Habib Metropolitan Financial Services

TRE Certificate Holder of Pakistan Stock Exchange Limited
(Subsidiary of Habib Metropolitan Bank Limited)

KYC / AML / CFT Policy

Name	**KYC / AML / CFT Policy**
Classification	***Confidential***
Prepared By	**Compliance Division**
Date	**September – 2013**
Revision Date	**October – 2019**
Version	**1.3**
Approved By	**Board of Directors**

PREAMBLE

This policy document has been prepared in line with guidelines issued by SECP (Apex Capital Market Regulator), PSX (Stock Market Regulator), and Habib Metro Compliance Division, Group Standards, FATF recommendations and international practices. It incorporates the HMFS approach to customer identification, customer profiling based on the risk assessment and monitoring of transactions on an ongoing basis. Money Laundering ("**ML**") and Terrorist Financing ("**TF"**) are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF.

The policy primarily aligns the Habib Metro Financial Services (hereinafter referred to as HMFS) with Regulatory requirement.

PURPOSE OF POLICY

The primary purpose of the Compliance Policy is to establish a strong compliance culture within HMFS, by providing a framework of guidelines. This policy introduces and defines the KYC/AML/CFT guidelines of HMFS which will allow appropriate management of money laundering & terrorist financing risks and discharging its responsibilities relating to regulatory requirements.

Responsibility for ensuring Compliance with this policy rests with all employees of HMFS. They must act prudently and vigilantly when assessing prospective customers, handling customer requests and processing customer regular or one-off transactions. With commitment and determination, it is possible to translate the business principles into daily practice, continue to protect the integrity of the Capital Market system and maintain HMFS reputation as a respectable and trustworthy institution.

HMFS shall also follow the methodology for Internal Risk Assessment as required by PNRA Report. The concepts as defined by PNRA report, i.e. threat, vulnerabilities, inherent risk, consequences and likelihood of ML/TF and remedial measures / controls will be taken into consideration. The vulnerabilities will be assessed by considering the products and services offered, the customers, the geographical reach and delivery channels available.

SCOPE OF POLICY

This policy is applicable to Habib Metro Financial Services businesses and operations and all staff (Regular, Contractual, Consultant, etc.) Efforts are made to cover all applicable local regulations. All staff must ensure that they have read and understood the contents of the policy, SECP and PSX Regulations and applicable local laws.

Below are key areas that this policy covers:

1. Risk Assessment
2. Risk Mitigation and Application of Risk Based Approach
3. Customer Due Diligence
4. Circumstances where Enhanced Due Diligence is required
5. On-going due Diligence
6. Circumstances where Simplified Due Diligence (SDD) can be adopted
7. Three Lines of Defense
8. Record Keeping
9. Training and employee screening
10. Suspicious Transaction Report (STR)
11. Currency Transactions Report (CTR)
12. Appointment of Compliance Officer
13. Internal Audit Process
14. New Products, Practice and Technologies
15. Tip-Off
16. Action to be Taken on Become Aware of a Proscribed Person
17. Sanctions Compliance- Implementation of UN Security Council Resolutions
18. ML/TF Warning Signs / Red Flags

1. Risk Assessment

IDENTIFICATION OF CUSTOMERS, ASSESSMENT AND UNDERSTANDING OF RISK:

HMFS shall understand, identify and assess the inherent ML/TF risks posed by its:

- customer base
- products and services offered
- delivery channels
- the jurisdictions within which it or its Customers do business
- another relevant risk category.

HMFS will measure MT/TF risks using a number of risk categories while applying various factors to assess the extent of risk for each category for determining the overall risk classification, such as

- High
- Medium
- Low

HMFS will follow the probability and likelihood risk rating matrix as defined in the SECP Guideline for AML/CFT Regulations; however, it will make its own determination as to the risk weights to individual risk factors or combination of risk factor taking into consideration the relevance for different risk factors in the context of a particular customer relationship. HMFS shall assess and analyze as a combination of the likelihood that the risk will occur and the impact of cost or damages if the risk occur. The impact of cost or damage may consist of:

- Financial loss to HMFS from the crime
- Monitory penalty from Regulatory Authorities
- Reputational damages to the business or the entity itself

HMS shall analyze and identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance;

- High if it can occur several times per year;
- Medium if it can occur once per year; and
- Low if it is unlikely, but not possible.

HMFS should update its risk assessment every 12 to 18 months taking into account:

- new products are offered
- new markets are entered
- high risk customers open or close their account
- the products, services, policies and procedures are changed

HMFS shall have appropriate mechanism to provide risk assessment information to the Commission if required.

High-Risk Classification Factors:

HMFS shall describe all types or categories of customers that it provide business to and make an estimate of the likelihood that these types or category of customers may misuse the HMFS for ML or TF, and the consequent impact if indeed occurs. Risk Factor that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:

The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between HMFS and the customer):

- Non-resident customers;
- Legal persons or arrangements;
- Companies that have nominee shareholders;
- Business that is cash-intensive;
- The ownership structure of the customer appears unusual or excessively complex given the nature of the customer's business such as having many layers of shares registered in the name of other legal persons;
- Politically Exposed Persons;
- Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions;
- Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets;

- Requested/Applied quantum of business does not match with the profile/particulars of client.

Country or Geographic Risk Factor:

Due to location of a customer, the origin of a destination of transactions of the customer, business activities of HMFS itself, its location and location of its geographical units, country or geographical risk may arise. Country or geographical risk combined with other risk categories, provides useful information on potential exposure to ML/TF. HMFS may indicate High Risk to its customers based on following factors:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems;
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity;
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

Product, Service, Transaction or Delivery Channel Risk Factor:

HMFS taking into account the potential risks arising from the products, services and transactions that it offers to its customers and the way these products and services are delivered, shall consider the following factors:

- Anonymous transactions (which may include cash);
- Non-face-to-face business relationships or transactions;
- Payments received from unknown or un-associated third parties;
- International transactions, or involve high volumes of currency (or currency equivalent) transactions;
- New or innovative products or services that are not provided directly by HMFS, but are provided through channels of the institution;
- Products that involve large payment or receipt in cash;
- One-off transactions.

Low Risk Classification Factor:

Customer risk factors:

HMFS shall rate a customer as Low Risk and justify in writing who satisfies the requirements under regulation 11 (2) (a) and (b) of the SECP AML/CFT Regulations as under:

- Regulated entities and banks provided they are subject to requirements to combat money laundering and terrorist financing consistent with the FATF recommendations and are supervised for compliance with those requirements;
- public listed companies that are subject to regulatory disclosure requirements to ensure adequate transparency of beneficial ownership;

Product, service, transaction or delivery channel risk factors:

HMFS rate the product, service, transection or delivery channel that satisfy the requirement under regulation 11(2) (g) of the SECP AML/CFT Regulations, such as the financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

Country risk factors:

HMFS taking into account possible variations in ML/TF risk between different regions or areas within a country, shall rate the customer as Low Risk who belongs to:

- Countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems;
- Countries identified by credible sources as having a low level of corruption or other criminal activity.

Risk Matrix:

- HMFS may use risk matrix annexed as Annexure-1 to SECP Guideline on AML/CFT Regulations as a method of assessing risk in order to identify the types or categories of Customers that are;
- in Low Risk category;
- those that carry somewhat higher risk, but still acceptable risk; and
- those that carry a high or unacceptable risk of money laundering and terrorism financing.

Risk Management:

Risk Tolerance:

Risk tolerance is the amount of risk that HMFS is willing and able to accept and correlate its Risk Mitigation Measures and Controls accordingly, for example:

If HMFS determines that the risk associated with a particular type of customer exceed its risk tolerance, it may decide not to accept or maintain that particular type of customer(s).

Conversely, if HMFS determine that the risk associated with a particular type of customer are within the bound of its risk tolerance, it must ensure that risk mitigation measures it applies are commensurate with the risk associated with that type of customer(s).

Senior Management and the Board of HMFS shall establish their risk tolerance, based on which the HMFS shall have sufficient capacity and expertise to effectively manage the risk acceptable in line with their risk tolerance and the consequences such as legal, regulatory, financial and reputation, of AML/CFT compliance failure.

If the management of HMFS decides to establish a high-risk tolerance and accept high risk then it shall have mitigation measures and controls in place commensurate with those high risks.

All customers are classified as low, medium or high risk profile. This risk assessment has to be done on the basis of information obtained at the time of client account opening and has to be updated on the basis of information obtained during the relationship and doing business with the customer. It will be based on customer's identity, nature of income, source of funding, geographic location / domicile of customer, etc.

The Compliance Officer shall do the Risk Assessment of the customer as per AML/CFT Risk Assessment Matrix annexed to SECP Guidelines on AML/CFT Regulations and the Compliance Officer shall do the Risk Profiling of the Customer based on Risk Assessment of the Customer.

Following customers will be classified as HIGH RISK and require Enhance Due Diligence before establishing the account relationship.

- Non-resident customers;
- Legal persons or arrangements including non-governmental organizations; (NGOs)/ not-for-profit organizations (NPOs) and trusts / charities;
- Customers belonging to countries where CDD/KYC and anti- money laundering regulations are lax or if funds originate or go to those countries
- Customers whose business or activities present a higher risk of money laundering such as cash based business;
- Customers with links to offshore tax havens;
- There is reason to believe that the customer has been refused brokerage services by another brokerage house;
- Non-face-to face / on-line customers;
- Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations; and
- Politically Exposed Persons (PEPs) or customers holding public or high profile positions
- Accounts of Exchange Companies / Exchange members

"Politically Exposed Persons" (PEPs), PEP's also fall under HIGH RISK CATEGORY. These generally include individuals in prominent positions such as senior politicians, senior government, judicial or military officials; senior executives of State Corporations AND their family members and close associates. These individuals present reputational risk and potential conflict of interest and extra caution is required when opening their brokerage account and monitoring their account activity. The above definition is not intended to cover middle ranking / junior officials in above noted categories

HMFS will take appropriate steps to identify, assess and understand, the money laundering and terrorism financing risks in relation to-

- the customers;
- the jurisdictions or countries the customers are from or in;
- the jurisdictions or countries the HMFS has operations or dealings in; and
- the products, services, transactions and delivery channels;
- documenting the risk assessments;
- considering all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied;
- keeping the risk assessments up-to-date;
- categorizing the overall entity level risk as high, medium or low based on the result of risk assessment; and
- having appropriate mechanisms to provide Risk Assessment information to the Commission.

2. Risk Mitigation and Application of Risk Based Approach

HMFS will develop and implement policies, procedures and controls, which are approved by the board of directors, to enable to effectively manage and mitigate the risks that are identified in the risk assessment of ML/TF or notified by the Commission. HMFS will monitor the implementation of those policies, procedures and controls and enhance them if necessary and will perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks and have an independent audit function to test the system.

HMFS shall consider the following Risk Mitigation Measures:

Determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers and setting transaction limits for higher-risk customers such as:

- For Individual Customer, Rs. 5 million net of Sale and Purchase for a particular date;
- For Corporate Customer, Rs. 25 million net of Sale and Purchase for a particular day.
- For Foreigner Individual, $ 1 million net of Sale and Purchase for a particular day.
- For Foreigner Corporate, $ 5 million net of Sale and Purchase for a particular day.

Requiring senior management approval for higher-risk transactions, including those involving PEPs. Determining the circumstances under which they may refuse to take on or terminate/cease high risk customers. Determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs).

3. Customer Due Diligence

a. Customer Acceptance

HMFS shall not open an Account and/or maintain Business Relation of/with the following:

- Anonymous accounts;
- Account in the name of fictitious persons;
- Blacklisted by a regulatory body;
- Unregistered Money Changers;
- Shell Banks;
- Foreign PEPs
- Sanctioned Entity / Individual (i.e. Specially Designated National)

- Government Accounts in the personal names of government official(s); (Any such account, which is to be operated by an officer of the Federal/Provincial/Local Government in his/her official capacity, shall be opened only on production of a special resolution/authority from the concerned administrative department duly endorsed by the Ministry of Finance or Finance Department of the concerned Government);
- Doubtful Identity;
- High net worth customers with no clearly identifiable source of income;
- Where compliance officer has strong reason to believe that Account may be used for scams;
- Account should not be opened of NPO/NGO where the title is not as per its constituent documents;
- Where HMFS have strong reason(s) to believe that the Account/Business Relationship will expose the institution to Money Laundering, and reputational Risks;
- Business relationships with any individuals or undertakings which it knows, or is expected to know, constitute a terrorist or criminal organization, or which are affiliated to, or support or finance such an organization;
- Residents of prohibited countries as per group directives(Afghanistan, Belarus, Cuba, Eritrea, Iran, North Korea, Syria)

b. Customer Identification

It is a basic principle of any business to know who its customers are. This helps us protect ourselves from being used by unscrupulous and/or criminal elements. In this regard, HMFS will take all reasonable care to establish the true identity of customers. A minimum set of documents mentioned in Annexure 'A' that need to be obtained from customers/potential customers at the time of opening their brokerage account as prescribed by the SECP. To be prudent with applicable laws, HMFS will obtain any other document from the account opener if they believe it will help in establishing the true identity of the customer and the real controlling person behind the account. HMFS will not open anonymous or obviously fictitious accounts.

It is important to recognize if a customer is acting on behalf of another person. If this is the case, then the identity of that person should be ascertained and relevant documents of that person need to be obtained also. Beneficial Ownership must be identified for each account.

For legal person (e.g. companies, pension funds, government owned entities, non-profit organizations, foreign companies/ organizations) additional care will be taken to establish the ownership and control structure of such an organization and who (i.e. person(s)) actually owns the organization and who manages it. HMFS will verify that the person who represents himself as authorized signatory with powers to open and operate the brokerage account is actually authorized by the organization.
HMFS will make sure and be careful that accounts of Institutions/ organizations / corporate bodies are not opened in the name of employee(s)/official(s) because of sensitive nature of public sector (government) entities and risk of potential conflict of interest or embezzlement.

When an individual or an organization/institution opens brokerage account with HMFS, it is important to find out and document in broad terms what does the customer intend to do. Purpose / Intention of Account Opening should also be recorded in the Assessment of Information form.

It is not the policy of HMFS to receive any payment through cash. All receipts/payments are made through cross – cheques, bank drafts, pay- orders or other crossed banking instruments.

Any prospective customer who wants to open brokerage account must physically present himself to the account opener/authorized representative at the time of opening of the account. In the case of non-resident/overseas customers or customers in other cities where the HMFS does not have a branch/office, stronger identity verification procedures should apply. These include verification by a reliable third party, reference of an existing customer, confirmation from another broker/bank with whom the customer had an account etc.

c. Verification of Customer Identity

Verification is an internal part of KYC/CDD Policy measures which include:

- Copies of CNIC wherever required are invariably verified.
- For all existing customers, HMFS will obtain the valid copies of CNICs and all required information/documents.

d. Sanction / Blacklist Filtration

Certain countries face extensive financial sanctions and trade embargoes. For these countries, the following approach will be required:

- no accounts can be maintained for National / Residents of Afghanistan, Belarus, Cuba, Eritrea, Iran, Syria & North Korea (D.R.N.K)
- no accounts can be maintained for companies incorporated in above mentioned countries
- no remittances from/to these countries are permitted
- Every Prospective client must be screened before establishing the relationship. Through manual search from Excel File of Sanctions Entities / SDNs List provided by SECP / PSX prior to the establishment of a business relationship on the basis of applicable sanctions lists
- Existing clients must be screened on every update of sanction list.

4. Circumstances where Enhanced Due Diligence is required

Once a customer has been categorized as HIGH RISK, HMFS will conduct Enhanced Due Diligence (EDD) when dealing with such a customer. Activities and transactions of HIGH RISK customers are monitored.

When dealing with high-risk customers, including Politically Exposed Persons (PEP's) the CEO and the compliance head would approve the opening of brokerage account. In the case of HIGH RISK CATEGORY customers, it is important to determine the source of wealth and funds being invested.

If an existing customer falls into the HIGH RISK CATEGORY, the requirements mentioned in these policy guidelines for monitoring and reporting suspicious transactions and senior management approval for continuing with the customer will also apply to such customer(s).

5. On-going due Diligence

Customer Due Diligence (CDD) is not a one-time exercise that is conducted at the time of account opening only. In order to guard against misuse of their good offices against criminal transactions Compliance officer of HMFS will be vigilant at all the times, and keep monitoring transactions of their customers to ensure that the transactions executed in any particular account are within defined customer's profile, risk category, historical pattern of the transactions and as per their source of funds. For example, if a domestic individual customer orders a transaction that is significantly different from the average historical transaction size, the Compliance Officer has to be alert and be satisfied that no suspicious reportable activity has taken place and activity is in line with customer profile. Similarly, if a regular domestic customer, all of a sudden shows foreign un-identified sources of funds, this is likely to require further the investigation.

HMFS will keep all customer records updated. All high risk account to be reviewed at least on the Annual basis to assess and ensure customer records/information is updated; other accounts will be reviewed if activity is captured during activity monitoring or at least once in 3 years.

6. Circumstances where Simplified Due Diligence (SDD) can be adopted

It is acceptable for HMFS to apply simplified or reduced CDD measures in the following circumstances:
a) Risk of money laundering or terrorist financing is lower
b) Information on the identity of the customer and the beneficial owner of a customer is publicly available
c) Adequate checks and controls exist

Accordingly, following customers may be considered for simplified or reduced CDD:

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

Simplified CDD should not be followed when there is an identified risk of money laundering or terrorist financing.

7. THREE LINES OF DEFENSE:

The HMFS shall establish the following three (3) lines of Defense to combat ML/TF:

Front Office (Customer-Facing Activity):

- Front Office / Dealers / Sale Persons shall be required to know and carry-out the AML/CFT due diligence related policies and procedures when a customer opens an account with HMFS which include the following:
- Account Opening Forms should be completed in the presence of the Customer with mandatory fill-in mandatory fields and all not relevant spaces shall be marked as "Not Applicable or Crossed";
- KYC forms shall be completed in the presence of the Customer;
- All attachments needed as per Standard Account Opening Forms of CDC and PSX shall be completed;
- Account Opening amount shall be accepted in cheque/pay-order/demand draft on the bank of beneficial owner of the customer.
- Account Opening confirmation along with all details entered into back-office, CDC and NCCPL shall be communicated to the Customer on his/her registered address/email or handed over to the Customer if physically available.

Compliance Function:

- Compliance Officer will report to the Board of Directors. It is the responsibility of the compliance officer to ensure that KYC/CDD and AML/CFT guidelines are being complied with as well as with regulatory requirements. This includes maintaining record of violations / non-compliance identified during the normal course of business. These incidents have to be reported to the Board of Directors. Any such record has to be available for inspection by SECP and PSX as and when required.
- The Compliance Officer will check the account opening forms along with all Annexures before allowing the Customer to start Business Relation with HMFS;
- If there is any discrepancy in the Account Opening process, the Compliance Officer will communicate the same to Front Office/Dealer/Sales Person for rectification before start of Business Relation with the HMFS;
- The Compliance Officer will do the Risk Assessment of the Customer as per AML/CFT Risk Assessment Matrix annexed to SECP Guidelines on AML/CFT Regulations; and
- The Compliance Officer will do the Risk Profiling of the Customer based on Risk Assessment of the Customer.

Internal Audit Process:

- Internal Auditor shall periodically conduct AML/CFT audits on an Institution-wide basis;
- In case of discrepancies/non-compliances observed during audit process, he/she will communicate his/her findings and along with recommendations to the Senior Management and relevant staff designated for the purposes he/she will directly be reporting to the Board of Directors;
- Internal Auditor shall follow-up their findings and recommendation until their complete rectifications.

8. Record-Keeping

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

a) recording the documents the HMFS is provided with when verifying the identity of the customer or the beneficial owner, and
b) transcription in our IT systems of the relevant CDD information contained in such documents or obtained by other means.

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

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

HMFS should also keep records of identification data obtained through the customer due diligence process, account files and business correspondence that would be useful to an investigation for a period of 5 years after the business relationship has ended. This includes records pertaining to enquiries about complex, unusual large transactions, and unusual patterns of transactions. Identification data and transaction records should be made available to relevant competent authorities upon request.

Beneficial ownership information must be maintained for at least 5 years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or five years after the date on which the customer ceases to be a customer of the HMFS.

Records relating to verification of identity will generally comprise:

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

Records relating to transactions will generally comprise:

1). details of personal identity, including the names and addresses, of:

a) the customer;
b) the beneficial owner of the account or product; and
c) Any counter-party

2). details of securities and investments transacted including:

a) the nature of such securities/investments;
b) valuation(s) and price(s);
c) memoranda of purchase and sale;
d) source(s) and volume of funds and securities;
e) destination(s) of funds and securities;
f) memoranda of instruction(s) and authority(ies);
g) book entries;
h) custody of title documentation;
i) the nature of the transaction;
j) the date of the transaction;
k) the form (e.g. cash, cheque) in which funds are offered and paid out.

9. Training and employee screening

Annual training of HMFS Staff on AML/CFT and regulatory issues to ensure that they understand their duties under KYC/CDD and are able to perform those duties satisfactorily. HMFS will conduct a training session on annually basis or whenever required.

Employee Training

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

Training to staff should be provided at least annually, or more frequently where there are changes to the applicable legal or regulatory requirements or where there are significant changes to the business operations of HMFS or customer base.

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

Staff should be aware on the AML/CFT legislation and regulatory requirements, systems and policies. They should know their obligations and liability under the legislation should they fail to report information in accordance with internal procedures and legislation. All staff should be encouraged to provide a prompt and adequate report of any suspicious activities.

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

HMFS shall consider obtaining an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT matters, read the AML/CFT manuals, policies and procedures, and understand the AML/CFT obligations under the relevant legislation.
Staff members who deal with the public such as sales persons are the first point of contact with potential money launderers, and their efforts are vital to an organization's effectiveness in combating ML/TF. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to verify the customer's identity, for new and existing customers. Training should be given on the factors which may give rise to suspicions about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

Staff involved in the processing of transactions should receive relevant training in the verification procedures, and in the recognition of abnormal settlement, payment or delivery instructions. Staff should be aware of the types of suspicious activities which may need reporting to the relevant authorities regardless of whether the transaction was completed. Staff should also be aware of the correct procedure(s) to follow in such circumstances.

All staff should be vigilant in circumstances where a known, existing customer opens a new and different type of account, or makes a new investment e.g. a customer with a personal account opening a business account. Whilst the HMFS may have previously obtained satisfactory identification evidence for the customer, the HMFS should take steps to learn as much as possible about the customer's new activities.

Although Directors and Senior Managers may not be involved in the handling ML/TF transactions, it is important that they understand the statutory duties placed upon them, their staff and the firm itself given that these individuals are involved in approving AML/CFT policies and procedures. Supervisors, managers and senior management (including Board of Directors) should receive a higher level of training covering all aspects of AML/CFT procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.

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

Employee Screening

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

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

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

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

10. Suspicious Transaction Report:

Where the HMFS is not able to complete required CDD measures, account shall not be opened or existing business relationship shall be terminated and consideration shall be given if the circumstances are suspicious to warrant the filing of an STR in relation to the customer. The basis of deciding whether an STR is to be filed or not shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that the transaction is subsequently reported or not.

HMFS shall file with the FMU, Suspicious Transaction Report , conducted or attempted by, HMFS knows, suspects or has reason to suspect that the transaction or a pattern of transactions of which the transaction is a part –

- Involves funds derived from illegal activities or is intended or conducted in order to hide or disguise proceeds of crime;
- Has no apparent lawful purpose after examining the available facts, including the background and possible purpose of the transaction;
- Or; Involves financing of Terrorism
- Any unusual transactions that cannot be justified by the customer are reported in a Suspicious Transaction Report (STR)

If customer is unable to fulfill the KYC/CDD requirement mentioned in the policy, account relationship should not be established and if deemed necessary, HMFS may also consider filing a Suspicious Transactions Report (STR).

In case an existing customer falls into HIGH RISK CATEGORY and customer is unable to fulfill the requirements of this policy guidelines, such account should be closed and if deemed necessary a Suspicious Transaction Report (STR) filed.

Account should not be opened if the verification of the identity of the customer / beneficial owner of the account is not positive or a positive link is identified with the prescribed entities or persons, or if it is unclear what the purpose and intention of customer is and filing an STR be considered. If there are any such existing accounts they should be closed and a Suspicious Transaction Report (STR) be filed".

11. Currency Transactions Report (CTR):

Where cash transactions are being proposed by Customers, and such requests are not in accordance with the customer's known reasonable practice, the HMFS will need to approach such situations with caution and make further relevant enquiries.

Where the HMFS has been unable to satisfy that any cash transaction is reasonable, and therefore should be considered as suspicious. It is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

12. APPOINTMENT OF COMPLIANCE OFFICER:

The HMFS is required to appoint a management level officer as Compliance Officer (**"CO"**), who shall report directly, and periodically to the Board of Directors (**"Board"**) or to another equivalent executive position or committee. The CO must be a person who is fit and proper to assume the role and who:

- has sufficient skills and experience to develop and maintain systems and controls (including documented policies and procedures);
- has sufficient resources, including time and support staff;
- has access to all information necessary to perform the AML/CFT compliance function;
- ensure regular audit of the AML/CFT program;
- maintain various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and request from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigation ; and
- respond promptly to requests for information by the SECP/LEAs.

13. Internal Audit Process:

Internal Auditor team will periodically conduct AML/CFT audit on an Institution-wide basis;

In case of discrepancies/non-compliances observed during audit process, they will communicate their findings and along with recommendations to the Senior Management including Compliance Officer;

Internal Auditors will follow-up their findings and recommendation until their complete rectifications.

14. New Products, Practice and Technologies

New Products, Practices and Technologies:
a) HMFS will develop a mechanism to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products to wit:

i. electronic verification of documentation;
ii. data and transaction screening systems.

b) HMFS will identify and assess the money laundering and terrorism financing risks that may arise in relation to-
i. the development of new products and new business practices, including new delivery mechanisms; and
ii. the use of new or developing technologies for both new and pre-existing products.

c) HMFS will undertake the risk assessments, prior to the launch or use of such products, practices and technologies, and shall take appropriate measures to manage and mitigate the risks.

d) HMFS will pay special attention to any of the products and business practices that might favor anonymity.

15. Tipping-off and Reporting

Where HMFS forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer or intimates him, it will not perform the CDD process, and instead it file a STR accordingly.

16. Action to be Taken on become aware of a proscribed person

HMFS will not form business relationship with entities / individuals that are:
(a) proscribed under the United Nations Security Council Resolutions and adopted by the Government of Pakistan;
(b) proscribed under the Anti-Terrorism Act, 1997(XXVII of 1997); and
(c) associates/facilitators of persons mentioned in (a) and (b).

HMFS will monitor the relationships on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, we will take immediate action as per law, including freezing the funds and assets of such proscribed entity/individual and will report to the Commission.

17. Sanctions Compliance- Implementation of UN Security Council Resolutions

Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They generally target specific individuals or entities; or particular sectors, industries or interests. They may be aimed at certain people and targets in a particular country or territory, or some organization or element within them. There are also sanctions that target those persons and organizations involved in terrorism. The types of sanctions that may be imposed include:

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

The Regulations require HMFS not to form business relationship with the individuals/entities and their associates that are either, sanctioned under United Nations Security Council (UNSC) Resolutions adopted by Pakistan or proscribed under the Anti-Terrorism Act, 1997.

The UNSC, acting under chapter VII of the United Nations Charter, adopts the Resolutions on counter terrorism measures and proliferation of WMD, in particular;

a) the UNSC Resolution 1267 (1999), 1989 (2011), 2253 (2015) and other subsequent resolutions, which impose sanctions covering; asset freeze, travel ban and arms embargo, against individuals and entities associated to Al-Qaida, Taliban, and the Islamic State in Iraq (Daésh) organizations.

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

c) the UNSC Resolution 1718(2006), 2231(2015) and its successor resolutions 1 on proliferation of WMD and its financing, and Targeted Financial Sanctions (TFS) on countries and specifically identified individual and entities associated with it. The resolution require, inter-alia freezing without delay the funds or other assets of, any person or entity designated, or under the authority of UNSC. The regularly updated consolidated lists of person and entities designated under UNSCRR 1718(2006) and its successor resolutions (on the DPRK).

Government of Pakistan, Ministry of Foreign Affairs issues Statutory Regulatory Orders (SROs) under the United Nations (Security Council) Act, 1948 (Act No XIV of 1948) to give effect to the UNSC Resolutions and implement UNSC sanction measures in Pakistan. HMFS should ensure compliance with the sanctions communicated through SROs.

The Federal Government, Ministry of Interior issues Notifications of proscribed individuals /entities pursuant to the Anti-Terrorism Act, 1997, to implement sanction measures under UNSCR 1373(2001).

The individuals and entities designated under the aforementioned resolutions are subject to sanctions including assets freeze, travel ban and ban on provision of any funds, financial assets or economic recourses. Such sanctions also extend to any funds, financial assets and economic resources indirectly owned by the designated individuals, and to individuals or entities acting on their behalf or on their direction.

HMFS shall, taking note of the circumstances where customers and transections are more vulnerable to be involved in TF and PF activities, identify high-risk customers and transections, and apply enhanced scrutiny. RP shall conduct checks on the names of potential and new customers, as well as regular checks on the names of existing customers, beneficial owners, transactions, and other relevant parties against the names in the abovementioned lists, to determine if the business relations involves any sanctioned person/entity, or person associated with a sanctioned person/entity/country.

HMFS is also required to screen its entire customer database when the new names are listed through UNSC Resolution or the domestic NACTA list.

HMFS shall undertake reasonable efforts to collect additional information in order to identify, and avoid engaging in prohibited activities and, to enable follow-up actions.

Where there is a true match or suspicion, HMFS shall take steps that are required to comply with the sanctions obligations including immediately–

a) freeze without delay the customer's fund or block the transaction, if it is an existing customer;
b) reject the customer, if the transaction has not commenced;
c) lodge a STR with the FMU; and
d) notify the SECP and the MOFA.

HMFS is required to submit a STR when there is an attempted transaction by any of the listed persons.

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

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

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

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

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

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

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

18. ML/TF Warning Signs / Red Flags

1. Customers who are unknown to the broker and verification of identity / incorporation proves difficult;
2. Customers who wish to deal on a large scale but are completely unknown to the broker;
3. Customers who wish to invest or settle using cash;
4. Customers who use a cheque that has been drawn on an account other than their own;
5. Customers who change the settlement details at the last moment;
6. Customers who insist on entering into financial commitments that appear to be considerably beyond their means;
7. Customers who accept relatively uneconomic terms, when with a little effort they could have a much better deal;
8. Customers who have no obvious reason for using the services of the broker (e.g.: customers with distant addresses who could find the same service nearer their home base; customers whose requirements are not in the normal pattern of the service provider's business which could be more easily serviced elsewhere);
9. Customers who refuse to explain why they wish to make an investment that has no obvious purpose;
10. Customers who are introduced by an overseas agent based in a country noted for drug trafficking or distribution
11. Customers who carry out large numbers of transactions with the same counterparty in small amounts of the same security, each purchased for cash and then sold in one transaction, particularly if the proceeds are also then credited to an account different from the original account;
12. Customer trades frequently, selling at a loss
13. Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
14. Customers who wish to maintain a number of trustee or customers' accounts which do not appear consistent with the type of business, including transactions which involve nominee names;
15. Any transaction involving an undisclosed party;
16. transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral; and
17. Significant variation in the pattern of investment without reasonable or acceptable explanation
18. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
19. Transactions involve penny/microcap stocks.
20. Customer requests a securities provider to execute and/or clear a buy order and sell order for the same security or similar or correlated securities (and/or on behalf of the same beneficial owner), in close chronology.
21. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
22. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
23. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
24. Customer conducts mirror trades.
25. Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

19. Proliferation Financing Warning Signs/Red Alerts

HMFS 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, HMFS 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 basis in advance;38 or

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

Annexure - A

Minimum information / Documents to be provided by Investor/Client

Individual (Natural Person)

CNIC of all Principal / Joint holders and Nominee (where applicable)
Passport for Foreign Nationals
NICOP for non-resident Pakistanis
Proof of Income / Employment / Business
NTN Certificate, where available

Partnership (Natural Person)

CNICs / NICOP of all partners as applicable
Partnership Deed
Latest Financial Statements
Certificate of Registration (in case of registered partnership firm)
NTN Certificate

Institution / Corporate (Legal Person)

CNIC / NICOP of Authorized Signatories and Directors
List of Directors and Officers
NTN Certificate
Documentary Evidence of Tax Exemption (if applicable)
Certificate of Incorporation
Certificate of Commencement of Business
Certified Copy of Board Resolution
Memorandum and Articles of Association / Bye Laws / Trust Deed
Audited Accounts of the Company

Trusts (Legal Person)

CNICs of all Trustees
Certified copy of Trust Deed
Latest Financials of the Trust
Documentary Evidence of Tax Exemption (if applicable)
Trustee / Governing Body Resolution

Clubs Societies and Associations (Legal Person)

Certified copy of certificate of Registration
List of Members
CNIC/NICOP of members of Governing Board
Certified copy of Bylaws / Rules and Regulations
Copy of latest financials of Society / Association
Board / governing Body Resolution