POLICY DOCUMENT ON;

- Know Your Customer
- Client Due Diligence
- Anti-Money Laundering and
- Countering Financing of Terrorism
- Including National Risk Assessment of Money Laundering (ML) and Terrorist Financing (TF) - 2019 Update.

Prepared by: Compliance Department
Fortune Securities Limited

Table of Contents

Document Name	Policy Document on Know Your Customer, Client Due Diligence, Anti-Money Laundering & Countering Financing of Terrorism.		
Reviewed By:	Chief Executive & CO		
Approved By:	To be approved by BOD in upcoming meeting	**Approval Date:**	-

1. Introduction

This policy is prepared under the Guidelines issued by Securities and Exchange Commission of Pakistan on Anti-Money Laundering (AML) and Countering Financing of Terrorism (CFT) Regulations, 2018. As a regulated person, FSL is required to adopt and effectively implement appropriate Money Laundering (ML) and Terrorist Financing (TF) control processes and procedures as described in Guidelines, to develop an effective AML/CFT risk assessment and compliance framework to maintain the integrity of in respect of preventing, detecting and combating ML/TF & reporting suspicious activities.

2. Objectives

The objective of this policy is to ensure that the services of Fortune Securities Limited (FLS) "the Company" are not used to launder the proceeds of crime and that all staff of FSL is aware of their obligations and the need to remain vigilant in the fight against money laundering and terrorist financing. Further to perform overall entity level risk assessment in relation to ML and TF. The document also provides a framework to comply with following applicable Laws, Regulatory Guidelines specially related with detection and reporting of suspicious activities.

- Securities Act, 2015 and related regulations issued hereunder;
- PSX Rule Book,
- Anti-Money Laundering Act, 2010, and
- Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations 2018.
- International best practices recommended from Financial Action Task Force (FATF) published in February 2012. http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)
- Guidelines on SECP (AML & CFT) Regulations, 2018 issued by SECP in September 2018.
- Pakistan National Inherent Risk Assessment on Money Laundering and Terrorist Financing -2019 Update

-

3. Scope

This policy is applicable to all operations of Fortune Securities Limited including business of other Financial Institutions routed through the Company in order to ensure compliance with the Regulations of the country on KYC, CDD AML/CFT or that of the SECP, and recommendations of FATF.

4. FSL insight towards AML / CFT Compliance

FSL has used SECP Guidelines of Anti-Money Laundering, Countering Financing of Terrorism, and Proliferation Financing to formulate its own AML & CFT Policy. The consequence of contravening the Regulations or failing to comply can be significant and include disciplinary measures, imprisonment or fine or both under local laws as well as the loss of reputation.

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

- Reputational
- Operational
- Legal
- Financial

5. Responsibilities

- ***Responsibility of Board of Directors:***

Board of Directors of FSL is cognizant to the implications of AML contravention and effect on reputation of the Company. To be utmost compliant to this AML Policy, the board will oversee and ensure the effective implementation of the Policy.

Further, the Board shall periodically review significant AML updates and in order to discharge its responsibility, the Board will:

(a) Authorize the CEO to implement AML CFT Policy
(b) Receive periodic reports summarizing the outcome, updates, challenges and STR / CTR reporting.
(c) Approve the Policies including any amendments/addendums on post-facto basis.

- ***Responsibility of Compliance Department:***

Compliance officer shall be responsible for:

(a) Periodic review of the policy
(b) Reporting of suspicious transactions activities to CEO, Board & FMU (if need arises)

- ***Responsibility of All Staff:***

All FSL staff shall be responsible for:

(a) Understanding Money Laundering, its implications and AML policy.
(b) Escalating any and all transactions which they feel are suspicious to the best of their knowledge and ability.

6. Our Obligations being a Regulated Person

Being a regulated person of SECP, FSL is required to establish an effective AML /CFT Governance and Compliance Regime, which includes but not limited to:

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

ii. Board of Directors and senior management of FSL be engaged in decision makng on Anti-Money Laundering & Countering Finance of Terrorism policies, procedures and controls and take ownership of the risk based approach.

iii. Establishing and maintaining an effective AML/CFT compliance culture and adequately train staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations.

iv. Establish written internal procedures so that, in the event of a suspicious activity being discovered, FSL employees are aware of the reporting chain and the procedures to be followed. Such procedures should be periodically updated to reflect any legislative changes.

v. To oversee the compliance function, who shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit (FMU).

vi. Ensure that all suspicious transactions intimated by employees to the Compliance officer.

vii. Ensuring that employees should be aware of their reporting obligations and the procedure to follow when making a suspicious transaction report.

7. Main areas to combat Money laundering & Terrorism Financing

The above obligatory requirements would be met by FSL using the following deterrents factors:

Areas of Combating	Tools	Deterring action
Customer Dealing Personnel	- Policies & procedures contain guidance for employee obligations towards detecting, monitoring and reporting suspicious transactions.	- To carry out due diligence of customers, their countries, jurisdictions, transactions to deter ML / CFT risks
Compliance Function	- Skills and experience to develop and maintain systems and controls. - Sufficient resources and support staff. - Access to all information necessary to perform AML/CFT compliance	- Must have authority and ability to evaluate system to combat ML / CFT. - Provide guidance in day-to-day operations of AML / CFT polices & procedures - Reports directly and periodically to the Board of Directors on AML/CFT systems and Controls - Ensure regular audits of AML/CFT areas. - Keep records of PEPs, and request from Commission, FMU, & LEAs.
Internal Audit Function	- TORs approved by Board covering AML & CFT. - Guidelines issued by SECP for ML & CFT. - FSL policies and procedure - Auditing requirements applicable to AML & CFT measures.	- Periodically conduct AML/CFT audits. - Direct report to Board and seek prompt feedback from it. - Proactive follow-ups on findings.

8. Know Your Customer (KYC)

Policy & Guideline

a. Every customer individual or institution who wishes to open trading account with FSL, must provide the required documents as described in our account opening form. Any other additional document may be needed if the identification of customer requires more evidence. No anonymous or obviously fictitious account ought to be opened. It is important to find out and document in broad terms what does the customer intend to do. For example, are there any specific sectors or stocks that the customer does not wish to participate in; is the customer intending to invest for short-term only or longer term only; will investment be only in liquid scrips or any scrip; or any other special needs or requirements of the customer.

b. Obtain customer's other information such as age, gender, occupation, knowledge of market, etc. This will help us to develop a sense of the risk taking capacity and profile of the customer and thus

guide the customer in more effective manner. It will also help us to understand whether the customer should be classified as a low risk or a high risk customer from the KYC /CDD perspective. For example, a domestic customer working in a company with regular income would be low risk category; on the other hand, a government employee may be in a higher risk category because of the potential for conflict of interest; or a foreign organization having foreign currency sources would be in high risk category requiring more careful identification procedure and close monitoring of account operations.

c. In case of corporate clients, a careful care has to be taking to know the ownership and controlling parties. Authorization of person who is authorized to operate the account on company's behalf must be checked.

d. Ensure that accounts of institutions (Private as well as Public) should not be opened in names their employees, officers /Officials in individual capacity.

e. Physical presence of the account opener/authorized representative is necessary at the time of opening any account. In the case of non-resident /overseas customers or customers in other cities, following actions should be adopted

- Verification by a reliable third party,
- Verification by NADRA Verysis System
- Reference of an existing customer
- Confirmation from another broker with whom the customer had an account

9. Risk Evaluation and Alleviation Process at FSL

In order to identify, assess and evaluate the risk(s) related to customers, countries & activities and mitigation thereof; a comprehensive risk based approach has been developed. FSL adopts the following framework:

9.1. Risk Assessment
9.2. Applying Risk Based Approach to mitigate ML and TF Risks
9.3. Customer Due Diligence
9.4. Enhanced Due Diligence
9.5. Politically Exposed Persons (PEPs)
9.6. Simplified Due Diligence
9.7. Reporting of Suspicious Transactions Reports /Cash Transactions Reports
9.8. Monitoring Systems and Controls
9.9. Documentation and Reporting
9.10. Compliance Function
9.11. Screening and Training Employees
9.12. Record-keeping Procedure
9.13. Sanction Compliance
9.14. Internal Audit Function

9.1. *Risk Assessment*

Following risk factors would be considered while assessing the risk.

High-Risk Factors	Indicator / Area prone to ML/CFT Risks
Related to Customer	- Non-resident/Foreign Clients - Legal person or arrangement - Geographic distant customers - Companies that have nominee shareholders - Cash-intensive business - Unusual or complex ownership structure - Politically Exposed Persons (PEPs) - Shell companies - Trusts - Splinter Groups associated with Talban & Daesh - Criminal Groups - Quantum of business does not match with the profile of client. - Whether client has been met in person? - Private Companies using formal (contractual) or informal nominee shareholders or directors where nominator identity undisclosed; - Domestic Limited Liability Partnership - Foreign Limited Liability Partnership - Importers/Exporters - Real Estate Dealers - Illegal Money Value Transfer Services & Cash Couriers - Wife of Proscribed Person (Also check the CNIC of husband of Housewife client in order check any link of proscribed person
Related to Countries or Geographic area of customer	- Countries identified by credible sources such as published follow-up reports by FATF as not having adequate AML/CFT systems - Countries subject to sanctions, embargos or similar measures by United Nations. - Countries identified by credible sources as having significant levels of corruption or criminal activity - Pakistan Porous Border Areas - Vulnerable Areas Highlighted in NRA 2019 - NPOs (based in Kuwait, Egypt, Qatar, KSA, Germany, Switzerland and sending funds to local Madrassas/local NPOs
Related to Product, Services,	- Cash transactions - Non-face-to-face business relationship or transactions - Payments received from third party (Un-associated person)

transactions and delivery channel	- International transactions involving high volumes of currency - One-off transaction - Wire Transfers - Western Union - Money Gram - Online Transactions - Branchless banking - Microfinance Banks - Virtual Currencies / VC Exchanges - Central Directorate of National Savings - Hawala / Hundi - Pakistan Post
Low-Risk Factors	**Indicator / Area prone to ML/CFT Risks**
Related to Customer	- Regulated person and banks consistent with FATF recommendations - Public listed companies that are subject to regulatory requirements to ensure adequate transparency of beneficial ownership.
Related to Country.	- Countries identified by credible sources such as mutual evaluation or detailed assessment reports, as having adequate AML/CFT systems. - Countries identified by credible source as having a low level of corruption or crimes.
Related to Product, Service, transaction or delivery channels	- Financial products or services, that provide appropriately defined and limited services to certain types of customer, so as to increase access for financial inclusion purposes.

NATIONAL RISK ASSESSMENT FOR MONEY LAUNDERING AND TERROIST FINANCING - 2019

INHERENT RISK ASSESSMENT

The inherent ML/TF risk assessment considers the ML/TF threats and inherent vulnerabilities of Pakistan as a whole through a coordinated approach

A - The assessment of ML / TF threats include:

a) A review of all crimes - A threat analysis concerning all crimes 23 ML threats were rated.

High	Medium-high	Medium	Medium low
1. Illicit Trafficking in Narcotic Drugs 2. Corruption and Bribery 3. Smuggling, 4. Cash Smuggling, 5. Tax Crimes 6. Illegal MVTS, 7. Terrorism/TF	1. Organized Crime 2. Human Trafficking, 3. Arm Trafficking, 4. Robbery 5. Market Manipulation 6. Cybercrime 7. Fraud and forgery, 8. Kidnapping 9. Extortion	1. Sexual Exploitation 2. Trafficking of Good 3. Counterfeiting Currency 4. Piracy of Products 5. Murder	1. Environmental Crime 2. Marine Piracy.

b) Amount of potential proceeds generated

c) Capacity of the criminal actors to launder proceeds

d) Sectors used to launder proceeds

B - The assessment of inherent ML/F vulnerabilities

a) financial sectors

Highly Vulnerable	Medium-high	Medium	Low
1. Banking, 2. Microfinance banks, 3. Exchange Companies 4. EC B category, 5. Real Estate Dealers, 6. Hawala/Hundi, 7. Central Directorate of National Savings 8. Pakistan Posts 9. NPOs 10. Unlisted Legal Entities	1. Lawyers & Notaries 2. Securities, 3. AMCs & CISs 4. Dealers in Precious Metals 5. NBFCs & Modaraba	1. life insurance 2. Auditors 3. Accountants	1. Non-life insurance 2. Development Financial Institution (DFIs)

b) Others factors include;

Porous border.

Hostile neighborhood

High number of afghan migrants

Long coastal line

The level of poverty

9.2. Risk-based approach to mitigate ML and CFT Risks

Money Laundering and Counter Financing of Terrorism risks mitigation depends on risk tolerance which impacts the mitigation measures and controls. Establishment of risk tolerance within FSL is to be done by senior management and the Board considering the sufficient capacity and expertise to manage the risks along with the consequences of compliance failure.

All policies, procedures and controls related to ML & CFT risk mitigation would be reviewed and approved by senior management. Policies and controls should be consistent with legal and regulatory requirements of FSL and will depend on Nature, scale, geographical diversity, customer profile, volume of transactions, & extent of reliance on third parties.

Following are some mitigating measures which FSL will follow:

i. Determine the scope of identification and verification requirements according to risk posed by customer.
ii. Setting transaction limits for higher-risk customers.
iii. For high-risk customer/transactions including PEPs, senior management approval is taken.
iv. Determining the circumstances wherein high-risk customer may be refused.

Risk identified and assessed may change due to changes in risk factors, such as changes in customer conduct, development of new technologies, new embargo and new sanctions. To assess the effectiveness of risk mitigation procedures and controls following areas should be monitored:

i. Changes in customer profile
ii. Potential for abuse of product and services to be used for ML / TF purposes.
iii. Adequacy of employees' trainings and awareness
iv. Adequacy of internal coordination mechanism between Compliance and other functions at FSL
v. The performance of third parties (when required) who were relied on for CDD purposes
vi. Changes in relevant laws or regulatory requirements and their adoption and implementation.
vii. Changes in the risk profile of countries of customers

In order have appropriate mechanism to provide risk assessment information to the Commission, FSL documents the following:

i. ML / TF risk assessment system
ii. Evidence of implementation of systems and procedures for risk mitigation including due diligence requirements
iii. Monitoring and improvement in the effectiveness of systems and procedures
iv. Arrangement for reporting to the Board /senior management regarding results of ML/TF risk assessment and mitigation
v. Maintain AML / CFT Compliance Assessment Checklist **(Annexure-3).**

9.3. *Customer Due Diligence*

This is the policy of FSL that it will not open or maintain any anonymous or fictitious account. When there is doubt about the veracity or adequacy of previously obtained customer identification data, or there is a suspicion / red flags warning mentioned in **Annexure-4**, CDD measures would be applied which include the following:

(a) Identifiction and verification of the customer including beneficial ownership on the basis of documents, data or information obtained from customer and from reliable and independent sources;

(b) Understanding and, obtaining information on the purpose and intended nature of the business relationship; and

(c) Monitoring of accounts/transactions on on-going basis to ensure that the transactions being conducted are consistent with the FSL knowledge of the customer, the customer's business and risk profile **(Annexure-2)**, including the source of funds and updating records and data/information to take prompt action when there is material departure from usual and expected activity through regular matching with information already available with FSL.

(d) FSL will obtain such documents from different types of customer as provided in **Annexure -1**.

Determine whether the person is acting on behalf of a customer and should take reasonable steps to obtain.

(i) Evidence to determine authority of such person to act on behalf of the customer, which shall be verified through documentary evidence including specimen signature of the customer;

(ii) Identification and verification of the person purporting to act on behalf of the customer.

(iii) Identification and verification of the customer.

(e) Each customer shall be categorized as high or low risk, depending upon the otcome of the CDD process;

(f) When FSL has reason to believe that a customer has been refused by an other brokerage house due to concers over illicit activities, that customer shouldl be classifyed as higher-risk and apply enhanced due diligence procedures. FSL will maintain a list of all such customers where the business relationship was refused or needed to be closed on account of negative verification;

(g) if the CDD measure could not be completed satisfactorily, the account shall not be opened or if already opened, the relationship should be treated as high risk and reporting of suspicious transaction with FMU will be considered with the approval of senior management.

(h) If there is doubt of money laundering or terrorist financing activity by any customer, and it is believed that initiating CDD process will tip-off the customer, FSL will not persue CDD process rather tile STR with the approval of senior management.

(i) Government entities accounts shall not be opened in the personal names of the government officials and account which is to be operated by an officer of the Federal or Provincial or Local Government in his/her official capacity, shall be opened only on production of a special resolution or authority from the concerned administrative department or ministry duly endorsed by the Ministry of Finance or Finance Department/Division of the concerned Government. Any rules,

regulations or procedures prescribed in the governing laws of such entities relating to opening and maintaining of their bank accounts should be taken into consideration.

If the customer is a legal person, In addition to above measures, FSL takes the following specific measures:

i. Understnd the nature of customer's business and its ownership and control structure

i. Identify and verify the identity of the natural persons (whether acting alone or together) who ultimately own the legal person by obtaining relevant information from the customer;

ii. Where there is doubt as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person; and

iii. Where no natural persons are identified, identify the natural persons having executive authority in the legal person, or in equivalent or similar positions.

9.4. Enhanced Due Diligence

FSL will apply Enhanced Due Diligence (EDD) on the customers that are identified as high risk. circumstances where a customer presents high risk of ML/TF include but are not limited to the following-

i. Customers belonging to countries which are non-compliant with anti-money laundering regulations according to FATF.
ii. Such body corporate, partnership, associations and legal arrangements including non-government organization or not-for-profit organization which receive donations; and
iii. Legal persons or arrangements with complex ownership structures.

Enhanced Due Diligience measures include but are not limited to the following:

i. Obtain approval form senior management to establish or continue business relations with the such customers,
ii. Obtain additional information of customer related to occupation, volume of assets, and information availabe by public database.
iii. Update regularly the identification data of customer and beneficial owner if any;
iv. Obtain additional information on the intended nature of the business relationship
v. Establish, by appropriate means, the sources of wealth and/or funds or beneficial ownweship of funds.
vi. Obtain additional information on the reasons for intended or performed transactions.
vii. Conduct during the course of business relations, enhanced monitoring of business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
viii. Where customer hesitate to receive any correspondence to his mailing address, FSL perfoms identity procedures and keep monitor and review these types of "Hold Mail" accounts.

9.5. Politically Exposed Persons (PEPs)

PEPs are the persons holding important public positions and include heads of state, ministers, influential public officials, judges and military commanders including their family members and close associates either socially or professionally.

Relationship with these PEPs exposes reputational risks, and extra information requests from law enforcement or judicial authorities including seizure order of these account. This creats lack of confidence by public investing in brokerage industry.

FSL is more vigilant in establishing relationship with PEPs and has following controls while dealing with these PEPs.

i. Apply additional Identification procedures to determine whether the customer is a politically exposed person;
ii. Obtain senior management approval for establishing business relationships with such customers;
iii. Take reasonable measures to establish the source of wealth and source of funds; and
iv. Conduct enhanced ongoing monitoring of the business relationship.

Senior management approval is obtained to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP.

In assessing the ML/TF risks of a PEP, FSL shall 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 FSL shall consider include:

(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.

9.6. Simplified Due Diligence

a. FSL shall apply simplified or reduced CDD measures in the following **circumstances** in order to guard against money laundering activities.

   i. Risk of money laundering or terrorist financing is lower
   ii. When the information regarding identity of the customer and beneficial owner of a customer is publicly available
   iii. Adequate checks and controls exist
   iv. Financial institutions which are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those controls.
   v. Public companies that are subject to regulatory disclosure requirements
   vi. Government administrations or enterprises

b. Normally regulated customers such as Banks, Public Listed Companies, Modaraba, NBFC, & Insurance Companies are considered as low risk customers but proper risk analysis is required to justify the simplified due diligence (SDD). Unless there is suspicion of money laundering or terrorist financing, FSL applies following **measures** of simplified due diligences:

i. Reducing the frequency of customer identification updates.
ii. Rely on third parties for verifying the identity of customer and beneficial owners.
iii. Reducing degree of on-going monitoring and scrutinizing transactions, based on reasonable monetary threshold.
iv. Not collecting specific information.

Review Period

Category of initial Due Diligence	Recommended Review
Simplified	After three years
Standard	After two years
Enhanced	After one year*

* If there are continued red flags in trading activities, then the Enhanced CDD will be immediately triggered

9.7. Reporting of Suspicious Transactions / Currency Transaction Report

Reporting of suspicious or unusual transactions involves some procedures which FSL adopt before reporting STRs or CTRs.

- *Identifying the Suspicious transactions:*

STRs or CTRs are generated and reported for any suspicious or unusual transactions which include:

- Transaction which is inconsistent in amount, origin, destination, or type with a customer's known, ligitimate activities or with the normal business.
- Complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.
- Investigation / inquiries conducted do not provide satisfactory explanation of the transactions.
- Cash-based transaction involving payment, receipt, or transferred of Rs. 2 million and above.

- *Investigatiing the Suspicious transactions:*

Once suspicion has been establish related to any customer or transaction, appropriate action is taken to adequately mitigate the risk associated with this suspicious activity which could be used for money laundering or terrorism financing. This may include review of customer risk profleor review of relationship.

- *Reporting of suspicious or unusual transactions:*

FSL has process to raise and report all suspicicous transactions to Board/CEO for getting approvalof senior management. Once senior management /Board approves the filing of any STRs or CTRs, compliance officer initiate to report such unusual transactions to FMU .

As required by Anti-money Laundering and Countering Financing of Terrorism Regulations 2018, FSL will intimate to the SECP on bi-annnual basis the total number of STRs reported to FMU. A status report of STRs so reported; will reach to AML Department of the Commission within seven days of close of each half year. The Compliance officer will ensure prompt reporting in this regard.

All reports made to FMU, should be entered in a register and contents of this register will be as follow:

(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.

FSL will keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed. In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, a STR tp FMU may be raised.

Following is the process of raising and reporting STRs & CTRs:-

Compliance officer will highlight a suspicious transaction/series of transactions/attempted transactions to the CEO. Compliance officerr can identify any such transaction through:

- Escalation of any suspicion by a dealer
- Escalation of any suspicion by settlement
- Escalation of any suspicion by Fortune Online advisors

The CEO will take the final decision for reporting the suspicious transaction after consultation with Compliance officer, relevant dealer/advisor, settlement team and any other person/entity which the CEO deems necessary.

In order to take this decision the CEO can, and may, use all private and public information at his disposal to establish suspicion.

Once CEO approves a transaction/series of transactions/attempted transactions to be suspicious, the Compliance officer will report them on the format attached as annexure 1 to FMU within 7 days of CEO's approval.

9.8. Monitoring Systems and Controls

Due to changes in circumstances or factors, identified and assessed risks may change which may include changes in customer conduct, development in new technologies, new embargoes and new sanctions. FSL updates its systems of controls in order to cope with changes in circustances, factors and changes in risks. In order to check the effectiveness of existing risk mitigation cotrols and areas for improvements, FSL contineously monitors the folloiwng aspects:

1) System's ability to identify changes in a customer profile or transaction activity/behaviour, which come to light in the normal course of business;
2) Unusual transactions and activities in normal course of business which could be abused and may be used for ML/TF purposes.
3) the adequacy of employee training and awareness;
4) the adequacy of internal coordination mechanisms i.e., between Compliance and other departments.
5) the compliance arrangements (Compliance audit)
6) the performance of third parties who were relied on for CDD purposes (if any)
7) changes in relevant laws or regulatory requirements; and
8) changes in the risk profile of countries to which its customers belong to.

9.9. Documentation and Reporting

FSL maintains proper documentation of each and every aspect of risk-based methodology towards customers profile, risk assessment, customer identity, relevant policies & procedures, review results, non-compliances, & reporting to Regulators. Completeness and appropriatness of documents ensures that FSL:

(a) Has proper risk asessment systems related to Money Laundering and Terrorist Financing.

(b) Has proper due diligence performed keeping in the light of risk assessment.

(c) Monitors the effectiveness of existing systems and procedures and improvement thereof;

(d) Has arrangements for reporting to senior management on the results of ML TF risk assessments and the implementation of ML/TF risk management systems and control processes.

(e) Timely reporting of STRs / CTRs to the FMU, Commission or any other Regulatory authority when required.

(f) Has policy to reviews the ML/TF risk management processes annually, this review period may be curtail depending upon the situation.

(g) Also reviewes the appropriatness /adequacy of procedures and controls of opening & closing of high-risk customers.

(h) Has procedures and policies concerning customer identification and verification; its ongoing monitoring and all measures taken in the context of AML/CFT.

(i) FSL adopts and maintains the AML / CFT Compliance Assessment Checklist, **Annexure-3** for the specific period as and when required by the Commssion.

(j) The company shall report total number of STRs, if any, filed to the Commission on bi-annual basis within seven days of close of each half year.

9.10. Compliance Function

FSL is equipped with a proper Compliance department, supervised by a qualified Compliance Officer, who has enromous experience of capital market. He holds a senior management level position in FSL. Our Compliance Office reports directly to the Board of Directors and in some circumstnces to CEO. He is responsible for the areas but not limited to:

(a) Effective compliance with the relevant provisions of SECP Anti-Money Laundering and Countering Financing of Terrorism Regulations, the AML Act, the Anti-Money Laundering Rules, 2008, and other directions and guidelines issued under the aforementioned regulations and laws, as amended from time to time;

(b) ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors and are effectively implemented;

(c) Monitoring, reviewing and updating AML/CFT policies and procedures,

(d) Providing assistance in compliance to other departments

(e) Timely submission of accurate data as required under all applicable laws;

(f) Monitoring and timely reporting of Suspicious and Currency Transactions to FMU;

(g) Preparing monthly Compliance Reports and submit to the Board of Directors.

(h) Maintain records of all violation /non-compliance identified and reported to the Board of Directors and are available for the inspection of Commission and PSX as and when required.

9.11. Screening and Training

In order to screen and train the employees; FSL has Human Resource policy and procedures to be applied at the time of hiring the emplyees.This shall include but not limited to verification of antecedents and screening procedures to verify that person being hired has a clean employment history. Following may be verfied:

- Reference provided by the prospective employee at the time of recruitment
- Employee's employment history, professional membership and qualifications.
- Details of any regulatory action(s) taken by professional body against him/her.
- Details of any criminal convictions; and
- Whether the emplyee has any connection with the sanctioned countries or parties.

Every employee of FSL is provided initial training and policy document on Anti-money Laundering and Countering Financing of Terrorism.

Suitable training program (internally or outside the office) are arranged for for relevant employees on annual basis. This enables the employees to understand money laundering and financing of terrorism techniques, method and trends along with their responsibilities towards AML & CFT.

Every staff member is encouraged to provide a prompt and adequate report of any suspicious activities.

All new employees are appraised regarding their legal obligation to report ML/TF activities.

FSL has a plocy to obtain an undertaking **(Annexure-6)** from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the FSL's AML & CFT policy, procedures, and understand the AML/CFT obligations under the relevant legislation.

Staff responsible for opening new accounts or dealing with new customers are encouraged verify the customer's identity, for new and existing customers.

Staff involved in the processing of transactions receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff is aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed.

FSL's directors and Senior Management personnel understand their statutory duties. They are given higher level training covering all aspects of AML/CFT procedures. .

The Compliance officer take is entitled to receive in-depth training on all aspects of the Anti-Money Laundering & Terrorist Financing. He is also encouraged to receive appropriate initial and ongoing training on the investigation, determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

9.12. Record-keeping procedures

FSL maintains all cutomer related documents during the relationship and for five years after termination of relationship. These records may be requested by the Regulator or Authorities to be used as an evidence for prosecution of criminal activity by customer. Where the transactions, customers, or accounts invlove any degal proceedings, these documents may be retained for longer period. Documents include but not limited to the following which FSL maintains records of:

Hard copey and scan copy of account opening form of client and all attached documents
Results of any analysis undertaken
Records of identification data obtain through CDD
Business Correspondence with customers
Records/documents related to beneficial ownership
Records of any litigation or investigation related to client.

Where documents related to any suspicous activity, investigation or litigation concerning any client, must be retained until the matter is resolved.

9.13. Sanction Compliance

This is the policy of FSL not to develop business relationship with those clients (individuals, entities & their associates) who are mentined in Anti-Terrorism Act, 1997 and are sanctioned under United Nation Security Council (UNSC) Resolution adopted by Pakistan.

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

Government of Pakistan publishes Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 in the official Gazettes to give effect to the decisions of the UNSC Sanctions

Committee and implement UNSC sanction measures in Pakistan. The regularly updated consolidated lists are available at the UN sanctions committee's website, at following link;

www.un.org/sc/committees/1267/aq_sanctions_list.shtml
https://www.un.org/sc/suborg/en/sanctions/1988/materials
https://www.un.org/sc/suborg/en/sanctions/1718/materials
http://www.un.org/en/sc/2231/list.shtml
https://www.un.org/sc/suborg/en/sanctions/1718/prohibited-items

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

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

FSL to have its sanctions compliance programs, procedures, & controls entact to ensure the compliance to UNSC sanctions and Govt. of Pakistanin measures for ML & TF. The Company shall provide adequate sanctions related training to their staff.

The Company shall screen customers, beneficial owners, transactions, and other relevant parties to determine whether they are conducting or may conduct business involving any sanctioned person or person associated with a sanctioned person/country. In the event of updates to the relevant sanctions lists, the Company may discover that certain sanctions are applicable to one or more of their customers, existing or new.

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

The obligations/ prohibitions regarding proscribed entities and persons mentioned in the above lists are applicable, on an ongoing basis, to prescribed entities and persons or to those who are known for their association with such entities and persons, whether under the proscribed name or with a different name.

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

The Company is expected to keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not in these sanciton lists.

In case there is not 100% match but sufficient grounds of suspicion that customer/ funds belong to sanctioned entity/ individual, the Company may consider raising an STR to FMU.

9.14. Internal Audit Function

FSL has developed an effective Internal Audit department (IA) which is directly reportable to the Board. IA department proactively conducts periodic audits of ML / CF areas and adher to strict follow-ups on their findings. IA works on SECP's guidelienes of AML/CFT and FSL policies and procedures related to AML/CFt along with other auditing requirments applicable on AML /CFT measure.

Internal Audit department ensures the compliance to the AML / CFT Regulations, AML Act,UN Sanction list prohibitions,

The frequency of the audit should be commensurate with the company's nature, size, complexity, and risks identified during the risk assessments. The main areas of the audit shall include but not limited to:

The overall integrity and effectiveness of the AML/CFT systems and controls and compliance with relevant laws and regulations;

1. 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;
2. Employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
3. Completeness and adequacy of training programs
4. Emphasis on testing high risk areas identified in the organization
5. Adequacy of the process of identifying suspicious activities by employees and general controls to identify any ML/TF activities such as screening sanction lists.

10. Board Approval to the Policy Document

This draft policy document pertaining to KYC, CDD, AML, & CFT is to approved by our BOD in upcoming meeting.

Documents to be obtained **(Annexure – 1)**

Type of Customer	Information / Documents to be obtained
Individuals	A photocopy of any one 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)
Sole Proprietorship	(i) Photocopy of Computerized National Identity Card (CNIC) of proprietor issued by NADRA (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.
Partnership	(i) Photocopies of Computerized National Identity Card (CNIC) of all the partners issued by NADRA 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.
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 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 f) Photocopies of CNICs of all the directors and persons authorized to open and operate the account.
Branch Office or Liaison Office of Foreign Companies	(i) A copy of permission letter from relevant authority i.e. Board of Investments. (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 form Principal Office of the entity authorizing the person(s) to open and operate the account. (v) Branch / Liaison office address

Trusts, Clubs, Societies and Associations etc.	(i) Certified copies of: (a) Registration documents/Certificate (b) By-laws / Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustee / Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate account. (iii) Photocopy of CNIC of 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.
NGOs/NPOs/Charities	(i) Certified copies of: (a) Certificate of Registration / Instrument of Trust (b) By-laws / Rules & Regulations (ii) Resolution of the Governing Body/Board of Trustee / Executive Committee, if it is ultimate governing body, for opening of account authorizing the person(s) to operate account. (iii) Photocopies of CNIC of 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
Agent	(i) Certified copy of "Power of Attorney" of "Agency Agreement". (ii) Photocopy of CNICs of the agent and principal. (iii) The relevant documents / papers if agent or the principal is not natural person. (iv) Registered address /Business address
Executors and Administrators	(i) Photocopy of CNIC of the Executor / Administrator (ii) A certified copy of Letter of Administration or Probate. (iii) Registered address / business address.
Minor Accounts	(i) Photocopy of Form-B, Birth Certificate or Student ID card (as appropriate) (ii) Photocopy of CNIC of the guardian of the minor

Risk Profiling of Customer (Annexure – 2)

Risk factors should be considered when performing risk assessment. Where there is one or more "Yes" responses, professional judgement must be exercised, as to the nature and extent of customer due diligence to be carried out.

For internal Use

SECTION – A: if the response of any of the statements in Section-A is "Yes" FSL shall not establish business relationship with the client		**Yes/No**	**Remarks**
1.	Customer unable to provide all the required information in relevant forms		
2.	Information required to be verified as per the regulations, cannot be verified to independent and reliable documents		
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 lists: Proscribed under the united nations security council resolutions and adopted by the government of Pakistan; Proscribed under the Anti-Terrorism Act, 1997		
4.	There is suspicion of money laundering and/or terrorist financing		
SECTION-B: CUSTOMER RISK FACTORS			
1.	Is the customer, any of the beneficial owner of the client or person acting on behalf of the customer a politically exposed person (PEP), family member of a PEP or close associate of a PEP?		
2.	Is the customer non-resident Pakistani?		
3.	Is the customer foreign national?		
4.	Is the customer High net worth individual?		
5.	Legal persons:		
	(a) Companies – Local (b) Companies – Foreign (c) Foreign Trust or Legal arrangements (d) Local Trust or Legal arrangements (e) Partnership (f) NGOs and Charities		

	(g) Cooperative Societies		
6.	Intermediaries eg. 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 sanctions lists published and/or other third party screening database. Are there adverse news or information arising?		
8.	Customer's source of wealth/ income is high risk/ cash intensive		
9.	Does the customer have nominee shareholder(s) in the ownership chain where there is no legitimate rationale?		
10.	Is the customer a shell company?		
11.	Does the customer have unusual or complex shareholding structure (e.g. involving layers of ownership structure, different jurisdictions)?		
12.	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 FSL should give special attention to business relationships and transactions. (Countries having weak governance, law enforcement, and regulatory regimes). (b) Countries subject to sanctions, embargos or similar measures issued by international authorities (E.G. UN, WB, IMF). (c) Countries where protection for customers privacy prevents effective implementation of AML/CFT requirements and/or facilitates the framework for establishment of shell-companies. (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: SERVICE / TRANSACTION RISK FACTORS			
1.	Is the business relationship with the customer established through non face-to-face channel?		
2.	Has the customer given any instruction to perform a transaction (which may include cash) anonymously?		
3.	Has the customer transferred any funds without the provision of underlying services or transactions?		
4.	Are there unusual patterns of transactions that have no apparent economic purpose or cash payments that are large in amount, in which disbursement would have been normally made by other modes of payment (such as cheque, bank draft ect.		
5.	Are there unaccounted payments received from unknown or un-associated third parties for services and/or transactions provided by the customer?		
6.	Does the value of the transaction appear to fall within the financial means of your customer, given their income and savings?		
7.	Is there any divergence in the type, volume or frequency of services and/or transactions expected in the course of the business relationship with the customer?		
8.	Significant and unexplained geographic distance between residence or business location of the customer and the location where the product sale took place (or the location of the insurer's representative)		
9.	Customers seek or accept very unfavorable account/policy/contract provisions or riders and rely on free look up provisions		
10.	Customers transfer the benefit of a product to an apparently unrelated third party		
11.	Customer uses brokerage accounts as long term depository accounts for funds		
12.	Customer is conducting transactions that do not have apparent economic rationale		
13.	Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting Thresholds		
14.	Transactions involve penny/microcap stocks		

15.	Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation		
16.	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.		
17.	Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason		
18.	Customer trades frequently, selling at a loss		
19.	Customer invests in securities suddenly in large volumes, deviating from previous transactional activity		
20.	Cross border correspondent financial institutions relationships		
21.	Products/ Services		
22.	Transaction Amount		

SECTION – E: CUSTOMER RISK ASSESSMENT		
☐ Low – Simplified CDD	☐ Medium – Standard CDD	☐ High – Enhanced DD
Document reasons for cutomer risk rating:		

SECTION – F: RECOMMENDATON	
☐ Accept customer	☐ Reject customer
Assessed by:	Approved by:
Designation:	Designation:
Signature:	Signature:
Date:	Date:

AML/CFT Compliance Assessment Checklist *Annexure-3*

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. Note: *This AML / CFT Self-Assessment Checklist is neither intended to, nor should be construed as, an exhaustive list of all AML/CFT requirements.*

Sr. No.	*Question*	*Yes/No (N/A)*	*If No, provide explanation and plan of action for remediation.*
	(A) AML/CFT Systems		
1	RPs are required to assess their 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	RPs are 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 business		
	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 systems?		
	(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	RP 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) Risk-Based Approach ('RBA')

	(b) take additional measures to effectively mitigate ML/TF risks faced by them		
4	RPs are required to determine the extent of CDD measures and ongoing monitoring, using an RBA depending upon the background of the customer and the product, transaction or service used by that customer.		
	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 ('PEPs')		
	(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 be applied?		
	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	RPs are 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 trust		
	(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 resolution)		
	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	RPs are required to identify and take reasonable measures to verify the identity of a beneficial owner.		
	When an individual is identified as a beneficial owner, do you obtain the following identification information?		
	(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 ML/TF risks, so that you know who the beneficial owner(s) is?		
7	RPs are 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 requirements?		
	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	RPs are 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 authorities)		
	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 eliminated?		
9	RPs are 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	RPs are required to complete the CDD before establishing business relationships.		
	Do you always complete the CDD process before establishing business relationships? If you always complete CDD process before establishing a business relationship		
	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	RPs are 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	RPs are 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 registered and/or operating in Pakistan.		
	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	RPs are 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 reasons are not obvious?		
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 of the company?		
	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 of the ultimate beneficial owners?		
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	RPs 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 process is completed, rather than reducing what needs to be obtained, under a risk-based approach.		
	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	RPs are 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 ML/TF?		
	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	RPs are 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 account?		
	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	RPs are 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 arise?		
	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	RPs have 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 intermediaries that:		
	(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 CDD measures on behalf of you upon request.		
	When you use an intermediary, are you satisfied that it has adequate procedures in place to prevent ML/TF?		
	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 either domestic or 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	RPs are required to perform CDD measures on pre-existing customers when trigger events occur.		
	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 customer's funds		
	(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	RPs are 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 names?		
25	RPs are 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

	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 procedures to ensure that the ML/TF risk and basis of the relationship are fully understood?		
	Have you established procedures to conduct a review of a business relationship upon the filing of a report to the FMU and do you update the CDD information thereafter?		
27	RPs are 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 accounts or relationships		
	(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	RPs have 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 made		
	(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 TF?		
	(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 ML		
	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 been made known to it?		
	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	RPs are 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 FMU?		
	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 inquirey with customers an performing attitional or enhanced CDD process, committing the offence of tipping off the customer or any other person who is the subject of the disclosure		
	Do you provide sufficient guidance to your staff to enable them to form a suspicion or to recognise when ML/TF is taking place?		
	If yes, do you provide guidance to staff on identifying suspicious activity taking into account the following:		
	(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 RPs.		
	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: RPs are required to make prompt disclosure to FMU in any event, but the following requests are considered to be more urgent.		
	(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	RPs are 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 requirements?		
(H) - Staff Training			
31	RPs are 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 AML/CFT training?		
	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 respect to AML/CFT		
	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 instructions		
	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 business and risk profile?		

Money Laundering / Terrorist Financing Warning signs or Red Flag Signs Annexure - 4

The following are some of the warning signs or "red flags" to which FSL 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 bankers drafts, money transfers or other negotiable and readily marketable money instruments;
(14) Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
(15) Any transaction involving an undisclosed party;
(16) transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
(17) Significant variation in the pattern of investment without reasonable or acceptable explanation
(18) Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
(19) Transactions involve penny/microcap stocks.
(20) Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
(21) Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
(22) Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.

(23) Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
(24) Customer conducts mirror trades.
(25) Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

Employee Declaration for AML Policy — Annexure – 6

Date:	
Name:	
Date of joining:	
Designation:	
Department:	

I confirm that:

- ☐ I have read the AML Policy of Fortune Securities Limited
- ☐ I understand Money Laundering and its stages
- ☐ I understand the need to stop Money Laundering globally
- ☐ I understand the need for Fortune Securities Limited to make efforts to ensure FSL is not used by anyone for illegitimate purposes
- ☐ I fully understand the AML Policy adopted by FSL
- ☐ I will abide by the policy and highlight any/all suspicious transactions if witnessed by me

Employee Name : _____

Employee Signature : _____

Proliferation Financing Warning Signs/Red Alerts — Annexure - 7

FSL should 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;

(b) Instruments that could particularly be used to finance prohibited transactions, such as certain trade financing products and services;

(c) Customers involved with and/or transactions related to items, materials, equipment, goods and technology prohibited by UNSCRs;

(d) Reasonableness of invoiced goods against market value, inconsistency or discrepancies in trade-related documentation.

In particular, RPs should be alert 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);

(c) clearing of funds, granting of export credits or guarantees to persons or entities that are associated with trading transactions relating to the DPRK;

(d) providing insurance or re-insurance services to maritime vessels owned, controlled or operated, including through illicit means, by the DPRK or classification services to vessels which there are reasonable grounds to believe were involved in activities, or the transport of items, prohibited by UNSCRs concerning the DPRK, unless the Security Council 1718 Committee determines otherwise on a case-by-case basis;

(e) direct or indirect supply, sale or transfer to the DPRK of any new or used vessels or providing insurance or re-insurance services to vessels owned, controlled, or operated, including through illicit means, by the DPRK, except as approved in advance by the Security Council 1718 Committee on a case-by-case basis; or

(f) the leasing, chartering or provision of crew services to the DPRK without exception, unless the Security Council 1718 Committee approves on a case-by-case basisin advance; or

(g) using real property that DPRK owns or leases in Pakistan for any purpose other than diplomatic of counselor activities.

Definitions:

AML / CFT means Anti-Money Laundering and Countering Financing of Terrorism

Customer means any natural person, legal person or legal arrangement that applies for or maintains a trading account with the FSL.

Legal Person means entities other than natural persons whether incorporated or not or a legal arrangement that can establish a permanent customer relationship with FSL or otherwise own property and include companies, bodies corporate, foundations, limited liability partnerships (LLP) Partnerships or associations and similar entities.

Legal arrangements includes express trusts or any other similar legal arrangements.

High Net worth Customer for FSL, those customers who hold portfolio amounting to Rs. 2,000,000 at at any specific date or any person who traded of Rs. 10,000,000 during one month are treated as High Net worth customers.

Politically Exposed Persons (PEPs) includes foreign PEPs, individuals who are or have been entrusted with prominent public functions nu a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs, individuals who are or have been entrusted with prominent public functions nu a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization, means members of senior management and members of the board or equivalent functions.

Know your customer (**KYC**) is the process of a business 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
- 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 and terrorist financing.

Financing of Terrorism means financing of terrorist acts, and of terrorist and terrorist organization.

Risk based approach or RBA means applying measures to prevent or mitigate money laundering and terrorist financing risks that are commensurate with the risks identified.

Risk refers to Risk associated with money laundering and financing of terrorism.

All terms used in this policy document will have the same meaning as defined in Anti-Money Laundering Act, 2010, and Securities and Exchange Commission of Pakistan (Anti Money Laundering and Countering Financing of Terrorism) Regulations 2018.

NATIONAL RISK ASSESSMENT FOR MONEY LAUNDERING AND TERROIST FINANCING - 2019

INHERENT RISK ASSESSMENT

The inherent ML/TF risk assessment considers the ML/TF threats and inherent vulnerabilities of Pakistan as a whole through a coordinated approach

A - The assessment of ML / TF threats include:

b) A review of all crimes - A threat analysis concerning all crimes 23 ML threats were rated.

High	Medium-high	Medium	Medium low
8. Illicit Trafficking in Narcotic Drugs 9. Corruption and Bribery 10. Smuggling, 11. Cash Smuggling, 12. Tax Crimes 13. Illegal MVTS, 14. Terrorism/TF	10. Organized Crime 11. Human Trafficking, 12. Arm Trafficking, 13. Robbery 14. Market Manipulation 15. Cybercrime 16. Fraud and forgery, 17. Kidnapping 18. Extortion	6. Sexual Exploitation 7. Trafficking of Good 8. Counterfeiting Currency 9. Piracy of Products 10. Murder	3. Environmental Crime 4. Marine Piracy.

e) Amount of potential proceeds generated

f) Capacity of the criminal actors to launder proceeds

g) Sectors used to launder proceeds

B - The assessment of inherent ML/F vulnerabilities

c) financial sectors

Highly Vulnerable	Medium-high	Medium	Low
11. Banking, 12. Microfinance banks, 13. Exchange Companies 14. EC B category, 15. Real Estate Dealers, 16. Hawala/Hundi, 17. Central Directorate of National Savings 18. Pakistan Posts 19. NPOs 20. Unlisted Legal Entities	6. Lawyers & Notaries 7. Securities, 8. AMCs & CISs 9. Dealers in Precious Metals 10. NBFCs & Modaraba	4. life insurance 5. Auditors 6. Accountants	3. Non-life insurance 4. Development Financial Institution (DFIs)

d) Others factors include;

Porous border.

Hostile neighborhood

High number of afghan migrants

Long coastal line

The level of poverty

Designated Non-Financial Businesses and Professions (DNFBPs)