HABIBMETRO
Financial Services

HABIB METROPOLITAN FINANCIAL SERVICES

KYC / AML / CFT POLICY

Name	**KYC / AML / CFT Policy**
Classification	**Confidential**
Prepared By	**Compliance Division**
Prepared Date	**September – 2013**
Revision Date	**June – 2022**
Version	**1.4**
Approved By	**Board of Directors**

Table of Contents

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.

As required under clause 4 (a) of the SECP AML/CFT Regulations, HMFS is required to develop and implement policies, procedures and controls with the approval by the Board of Directors for enabling the HMFS to effectively manage and mitigate the risk that are identified in the risk assessment of ML/TF or notified to it by the Commission. HMFS shall monitor the implementation of those policies, procedures and controls and enhance them if necessary and 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.

The Policies, Procedures and Controls should contain a clear description for employees of their obligations and instructions as well as guidance on how to keep the activity of the reporting entity in compliance with the Regulations. There should be internal procedures for detecting, monitoring and reporting suspicious transactions.

HMFS shall also follow the methodology for Internal Risk Assessment as required by NRA Report. The concepts as defined by NRA 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.

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.

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. The policy will be reviewed at least once every three years and as and when required and / or warranted under applicable laws / rules / regulations.

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 ML/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 may 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

HMFS 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 three years 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 of high risk jurisdictions;
- 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;
- 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.
- Real estate dealers
- Dealers in precious metals and stones
- Lawyers and notaries

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. The factors that may indicate a high risk are as follow:

- 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 (refer to point 5d (Sanctions / Blacklist Filtration);
- 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.
- Jurisdictions in which the customer and beneficial owner are based;
- Jurisdictions that are the customer's and beneficial owner's main places of business.
- Porous Borders of Pakistan as identified in NRA report 2019.

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.
- To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions.
- Any introducers or intermediaries the firm might use and the nature of their relationship with the HMFS.
- Is the customer physically present for identification purposes? If they are not, has the firm used a reliable form of non-face-to-face CDD? Has it taken steps to prevent impersonation or identity fraud?
- Has the customer been introduced by another part of the same financial group and, if so, to what extent can the firm rely on this introduction as reassurance that the customer will not expose the firm to excessive ML/TF risk? What has the firm done to satisfy itself that the group entity applies CDD measures?
- Has the customer been introduced by a third party, for example, a Financial Institution that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision? What has the firm done to be satisfied that:
- The third party applies CDD measures and keeps records to standards and that it is supervised for compliance with comparable AML/CFT obligations;

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; and
- 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.

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. 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.
When a client relationship has been identified as involving higher risk, then enhanced due diligence (EDD) obligations come into force. For each such relationship the HMFS must carry out additional investigations which are proportional to the circumstances, thus applying a risk-based approach.

EDD process shall be initiated by the Compliance Functions immediately after an account has been identified as higher risk, either at account opening or through the automated risk scoring and shall be completed as quickly as possible, but in any case within 90 days.

Following customers will be required Enhanced Due Diligence before establishing the account relationship as these are falling in High Risk Categories.

- Non-resident customers of high risk jurisdictions;
- 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;
- Establishing business relationship or transactions with counterparts from or in countries not sufficiently applying FATF recommendations;
- Politically Exposed Persons (PEPs) or customers holding public or high profile positions;
- Accounts of Exchange Companies / Exchange members.

2. Politically Exposed Persons (PEPs)

DEFINITION OF PEP:

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

POLITICALLY EXPOSED PERSONS CATEGORIES

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

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

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

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

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

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

Screening of PEPs
HMFS will screen its clients in DOW Jones before establish business relationship. The Database contains all international lists along with PEP & adverse media.

Approval from senior management

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

- From a high risk country;
- Has prominent public function in sectors know to be exposed to corruption;
- Has business interests that can cause conflict of interests (with the position held).

Take adequate measures to establish source of wealth and source of funds.

HMFS shall consider other red flags include (in addition to the Red Flags that they consider for other applicants):

- The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
- Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;
- A PEP uses multiple bank accounts for no apparent commercial or other reason;
- The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

HMFS shall take a risk based approach in determining whether to continue to consider a customer as a PEP who is no longer a PEP. The factors that they should consider include:

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

Revocation of PEP status
The revocation of PEP status is subject to a risk-based assessment, as the risks associated with PEPs are not automatically mitigated after the PEP has left the function. The following considerations are relevant:

- at least 18 months must have passed since a domestic PEP has left the function
- at least 24 months must have passed since a foreign PEP or a PEP in an international organization has left the function
- the seniority of the PEP function. The higher the PEP, the longer the past function remains relevant. In the case of heads of state or heads of international organizations, they could continue to be considered PEPs for the rest of their lives
- the influence that the PEP continues to have after having left the function
- the association with prominent PEPs which the PEP may continue to have
- the money laundering and reputational risk associated with the PEP
- any negative information about the PEP, or any allegation, investigation or conviction for financial crime.

In order to revoke a PEP status, these considerations must be documented on the form (Enhanced Due Diligence for PEPs) in case of a foreign PEP or a PEP in an international organization. For domestic PEPs, these considerations must be documented either on the same form.

Annual review
Foreign PEPs and PEPs in international organizations must be annually reviewed and re-approved using the form (Enhanced Due Diligence for PEPs). Domestic PEPs shall be reviewed according to the annual higher risk relationship review.

3. Risk Mitigation and Controls Measures

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 Corporate Customer, Rs. 25 million net of Sale and Purchase.
- For Foreigner Individual, $ 1 million (or equivalent) net of Sale and Purchase for a particular day.
- For Foreigner Corporate, $ 5 million (or equivalent) net of Sale and Purchase for a particular day.

The Company shall also consider adopting appropriate risk management procedures for effectively managing Money Laundering/ Terrorist Financing risks by setting transaction limitations (i.e. limited deposits or withdrawals, until verification requirements are completed) and account monitoring or other appropriate risk management procedures.

4. Customer Due Diligence

For Natural Persons:

HMFS is required to know who its Customers are and it shall not keep anonymous accounts or accounts in fictitious names. HMFS shall take the following steps to ensure that its Customers are who they purport themselves to be:

- To identify and verify the Customers including their Beneficial Owners, if any, for example: House Wife, House Hold, Student and Minor;
- To understand the intended nature and purpose of the relationship;
- To know actual ownership; and
- To know control structure of the Customer.

HMFS shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that transactions being conducted are consistent with:

- Knowledge of the Customer;
- Business and Risk Profile as assessed through SECP Guidelines on AML/CFT Regulations;
- Where necessary, the source of funds.

HMFS shall conduct CDD when establishing a business relationship if:

- There is a suspicion of ML/TF, Annex 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF; or
- There are doubts as to the veracity or adequacy of the previously obtained customer identification information.

In case of suspicion of ML/TF, HMFS should:

- Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and
- File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law.

HMFS shall monitor transactions to determine whether they are linked and restructured into two or more transactions of smaller values to circumvent the applicable threshold.

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

HMFS shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction.

HMFS shall also verify whether that authorized person is properly authorized to act on behalf of the customer while conducting CDD on the authorized person(s) using the same standards that are applicable to a customer and ascertaining the reason for such authorization and obtain a copy of the authorization document.

Ultimate Beneficial Ownership of Legal Persons and Legal Arrangements:

Any individual owning more than a certain percentage of the company i.e. 25%. If 25% is the threshold there can only be a maximum of 4 beneficial owner as provided in Section 123A of the Companies Act. While 25% or more may be used for the controlling ownership test, If the 25% threshold does not identify any beneficial owners, or there are concerns or doubts that the 25% threshold has correctly identified all the beneficial owners , it is recommended that a lower threshold of 20% be used, and then 10%, if needed.

HMFS shall identify and verify the identity of the customer and beneficial owner before establishing a business relationship or during the course of establishing a business relationship, and understand the nature of its business, and its ownership and control structure.

The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold:

- first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and
- second, to take appropriate steps to mitigate the risks.

If HMFS has any reason to believe that an applicant has been refused facilities by another Securities Broker due to concerns over illicit activities of the customer, it should consider classifying that applicant:

- as higher-risk and apply enhanced due diligence procedures to the customer and the relationship;
- filing an STR; and/or
- not accepting the customer in accordance with its own risk assessments and procedures.

HMFS shall accept copies of the documents for identifying a Customer verified by seeing originals during establishing business relationship.

Identification of Customers that are not physically present:

HMFS shall apply equally effective Customers identification procedures and ongoing monitoring standards for Customers not physically present for identification purposes as for those where the client is available for interview.

Where a Customer has not been physically present for identification purposes, practices will generally not be able to determine that the documentary evidence of identity actually relates to the Customers they are dealing with.

Consequently, there are increased risks and practices must carry out at least one of the following measures to mitigate the risks posed:

- further verifying the Customer's identity on the basis of documents, data or information referred in Annexure-1 to AML/CFT Regulations, but not previously used for the purposes of verifying the client's identity;
- taking supplementary measures to verify the information relating to the client that has been obtained by the practice.

If Customer Due Diligence Measures are Not Completed.

Where HMFS is unable to complete and comply with CDD requirements as specified in the Regulations:

For New Customers:

- it shall not open the account;
- commence a business relationship; or
- perform the transaction.

For Existing Customers:

- HMFS shall terminate the relationship.
- Additionally, HMFS shall consider making a STR to the FMU.

5. Circumstances where Enhanced Due Diligence Required

High Risk Persons or Transactions:

HMFS shall be required to perform Enhanced Due Diligence on the following:

- Persons or transactions involving a country identified as higher risk by FATF;
- Persons or transactions involving higher risk countries for ML, TF and corruption or subject to international sanctions; and
- Any other situation representing a higher risk of ML/TF including those that you have identified in your Risk Assessment.
- Such body corporate, partnerships, associations and legal arrangements including non-governmental organizations or not-for-profit organizations which receive donations.
- Customers from high risk areas in Pakistan (e.g. border areas, areas where there is significant ethnic or sectarian conflict) overseas branches/subsidiaries/correspondent
- PEPs, High Net-Worth Individuals, Foreign and Non-Resident Clients will be at high risk.
- Customers likely to pose a higher than average risk will be categorized as medium or high risk depending on their background, nature, and location of activity, country of origin and sources of funds etc. Enhanced Due Diligence measures will be applied based on the risk assessment.
- If a prospective client refuses and/or reluctant to provide evidence of identity or other information properly which is requested as part of its Due Diligence, the business relationship will not proceed further. In the case of an existing relationship, the company may consider the relationship to be ceased by restricting the trading & transfer of securities facility of such client and shall only allow it to close out the open position in a controlled environment.

High Risk Business Relationship:

HMFS shall apply enhanced due diligence measures for high risk business relationships include:

- Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
- Updating more regularly the identification data of applicant/customer and beneficial owner;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining additional information on the source of funds or source of wealth of the applicant/customer;
- Obtaining additional information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship; and
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- ***Review high risk accounts once in a year from establishing the business***.

High Risk Countries and Territories:

HMFS is required to consult the following to identify above persons or transactions to be aware of the high risk countries/territories:

- Publicly available information;
- Sanctions list issued by the UN;
- FATF high risk and non-cooperative jurisdictions;
- FATF and its regional style bodies (FSRBs) and Transparency international corruption perception index;
- Useful websites include:
    - FATF website:www.fatf-gafi.org ; and
    - Transparency International website:www.transparency.org.

Complex and Unusual Transactions:

HMFS shall examine the background and purpose of all complex, unusual large transaction, and all unusual patterns of transactions, that have no apparent economic or lawful purpose and conduct enhanced CDD Measures consistent with the risk identified.

6. On-going Due Diligence

On-going Monitoring of Business Relationships

Once the identification procedures have been completed and the business relationship is established, HMFS is required to monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was opened. HMFS shall conduct ongoing monitoring of its business relationship with the customers. Ongoing monitoring helps HMFS to keep the due diligence information up-to-date, and review and adjust the risk profiles of the customers, where necessary.

HMFS shall conduct on-going due diligence which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer.

- Material changes to the customer risk profile or changes to the way that the account usually operates;
- Where it comes to the attention of HMFS that it lacks sufficient or significant information on that particular customer;
- Where a significant transaction takes place;
- Where there is a significant change in customer documentation standards;
- Significant changes in the business relationship.

Examples of the above circumstances include:

- New products or services being entered into,
- A significant increase in a customer's funds being deposited as compared to previous transactions patterns,
- The stated turnover or activity of a corporate customer increases,
- A person has just been designated as a PEP,
- The nature, volume or size of transactions changes.

HMFS should be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be:

- transaction type
- frequency
- amount
- geographical origin/destination
- account signatories

However, if HMFS has a suspicion of ML/TF or becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible

It is recognized that the most effective method of monitoring of accounts is achieved through a combination of computerized and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring mechanism.

The HMFS shall block accounts without identity document (after serving one-month prior notice) for all withdrawals, until the subject regulatory requirement is fulfilled. However, upon submission of attested copy of identity document and verification of the same from NADRA Verisys or biometric verification, the block from the accounts shall be removed.

For customers whose accounts are dormant or in-operative, withdrawal shall not be allowed until the account is activated on the request of the customer. For activation, HMFS shall conduct NADRA Verisys or biometric verification of the customer and obtain attested copy of customer's valid identity document (if already not available) and fulfill the regulatory requirement.

"Dormant or In-operative account" means the account in which no transaction or activity or financial service has been taken from last five years.

7. Simplified Due Diligence (SDD)

HMFS may conduct SDD in case of lower risks identified by HMFS. However, HMFS shall ensure that the low risks it identifies are commensurate with the low risks identified by the country or the Commission. While determining whether to apply SDD, HMFS should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity.

The simplified measures should be commensurate with the low risk factors.

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

Where HMFS decides to take SDD measures on an applicant/customer, it should document the full rationale behind such decision and make available that documentation to the Commission on request.

SDD Measures:

HMFS shall apply following Simplified Due Diligence measures on Low risk Customer:-

- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold; and
- not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established:

8. 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 Form 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 Customer Relationship Form (CRF) shall be completed;
- Amount shall be accepted from the customer in form of cheque/pay-order/demand draft only.
- 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 Checks:

- 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 customer relationship form 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 report his/her findings along with recommendations directly to the Board of Directors or to another equivalent executive position;
- Internal Auditor shall follow-up their findings and recommendation until their complete rectifications.

9. Documentation and Reporting

HMFS must document the Risk Based Approach (RBA). Documentation of relevant policies, procedures, review results and responses should enable to demonstrate to the Commission:

- risk assessment systems including how the HMFS assesses ML/TF risks;
- details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
- how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
- the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes.

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

HMFS should be able to demonstrate to the Commission, the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its procedures and policies concerning customer identification and verification; its ongoing monitoring and procedures for reporting suspicious transactions; and all measures taken in the context of AML/CFT, during the SECP's on-site inspection. HMFS shall maintain Risk Assessment Tables (Annex 1) and AML/CFT Compliance Assessment Template (Annex 2) of ***"SECP – AML/CFT/PF Guidelines"*** within the period as required by the Commission from time to time.

10. 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 10 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 10 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 10 years after the date on which the customer (a legal entity) is dissolved or otherwise ceases to exist, or 10 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.

11. 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.

12. Suspicious Transaction Report (STR)

Defining what is a suspicious transaction?

A suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted.

The basis of deciding whether an STR should be filed or not shall be documented and kept on record together with all internal working done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.

The Company shall note that STRs, including attempted transactions, should be reported regardless of the amount of the transactions; and, the CTRs should be reported for the transactions of rupees two million and above as per requirements laid down in the purpose Regulations.

HMFS may assess the following transactions as suspicious where a transaction is inconsistent in amount, origin, destination, or type with a Customer's know, legitimate business or personal activities;

HMFS shall put on enquiry if transaction is considered unusual.
HMFS shall pay special attention to the following transactions:

- All complex transactions;
- Unusual large transactions; and
- Unusual pattern of transactions.
- Which have no apparent economic or visible lawful purpose.

Reporting to Compliance Officer:

Where the enquiries conducted by HMFS do not provide a satisfactory explanation of the transactions, respective dealer/sale agent may consider that there are grounds for suspicion requiring disclosure and escalating the matter to the Compliance Officer.

Reporting to Relevant Authority:

The Compliance Officer of HMFS shall conduct enquiries regarding complex, unusual large transaction, and unusual patterns of transactions, their background and document their results properly. He may make such transaction available to relevant authorities upon their request.

Activities which should require further enquiry may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive, but includes:

- any unusual financial activity of the Customer in the context of the Customer's own usual activities;
- any unusual transaction in the course of some usual financial activity;
- any unusually-linked transactions;
- any unusual method of settlement;
- any unusual or disadvantageous early redemption of an investment product;
- any unwillingness to provide the information requested.

13. 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, 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 or foreign currency transaction involving payment, receipt, or transfer of two million and above or equivalent. CTR is to be filed within 7 working days after the currency transaction.

Vigilance systems should require the maintenance of a register of all reports made to the FMU. Such registers should contain details of:

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

Where an applicant or a Customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), HMFS shall consider filing a STR.

Where an attempted transaction gives rise to knowledge or suspicion of ML/TF, HMFS shall report attempted transaction to the FMU.

Once suspicion has been raised in relation to an account or relationship, in addition to reporting the suspicious activity HMFS shall ensure that appropriate action is taken to adequately mitigate its risk being used for criminal activities.

The HMFS may include a review of either the risk classification of the Customer or account or of the entire relationship itself.

Appropriate action may necessitate escalation to the appropriate level of decision-maker to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

14. Appointment of Compliance Officer and His Role:

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;
- ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board or directors and are effectively implemented.
- monitoring, reviewing and updating AML/CFT policies and procedures.
- timely submission of accurate data / returns as required under the applicable laws;
- monitoring and timely reporting of Suspicious and Currency Transactions to FMU;
- 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.

As part of first line of defense, the CO shall clearly specify the Policies, Procedures and Controls duly approved by the Board in writing, and communicated to all employees including those employed at branches through Inter-Office Memo ("IOM").

The CO must have the authority and ability to oversee the effectiveness of AML/CFT systems, compliance with applicable AML/CFT legislation and provide guidance in day-to-day operations of the AML/CFT Policies and Procedures especially at the branches.

The CO shall update/amend the Policies, Procedures and Controls in line with the changes/amendments in SECP KYC/AML/CFT Regulations and other relevant regulations with the approval of the Board or Equivalent and communicate in writing to all relevant employees through IOM; and

The CO shall provide amendments in the Policies, Procedures and Controls separately attached to amendment Policies, Procedure and Controls showing impact of such changes on AML/CFT Regime. As and when any change/amendment is affected in AML/CFT legislation applicable to the HMFS, the CO shall immediately update the Policies, Procedures and Controls in line with the changes/amendment in legislatives.

The CO will communicate in writing to all employees after getting Board's approval on such changes. The CO will update the risk profile of the country to which the Securities Broker or its Customers are exposed to as and when it comes in his knowledge.

15. Internal Audit Function:

HMFS should, on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit should be commensurate with the broker's nature, size, complexity, and risks identified during the risk assessments. The AML/CFT audits should be conducted to assess the AML/CFT systems which include:

1. Test the overall integrity and effectiveness of the AML/CFT systems and controls;
2. Assess the adequacy of internal policies and procedures in addressing identified risks, including;
   a) CDD measures;
   b) Record keeping and retention;
   c) Third party reliance; and
   d) Transaction monitoring;

3. Assess compliance with the relevant laws and regulations;
4. Test transactions in all areas of the HMFS, with emphasis on high–risk areas, products and services;
5. Assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
6. Assess the adequacy, accuracy and completeness of training programs;
7. Assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and
8. Assess the adequacy of process of identifying suspicious activity including screening sanctions lists.

16. New Products, Practice and Technologies

HMFS shall have systems in place to identify and assess ML/TF/PF risks that may arise from new and pre-existing product such as:

a) New products, markets or sales channels;
b) New internal organization or new offices and departments;
c) New data and transaction screening systems and verification of documentation:

HMFS shall identify and assess the money laundering and terrorism financing risks that may arise in 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 technologies.

HMFS shall 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.

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

17. Tipping-off & Reporting:

The Law prohibits tipping-off:

A risk exists that Customers could be unintentionally tipped off when HMFS is seeking to complete its CDD obligations or obtain additional information in case of suspicion of ML/TF.

The applicant/customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected ML/TF operation.

If HMFS forms a suspicion of ML/TF while conducting CDD or ongoing CDD, it should take into account the risk of tipping-off when performing the CDD process.

If HMFS reasonably believes that performing the CDD or on-going process will tip-off the applicant/customer, it may choose not to pursue that process, and may file a STR.

HMFS shall ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

18. Risk-Based Approach during the Challenging Environment / Extraordinary Circumstances:

The criminals may take advantage of any unprecedented situation such as economic uncertainty, fears of pandemics, forced seclusions, etc, to carry out financial fraud and exploitation scams including but not limited to investment and product scams. In this extraordinary circumstance when there is a probability to face difficulties in carrying out CDD, the following risk-based approach will be used by the Company:

Scanned/Digital copies of documents will be accepted in such a situation as described above, to be followed by obtaining the originals at a reasonable later time when the situation has settled down;

Once customers have provided copies of identification documents, additional verification will be done using immediately available video call feature to compare the physical identity of a customer with scanned copies of identification documents;

Procedures such as telephoning the customer to ask questions about their identification, understanding and obtaining information on the purpose and intended nature of the business relationship or other questions that would assist in ascertaining whether the customer is who they claim and categorize to be;

Obtaining disclosures from customers to verify certain types of information provided and the accuracy and completeness of documents;

The Company shall use and allow digital/online payment methods to carry out transactions within the prescribed limits.

The Company shall maintain the database of all its customers, their beneficial owners/associates, board of directors, trustees, and office bearers of its customers, for the required matching, screening, etc.

Following the above, required actions will be taken immediately on the receipt of notifications issued by the Ministry of Foreign Affairs on United Nations Security Council Resolutions, intimation from the National Counter Terrorism Authority or Securities and Exchange Commission of Pakistan regarding updates in the list of proscribed persons.

The Company shall allocate appropriate human/technological resources to immediately scan their customer databases, their beneficial owners/associates, board of directors, trustees, and office bearers of its customers, for any matches with the stated designated/proscribed person(s)/entity(ies).

The Company shall not form business relationship with the person(s)/entity(ies) if the name(s) are appearing in the said list.

The Company shall maintain a list of all such customers/accounts where the business relationship was refused or needed to be closed on account of false verification.

The requirements as contained in AML/CFT Regulations 2020 dated 28 Sept, 2020 shall be followed in letter and spirit.

19. Action to be taken on Become Aware of a Proscribed Person and/or Entity

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 through the system which is connected with UNSC and NACTA website 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.

20. 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. HMFS 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 the relevant funds and assets without delay the customer's fund or block the transaction without prior notice if it is an existing customer in accordance with the respective SRO;
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.

Swiss State Secretariat for Economic Affairs (SECO)
The Swiss federal government may impose restrictive measures to enforce sanctions that have been imposed by the UN, the Organization for Security and Cooperation in Europe (OSCE), or by the main trading partners of Switzerland and are designed to comply with the Laws of Nations, including human rights standards (Article 1, Section 1 of the Embargo Act). The Swiss Federal Council is responsible for the imposition, adaptation and implementation of restrictive measures (Article 2, Section 1 of the Embargo Act). SECO is responsible for the administration of restrictive measures. Further information on sanction programmes are available under www.seco.admin.ch/seco/en/home.

European Union (EU)
Sanctions or restrictive measures (the two terms are used interchangeably) have been frequently imposed by the EU in recent years, either on an autonomous EU basis or implementing binding Resolutions of the Security Council of the UN. Restrictive measures imposed by the EU may target governments of third countries, or non-state entities and individuals (such as terrorist groups and terrorists). They may comprise arms embargoes, other specific or general trade restrictions (import and export bans), financial restrictions, restrictions on admission (visa or travel bans), or other measures, as appropriate. Further information can be found under https://sanctionsmap.eu.

United States Office of Foreign Assets Control (OFAC)

The OFAC administers and enforces financial and trade sanctions in the United States of America (U.S.). The U.S. Treasury maintains jurisdiction over all USD transactions, and its aims are to ensure no sanctioned countries, entities or individuals engage improperly in USD denominated transactions and / or that no (U.S. Persons) are involved in processing such sanctioned transactions.

This means that all USD transactions involving an OFAC sanctioned party are liable to be blocked or frozen by U.S. correspondent banks. It is therefore the strict policy of the Group not to establish and / or continue a customer relationship with individuals or entities sanctioned by OFAC and to strictly comply with OFAC regulations on all its USD denominated transactions (see also section 8.2 – (Unilateral OFAC sanctions regimes (B-countries in appendix 3))). Further information on countries and regimes subject to U.S. sanctions can be found under https://www.treasury.gov.

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 (DPRK)
- 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 automated search from our system of Sanctions Entities / SDNs List, other lists as provided by SECP / PSX prior to the establishment of a business relationship on the basis of applicable negative lists.
- Existing clients must be screened on every update of screening list.

21. ML/TF Warning Signs/ Red Flags

1. Customers who are unknown to the HMFS and verification of identity / incorporation proves difficult;
2. Customers who wish to deal on a large scale but are completely unknown to the HMFS;
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 HMFS (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. Customer trades frequently, selling at a loss
12. Customers who constantly pay-in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments;
13. 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;
14. Any transaction involving an undisclosed party;
15. transfer of the benefit of an asset to an apparently unrelated third party, or assignment of such benefit as collateral;
16. Significant variation in the pattern of investment without reasonable or acceptable explanation
17. Transactions appear to be undertaken in a structured, sequential manner in order to avoid transaction monitoring/ reporting thresholds.
18. Transactions involve penny/microcap stocks.
19. 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.
20. Transfers are made to the same person from different individuals or to different persons from the same individual with no reasonable explanation.
21. Unusually large aggregate wire transfers or high volume or frequency of transactions are made with no logical or apparent reason.
22. Customer invests in securities suddenly in large volumes, deviating from previous transactional activity.
23. Customer conducts mirror trades.
24. Customer closes securities transaction before maturity, absent volatile market conditions or other logical or apparent reason.

22. 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.

23. Minimum Documents required for Customer Due Diligence (CDD)

S No.	Type of Customer	Minimum Documents required for CDD
1.	Individuals	A photocopy of any one of the following valid identity documents: i. Computerized National Identity Card (CNIC)/Smart National Identity Card (SNIC) issued by NADRA. ii. National Identity Card for Overseas Pakistani (NICOP/SNICOP) issued by NADRA. iii. Form-B/Juvenile card issued by NADRA to children under the age of 18 years. iv. Pakistan Origin Card (POC) issued by NADRA. v. Alien Registration Card (ARC) issued by National Aliens Registration Authority (NARA), Ministry of Interior (local currency account only). vi. Valid Proof of Registration (POR) Card issued by NADRA vii. Passport; having valid visa on it or any other proof of legal stay along with passport (foreign national individuals only).
2.	Joint Account	i. A photocopy of any one of the documents mentioned at Serial No. 1; ii. In the case of joint accounts, CDD measures on all of the joint account holders shall be performed as if each of them is individual customers of the HMFS.
3.	Sole proprietorship	i. Photocopy of identity document as per Sr. No. 1 above of the proprietor. ii. Attested copy of registration certificate for registered concerns. iii. Sales tax registration or NTN, wherever applicable iv. Account opening requisition on business letter head. v. Registered/ Business address.
4.	Partnership	i. Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. ii. Attested copy of 'Partnership Deed' iii. Attested copy of Registration Certificate with Registrar of Firms. In case the partnership is unregistered, this fact shall be clearly mentioned on the Account Opening Form iv. Authority letter from all partners, in original, authorizing the person(s) to operate firm's account. v. Registered/ Business address.

5.	Limited Liability Partnership (LLP)	i. Photocopies of identity documents as per Sr. No. 1 above of all the partners and authorized signatories. ii. Certified Copies of: a. Limited Liability Partnership Deed/Agreement. b. LLP-Form-III having detail of partners/designated partner in case of newly incorporated LLP. c. LLP-Form-V regarding change in partners/designated partner in case of already incorporated LLP. Authority letter signed by all partners, authorizing the person(s) to operate LLP account.
6.	Limited Companies/ Corporations	i. Certified copies of: a) Resolution of Board of Directors for opening of account specifying the person(s) authorized to open and operate the account; b) Memorandum and Articles of Association; ii. Certified copy of Latest 'Form-A/Form-B'. iii. Incorporate Form II in case of newly incorporated company and Form A / Form C whichever is applicable; and Form 29 in already incorporated companies iv. Photocopies of identity documents as per Sr. No. 1 above of all the directors and persons authorized to open and operate the account; v. Photocopies of identity documents as per Sr. No. 1 above of the beneficial owners.
7.	Branch Office or Liaison Office of Foreign Companies	i. A copy of permission letter from relevant authority i-e Board of Investment. ii. Photocopies of valid passports of all the signatories of account. iii. List of directors on company letter head or prescribed format under relevant laws/regulations. iv. Certified copies of v. Form II about particulars of directors, Principal Officer etc. in case of newly registered branch or liaison office of a foreign company vi. Form III about change in directors, principal officers etc. in already registered foreign companies branch or liaison office of a foreign company vii. A Letter from Principal Office of the entity authorizing the person(s) to open and operate the account. viii. Branch/Liaison office address.

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

List of appropriate information and/or supporting documentation required to establish source of wealth and funds is as follows (any one of the documents may be obtained):

a) Employment Income: • Last month/recent pay slip; • Annual salary and bonuses for the last couple of years; • Confirmation from the employer of annual salary; • Income Tax Returns/ Wealth Statement.	**b) Business Income/ Profits / Dividends** • Copy of latest audited financial statements; • Rental statements • Dividend statements
c) Savings / deposits/ assets/property: • Statement from financial institution • Bank Statement • Taxation returns • Accountant's statements • Property ownership certificate • Share certificates	**d) Inheritance:** • Succession Certificate.
e) Sale of Property/ Business: • Copy of sale agreement/Title Deed	**f) Loan** • Loan agreement
g) Gift: • Gift Deed; • Source of donor's wealth; • Certified identification documents of donor.	**h) Other income sources:** • Nature of income, amount, date received and from whom along with appropriate supporting documentation. • Where there nature of income is such that no supporting documentation is available (for eg. Agricultural Income) Bank Statement may be obtained.

Note:
For due diligence purposes, at the minimum following information shall also be obtained and recorded on KYC (Know Your Customer)/CDD form or account opening form:

a) Full name as per identity document;
b) Father/Spouse Name as per identity document;
c) Mother Maiden Name;
d) Identity document number along with date of issuance and expiry;
e) Existing residential address (if different from CNIC);
f) Contact telephone number(s) and e-mail (as applicable);
g) Nationality-Resident/Non-Resident Status
h) FATCA/CRS Declaration wherever required;
i) Date of birth, place of birth;

j) Incorporation or registration number (as applicable);
k) Date of incorporation or registration of Legal Person/ Arrangement;
l) Registered or business address (as necessary);
m) Nature of business, geographies involved and expected type of counter-parties (as applicable);
n) Type of account/financial transaction/financial service;
o) Profession / Source of Earnings/ Income: Salary, Business, investment income;
p) Purpose and intended nature of business relationship;
q) Expected monthly turnover (amount and No. of transactions); and
r) Normal or expected modes of transactions/ Delivery Channels.

The photocopies of identity documents shall be validated through NADRA verisys or Biometric Verification. The regulated person shall retain copy of NADRA Verysis or Biometric Verification (hard or digitally) as a proof of obtaining identity from customer.

In case of a salaried person, in addition to CNIC, a copy of his salary slip or service card or certificate or letter on letter head of the employer will be obtained.

In case of expired CNIC, account may be opened on the basis of attested copies of NADRA receipt/token and expired CNIC subject to condition that regulated person shall obtain copy of renewed CNIC of such customer within 03 months of the opening of account.

For CNICs which expire during the course of the customer's relationship, regulated person shall design/ update their systems which can generate alerts about the expiry of CNICs at least 01 month before actual date of expiry and shall continue to take reasonable measures to immediately obtain copies of renewed CNICs, whenever expired. In this regard, regulated person are also permitted to utilize NADRA Verisys reports of renewed CNICs and retain copies in lieu of valid copy of CNICs. However, obtaining copy of renewed CNIC as per existing instructions will continue to be permissible.

The condition of obtaining Board Resolution is not necessary for foreign companies/entities belonging to countries where said requirements are not enforced under their laws/regulations. However, such foreign companies will have to furnish Power of Attorney from the competent authority for establishing Business Relationship to the satisfaction of the regulated person.

The condition of obtaining photocopies of identity documents of directors of Limited Companies / Corporations is relaxed in case of Government/Semi Government entities, where regulated person should obtain photocopies of identity documents of only those directors and persons who are authorized to establish and maintain Business Relationship. However, regulated person shall validate identity information including CNIC numbers of other directors from certified copies of 'Form-A/Form-B' and verify their particulars through NADRA Verisys. The Verisys reports should be retained on record in lieu of photocopies of identity documents.

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

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

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

24. Reliance on third parties:—

HMFS may rely on a third party to conduct CDD on its behalf after approval of the Board, provided that the HMFS shall-

a) remain liable for any failure to apply such indicated CDD measures above;
b) immediately obtain from the Third Party the required information concerning CDD;
c) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
d) keep that copies of identification; and
e) satisfy itself that the Third Party is supervised by an AML/CFT regulatory authority or an equivalent foreign authority and has measures in place for compliance with AML Act obligation of CDD and record keeping.

Where HMFS relies on a third party that is part of the same corporate group, the HMFS may deem the requirements as stated above to be met if:

a) the corporate group applies CDD and record-keeping requirements in accordance with the AML Act and its associated regulations;
b) the implementation of the requirements in paragraph (a) is supervised by an AML/CFT regulatory authority or an equivalent foreign authority; and
c) the corporate group has adequate measures in place to mitigate any higher country risks.

In addition to the above, when determining in which country a third party may be based, the HMFS shall have regard to available information on the level of country risk.

Notwithstanding any reliance upon a third party, the HMFS shall ultimately remain responsible for its AML/CFT obligations, including generating STRs and shall carry out ongoing monitoring of such customer itself.