suspended

(3) Product, service, transaction or delivery channel risk factors: Company, while doing its ML/TF risk assessment, takes into account the potential risks arising from the products, services, and transactions that the Company offers to its customers and the way these products and services are delivered. In identifying the risks of products, services, and transactions, the following factors are considered:

(a) Anonymous transactions (which may include cash)

(b) Non-face-to-face business relationships or transactions
(c) Payments received from unknown or un-associated third parties
(d) International transactions, or involve high volumes of currency (or currency equivalent) transactions
(e) One-off transactions
(f) Transaction for which payments are made from more than two bank accounts of a customer
(g) Products that involve large payment or receipt in cash; and
(h) One-off transactions.
(i) Is the customer physically present for identification purposes? If they are not, has the Company used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?

Low Risk Classification Factors

(1) Customer risk factors: The customer is a regulated person or bank and is subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements, or

Public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership;

(2) Product, service, transaction or delivery channel risk factors: Financial products or services that provide appropriately defined and limited services to certain types of customers.

(3) Country risk factors:
(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems.
(b) Countries identified by credible sources as having a low level of corruption or other criminal activity

In making a risk assessment, the Company could, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

Risk Matrix

In assessing the risk of money laundering and terrorism financing, the Company will establish whether all identified categories of risks pose a low, moderate, high or unacceptable risk to the business operations. The Company will review different factors, e.g., number and scope of transactions, geographical location, and nature of the business relationship. In doing so, it must also review the differences in the manner in which it establishes and maintains a business relationship with a customer (e.g., direct contact or non-face-to-face). It is due to the combination of these factors and the variety of their combinations, that the level of money laundering and terrorism financing differs from institution to institution. The geographical risk should be seen in correlation with other risk factors in order to come up with an assessment of the total money laundering and terrorism financing risk.

The Company will use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk category, those that carry somewhat higher, but still acceptable risk, and those that carry a high or unacceptable risk of money laundering and terrorism financing.

The development of a risk matrix can include the consideration of a wide range of risk categories, such as the products and services offered by the Company, the customers to whom the products and services are offered, the size and organizational structure, etc. A risk matrix is not static: it changes as the circumstances of the Company change. A risk analysis will assist the Company to recognize that ML/TF risks may vary across customers, products, and geographic areas and thereby focus its efforts on high-risk areas in its business.

The following is an example of a risk matrix of client product combination1.

Customer Transaction	Online Transactions	Domestic Transfers	Deposit or Investment	Securities Account
Domestic Retail Customer	Moderate	Moderate	Moderate	Low
High Net Worth Customers	High	Moderate	High	Moderate
SME Business Customer	High	Moderate	High	Moderate
International Corporation	High	Moderate	High	Moderate
Company Listed on Stock Exchange	Moderate	Low	Moderate	Low
PEP	High	Moderate	High	Moderate
Mutual Fund Transactions	High	Moderate	High	N/A

b) Risk Management

Risk Mitigation

i. Company will develop appropriate policies, procedures and controls that will enable it to manage and mitigate effectively the inherent risks that it has identified, including the national risks. Company will monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures will be approved by the senior management of the Company, and the measures will be taken to manage and mitigate the risks (whether higher or lower) to ensure that measures are consistent with legal and regulatory requirements.

ii. The nature and extent of AML/CFT controls the Company puts in place depends on a number of aspects, which include:

1) The nature, scale and complexity of the Company's business
2) Diversity, including geographical diversity of the Company's operations
3) Company's customer, product and activity profile
4) Volume and size of transactions
5) Extent of reliance or dealing through third parties or intermediaries, which is minimal in case of Company and restricted to Administration department related services

iii. Some of the risk mitigation measures that the Company may consider include:

[1] Note: When conducting risk assessment, the Company does not have to follow the processes in this document. As long as it complies with the obligations under the Act and any other applicable laws or regulations, the Company has a choice to select the method of risk.

1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers
2) setting transaction limits for higher-risk customers or products
3) requiring senior management approval for higher-risk transactions, including those involving PEPs
4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services
5) determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs)

Evaluating Residual Risk and Comparing with the Risk Tolerance
Subsequent to establishing the risk mitigation measures, the Company will evaluate its residual risk, which is the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks are kept in line with the Company's overall risk tolerance and this sets the cornerstone of accepting and continuing business relations.

8. Determination of Whether a Person acts on behalf of another Person

The Company will obtain following relevant documents for determination of whether a person acts on behalf of another person:

i. Authority Letter
ii. Power of Attorney in case of trading
iii. CNIC copy duly verified by the customer with original signatures on CNIC.
iv. Address of the authorized person.
v. Reason of Authorizing another person for trading or appearing on behalf of customer.

9. Steps to be taken in case Negative Verification

Step 1
The applicant to be informed about the reason(s) of negative verification/identification, and give an opportunity to rectify and provide necessary document portion to resolve negative verification:

Step 2

In case applicant is still unable to provide necessary documentation for positive verification the application to be rejected.

Step 3

The client to be informed about the rejection and maintain at office following record of the applicant:

i) Application
ii) Negative Verification Report
iii) Copy of the Letter informing applicant for rectification of negative verification
iv) Final Interview sheet of the applicant.

The above documents will be retained at office for five years.

10. Monitoring AML/CFT Systems and Controls.

The Company will have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. The Company will update their systems as appropriate to suit the change in risks.

Additionally, the Company will assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed. For that purpose, the Company will need to consider monitoring certain aspects which include:

1) the ability to identify changes in a customer profile or transaction activity/behavior, which come to light in the normal course of business;
2) the potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;
3) the adequacy of employee training and awareness;
4) the adequacy of internal coordination mechanisms i.e., between AML/CFT compliance and other functions/areas;
5) the compliance arrangements (such as internal audit);
6) changes in relevant laws or regulatory requirements; and
7) changes in the risk profile of countries to which the Company or its customers are exposed to.

11. Documentation and Reporting

i. Documentation of relevant policies, procedures, review results and responses will enable the Company to demonstrate to the Commission:

1) risk assessment systems including how the Company will assess ML/TF risks;
2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
3) how it will monitor and, as necessary, improves the effectiveness of its systems and procedures; and
4) the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

ii. The Company / the Professional Clearing Member will note that the ML/TF risk assessment is not a one-time exercise and therefore, they must ensure that their ML/TF risk management processes are kept under regular review which is at least annually. Further, the Company management should review the program's adequacy when the reporting entity adds new products or services, opens or closes accounts with high-risk customers, or expands through mergers or acquisitions.

iii. The Company / the Professional Clearing Member will demonstrate to the Commission, the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its procedures and policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT, during the SECP's on-site inspection. The Company will maintain Risk Assessment Tables (Annexure 1), AML/CFT Compliance Assessment

Template (Annexure 2) and Control Assessment Template (Annexure 3) within the period as required by the Commission from time to time.

12. New Products and Technologies

The Company will design a special template to identify and assess ML/TF risks that may arise in relation to the development of and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:
1) Electronic verification of documentation;
2) Data and transaction screening systems; or
3) The use of virtual or digital currencies Company will undertake a risk assessment prior to the launch or use of such products, practices and technologies;
and take appropriate measures to manage and mitigate the risks.

These policy and procedures provides governance framework to prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favour anonymity. For example, securities trading and investment business on the Internet, add a new dimension to the Company's activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF, and fraud.
To insulate itself against risk of anonymity of customer, Company will offer an on-line account opening only after appropriate identification checks and fulfillment of its all applicable KYC requirements.

To maintain adequate systems, the Company will ensure that its systems and procedures will be kept up to date with such developments and the potential new risks and impact they may have on the products and services offered by the Company. Risks identified must be fed into the Company business risk assessment.

13. Cross-border Correspondent Relationship

Cross-border correspondent relationships is the provision of services by one institution to another institution (the respondent institution). Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require Enhanced Due Diligence ("EDD").

14. Customer Due Diligence

Company will take steps to know who their customers are. The Company as a policy matter will not open anonymous accounts or accounts in fictitious names and alias. Hence, for customers which are natural person, names contained in their CNIC / NICOP / Passports will be used as title of account, and same is verified from NADRA Verisys record. For entities the title of account offered is same as the one contained in their establishing/incorporation document. The Company will conduct CDD, which will comprise of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer.

Additionally, Company will conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are

consistent with the Company's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds. The Company will conduct CDD when establishing a business relationship if:

(1) There is a suspicion of ML/TF, Annexure 5 gives some examples of potentially suspicious activities or "red flags" for ML/TF. Although these may not be exhaustive in nature, it may help the Company to recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or

(2) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.
In case of suspicion of ML/TF, the Company will:
(1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and

(2) File an STR with the FMU, in accordance with the requirements under the Law.
Company will monitor transactions to determine whether they are linked. Transactions could be deliberately restructured into two or more transactions of smaller values to circumvent the applicable threshold.

Company will verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from Verisys. Similarly, the Company will identify and verify the customer's beneficial owner(s) to ensure that the Company understands who the ultimate beneficial owner is.

Company will ensure that it understands the purpose and intended nature of the proposed business relationship or transaction. The Company will assess and ensures that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring.

The Regulations require the Company to identify and verify the identity of any person that is purporting to act on behalf of the customer ("authorized person"). In this regard Company will also verify whether that authorized person is properly authorized to act on behalf of the customer by demanding an authorization letter in Company's designed pro-forma (which requires reason for using third person) and matching customer signatures against those in Company's record. Customer Call Back confirmation will also performed where customer signatures would be doubtful. The Company will conduct CDD on the authorized person(s) using the same standards that are applicable to a customer.

Company may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa.

When performing CDD measures in relation to customers that are legal persons or legal arrangements, the Company identifies and verifies the identity of the customer, and understand the nature of its business, and its ownership and control structure.

The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the

business relationship; and second, to take appropriate steps to mitigate the risks. In this context, the Company will identify the customer and will verify its identity. The type of information that will be needed to perform this function shall be as specified in Annexure 6.

If the Company will have any reason to believe that an applicant has been refused facilities by another Brokerage house due to concerns over illicit activities of the customer, it will consider classifying that applicant as higher-risk and will apply enhanced due diligence procedures to the customer and the relationship, filing an STR and/or not accepting the customer in accordance with its own risk assessments and procedures.

a) Timing of Verification
i. The Company will undertake verification prior to entry into the business relationship or conducting a transaction.

ii. Where CDD checks will raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/TF, the Company will decline trading accounts to such customers. In such situations, the Company will consider filing an STR with the FMU and will ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

b) Existing Customers
The Company will apply CDD/EDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. For this purpose, Company will perform CDD/EDD measures on its existing customers at the frequency as defined in the following section of Period Risk Reviews.

Further, if the Company will have suspicion of ML/TF or will become aware at any time that it lacks sufficient information about an existing customer, it will take steps to ensure that all relevant information is obtained as quickly as possible irrespective of CDD/EDD revised information collection frequency set as per risk classification of customer.

Company will rely on the identification and verification steps that it has already undertaken, unless it has doubts about the veracity of that information. Examples of situations that might lead Company to have doubt include significant change in the value of injections into his/her trading account, or change in correspondent address to an area / country with high susceptibility to money laundering, terrorist financing or other predicated offences.

Where the Company will be unable to complete and comply with ongoing CDD/EDD requirements as specified above, the Company will terminate the relationship. Additionally, the Company will consider filing an STR to the FMU.

c) Tipping-off & Reporting
The Law prohibits tipping-off any information about the suspicious matter to the concerned customer or to a person not relevant in the process of filing an STR. However, a risk exists that customers could be unintentionally tipped-off when the Company is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF. The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

Therefore, if the Company will form a suspicion of ML/TF while conducting ongoing CDD/EDD, it will take into account the risk of tipping-off when performing the CDD process. If the Company reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it might not pursue that process, and will file an STR. For this Company will ensure that its employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD/EDD.

d) No Simplified Due Diligence for Higher-Risk Scenarios
The Company will not adopt simplified due diligence measures where the ML/TF risks are high. The Company will identify risks and have regard to the risk analysis in determining the level of due diligence to be performed in each case.

15. Period Risk Review ("PRR")

The Company will perform periodic customer profile updating exercise every two years for customers classified as high risk while perform this exercise every four years for Low risk classified customers.

The Company will consider updating customer CDD records as a part its periodic reviews (within the timeframes set by the Company based on the level of risk posed by the customer) or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:
(1) Material changes to the customer risk profile or changes to the way that the account usually operates;
(2) Where it comes to the attention of the Company that it lacks sufficient or significant information on that particular customer;
(3) Where a significant transaction takes place;
(4) Where there is a significant change in customer documentation standards;
(5) Significant changes in the business relationship.

Examples of the above circumstances include:
(1) A significant increase in a customer's deposits,
(3) The stated turnover or activity of a customer increases,
(4) A person has just been designated as a PEP,
(5) The nature, volume or size of transactions changes.

16. On-going Monitoring of Business Relationships

i. Once the identification procedures will be completed and the business relationship will be established, the Company will monitor the conduct of relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened. The Company will conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps the Company to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

ii. The Company will conduct an on-going due diligence which will include scrutinizing the transactions undertaken throughout the course of the business relationship with a customer. Further, the Company' risk department has put in place a weekly review mechanism which includes comparison of client deposits and available KYC/CDD clients' information to confirm that the clients have disclosed adequate income sources to justify the value of deposits. Where inadequacy is identified additional documents/information is obtained

from the clients by sending emails and making follow-up calls. Where clients provides the required document, their profile is updated. In cases where clients do not provide the requisite information, the same is discussed with Head of Risk on a client to client basis and recommendation is made to CO for necessary course of action including re-categorization of client's risk category and/or filing STR with FMU.

Company will stay vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts and the customer updated KYC profile. Possible areas to monitor could be:

(1) transaction type
(2) frequency
(3) amount
(4) geographical origin/destination
(5) account signatories
(6) mandate

It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring mechanism. Hence, Company take support of the technology to the extent possible while use manual procedures where current technology does not support certain report types and analysis. For example, screening against UNSC consolidate sanctions list is performed daily through an internally developed matching and alerts-based solution while individual transactions of customers are matched against customer profiles using Microsoft Excel spreadsheet analytical tool.

17. Simplified Due Diligence Measures ("SDD")

The Company may conduct SDD in case of lower risks identified by it. However, the Company will ensure that the low risks it identified commensurate with the low risks identified by the country or the Commission. While determining whether to apply SDD, Company pays particular attention to the level of risk assigned to the relevant sector, type of customer or activity.

The simplified measures Company will apply shall be commensurate with the low risk factors.

Company however will not use SDD procedures in higher-risk scenarios where there is an increased risk, or suspicion that the applicant is engaged in ML/TF, or the applicant is acting on behalf of a person that is engaged in ML/TF.

Where the Company to take SDD measures on an applicant/customer, it will document the full rationale behind such decision and maintain its record to make it available to the Commission on request.

18. Enhanced CDD Measures ("EDD")

The Company will examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose.

Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, the Company will conduct enhanced CDD measures, consistent with the risks identified. In particular, the Company will increase the degree

and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

iii. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

(1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
(2) Updating more regularly the identification data of applicant/customer and beneficial owner.
(3) Obtaining additional information on the intended nature of the business relationship.
(4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer. (5) Obtaining additional information on the reasons for intended or performed transactions.
(6) Obtaining the approval of senior management to commence or continue the business relationship.
(7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

High-Risk Countries

Certain countries are associated with crimes such as drug trafficking, fraud and corruption, and consequently pose a higher potential risk to the Company. Conducting a business relationship with an applicant/customer from such a country exposes the Company to reputational risk and legal risk.

The Company will exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

Caution will also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks will be undertaken on such individuals/entities to ensure their legitimacy and reliability.

Company therefore will consult publicly available information to ensure that they are aware of the high-risk countries/territories. While assessing risk of a country, the Company will also consider among the other sources, sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions, the FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index.

Useful websites include: FATF website at www.fatf-gafi.org and Transparency International, www.transparency.org for information on countries vulnerable to corruption.

Information about these high-risk geographies will be provided to employees in on-going trainings and will be disseminated through pan-Company broadcast messages once every six months.

19. Politically Exposed Persons

i. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose the Company to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes, grease money or commit fraud. Such persons, commonly referred to as PEPs

and defined in the Regulations, an include inter-alia, heads of state, ministers, influential public officials, judges and senior military officials and includes their family members and close associates, hereinafter referred to as linked PEPs.

Family members of a PEP are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Close associates to PEPs are individuals who are closely connected to PEP, either socially or professionally.

Provision of financial services to corrupt PEPs exposes the Company to reputational risk and costly information requests and seizure orders from law enforcement or judicial authorities. Hence, Company will remain extra vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. The Company should, in relation to PEPs, in addition to performing normal due diligence measures will:

(1) have appropriate risk management systems to determine whether the customer is a PEP;
(2) obtain senior management approval for establishing business relationships with such customers;
(3) take reasonable measures to establish the source of wealth and source of funds; and
(4) conduct enhanced ongoing monitoring of the business relationship.

Company will obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.

Company will take a risk-based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, Company will consider factors such as whether the customer who is a PEP:
(1) Is from a high-risk country;
(2) Has prominent public functions in sectors known to be exposed to corruption;
(3) Has business interests that can cause conflict of interests (with the position held).

The other red flags that the Company will consider include (in addition to the above and the red flags that they consider for other applicants):
(1) The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
(2) Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties; (3)
A PEP uses multiple bank accounts for no apparent commercial or other reason;
(4) The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

Company will 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:
(1) the level of (informal) influence that the individual could still exercise; and
(2) 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).

20. Overview of the National Setting for ML/TF Threats and Vulnerabilities

Those national characteristics that can be exploited or abused for ML/TF purposes should be identified and understood with a view to apply effective AML/CFT measures. In the context of Pakistan, it is important to consider the following when assessing ML/TF risks.

a. Geography:
   Pakistan's geographical landscape and porous borders increase its vulnerability to both ML and TF, heightening in particular Pakistan's TF risks associated to cash smuggling. Pakistan is bordered by India to the east, Afghanistan to the west, Iran to the southwest, and China in the far northeast. This makes both eastern and western borders vulnerable for ML and TF through drug trafficking, bulk cash movements, and other illicit forms of trade.

The Compliance Officer will check all the relevant data before approving any new account at the time of account opening and after every month screen the existing clients from the list provided by the Government Departments and report to the Board if any suspicious event found.

b. Afghan Diaspora

Pakistan is host to approximately 1.4 million registered and 1.0 million unregistered Afghans. These Afghan refugees have been mostly settled in Khyber Pakhtunkhwa and Balochistan for the last 40 years. Their children are educated and settled in Pakistan. Most second and third generation Afghan refugees are born in Pakistan and are culturally, economically and socially integrated. In some cases, they are also married to Pakistanis and the families are now integrated. In addition, the border areas of Khyber Pakhtunkhwa and parts of Balochistan are highly active, with fast moving populations across the border because of common history, culture, language and blood ties. There are eight formal border crossings jointly managed by the Afghan and Pakistan governments, as well as many informal crossings, which remains permeable despite increased fencing and border management systems.

c. Conflict and Terror

The mountainous terrain on the eastern and northern borders also provides isolated and largely hidden routes to organized international groups/organizations. Additionally, maritime frontiers remain vulnerable to illicit trade and trafficking as scores of trespassers are frequently apprehended for crossing into Pakistan "by mistake".

The risks maybe greatest in Balochistan, which has the longest border among Pakistan's subnational units, and is relatively arid and unpopulated compared to the rest of Pakistan. Here, Baloch militants, who are largely secular nationalists, operate. Balochistan has historically suffered from ethno-sectarian tensions and politically motivated violence, including violence from an active separatist movement. Separatist groups such as the BLA have targeted and killed ethnic Punjabi settlers and others as part of their terror reign.

d. Social and Religious Norms

The concept of person to person charity, khairat, sadqa, zakat or helping orphans / widows or religious organization serving Islam stems from Pakistan socio-economic and religious culture. Donations are a principle source of funding for nearly all assessed NPOs in Pakistan create a significant risk including channels for transfer of funds particularly in the transnational context. International reports and open source information suggests that many terrorist organizations derive their funding from licit sources such as donations through fund-raising.

Branches/Agents located in High Risk Jurisdiction and areas as identified in latest NRA.

The Company has the clear policy not to open, operate Branches in the high Jurisdiction and areas as identified in the latest NRA. Furthermore, Company will not make any agent from the areas/locations specified in the latest NRA.

21. Record-Keeping Procedures

Company will ensure that all information obtained in the context of CDD is recorded. This includes both;

a. recording the documents the Company is provided with when verifying the identity of the customer or the beneficial owner, and

b. transcription into the Company own IT systems of the relevant CDD information contained in such documents or obtained by other means.

Company will maintain, for at least five 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 Company becomes 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 will be retained until confirmation is received from the relevant authority in writing that the matter has been concluded.

Company will also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of five years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

Beneficial ownership information will be maintained for at least five years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of the Company.

Records relating to verification of identity will generally comprise:
1) a description of the nature of all the evidence received relating to the identity of the verification subject; and
2) 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:
1) details of personal identity, including the names and addresses, of:
a) the customer; and
b) the beneficial owner of the account or product

2). details of securities and investments transacted including:
a. the nature of such securities/investments;
b. valuation(s) and price(s);
c. memoranda of purchase and sale;
d. source(s) and volume of funds and securities;
e. destination(s) of funds and securities;
f. memoranda of instruction(s) and authority(ies);
g. book entries;

h. custody of title documentation;
i. the nature of the transaction;
j. the date of the transaction;
k. the form (e.g. cash, cheque) in which funds are offered and paid out.

22. Reporting of Suspicious Transactions

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 will be considered unusual, and Company will put the case "on enquiry". The Company will 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 Company 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 CO.

Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result will be properly documented, and made available to the relevant authorities upon request. Activities which will require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

(1) any unusual financial activity of the customer in the context of the customer's own usual activities;
(2) any unusual transaction in the course of some usual financial activity;
(3) any unusually-linked transactions;
(4) any unusual method of settlement;
(5) any unwillingness to provide the information requested.

Where cash transactions are being proposed by customers, and such requests are not in accordance with the customer's known reasonable practice, the Company will need to approach such situations with caution and make further relevant enquiries. Company will set its own parameters at Rs. 25,000 for the identification and further investigation of cash transactions.

Where the Company will be unable to satisfy that any cash transaction is reasonable it will be considered as suspicious. The Company will also be obligated to file Currency Transaction Report ("CTR"), to FMU for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

If the Company decides that a disclosure should be made, the law require the Company to report STR 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.

The process for identifying, investigating and reporting suspicious transactions to the FMU is clearly specified in the Company's KYC/CDD SOPs and communicated to all personnel through regular training.

The Company will also be required to report total number of STRs filed to the Commission on a bi-annual basis within seven days of close of each half year. The CO will ensure prompt reporting in this regard.

Company will evolve a vigilance systems for the purpose of control and oversight, which requires maintenance of a register of all reports made to the FMU. Such registers will be maintained and updated by CO (in case if any such transaction found) and will contain details of:

(1) the date of the report;
(2) the person who made the report;
(3) the person(s) to whom the report was forwarded; and
(4) reference by which supporting evidence is identifiable.

Company as a matter of policy will turn away business where an applicant or a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration will be given to filing an STR to the FMU.

For existing customers, once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity, the Company will ensure that appropriate action is taken to adequately mitigate the risk of the Company being used for criminal activities. This will include a review of either the risk classification of the customer or account or of the entire relationship itself. In such cases an escalation will be made to the Chief Executive Officer to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

23. Sanctions Compliance

There are sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:
(1) targeted sanctions focused on named persons or entities, generally freezing assets and prohibiting making any assets available to them, directly or indirectly;
(2) economic sanctions that prohibit doing business with, or making funds or economic resources available to, designated persons, businesses or other entities, directly or indirectly;
(3) currency or exchange control;
(4) arms embargoes, which would normally encompass all types of military and paramilitary equipment;
(5) prohibiting investment, financial or technical assistance in general or for particular industry sectors or territories, including those related to military or paramilitary equipment or activity;
(6) import and export embargoes involving specific types of goods (e.g. oil products), or their movement using aircraft or vessels, including facilitating such trade by means of financial or technical assistance, brokering, providing insurance etc.; and
(7) visa and travel bans.
(8) Targeted financial sanctions relating to the prevention, suppression and disruption of proliferation of Weapons of Mass Destruction (WMD) and its financing.

As required by Regulations Company will screen all its customers against consolidated sanctions list available on UNSC's website and will decline business relationship with the individuals/entities and their associates that are either, sanctioned under UNSC Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

The UNSC Resolution 1267 (1999), 1989 (2011), 2253 (2015) and other subsequent resolutions, which impose sanctions covering; asset freeze, travel ban and arms embargo, against individuals and entities associated to Al-Qaida, Taliban, and the Islamic State in Iraq (Daésh) organizations. The regularly updated consolidated lists is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list

The UNSC Resolution 1373 (2001), 1998 (2011) on terrorism and financing of terrorism requiring member states to proscribe individual and entities, who commit or attempt to commit terrorist act, freeze without delay the funds and other financial assets or economic resources, and prohibit making any funds or financial or other related services available to such proscribed persons and entities.

c. the UNSC Resolution 1718(2006), 2231(2015) and its successor resolutions 1 on proliferation of WMD and its financing, and Targeted Financial Sanctions (TFS) on countries and specifically identified individual and entities associated with it. The resolution requires, inter-alia freezing without delay the funds or other assets of, any person or entity designated, or under the authority of UNSC. The regularly updated consolidated lists of person and entities designated under UNSCRR 1718(2006) and its successor resolutions (on the DPRK) and listed under UNSCR 2231 (2015) (on Iran) is available at the UN sanctions committee's website, at following link;

https://www.un.org/sc/suborg/en/sanctions/1718/materials
https://www.un.org/sc/2231/list.shtml2

Government of Pakistan, Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 (Act No XIV of 1948) to give effect to the UNSC Resolutions and implement UNSC sanction measures in Pakistan. The said SROs are communicated to the Company, from time to time, and have a binding legal effect under the Act No. XIV of 1948. Company will ensure compliance with the sanctions communicated through SROs. A list of such SROs issued by the Federal Government till date is also available at the following links:

UNSCR 1267

http://www.mofa.gov.pk/contentsro1.php
http://www.mofa.gov.pk/contentsro2.php

UNSCR 1718

http://www.secdiv.gov.pk/page/sro-unscr-sanctions

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

[2] The UNSC sanctions with respect to proliferation of WMD primarily encapsulates currently the Islamic Republic of Iran and the Democratic People's Republic of Korea's sanctions regime. The UNSC resolution on Iran is 2231 (2015). The UNSC resolution on Democratic People's Republic of Korea are 1718 (2006), 1874 (2009), 2087 (2013), 2094 (2013), 2270 (2016), 2321 (2016), 2356 (2017), 2371 (2017), 2375 (2017) and 2397 (2017). also extend to any funds, financial assets and economic resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

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

The individuals and entities designated under the aforementioned resolutions are subject to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses.

Company will, taking note of the circumstances where customers and transactions are more vulnerable to be involved in TF and PF activities3, identify high-risk customers and transactions, and apply enhanced scrutiny.

Company will conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relations involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

Company will also screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list. Company will undertake reasonable efforts to collect additional information in order to identify, and avoid engaging in prohibited activities and, to enable follow-up actions.

Where there is a true match or suspicion, Company will take steps that are required to comply with the sanction's obligations including immediately –
(a) freeze without delay4 the customer's fund or block the transaction, if it is an existing customer;
(b) reject the customer, if the transaction has not commenced; (c)
lodge a STR with the FMU; and
(d) notify the SECP and the
MOFA.

Company will submit an STR when there is an attempted transaction by any of the listed persons.

Company will ascertain potential matches with the UN Consolidated List to confirm whether they are true matches to eliminate any "false positives". The reporting institution must make further enquiries from the customer or counter-party (where relevant) to assist in determining whether it is a true match. In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, the Company will consider raising an STR to FMU.

Notwithstanding the funds, properties or accounts are frozen, Company will continue receiving dividends, interests, or other benefits, but such benefits shall still remain frozen, so long as the individuals or entities continue to be listed.

Company will make their sanctions compliance program an integral part of their overall AML/CFT compliance program and accordingly should have policies, procedures, systems and controls in relation to sanctions compliance. Company will provide adequate sanctions related training to their staff. When conducting risk assessments, Company will take into account any sanctions that may apply (to customers or countries).

The obligations/ prohibitions regarding proscribed entities and persons mentioned in the above lists are applicable, on an ongoing basis, to proscribed/ designated entities and persons or to those who are known for their

[3] The circumstances that the Company shall take note of where customers and transactions are more vulnerable to be involved in PF activities relating to both DPRK and Iran sanction regime are listed on Annexure 7 as PF Warning Signs/Red Alerts.
[4] According to FATF, without delay is defined to be ideally within a matter of hours of designation by the UNSC.

association with such entities and persons, whether under the proscribed/ designated name or with a different name. Therefore, to mitigate the risk of having a sanctioned individual / entity in the portfolio of customer Company has implemented an in-house solution to screen the updated customer portfolio against

Alerts are raised by the system on daily basis, which are reviewed and closed by CO on daily basis. Where there is a true match or suspicion, the CO raise the matter with the CEO with his proposal to comply with 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.

Company will document and record all the actions that have been taken to comply with the sanctions regime, and the rationale for each such action.

Company will keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed.

Company will also educate its customers that in case of wrongful or inadvertent freezing, they may apply in writing for de-listing to Federal Government through relevant Ministry or to the UN's Ombudsman, as the case may be.

24. Internal Controls (Audit Function, employee screening and training)

Company will put in place systems and controls that are comprehensive and proportionate to the nature, scale and complexity of its activities and the ML/TF risks they identified. The Company will establish and maintain internal controls in relation to:
(1) an independent internal audit function to test the AML/CFT systems, policies and procedures;
(2) employee screening procedures to ensure high standards when hiring employees; and
(3) an appropriate employee training program.

a) Internal Audit Function
Company will, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit will be determined through quarterly risk assessment exercise and will commensurate with the Company nature, size, complexity, and risks identified during the risk assessments. The scope of AML/CFT audits will cover assessment of the AML/CFT systems which include:
(1) testing the overall integrity and effectiveness of the AML/CFT systems and controls;
(2) assessing the adequacy of internal policies and procedures in addressing identified risks, including;
(a) CDD measures;
(b) Record keeping and retention;
(c) Third party reliance; and
(d) Transaction monitoring;
(3) assessing compliance with the relevant laws and regulations;
(4) testing transactions in all areas of the Company, with emphasis on high–risk areas, products and services;
(5) assessing employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
(6) assessing the adequacy, accuracy and completeness of training programs;
(7) assessing the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and

(8) assessing the adequacy of the Company's process of identifying suspicious activity including screening sanctions lists.

b) Employee Screening

Company's policy and procedures with regards to screening prospective and existing employees to ensure abidance with high ethical and professional standards are defined in this sections. The extent of employee screening will be proportionate to the particular risks associated with the individual positions.

Employee screening will be conducted at the time of recruitment and periodically thereafter, i.e., at least annually and where a suspicion has arisen as to the conduct of the employee.

The Company will 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 Company will:
(1) Verify the references provided by the prospective employee at the time of recruitment
(2) Verify the employee's employment history, professional membership and qualifications from his resume and original copies of education documents.

c) Employee Training

The Company will ensure, when new amendments are there, employees receive training on ML/TF prevention on a regular basis, ensure all staff fully understand the procedures and their importance, and ensure that they fully understand that they will be committing criminal offences if they contravene the provisions of the legislation.

Training to staff will be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to the Company's business operations or customer base. Company will provide their staff training in the recognition and treatment of suspicious activities. Training will also be provided on the results of the Company's risk assessments. Additionally, this training will be structured to ensure compliance with all of the requirements of the applicable legislations pertaining to AML/CFT.

25. COMPLIANCE FUNCTION

AML/CFT guidelines are being provided to help AMS Staff to understand the processes involved under AML/CFT regulations 2020. It is important that a system be developed to monitor customer transactions and report any suspicious activity in a timely manner, if any.

This includes maintaining record of violations/non-compliance identified which has to be reported to the Board of Directors. Any such record has to be available for inspection by SECP and PSX as and when required.

- RECORD KEEPING:

  AMS shall maintain all necessary records on transactions, both trading and banking, for any analysis, background and purpose of complex, unusual large transactions in case for a minimum period of five years from completion of the transaction.

  The records of identification data obtained through CDD process like copies of identification documents, account opening forms, KYC forms, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of five years. The identification records may be maintained in document as originals or copies subject to bank's attestation.

- TRAINING:

There will be on-going training employees and Dealer/Agents to ensure that they understand their duties under AML/CFT regulations 2020 and are able to perform those duties satisfactorily.

- SCREENING:

In order to ensure, that unscrupulous elements do not become employees/agents, AMS would adopt appropriate screening procedures when hiring and also on an ongoing basis to ensure high standards of staff in terms of honesty, integrity, ethics and professionalism.

AMS like any other financial institutions is bound by the requirements of AML/CFT regulations 2020, as applicable to them and must comply with the provisions of this Act. This includes filing of suspicious Transactions Reports and complying with any directives, circulars, guidelines with regard to KYC/CDD/Anti-Money Laundering/Terrorist Financing, issued by the Federal Government.

OTHER OFFENCES – FAILURE TO REPORT OFFENCES

- Failure by an individual in the regulated sector to inform the Regulatory Authority or the AMS's Compliance Officer, as soon as practicable, of knowledge or suspicion (or reasonable grounds for knowing or suspecting) that another person is engaged in money laundering.

- Failure by Compliance Officers in the regulated sector to make the required report to Regulatory Authority as soon as practicable, if an internal report leads them to know or suspect that a person is engaged in money laundering.

DE MINIMIS CONCESSIONS

Note that the obligation to report does not depend on the amount involved or the seriousness of the offence. There are no de-minimis concessions.

Copies of all documents related to AMS's Client Identification Procedures will be retained for an appropriate period of time and, at a minimum, the period of time required by applicable law or regulation.

The documents AMS retains are copies of documents reviewed in connection with Client Identification Procedures or enhanced due diligence procedures, Client identification checklists, if any, or similar due diligence documentation, and any other documents required to be retained by applicable anti-money laundering legislation.

AMS will retain documents for so long as a Person/Entity is a client of AMS and for a minimum of five years after this relationship ends.

PROCEDURE WHERE ENCHANCED DUE DILIGENCE IS REQUIRED

Below is the procedure whereby risk assessment of client due diligence instigate the AMS to conduct Enhanced Due Diligence (EDD);

AMS shall monthly prepare a compliance status report of customers whose net traded/Investment value (value bought less value sold) would be equal to or greater than the below thresholds;

i. For Corporate Entities minimum threshold is PKR. 50 million.
ii. For Individual Investor minimum threshold is PKR. 25 million

- If any client is in non-compliance of the above specified threshold limits than that client EDD will be conducted, the same is being kept in record and trail of the same is being maintained at all material times.
- AMS will also maintain a summary report of the investors, whom falls under the above category. The summary report covers the following details;

a. At Client Level: UIN number, Name, Address Contact Number, Email address, Profession
b. At Risk Category Level: Initial risk level and Revision made thereunder.
c. Compliance Status
d. Action initiated, if any required.

R REVIEW/AUDIT OF THE MANUAL

A regular review of the program should be undertaken to ensure that it is functioning as designed. Such a review could be performed by external or internal resources, and should be accompanied by a formal assessment or written report.

If and when regulations are amended concerning reporting of suspicious activities, AMS will amend this Compliance Manual to comply with those regulations.

Preparing AML/CFT Risk Assessment

"Establish KYC-CDD and customer risk profiling prior to Risk Assessment process"

Annex 1

Step 1 – Identify Customer Risk

Customer Risk Type					
			Internal Risk Rating by the Company		
Customer Type	Number of Customers	Total Amount on Deposit/Value of Trade (Buy and Sale)	Total Number Classified as Low Risk	Total Number Classified as Medium Risk	Total Number Classified as High Risk
1. Natural Persons					
Resident					
Non-Resident					
Total Natural Persons	0	0.00	0	0	
2. Legal Persons					
Resident					
Non-Resident					
Total Legal Persons	0	0.00	0	0	0
Total Exposure	0	0	0	0	0

Step 2- Politically Exposed Persons and High Net worth Individuals

Politically Exposed Persons ('PEP's), and or, High Net Worth Individuals				
Customer Risk	Politically Exposed Persons and or Related Companies		High Net Worth Individuals	
Type	Total Number		Total Number	
	Domestic PEP	Foreign PEP	Domestic	Foreign
Product 1				
Product 2				
Product 3				
Other (specify)				
Total	0.00	0.00	0.00	0.00

Step 3 - Identify Risk by Product, Services and Transactions

Business Risk	Products and Services									
	Domestic					Foreign				
Type	Total Deposits/Securities Purchased		Total Withdrawals/Securities Sold		Total Exposure/Value of Customers Assets in hand	Total Deposits/Securities Purchased		Total Withdrawals/Securities Sold/Claims & Maturities Paid		Total Exposure/Value of Customers Assets in hand
	Number	Value in Rs.	Number	Value in Rs.	(on cutoff date)	Number	Value in Rs.	Number	Value in Rs.	(on cutoff date)
	Products and Services									
Product 1										
Product 2										
Product 3										
Product 4										
Other (specify)										
Other (specify)										
	Transactions									
Customer Type 1										
Customer Type 2										
Customer Type 3										
Customer Type 4										
Other (specify)										
Other (specify)										
Total	0.00		0.00		0.00	0.00		0.00		0.00

Step 4- Identify Wire Transfer Activity

Type	Number of Incoming Transfers over the	Total Value	Number of Outgoing Transfers over the	Total Value
Wire Transfers (SWIFT)				
Domestic Payments				
Total	0.00	0.00	0.00	0.00

Step 5 – Identify Customer Type by Geographic Location

Types of Customers	Number of Customers	Total Deposits/Value of Trade
Natural		
Of which, non-resident customers from 'High risk		
Of which, non-resident customers from 'High risk		
Legal		
Of which, non-resident customers from 'High risk		
Jurisdictions' as identified by the FATF		
Total	0.00	0.00

Step 6 - Develop Risk Likelihood Table

Customer Risk Likelihood			
Type of Customer	Custome	Transactio	Geograph
	Rating: (High/		

Product Risk Likelihood			
Product Type	Custome	Transactio	Geograph
	Rating: (High/		

Delivery Channels Risk Likelihood			
Delivery Channels	Custome	Transaction	Geograph
	Rating		

Overall Entity Level AML/CFT Risk	
Rating	
Customer Type	
Product Type	
Delivery Channels	
Geography	
Overall AML/CFT Risk Rating	

AML/CFT Compliance Assessment Checklist

Annex 2

SECP AML/CFT Compliance Assessment Checklist	
Name of the Financial Institution	
Checklist completed by (Name)	
(Designation)	
Date	
The AML / CFT Self-Assessment Checklist has been designed to provide a structured and comprehensive framework for RFIs and their associated entities to assess compliance with key AML / CFT requirements. RFIs are advised to use this as part of their regular review to monitor their AML/CFT compliance. The frequency and extent of such review should be commensurate with the risks of ML/TF and the size of the firm's business.	

Sr No.	Question	Yes/No (N/A)	If No, provide explanation and plan of action for
(A) AML/CFT Systems			
1	The Company is required to assess its ML / TF risk and then implement appropriate internal policies, procedures and controls to mitigate risks of ML/TF.		
	Have you taken into account the following risk factors when assessing your own ML / TF risk?		
	(a) Product / service risk		
	(b) Delivery / distribution channel risk		
	(c) Customer risk		
	(d) Country risk		
2	The Company is required to have effective controls to ensure proper implementation of AML/CFT policies and procedures.		
	Does your AML/CFT systems cover the following controls?		
	(a) Board of Director and Senior management oversight		

	(ii) Have you appointed an appropriate staff as a Compliance Officer ('CO')?		
	(iii) Do you ensure that CO is:		
	1. the focal point for the oversight of all activities relating to the prevention and detection of ML/TF		
	2. independent of all operational and business functions as far as practicable within any constraint of size of your institution		
	3. of a sufficient level of seniority and authority within your institution		
	4. provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and the measures against the risks of ML/TF is sufficient and robust		
	5. fully conversant in the statutory and regulatory requirements and ML/TF risks arising from your		
	6. capable of accessing on a timely basis all required available information to undertake its role		
	7. equipped with sufficient resources, including staff		
	8. overseeing your firm's compliance with the relevant AML requirements in Pakistan and overseas branches and subsidiaries		
	(b) Audit function		
	(i) Have you established an independent audit function?		
	(ii) If yes, does the function regularly review the AML/CFT systems to ensure effectiveness?		
	(iii) If appropriate, have you sought review assistance from external sources regarding your AML/CFT		
	(c) Staff screening		
	(i) Do you establish, maintain and operate appropriate procedures in order to be satisfied of the integrity of any new employees?		
3	The Company with overseas branches or subsidiary undertakings should put in place a group AML/CFT policy to ensure an overall compliance with the CDD and record-keeping requirements.		
	Does your firm have overseas branches and subsidiary undertakings?		
	Do you have a group AML/CFT policy to ensure that all overseas branches and subsidiary undertakings have procedures in place to comply with the CDD and record-keeping requirements similar to those set under the AML Regulations?		
	If yes, is such policy well communicated within your group?		
	In the case where your overseas branches or subsidiary undertakings are unable to comply with the above mentioned policy due to local laws' restrictions, have you done the following?		
	(a) inform the SECP of such failure		
	(b) take additional measures to effectively mitigate ML/TF risks faced by them		
(B) Risk-Based Approach ('RBA')			
4	The Company is required to determine the extent of CDD measures and ongoing monitoring, using an RBA		

	Does your RBA identify and categorize ML/TF risks at the customer level and establish reasonable measures based on risks identified?		
	Do you consider the following risk factors when determining the ML/TF risk rating of customers?		
	(a) Country risk - customers with residence in or connection with the below high-risk jurisdictions		
	(i) countries identified by the FATF as jurisdictions with strategic AML/CFT deficiencies		
	(ii) countries subject to sanctions, embargoes or similar measures issued by international authorities		
	(iii) countries which are vulnerable to corruption		
	(iv) countries that are believed to have strong links to terrorist activities		
	(b) Customer risk - customers with the below nature or behavior might present a higher ML/TF risk		
	(i) the public profile of the customer indicating involvement with, or connection to, politically exposed persons		
	(ii) complexity of the relationship, including use of corporate structures, trusts and the use of nominee and bearer shares where there is no legitimate commercial rationale		
	(iii) request to use numbered accounts or undue levels of secrecy with a transaction		
	(iv) involvement in cash-intensive businesses		
	(v) nature, scope and location of business activities generating the funds/assets, having regard to sensitive or high-risk activities		
	(vi) the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified		
	(c) Product/service risk - product/service with the below factors might present a higher risk		
	(i) services that inherently have provided more anonymity		
	(ii) ability to pool underlying customers/funds		
	(d) Distribution/delivery channels		
	(i) a non-face-to-face account opening approach is used		
	(ii) Business sold through third party agencies or intermediaries		
	Do you adjust your risk assessment of customers from time to time or based upon information received from a competent authority, and review the extent of the CDD and ongoing monitoring to		
	Do you maintain all records and relevant documents of the above risk assessment?		
	If yes, are they able to demonstrate to the SECP the following?		
	(a) how you assess the customer		
	(b) the extent of CDD and ongoing monitoring is appropriate based on that customer's ML/TF risk		
(C) - Customer Due Diligence ('CDD')			
5	The Company is required to carry out CDD, which is a vital tool for recognizing whether there are grounds for knowledge or suspicion of ML/TF.		
	Do you conduct the following CDD measures?		
	(a) identify the customer and verify the customer's identity using reliable, independent source documents, data or information		

	(b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity, including in the case of a legal person or trust, measures to enable you to understand the ownership and control structure of the legal person or		
	(c) obtain information on the purpose and intended nature of the business relationship established with you unless the purpose and intended nature are obvious		
	(d) if a person purports to act on behalf of the customer:		
	(i) identify the person and take reasonable measures to verify the person's identity using reliable and independent source documents, data or information		
	(ii) verify the person's authority to act on behalf of the customer (e.g. written authority, board		
	Do you apply CDD requirements in the following conditions?		
	(a) at the outset of a business relationship		
	(b) when you suspect that a customer or a customer's account is involved in ML/TF		
	(c) when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity		
6	The Company is required to identify and take reasonable measures to verify the identity of a beneficial		
	When an individual is identified as a beneficial owner, do you obtain the following identification		
	(a) Full name		
	(b) Date of birth		
	(c) Nationality		
	(d) Identity document type and number		
	Do you verify the identity of beneficial owner(s) with reasonable measures, based on its assessment of the		
7	The Company is required to identify and take reasonable measures to verify the identity of a person who purports to act on behalf of the customer and is authorized to give instructions for the movement of funds or assets.		
	When a person purports to act on behalf of a customer and is authorized to give instructions for the movement of funds or assets, do you obtain the identification information and take reasonable measures to verify the information obtained?		
	Do you obtain the written authorization to verify that the individual purporting to represent the customer is authorized to do so?		
	Do you use a streamlined approach on occasions where difficulties have been encountered in identifying and verifying signatories of individuals being represented to comply with the CDD		
	If yes, do you perform the following:		
	(a) adopt an RBA to assess whether the customer is a low risk customer and that the streamlined approach is only applicable to these low risk customers		

	(b) obtain a signatory list, recording the names of the account signatories, whose identities and authority to act have been confirmed by a department or person within that customer which is independent to the persons whose identities are being verified		
8	The Company is required to take appropriate steps to verify the genuineness of identification provided if suspicions are raised.		
	In case of suspicions raised in relation to any document in performing CDD, have you taken practical and proportionate steps to establish whether the document offered is genuine, or has been reported as lost or stolen? (e.g. search publicly available information, approach relevant		
	Have you rejected any documents provided during CDD and considered making a report to the authorities (e.g. FMU, police) where suspicion on the genuineness of the information cannot be		
9	The Company is required to understand the purpose and intended nature of the business relationship established.		
	Unless the purpose and intended nature are obvious, have you obtained satisfactory information from all new customers (including non-residents) as to the intended purpose and reason for opening the account or establishing the business relationship, and record the information on the relevant account opening documentation?		
10	The Company is required to complete the CDD before establishing business relationships.		
	Do you always complete the CDD process before establishing business relationships? If you always complete		
	If you are unable to complete the CDD process, do you ensure that the relevant business relationships must not be established and assess whether this failure provides grounds for knowledge or suspicion of ML/TF to submit a report to the FMU as appropriate?		
	If the CDD process is not completed before establishing a business relationship, would these be on an exception basis only and with consideration of the following:		
	(a) any risk of ML/TF arising from the delayed verification of the customer's or beneficial owner's identity can be effectively managed.		
	(b) it is necessary not to interrupt the normal course of business with the customer (e.g. securities transactions).		
	(c) verification is completed as soon as reasonably practicable.		
	(d) the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable.		
	Have you adopted appropriate risk management policies and procedures when a customer is permitted to enter into a business relationship prior to verification?		
	If yes, do they include the following?		

	(a) establishing timeframes for the completion of the identity verification measures and that it is carried out as soon as reasonably practicable		
	(b) placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification		
	(c) ensuring that funds are not paid out to any third party		
	(d) other relevant policies and procedures		
	When terminating a business relationship where funds or other assets have been received, have you returned the funds or assets to the source (where possible) from which they were received?		
11	The Company is required to keep the customer information up-to-date and relevant.		
	Do you undertake reviews of existing records of customers to ensure that the information obtained for the purposes of complying with the AML requirements are up-to-date and relevant when one of the following trigger events happen?		
	(a) when a significant transaction is to take place		
	(b) when a material change occurs in the way the customer's account is operated		
	(c) when your customer documentation standards change substantially		
	(d) when you are aware that you lack sufficient information about the customer concerned		
	(e) if there are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box		
	Are all high-risk customers subject to a review of their profile?		
12	The Company is required to identify and verify the true and full identity of each natural person by using reliable and independent sources of information.		
	Do you have customers which are natural persons?		
	Do you collect the identification information for customers:		
	(i) Residents		
	(ii) Non-residents		
	(iii) Non-residents who are not physically present		
	Do you document the information?		
	If yes, please provide a list of acceptable documents that you obtain for verifying residential address (e.g. utility bills or bank statements). For the avoidance of doubt, please note according to the Guideline on AML and CFT that certain types of address verification should not be considered sufficient, e.g. a post office box address, for persons residing in Pakistan or corporate customers		
	In cases where customers may not be able to produce verified evidence of residential address have you adopted alternative methods and applied these on a risk sensitive basis?		
	Do you require additional identity information to be provided or verify additional aspects of identity if the customer, or the product or service, is assessed to present a higher ML/TF risk?		

13	The Company is required to identify and verify the true and full identity of each legal person and trust and its beneficial owners by using reliable and independent sources of information.		
	Do you have measures to look behind each legal person or trust to identify those who have ultimate control or ultimate beneficial ownership over the business and the customer's assets?		
	Do you fully understand the customer's legal form, structure and ownership, and obtain information on the nature of its business, and reasons for seeking the product or service when the		
14	Corporation		
	Do you have customers which are corporations?		
	Do you obtain the following information and verification documents in relation to a customer which is a corporation?		
	For companies with multiple layers in their ownership structures, do you have an understanding of the ownership and control structure of the company and fully identify the intermediate layers		
	Do you take further measures, when the ownership structure of the company is dispersed/complex/multi- layered without an obvious commercial purpose, to verify the identity		
15	Partnerships and unincorporated bodies		
	Do you have customers which are partnerships or unincorporated bodies?		
	Do you take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated bodies?		
	Do you obtain the information and verification documents in relation to the partnership or unincorporated body?		
	Do you have customers which are in the form of trusts?		
	Do you obtain the information and verification documents to verify the existence, legal form and parties to a trust?		
	Have you taken particular care in relation to trusts created in jurisdictions where there is no or weak money laundering legislation?		

16	The Company may conduct simplified 'Know Your Customer' due diligence ('SDD') process instead of full CDD measures given reasonable grounds to support it. Simplified due diligence is the lowest level of due diligence that can be completed on a customer. This is appropriate where there is little opportunity or risk of your services or customer becoming involved in money laundering or terrorist financing. SDD is a condition where the timing of the actual verification of a particular customer is deferred until such time the entire CDD		
	Have you conducted SDD instead of full CDD measures for your customers?		
	Do you refrain from applying SDD when you suspect that the customer, the customer's account or the transaction is involved in ML/TF, or when you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying or verifying the customer?		
	Before the application of SDD on any of the customer categories, have you performed checking on whether they meet the criteria of the respective category?		
17	The Company is required, in any situation that by its nature presents a higher risk of ML/TF, to take additional measures to mitigate the risk of ML/TF.		
	Do you take additional measures or enhanced due diligence ('EDD') when the customer presents a higher risk of		
	If yes, do they include the following?		
	(a) obtaining additional information on the customer and updating more regularly the customer profile including the identification data		
	(b) obtaining additional information on the intended nature of the business relationship, the source of wealth and source of funds		
	(c) obtaining the approval of senior management to commence or continue the relationship		
	(d) conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.		
18	The Company is required to apply equally effective customer identification procedures and ongoing monitoring standards for customers not physically present for identification purposes as for those where the customer is available for interview.		
	Do you accept customers that are not physically present for identification purposes to open an		
	If yes, have you taken additional measures to compensate for any risk associated with customers not physically present (i.e. face to face) for identification purposes?		
	If yes, do you document such information?		
19	The Company is required to determine whether a potential customer, a customer or the beneficial owner is a politically exposed person ('PEP') and to adopt EDD on PEPs.		
	Do you define what a PEP (foreign and domestic) is in your AML/CFT policies and procedures?		

	Have you established and maintained effective procedures for determining whether a customer or a beneficial owner of a customer is a PEP (foreign and domestic)?		
	If yes, is screening and searches performed to determine if a customer or a beneficial owner of a customer is a PEP? (e.g. through commercially available databases, publicly available sources and internet / media searches etc)		
20	Foreign PEPs		
	Do you conduct EDD at the outset of the business relationship and ongoing monitoring when a foreign PEP is identified or suspected?		
	Have you applied the following EDD measures when you know that a particular customer or beneficial owner is a foreign PEP (for both existing and new business relationships)?		
	(a) obtaining approval from your senior management		
	(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds		
	(c) applying enhanced monitoring to the relationship in accordance with the assessed risks		
21	Domestic PEPs		
	Have you performed a risk assessment for an individual known to be a domestic PEP to determine whether the individual poses a higher risk of ML/TF?		
	If yes and the domestic PEP poses a higher ML/TF risk, have you applied EDD and monitoring specified in question C.40 above?		
	If yes, have you retained a copy of the assessment for related authorities, other authorities and auditors and reviewed the assessment whenever concerns as to the activities of the individual		
	For foreign and domestic PEPs assessed to present a higher risk, are they subject to a minimum of an annual review and ensure the CDD information remains up-to-date and relevant?		
22	The Company has the ultimate responsibility for ensuring CDD requirements are met, even intermediaries were used to perform any part of the CDD measures.		
	Have you used any intermediaries to perform any part of your CDD measures?		
	When intermediaries (not including those in contractual arrangements with the RFI to carry out its CDD function or business relationships, accounts or transactions between RFI for their clients) are relied on to perform any part of the CDD measures, do you obtain written confirmation from the		
	(a) they agree to perform the role		
	(b) they will provide without delay a copy of any document or record obtained in the course of carrying out the		
	When you use an intermediary, are you satisfied that it has adequate procedures in place to prevent		

	When you use overseas intermediaries, are you satisfied that it:		
	(a) is required under the law of the jurisdiction concerned to be registered or licensed or is regulated under the law of that jurisdiction		
	(b) has measures in place to ensure compliance with requirements		
	(c) is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities in PK		
	In order to ensure the compliance with the requirements set out above for both domestic and overseas intermediaries, do you take the following measures?		
	(a) review the intermediary's AML/CFT policies and procedures		
	(b) make enquiries concerning the intermediary's stature and regulatory track record and the extent to which any group's AML/CFT standards are applied and audited		
	Do you immediately (with no delay) obtain from intermediaries the data or information that the intermediaries obtained in the course of carrying out the CDD measures?		
	Do you conduct sample tests from time to time to ensure CDD information and documentation is produced by the intermediary upon demand and without undue delay?		
	Have you taken reasonable steps to review intermediaries' ability to perform its CDD whenever you have doubts as to the reliability of intermediaries?		
23	The Company is required to perform CDD measures on pre-existing customers when trigger events		
	Have you performed CDD measures on your pre-existing customers when one of the following trigger events happens?		
	(a) a transaction takes place with regard to the customer, which is, by virtue of the amount or nature of the transaction, unusual or suspicious; or is inconsistent with your knowledge of the customer or the customer's business or risk profile or with your knowledge of the source of the		
	(b) a material change occurs in the way in which the customer's account is operated		
	(c) you suspect that the customer or the customer's account is involved in ML/TF		
	(d) you doubt the veracity or adequacy of any information previously obtained for the purpose of identifying and verifying the customer's identity		
	(e) Are other trigger events that you consider and defined in your policies and procedures, please elaborate further in the text box		
24	The Company is not allowed to maintain anonymous accounts or accounts in fictitious names for any new or existing customers.		
	Do you refrain from maintaining (for any customer) anonymous accounts or accounts in fictitious		

25	The Company is required to assess and determine jurisdictional equivalence as this is an important aspect in the application of CDD measures.		
	When you do your documentation for assessment or determination of jurisdictional equivalence, do you take the following measures?		
	(a) make reference to up-to-date and relevant information		
	(b) retain such record for regulatory scrutiny		
	(c) periodically review to ensure it remains up-to-date and valid		
(D) - Ongoing monitoring			
26	The Company is required to perform effective ongoing monitoring for understanding customer's activities and it helps the firm to know the customers and to detect unusual or suspicious activities.		
	Do you continuously monitor your business relationship with a customer by:		
	(a) monitoring the activities (including cash and non-cash transactions) of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds.		
	(b) identifying transactions that are complex, large or unusual or patterns of transactions that have no apparent economic or lawful purpose and which may indicate ML/TF		
	Do you monitor the following characteristics relating to your customer's activities and transactions?		
	(a) the nature and type of transaction (e.g. abnormal size of frequency)		
	(b) the nature of a series of transactions (e.g. a number of cash deposits)		
	(c) the amount of any transactions, paying particular attention to substantial transactions		
	(d) the geographical origin/destination of a payment or receipt		
	(e) the customer's normal activity or turnover		
	Do you regularly identify if the basis of the business relationship changes for customers when the following occur?		
	(a) new products or services that pose higher risk are entered into		
	(b) new corporate or trust structures are created		
	(c) the stated activity or turnover of a customer changes or increases		
	(d) the nature of transactions change or the volume or size increases		
	(e) if there are other situations, please specify and further elaborate in the text box		
	In the case where the basis of a business relationship changes significantly, do you carry out further CDD		
	Have you established procedures to conduct a review of a business relationship upon the filing of a report to the		

27	The Company is required to link the extent of ongoing monitoring to the risk profile of the customer determined through RBA.		
	Have you taken additional measures with identified high risk business relationships (including PEPs) in the form of more intensive and frequent monitoring?		
	If yes, have you considered the following:		
	(a) whether adequate procedures or management information systems are in place to provide relevant staff with timely information that might include any information on any connected		
	(b) how to monitor the sources of funds, wealth and income for higher risk customers and how any changes in circumstances will be recorded		
	Do you take into account the following factors when considering the best measures to monitor customer transactions and activities?		
	(a) the size and complexity of its business		
	(b) assessment of the ML/TF risks arising from its business		
	(c) the nature of its systems and controls		
	(d) the monitoring procedures that already exist to satisfy other business needs		
	(e) the nature of the products and services (including the means of delivery or communication)		
	In the case where transactions are complex, large or unusual, or patterns of transactions which have no apparent economic or lawful purpose are noted, do you examine the background and purpose, including where appropriate the circumstances of the transactions?		
	If yes, are the findings and outcomes of these examinations properly documented in writing and readily available for the SECP, competent authorities and auditors?		
	In the case where you have been unable to satisfy that any cash transaction or third party transfer proposed by customers is reasonable and therefore consider it suspicious, do you make a suspicious transaction report to the FMU?		
(E) - Financial sanctions and terrorist financing			
28	The Company has to be aware of the scope and focus of relevant financial/trade sanctions regimes.		
	Do you have procedures and controls in place to:		
	(a) ensure that no payments to or from a person on a sanctions list that may affect your operations is		
	(b) screen payment instructions to ensure that proposed payments to designated parties under applicable laws and regulations are not made		
	If yes, does this include:		
	(a) drawing reference from a number of sources to ensure that you have appropriate systems to conduct checks against relevant lists for screening purposes		
	(b) procedures to ensure that the sanctions list used for screening are up to date		

	Do you take the following measures to ensure compliance with relevant regulations and legislation on		
	(a) understand the legal obligations of your institution and establish relevant policies and procedures		
	(b) ensure relevant legal obligations are well understood by staff and adequate guidance and training are provided		
	(c) ensure the systems and mechanisms for identification of suspicious transactions cover TF as well as		
	Do you maintain a database (internal or through a third party service provider) of names and particulars of terrorist suspects and designated parties which consolidates the various lists that have		
	If yes, have you also taken the following measures in maintaining the database?		
	(a) ensure that the relevant designations are included in the database.		
	(b) the database is subject to timely update whenever there are changes		
	(c) the database is made easily accessible by staff for the purpose of identifying suspicious transactions		
	Do you perform comprehensive screening of your complete customer base to prevent TF and sanction violations?		
	If yes, does it include the following?		
	(a) screening customers against current terrorist and sanction designations at the establishment of the relationship		
	(b) screening against your entire client base, as soon as practicable after new terrorist and sanction designation are published by the SECP		
	Do you conduct enhanced checks before establishing a business relationship or processing a transaction if there are circumstances giving rise to a TF suspicion?		
	Do you document or record electronically the results related to the comprehensive ongoing screening, payment screening and enhanced checks if performed?		
	Do you have procedures to file reports to the FMU if you suspect that a transaction is terrorist-related, even if there is no evidence of a direct terrorist connection?		
(F) - Suspicious Transaction reports			
29	The Company is required to adopt on-going monitoring procedures to identify suspicious transactions for the reporting of funds or property known or suspected to be proceeds of crime or terrorist activity to the Joint Financial Intelligence Unit ('FMU').		
	Do you have policy or system in place to make disclosures/suspicious transaction reports with the		
	Do you apply the following principles once knowledge or suspicion has been formed?		
	(a) in the event of suspicion of ML/TF, a disclosure is made even where no transaction has been conducted by or through your institution		

	(b) internal controls and systems are in place to prevent any directors, officers and employees, especially those making enquiry with customers or performing additional or enhanced CDD process, committing the offence of tipping off the customer or any other person who is the subject of the		
	Do you provide sufficient guidance to your staff to enable them to form a suspicion or to recognise when ML/TF		
	If yes, do you provide guidance to staff on identifying suspicious activity taking into account the		
	(a) the nature of the transactions and instructions that staff is likely to encounter		
	(b) the type of product or service		
	(c) the means of delivery		
	Do you ensure your staff are aware and alert with the SECP's guidelines with relation to:		
	(a) potential ML scenarios using Red Flag Indicators		
	(b) potential ML involving employees of The Company.		
	Subsequent to a customer suspicion being identified, have you made prompt disclosures to the FMU if the following additional requests are made by the customer: Note: The Company is required to make prompt disclosure to FMU in any event but the following requests are		
	(a) instructed you to move funds		
	(b) close the account		
	(c) make cash available for collection		
	(d) carry out significant changes to the business relationship		
(G) - Record Keeping and Retention of Records			
30	The Company is required to maintain customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements.		
	Do you keep the documents/ records relating to customer identity?		
	If yes to the above documents/ records, are they kept throughout the business relationship with the customer and for a period of six years after the end of the business relationship? Note: While the AMLO identifies relevant documents to be retained for 6 years, the RFI should consider other SECP requirements when determining the record keeping and retention period of each document		
	Do you keep the following documents/ records relating to transactions?		
	(a) the identity of the parties to the transaction		
	(b) the nature and date of the transaction		
	(c) the type and amount of currency involved		
	(d) the origin of the funds		
	(e) the form in which the funds were offered or withdrawn		

	(f) the destination of the funds		
	(g) the form of instruction and authority		
	(h) the type and identifying number of any account involved in the transaction		
	Are the documents/ records, they kept for a period of five years after the completion of a transaction, regardless of whether the business relationship ends during the period as required under the AML/CFT Regulations?		
	In the case where customer identification and verification documents are held by intermediaries, do you ensure that the intermediaries have systems in place to comply with all the record-keeping		
(H) - Staff Training			
31	The Company is required to provide adequate ongoing training for staff in what they need to do to carry out their particular roles with respect to AML/CFT.		
	Have you implemented a clear and well-articulated policy to ensure that relevant staff receive adequate		
	Do you provide AML/CFT training to your staff to maintain their AML/CFT knowledge and competence?		
	If yes, does the training program cover the following topics?		
	(a) your institution's and the staff's own personal statutory obligations and the possible consequences for failure to report suspicious transactions under relevant laws and regulations		
	(b) any other statutory and regulatory obligations that concern your institution and the staff under the relevant laws and regulations, and the possible consequences of breaches of these obligations		
	(c) your own policies and procedures relating to AML/CFT, including suspicious transaction identification and reporting		
	(d) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by your staff to carry out their particular roles in your institution with		
	Do you provide AML/CFT training for all your new staff, irrespective of their seniority and before work commencement?		
	If yes, does the training program cover the following topics?		
	(a) an introduction to the background to ML/TF and the importance placed on ML/TF by your institution		
	(b) the need for identifying and reporting of any suspicious transactions to the Compliance Officer, and the offence of 'tipping-off'		
	Do you provide AML/CFT training for your members of staff who are dealing directly with the public?		
	If yes, does the training program cover the following topics?		
	(a) the importance of their role in the institution's ML/TF strategy, as the first point of contact with potential money launderers		
	(b) your policies and procedures in relation to CDD and record-keeping requirements that are relevant to their job responsibilities		

	(c) training in circumstances that may give rise to suspicion, and relevant policies and procedures, including, for example, lines of reporting and when extra vigilance might be required		
	Do you provide AML/CFT training for your back-office staff?		
	If yes, does the training program cover the following topics?		
	(a) appropriate training on customer verification and relevant processing procedures		
	(b) how to recognize unusual activities including abnormal settlements, payments or delivery		
	Do you provide AML/CFT training for managerial staff including internal audit officers and COs?		
	If yes, does the training program cover the following topics?		
	(a) higher level training covering all aspects of your AML/CFT regime		
	(b) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as reporting of suspicious transactions to the FMU		
	Do you provide AML/CFT training for your Compliance Officer?		
	If yes, does the training program cover the following topics?		
	(a) specific training in relation to their responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the FMU		
	(b) training to keep abreast of AML/CFT requirements/developments generally		
	Do you maintain the training record details for a minimum of 3 years?		
	If yes, does the training record include the following details:		
	(a) which staff has been trained		
	(b) when the staff received training		
	(c) the type of training provided		
	Do you monitor and maintain the effectiveness of the training conducted by staff by:		
	(a) testing staff's understanding of the LC's / AE's policies and procedures to combat ML/TF		
	(b) testing staff's understanding of their statutory and regulatory obligations		
	(c) testing staff's ability to recognize suspicious transactions		
	(d) monitoring the compliance of staff with your AML/CFT systems as well as the quality and quantity of internal reports		
	(e) identifying further training needs based on training / testing assessment results identified above		
(I) Wire Transfers			
	Do you ask for further explanation of the nature of the wire transfer from the customer if there is suspicion that a customer may be effecting a wire transfer on behalf of a third party?		
	Do you have clear policies on the processing of cross-border and domestic wire transfers?		

	If yes, do the policies address the following?		
	(a) record-keeping		
	(b) the verification of originator's identity information		
	Do you include wire transfers in your ongoing due diligence on the business relationship with the originator and the scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with your knowledge of the customer, its		

Annex 3

Controls Assessment Template

#	Controls	Weak	Satisfactory	Strong
1.	Governance Arrangements and Three Lines of Defense			
1.1	Written AML/CFT policies and procedures approved by			
1.2	Risk assessment reviewed and updated periodically			
1.3	Are policies, procedures and compliance program updated periodically?			
1.4	Oversight by the Board of Director and senior management			
2.	Three Lines of Defense			
2.1	AML/CFT Compliance Officer appointed			
2.2	Internal Audit Function			
2.3	Written policies and procedures communicated to all personnel			
2.4	Employee due diligence program			
2.5	Ongoing Employee Training Programs			
3	Program and Systems			
3.1	AML/CFT in a Group-Wide and Cross-Border			
3.2	Internal Procedures/system for Detecting and Reporting Suspicious Transactions			
3.3	Appropriate integrated management information systems			
3.4	Review of Exception Reports to alert Senior Management/ Board of Directors			
3.5	Mechanism for asset freezing and sanction			
3.6	Secrecy Privacy Of Information (Tip Off) ensured			
3.7	STR/CTR Cash generated and reported on timely			
3.8	Is there a procedure for independent review of AML/CFT program?			
4	Customer Identification, Verification and Acceptance Policy			
4.1	Written policies and procedures for CDD/KYC			
4.2	Approval by senior management before establishing business relationships with high-			
4.3	Customer due diligence programs			
4.4	Enhanced due diligence program for high risk customers			
4.5	Customer Risk Profiling			
4.6	Mechanism to review/update risk rating and profile of customers			
4.7	Systematic Procedure for Identifying and Verifying: a) Customers, b) Beneficial Owners, c) PEPs, d) Person acting on behalf, e) Geographic Verification			
4.8	Due diligence assessment of correspondent relationship			

#	Controls	Weak	Satisfactory	Strong
5	Ongoing Monitoring			
5.1	Transaction monitoring mechanism in place to detect unusual or suspicious transactions			
5.2	Screening of customer with database and changes to sanction lists			
5.3	Is transaction Monitoring System automated?			
5.4	Customer due diligence for existing customers			
6	Management of Information			
6.1	Customer identification, verification and due diligence information			
6.2	Record-keeping procedures allow for tracing transactions and provide a clear			
6.3	Are records maintained electronically?			

Annexure 4

RISK PROFILING OF CUSTOMER

The following sets out examples of factors that the Company will consider when performing initial risk assessment. Where there is one or more "yes" responses, professional judgment will be exercised with reference to the policies and procedures of the Company, as to the nature and extent of customer due diligence to be carried out.

For Internal Use

Section A: If the response to any of the statements in Section A is "Yes", the entity shall not establish business relationship with the client.		Yes / No	Remarks
1	Customer unable to provide all the required information in relevant forms		
2	Customer unable to provide identity document and source of funds		
3	Customer, Beneficial Owner of the customer, person acting on behalf of the customer, or connected party of the customer matches the details in the following a. Proscribed under the united nations security council resolution and adopted by the government b. Proscribed under the Anti-Terrorism Act 1997		
4	There is a suspicion of money laundering and/or terrorist financing		
	Section B; Customer Risk Factor		
1	Is the customer, any of the beneficial owners of the client or person acting on behalf of the customer, a politically exposed person (PEP), family member of a PEP or close		
2	Is the Customer non-resident Pakistani?		
3	Is the Customer foreign national?		
4	Is the Customer High net worth individual?		
5	Legal Person - Companies – Local - Companies - Foreign - Foreign Trust or Legal arrangements - Local Trust or Legal arrangements - Partnerships - NGOs and Charities - Cooperative Societies		
6	Intermediaries e.g. Third parties acting on behalf of customers (Lawyers, Accountants etc.)		
7	Performed further screening of details of customer, beneficial owner of the customer, person acting on behalf of the customer, or connected party of the customer against other information sources, for example, Google, the sanction lists published and/ or other third party		
8	Customer's source of wealth/ Income is high risk/ cash intensive		

9	Does the stated source of wealth / source of funds and the amount of money involved correspond with what you know of your customer?		
	Section C Country / Geographic Risk Factors		
1	Is the customer, beneficial owner of the customer or person acting on behalf of the customer from or based in a country or jurisdiction:		
	a. Identified as High-risk jurisdiction by the FATF and for which entity should give special attention to business relationships and transactions. (Countries having weak governance, law enforcement, and		
	b. Countries subject to sanctions, embargos or similar measures issued by international authorities (E.G.UN, WB.IMF)		
	c. Countries where protection to customers, privacy prevents effective implementation of AML/CFT requirements and/or facilitates the framework for establishment of shell-		
	d. Countries/ Geographies identified by recognized sources as having significant levels of organized crime, corruption or criminal activity.		
	e. Countries / Geographies identified by recognized sources as providing funding or support for terrorist activities or have terrorist organizations operating within them		
	Section D: Services/ Transactions Risk Factors		
1	Is the business relationship with the customer established through non face to face channel?		
2	Significant and unexplained geographic distance between residence in business location to the customer and the location where the product sale took place (or the location of the insurer'		

Sectio E: Customer Risk Assessment

☐ Low - Simplified ☐ Medium – Standard CDD ☐ High – Enhanced CDD

Document reasons for customer risk rating

Section F: Recommendation

☐ Accept customer ☐ Reject customer

Assessed by: Signature: Date:	Approved by Designation: Signature: Date:

Annex 5

ML/TF Warning Signs/ Red Flags

The following are some of the warning signs or "red flags" to which the Company should be alerted. The list is not exhaustive, but includes the following:

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 banker's 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.
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.

Annex 6

#	Type of Customer	Information/Documents to be Obtained
1	Individuals	A photocopy of anyone of the following valid identity documents; (i) Computerized National Identity Card (CNIC) issued by NADRA. (ii) National Identity Card for Overseas Pakistani (NICOP) issued by NADRA. (iii) Pakistan Origin Card (POC) issued by NADRA. (iv) Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). (v) Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2	Sole proprietorship	(i) Photocopy of identity document as per Sr. No.1 above of the proprietor. (ii) Copy of registration certificate for registered concerns. (iii) Copy of certificate or proof of membership of trade bodies etc., wherever applicable. (iv) Declaration of sole proprietorship on business letter head. (v) Account opening requisition on business letter head. (vi) Registered/ Business address.
3	Partnership	(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.
4	Limited Companies / Corporations	(i) Certified copies of: (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; (c) Certificate of Incorporation; (d) Certificate of Commencement of Business, wherever applicable; (e) List of Directors on 'Form-A/Form-B' issued under Companies Act, 2017, as applicable; and (f) Form-29, wherever applicable. (ii) Photocopies of identity documents as per Sr. NO.1 above of all the directors and persons authorized to open and operate the account;
5	Branch Office or Foreign Companies	(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) A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account. (v) Branch/liaison office address.

6	Trust, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Certificate of Registration/Instrument of Trust (b) By-laws/Rules & Regulations (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. (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. (iv) Registered address/ Business address where applicable.
7	NGOs / NPOs / Charities	(i) Certified copies of: (a) Registration documents/ certificate (b) By-laws/Rules & Regulations (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. (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. (iv) 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. (v) Registered address/ Business address.

Annex 7

Proliferation Financing Warning Signs/Red Alerts

Company will take note of the following circumstances where customers and transactions are more vulnerable to be involved in proliferation financing activities relating to both DPRK and Iran sanctions regimes:

(a) customers and transactions associated with countries subject to sanctions;

In particular, Company will be alerted to the following non-exhaustive list of factors that are relevant to the DPRK sanctions regime:

(a) significant withdrawals or deposits of bulk cash that could potentially be used to evade targeted financial sanctions and activity-based financial prohibitions;

(b) opening of banking accounts by DPRK diplomatic personnel, who have been limited to one account each under relevant UNSCRs (including number of bank accounts being held, holding of joint accounts with their family members);

RESOLUTION OF THE BOARD OF DIRECTORS

Annex 8

The Board of Directors of M/s Asad Mustafa Securities (Pvt.) Ltd. on November 22, 2019 passed the following resolution through circulation;

Resolution

"Resolved that the KYC and AML/CFT Policy of M/s Asad Mustafa Securities (Pvt.) Ltd. along with the amendments and updates stands approved and is adopted with immediate effect.

"Signed by CEO on Hard Copy"
Asad Ali Khan
CEO