DOCUMENT IDENTIFICATION INFORMATION	
Document Name:	**ANTI MONEY LAUNDERING AND CFT POLICY**
Version:	1.0
Date of Approval	July 30, 2016
Approved by :	Board of Directors

CHANGE HISTORY			
Ver.	**Date**	**Change Description**	**Approved by BOD on**
2.0	**30-11-2018**	**Revised Policy**	**30-11-2018**
3.0	**11-11-2019**	**Revision in the light of NRA 2019**	**12-11-2019**
4.0	**15-07-2020**	**Revision in the light of updated AML Guidelines issued in April, 2020**	**15-07-2020**
5.0	**25-02-2022**	**Revision in the light of updated AML Regulation,2020(28-09-2020) and Guidelines issued in January 2021**	**25-02-2022**

Anti-Money Laundering, Countering Financing of Terrorism and Proliferation Financing (AML&CFT) Policies, Procedures and Controls

BACK GROUND

Money Laundering ("ML") and Terrorist Financing ("TF") are economic crimes that threaten a country's overall financial sector reputation and expose financial institutions to significant operational, regulatory, legal and reputational risks, if used for ML and TF. An effective Anti-Money Laundering and Countering the Financing of Terrorism ("AML&CFT") regime requires financial institutions to adopt and effectively implement appropriate risk-based ML/TF/PF control framework and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF. It is important to highlight that money laundering and Terrorist financing activities is a very serious offense and the brokerage community must always remain vigilant that their good offices are not used for any such activity. This is important for the growth and development of individual brokerage houses and the securities industry in Pakistan.

2. POLICY STATEMENT

HSL is fully committed to combat any effort of laundering money and TF through drug trafficking, terrorism and any other means of organized and serious crimes by any individual or entity. HSL shall put in place all such policies and procedures of internal control aimed at preventing and impeding any attempt of money laundering and terrorist financing using the services offered by it. HSL shall ensure to AML&CFT measures, developing an effective AML/CFT risk assessment, risk mitigation, customer due diligence, identification of beneficial ownership of clients compliance framework suitable to its business, and in particular, in detecting and reporting suspicious activities. HSL will develop their own comprehensive risk-based AML/CFT compliance program to comply with all relevant and applicable laws and obligations

The policies and procedures to combat the money laundering and terrorist financing include :-

- Prevention of Money Laundering
  - Obligation of HSL in Establishing an Effective AML /CFT Governance and Compliance Regime
- Program and Systems to prevent ML and TF
- Risk Assessment, Mitigation and Applying a Risk based Approach
- New Products and Technologies
- Customer Due Diligence (CDD)
  a. Conducting CDD
  b. Risk-based implementation of Beneficial Ownership
  c. Timing of Due Diligence
  d. Ongoing Monitoring of Customers, Systems and Controls

e. Due Diligence of Existing Customers
f. Enhanced Due Diligence
g. Special Cases of Higher Risk and Enhanced Due Diligence
h. High-risk Countries and Higher Risk Regions within country
i. Simplified Due Diligence Measures
j. Reliance on Third Parties

- Targeted Financial Sanctions
- Record-Keeping Procedures
- Reporting of Suspicious Transactions
- Currency Transaction Report
- Internal Controls (Compliance Function, Audit Function, Employee Screening, Ongoing Training Program and Outsourcing)

Prevention of Money Laundering

i. Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untrained property shall be guilty of offence of money laundering.
ii. Whosoever commits the offence of money laundering shall be punishable as defined under the act, rules, regulations and guidelines.

Obligation of HSL in Establishing an Effective AML /CFT Governance and Compliance Regime

The Board of the Horizon Securities Limited ("HSL") understands its obligation of establishing an effective AML/CFT regime to deter criminals from using financial system for ML or TF purposes, and to develop a comprehensive AML/CFT compliance program to comply with the relevant and applicable laws and obligations. HSL shall ensure to establishing and maintaining an effective AML/CFT compliance culture and shall adequately train its staff to identify suspicious activities and adhere with the internal reporting requirements for compliance with the Regulations. HSL shall establish written internal procedures so that, in the event of a suspicious activity being discovered, employees are aware of the reporting chain and the procedures to be followed. Such procedures should be periodically updated to reflect any legislative changes. HSL shall appoint a Compliance Officer ("CO") at the management level, who shall be the point of contact with the supervisory authorities including the Commission and the Financial Monitoring Unit (FMU).

Program and Systems to prevent ML and TF

HSL shall establish and maintain programs and systems to prevent, detect and report ML/TF. The senior management shall ensure that appropriate systems are in place to prevent and report ML/TF and the HSL in compliance with the applicable legislative and regulatory obligations. The systems should include: -

(a) Policies, procedures and controls to undertake a Risk Based Approach ("RBA");
(b) Monitoring the implementation of policies, controls and procedures;
(c) Adequate systems to identify and assess ML/TF/PF risks relating to customers, products/services, delivery channels and geography (such as higher risk countries or regions within a country);

(d) Customer due diligence measures (enhanced or simplified due diligence) including identifying customers, beneficial owners and PEPs and verifying their identity;
(e) Ensure screening against all applicable sanctions lists;
(f) Ongoing monitoring of customers and transactions;
(g) Adequate record keeping procedures;
(h) Group-wide AML/CFT programs;
(i) Audit function to test the AML/CFT system;
(j) Screening procedures to ensure high standards, when hiring employees; and
(k) An appropriate employee-training program.

Risk Assessment, Risk Mitigation and Applying a Risk Based Approach

HSL will carryout ML/TF risk assessment, risk mitigation and will apply RBA to prevent or mitigate ML and TF. There are three levels of risk assessment. i. National Risk Assessment (NRA), ii. Sector Risk Assessment (SRA)and RP Risk Assessments. Together, the three assessments inform HSL of potential risks to help combat ML/TF. The three risk assessments inform each other and combined provide a picture of the ML/TF risks Pakistan faces. The three levels of risk assessments are: Under the RBA, where there are higher risks, HSL are required to take enhanced measures to manage and mitigate those risks; and where the risks are lower, simplified measures may be permitted. As a part of the RBA, the HSL shall
(a) Conduct a risk assessment to identify and determine the ML/TF/PF relevant to HSL;
(b) Develop and implement a programme containing the procedures, policies and controls to manage and mitigate those risks.
(c) Regular monitoring and review of those risks.

Risk assessments by HSL

HSL shall carry out a risk assessment of ML/TF in their business. taking into account guidance material from SECP and the Financial Monitoring Unit. The entity risk assessment is part of SECP anti-money laundering and countering financing of terrorism guidance materials. HSL shall regularly create and maintain an updated document that describes its current assessment of its ML/TF/PF risk in light of the latest National Risk Assessment. This document will be formally approved by the management and board of directors of the HSL and will provide a list of proposed actions needed to address any deficiencies in risk mitigants, controls processes and procedures identified by the assessment. In addition, the document shall include a view on the AML/CFT risks with respect to its customers, products, delivery channels, geography and the quality of the HSL risk mitigants, such as controls processes and procedures involving more detailed steps. Risk Assessment shall be sufficiently precise to allow the development of a Risk Matrix that grades customers, products, geography, and delivery channels into risk categories. Each customer shall receive an initial AML/CFT risk rating at the beginning of the business relationship, and it shall be kept current based on updates and changes in the relationship. The ML/TF/PF risk assessment shall be carried out annually

Identification, Assessment and Understanding Risks

The HSL will consider the following before assessing the level of risk involved in relation to customers, products/services, delivery channels and countries/regions:
(a) Latest National Risk Assessment;

(b) Sector Risk Assessment guidance by the SECP;
(c) Any applicable guidance by relevant authorities (such as FMU, SBP, MoFA, NACTA etc.);
(d) information and guidance published by international organisations such as the FATF, APG;
(e) business experience in relation to certain risks.
HSL shall address inherent risks (risks present before any controls and mitigations) and residual risk (the risk after your controls and mitigations) as part of risk assessment.
The first step in assessing ML/TF/PF risk shall be to identify the risk categories, i.e. customers, countries or geographical locations, products, services, transactions and delivery channels that are specific to the HSL.
In the second stage, HSL shall assess and analyse the ML/TF/PF risks that can be encountered as a combination of the likelihood that the risks will result in an ML/TF/PF event taking place and the impact of cost or damages resulting from the event.
HSL shall allow for the different situations that currently arise in their business or are likely to arise in the near future. For instance, risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF/PF risks will often operate together and represent higher risks in combination. Potential ways to assess risk include but are not limited to:
(a) How likely an event is;
(b) Consequence of that event;
(c) Vulnerability, threat and impact;
(d) The effect of uncertainty on an event.
vii. The assessment of risk should be informed, logical and clearly recorded. For example, if a HSL has identified gatekeepers as presenting higher inherent risk in relation to the delivery of a product, the risk assessment should indicate how HSL has arrived at this rating (domestic guidance, case studies, direct experience).

Approaches to Risk Assessment
HSL shall use e likelihood of ML/TF/PF activity for Risk Assessment keeping in view the likelihood in terms of threat and vulnerability. The likelihood rating shall be :
(a) Unlikely - There is a small chance of ML/FT/PF occurring in this area of the business;
(b) Possible - There is a moderate chance of ML/FT/PF occurring in this area of the business;
(c) Almost Certain - There is a high chance of ML/FT/PF occurring in this area of the business
When determining impact of AML/CFT activity HSL shall consider a number of factors, including:
(a) Nature and size of your business (domestic and international);
(b) Potential financial and reputational consequences;
(c) Terrorism-related impacts;
(d) Wider criminal activity and social harm;
(e) Political impact;
(f) Negative media.

Applying the Risk Assessment
The HSL will apply the risk assessment for rank and prioritize risks and will provide a framework for managing those risks. HSL will prepare a comprehensive program for meeting relevant obligations under the regulations, including obligations to conduct CDD, monitor

accounts and activities and report suspicious activity. HSL will conduct ongoing CDD. The risk assessment will help target and prioritize the resources needed for ongoing CDD..HSL will undertake account monitoring. The risk assessment will help to design the triggers, red flags and scenarios that can form part of account monitoring.

New and Developing Technologies and Products
The HSL will perform the risk assessment in new and developing technologies and products that can present unknown ML/TF risks and vulnerabilities.

New delivery Channel
The HSL will also apply the RBA for new methods of delivery that may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership.

Material Changes and Risk Assessment
i. The risk assessment should adapt when there is a material change in the nature and purpose of the business or relationship with a customer.
ii. Material change could include circumstances where HSL introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when HSL start using new methods of delivering services or have new corporate or organizational structures. It could result from deciding to outsource CDD functions or changing the processes for dealing with PEPs. In these circumstances, HSL may need to refresh their risk assessment.

Risk Classification Factors
The HSL will asses different risk categories relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.

i**. Customer risk factors:**
Risk factors that may be relevant when considering the risk associated with a customer or a customer's beneficial owner's business include:
(a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the HSL and the customer).
(b) Non-resident customers.
(c) Legal persons or arrangements
(d) Companies that have nominee shareholders.

(e) Business that is cash-intensive.
(f) 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.
(g) Politically exposed persons.
(h) Shell companies, especially in cases where there is foreign ownership which is spread across jurisdictions.
(i) Trusts and other legal arrangements which enable a separation of legal ownership and beneficial ownership of assets.

(j) Requested/applied amount of business does not match the profile/particulars of client.
(k) Designated Non-Financial Business and Professions: real estate dealers, dealers in precious metal and stones, accountants and lawyers/ notaries.

ii. **Country or geographic risk factors:**
The factors that may indicate a high risk are as follow:
(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports by international bodies such as the FATF, as not having adequate AML/CFT systems.
(b) Countries subject to sanctions, embargos or similar measures issued by the United Nations.
(c) Countries identified by credible sources as having significant levels of corruption or other criminal activity.
(d) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.
(e) Jurisdictions in which the customer and beneficial owner are based;
(f) Jurisdictions that are the customer's and beneficial owner's main places of business.

iii Product, service, transaction or delivery channel risk factors:
The HSL shall consider the following factors in identifying the risks of products, services, and transactions,
(a) Anonymous transactions (which may include cash).
(b) Non-face-to-face business relationships or transactions.
(f) International transactions, or transactions involving high volumes of currency (or currency equivalent) transactions
(h) Products that involve large payment or receipt in cash; and One-off transactions.

iv. Risk Matrix
In assessing the risk of ML/TF/PF, the HSL will establish whether all identified categories of risks pose a low, medium, high or unacceptable risk to the business operations. The HSL will review different factors, e.g., number and scope of transactions, geographical location, delivery channel and nature of the business relationship. The HSL will use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are in the low-risk medium-risk or high-risk

New Products and Technologies
HSL shall have systems in place to identify and assess ML/TF/PF 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 HSL shall undertake a risk assessment prior to the launch or use of new products, practices and technologies; and take appropriate measures to manage and mitigate the risks. HSL shall prevent the misuse of technological development in ML/TF schemes, particularly those technologies that favour anonymity. To maintain adequate systems, HSL should ensure that its systems and procedures are kept up to date with such developments and the potential new risks

and impact they may have on the products and services offered by the HSL. Risks identified will be fed into the HSL' business risk assessment.

Customer Due Diligence, Risk Profiling &Screening

HSL shall take steps to know who their customers are. HSL shall not open or keep anonymous accounts or accounts in fictitious names and shall take steps to ensure that their customers are who they purport themselves to be. .HSL shall conduct CDD, which comprises of identification and verification of customers including beneficial owners (such that it is satisfied that it knows who the beneficial owner is), understanding the intended nature and purpose of the relationship, and ownership and control structure of the customer. HSL shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the HSL's knowledge of the customer, its business and risk profile , including, where necessary, the source of funds.

If HSL has any reason to believe that an applicant has been refused facilities by another HSL 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.

Where an HSL is unable to complete and comply with CDD requirements as specified in the Regulations, it shall not open the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the HSL shall terminate the relationship. Additionally, the HSL shall consider making a STR to the FMU.

a. Conducting CDD

HSL shall take steps to know who all their customers are and shall not keep anonymous accounts or accounts in fictitious names. HSL shall take steps to ensure that their customers are who they purport themselves to be. HSL shall verify the identification of a customer using reliable independent source documents, data or information including verification of CNICs from NADRA Verisys/Biometric. The HSL shall identify and verify the customer's beneficial owner(s) to ensure that the HSL understands who the ultimate beneficial owner is.

HSL will assess each customer's risk to allow for correct application of enhanced due diligence, standard, simplified or special measures for PEPs and other designated categories. Necessary minimum customer risk rating for due diligence categories are:

(a) High
(b) Standard
(c) Low

Standard CDD is likely to apply to most of the customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners the verification is according to the level of risk involved.

Simplified CDD can only be conducted on a specified set of circumstances such as government departments, local authorities and certain listed companies.
EDD shall be conducted when HSL considers that the level of risk involved is such that EDD shall apply. EDD requires the collection and verification of the same information as standard CDD as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (SoW) and source of funds (SoF) of the customer.

The HSL will ask customers all relevant CDD questions and may refuse business if the necessary questions are not answered, or the necessary data and documents are not provided.
If HSL has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report (STR).

HSL should assess different levels of money laundering/terrorism financing risks posed by their customers' beneficial owners. For example, HSL should consider whether a beneficial owner is a politically exposed person or has links with a high-risk country or region.
For complex structures, foreign entities or foreign owned entities, HSL are required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.

Geography
HSL shall ensue that:-
•No branch alongside high risk jurisdiction, porous borders/in different provinces or business through agents/distributors belonging to porous borders be opened
•No business relationship from high-risk jurisdictions local or international will be accepted

Tipping-off & Reporting
If HSL form a suspicion of ML/TF/PF while conducting CDD or ongoing CDD, It shall take into account the risk of tipping-off when performing the CDD process. If the HSL reasonably believes that performing the CDD or on-going process will tip-off the customer, it may choose not to pursue that process and should file a STR. HSL will ensure that their employees are aware of these issues when conducting CDD or ongoing CDD.

b. Risk-based implementation of Beneficial Ownership (BO) obligations
HSL shall identify and verify the customer's beneficial owner(s) to ensure that the HSL understands who the ultimate beneficial owner is. HSL shall ensure that they understand the purpose and intended nature of the proposed business relationship or transaction. HSL shall assess and ensure that the nature and purpose are in line with its expectation and use the information as a basis for ongoing monitoring. HSL may adopt a risk-based approach to the verification of beneficial ownership of a customer.
Where a natural person seeks to open an account in his/her own name, the HSL shall inquire whether such person is acting on his own behalf. However, in relation to student, senior citizens and housewife accounts (where doubt exists that the apparent account holder is acting on his own behalf) the HSL may obtain a self-declaration for source and beneficial ownership of funds from the customer and perform further due diligence measures accordingly.

For legal persons or arrangements, it is essential to understand the ownership and control structure of the customer. In any case of lack of transparency or doubt, or higher risk, verification is needed. For legal persons, the primary source for verification of ultimate beneficial ownership is the Register of Ultimate Beneficial Ownership or other Corporate Documents

For complex structures, foreign entities or foreign owned entities, HSL shall be required to develop and have the necessary knowledge to correctly identify and verify such clients and their beneficial owners using information and data publicly available on the internet.

If an HSL has doubts about the veracity or adequacy of the information provided, it should not start a business relationship, or provide a financial service, and should consider making a suspicious transaction report to FMU.

c. **Timing of Due Diligence**

The HSL shall undertake the Customer Due Diligence and verification measure when establishing the business relationship and before any financial service or transaction occurs

The HSL, where the risks of ML/TF/PF are low, may complete verification after the establishment of the business relationship as soon as is practicable

.

iii. HSL need to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship. Where an HSL is unable to complete and comply with CDD requirements as specified in the Regulations, it shall not open the account

d. Ongoing Monitoring of Customers, Systems and Controls

The HSL will monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated, when the relationship/account was opened. The HSL shall conduct ongoing due diligence on the business relationship by:

a) scrutinizing transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the regulated person's knowledge of the customer, their business and risk profile, including where necessary, the source of funds;

b) Examining the background and purple of all complex and unusual transactions that have no apparent economic or visible lawful RP. The background and RP of these transactions will be inquired and findings documented with a view to making this information available to the relevant competent authorities, when required.

c) Carrying out reviews of existing records and ensuring that documents, data or information collected for CDD RP is kept up-to-date and relevant, particularly for higher risk categories of customers.

d) It is important to review and revise the profiles of customers identified in (b) that are involved in complex and unusual transactions that have no apparent economic or visible lawful purpose.

The HSL will also monitors:
a) changes in customer profile or transaction activity/pattern
b) changes in risk relative to countries and regions to which the HSL or its customers are exposed;
c) the potential for abuse of products and services because of their size, unusual patterns, ambiguity and complexity;
d) deficiencies in internal cooperation and coordination mechanisms, and employee awareness of their roles in AML/CFT compliance and other functions/areas; and
The HSL shall also ensure that CDD data or information is kept up-to-date by undertaking routine reviews of existing records. HSL shall consider updating customer CDD records within the time frames set by the HSL based on the level of risk posed by the customer or on the occurrence of a triggering event, whichever is earlier. Examples of triggering events include:
(a) Material changes to the customer risk profile or the way that account usually operates;
(b) HSL lacks sufficient or significant information on a particular customer;
(c) Where a significant transaction takes place;
(d) Where there is a significant change in customer documentation standards;
(e) Significant changes in the business relationship;
(f) Transaction restructuring to circumvent the applicable threshold
.
The HSL may mark the account inactive when a customer has no active business with the HSL, or cannot be reached, or refuses to engage in updating account profile and may also proceed for ending a customer relationship under the applicable laws, If due diligence cannot be updated.
HSL in addition to manually transaction monitoring system may maintain a computer system for transactions monitoring specifically designed to assist the detection of ML/TF/PF.

e. Due Diligence of Existing Customers
The HSL will assign to existing customer a risk rating and will apply CDD measures to existing customers on the basis of materiality and risk and will conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken, and the adequacy of data obtained. HSL if has a suspicion of ML/TF/PF or becomes aware at any time that it lacks sufficient information about an existing customer, will take steps to ensure that all relevant information is obtained as quickly as possible. The HSL will in-active accounts without identity document for all transaction until the subject regulatory requirement is fulfilled

f. Enhanced Due Diligence
Where the risks of ML/TF are higher, or in cases of unusual or suspicious activity, HSL shall conduct enhanced CDD measures, consistent with the risks identified. In particular, HSL shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

The enhanced CDD measures that could be applied for high-risk business relationships include:
(a) Obtaining additional information, about the volume of assets
(b) Obtaining additional information on the intended nature of the business relationship;
(c) Obtaining information about source of funds or source of wealth of the customer;

(d) Obtaining information on the reasons for intended or performed transactions;
(e) Obtaining approval of senior management to commence or continue the business relationship;
(f) 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.
(g) Enhanced CDD will be required again as a result of any material changes in your business relationship with your customer or due to ongoing CDD and account monitoring.

HSL shall conduct EDD when establishing a business relationship if:-

(1) There are doubts as to the veracity or adequacy of the previously obtained customer identification information.
(2) There is a suspicion of ML/TF, and shall
(1) Seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold that might otherwise apply; and
(2) File a Suspicious Transaction Reporting ("STR") with the FMU, in accordance with the requirements under the Law

g. Special Cases of Higher Risk and Enhanced Due Diligence

• Politically Exposed Persons (PEPs)
The HSL will remain vigilant in relation to domestic and foreign PEPs who are seeking to establish business relationships. HSL, in addition to performing standard due diligence measures should also:
(a) have appropriate risk management systems to determine whether the customer a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
(b) obtain approval from senior management to establish or continue a business relationship where the customer or a beneficial owner is a PEP, close associate or family member of a PEP or subsequently becomes a PEP, close associate and family member of a PEP;
(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as a PEP, close associate or family member of a PEP
(d) conduct enhanced ongoing monitoring of business relations with the customer or beneficial owner identified as a PEP, close associate and family member of a PEP.
(e). During ongoing monitoring HSL should later identify the customer and/or the beneficial owner as a PEP. This may occur if the individual customer is promoted into a more senior role, or a ownership of a company changes and an individual acquires 25% or more, or some other controlling interest, or for some other reasons.

•Non-Profit Organizations
HSL will apply the EDD to the NPOs to ensure that it is not misused by the terrorist organization and understand:
(a) Beneficiaries and Beneficial Owners including certain donors that maintain decision rights;
(b) Flow of funds, in particular the use of funds by an NPO.

• **High Net worth Individuals (HNWIs)**
HSL shall scrutinize HNWI customers to determine, whether they carry a higher risk of ML/FT and require additional due diligence measures. Such scrutiny will be documented and updated as part of the Risk Assessment of the HSL.

h. High-risk Countries and Higher Risk Regions within country
The HSL will apply appropriate counter measures and EDD against high risk countries or regions within country that have a specific higher AML/CFT risk profile. These includes border regions, large goods transit points such as ports, or regions experiencing social unrest, that can be associated with specific crime patterns Conducting a business relationship with a customer from such a country/region exposes the HSL to risk of channeling illicit money flows. The HSL shall exercise additional caution, and conduct enhanced due diligence on individuals and/or entities based in high-risk countries / regions HSL shall ensure the following to mitigate transnational risk in light of threats and vulnerabilities as highlighted in NRA 2019

•Identification and assessment of the existing customers of the HSL involving transactions with overseas jurisdictions and asses the degree of risk associated with these customers with the customers with respect to the transnational TF risk.
•Identification and evaluation of the existing customers or their nominees or authorized persons or directors or sponsors or major shareholders who are Afghan National or Afghan Refugee or national of Iran or Democratic People's Republic of Korea.
•Identification of, if any in the category of domestic NPOs/NGOs who is funded by foreign NPOs or NGOs that have presence in jurisdictions monitored by FATF as high risk or jurisdictions identified as high risk by the HSL who could have possibly links with proscribed entities or individuals.
•Assessment of funding of organizations / individuals at overseas jurisdictions by INGOs/NPOs/NGOs/individuals (including but not limited to Madrassas & religious charitable organizations), if any
•Assessment of the inflow and outflow of funds poured into the accounts of designated / proscribed persons and entities maintained with the HSL, if any, prior to the freezing of the account.
•Where outward remittances were processed through the accounts of exchange companies by the HSL, if any, ensure the CDD/EDD measures which were taken by the exchange company.
•Assessment of the customers involved in practices of hundi / hawala with a view to identify nexus of such customers with other individuals / entities and their methodology of operations.
•Evaluation of the possibility of the cyber frauds involving transfer of funds to accounts maintained in foreign jurisdictions and subsequently transferring these funds into the local jurisdiction by any of the existing customers.
•Assessment of the possible involvement in any criminal activity by any of the existing customers, which has a strong transnational element, such as drug trafficking or smuggling across the borders.

i. Simplified Due Diligence Measures
HSL may conduct SDD in case of lower risks customers and it will be justified in writing. Simplified measures may include the following measures:

(a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;
(b) Reducing the degree of on-going monitoring and scrutinizing of transactions;
(c) 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 transactions or business relationship established.

j. Reliance on Third Parties

When another financial sector entity has already established a relationship with a customer, the HSL may rely on the CDD performed by that other party provided if the information and CDD is shared directly between the HSL and the other entity. HSL may rely on the initial CDD information provided by another financial institution in Pakistan, where the third party is regulated and supervised by SPB or SECP and where HSL can immediately obtain necessary information from the third party.

k-Risk Profiling

On the basis of detailed risk assessment through CDD , each client shall be allotted a Risk profile, from any of the following categories:

- High
- Medium
- Low

HSL may review/change the risk profile allotted to customer in the light of the of any updation of the information obtained through continuous due diligence or otherwise.

l-Clients Screening

The HSL shall ensure that its clients and their nominees/joint account holders/authorized persons/BOD/Trustees/office bearers or other related persons have no relation or connection with proscribed/designated entities and individuals. HSL shall have a mechanism in place for ongoing screening of its clients data base against all applicable, national & international, sanctions lists, proscribed persons/entities list, publicly known information or linkage or on the basis of information received from Government, Regulatory bodies and also from reliable media. The HSL, before entering into business relationship with a new client, shall screen all the individual and legal persons connected with that account. Further HSL shall also screen its client data base against the SRO/letters/information received from government regulatory bodies and in the case of any proscribed person is found his/ their assets will be freezed immediately. Further HSL shall promptly inform to the concerned regulatory bodies, if during the screening, new client or existing client is found connected with any proscribed person/entity or sanction list.

Monitoring AML/CFT Systems and Controls

HSL shall have systems in place to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors HSL shall update their systems as appropriate to suit the change in risks. HSL shall also assess the effectiveness of their risk mitigation procedures and controls, and identify areas for improvement, where needed

Documentation and Reporting

HSL shall document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the HSL to demonstrate:

1) risk assessment systems including how the HSL assesses ML/TF risks;

2) details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;

3) how it monitors and, as necessary, improves the effectiveness of its systems and procedures; and

4) the arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk management systems and control processes. HSL shall ensure that their ML/TF risk management processes are kept under regular review which is at least annually. HSL shall be able to demonstrate 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.HSL shall maintain Risk Assessment Tables (Annex 1) and AML/CFT Compliance Assessment Template (Annex 2) within the period as required by the Commission from time to time

Cross-border Correspondent Relationship

Cross-border correspondent relationships is the provision of services by one institution to another institution (the respondent institution). Correspondent institutions that process or execute transactions for their customer's (i.e. respondent institution's) customers may present high ML/TF risk and as such may require EDD. In order for HSL to manage their risks effectively, they shall consider entering into a written agreement with the respondent institution before entering into the correspondent relationship. In addition to setting out the responsibilities of each institution, the agreement could include details on how the HSL will monitor the relationship to ascertain how effectively the respondent institution is applying CDD measures to its customers, and implementing AML/CFT controls.

Assessment of Money Laundering/Terrorist Financing Threats

The HSL shall ensure the following:

- Identification of any Customer/Joint account holder or their nominee or authorized persons or directors or beneficial owner or major shareholder who belongs to high-risk jurisdictions within Pakistan as identified in NRA update 2019.
- Identification of any Customer/Joint account holder or their nominee or authorized persons or directors or beneficial owner or major shareholder who belongs to high-risk jurisdictions outside Pakistan as identified in NRA update 2019.
- Asses the size, source and the nature of transaction whether incoming or outgoing by the customers pertaining to high risk jurisdictions both domestic and foreign.

Entities of concern

Given below is the summary position of ratings assigned to the TOs posing significant and lower TF threats:

No. of TOs	Risk	Names of Terrorist Organizations (TOs)
2	High	Daesh and TTP.
10	Medium High	AQ, JeM, JuD/ FIF, TTA, LeT, HQN, JuA, BLA, LeJ and BLF.
8	Medium	SSP, LeJ-Al-Almi, UBA, BRA, BLT, BRAS, HuA and Unknown.
21	Medium Low and Low	Jesh-ul-Islam, Lashkar-i-Islam, SMP, Lashkar-e-Balochistan, Balochistan Republican Guards, Self-radicalized (lone wolf) terrorists, Hazb-ul–Tehrir, Ahl-e-Sunnat Wal Jamat, Tehreek-e-Jafaria Pakistan, Jeay Sindh Mottahida Mahaz, Harkat-ul-Mujahideen, Tehreek - e-Taliban Swat, Al-Badar Mujahideen, Ansar-ul-Shariya, Balochistan Waja Liberation Army, Baloch Republican Party Azad, Balochistan United Army, Balochistan National Liberation Army, Balochistan Liberation United Front, Baloch Student Organization Azad, Balochistan Muslla Defa Tanzeem.

DNFBPS and its related ML/TF threats and vulnerabilities

HSL shall make the RBA assessment of the customers whose business and professions pertains to DNFBPs which has M/L threats and vulnerabilities as highlighted in NRA 2019.

Assessment of inherent vulnerability levels by type of legal persons

HSL shall a ensure the assessment of M/L threats and vulnerabilities of legal persons as highlighted in NRA 2019. HSL shall use the RBA while making the assessment/Identification of the customers;

- who are legal persons as private limited companies.
- who are legal person as Foreign companies.
- who are legal person as Domestic limited liability partnerships.
- who are legal person as Domestic Foreign limited liability partnerships.
- who are legal arrangement as WAQF.
- who are legal arrangement as Trust.
- who are NPO

Analyses of various types of crimes and their ML ratings

HSL shall make the assessment as to how various types of crimes and their ML threats will change the existing ratings assigned to various customers types such as the following:

- Illicit Trafficking in Narcotic Drugs and Psychotropic Substances;
- Corruption and Bribery;
- Smuggling; (Including in Relation to Customs and Excise Duties and Taxes);
- Tax Crimes (Related to Direct Taxes and Indirect Taxes);
- Illegal MVTS/Hawala/Hundi,
- Cash Smuggling;

- Terrorism, Including Terrorist Financing;
- Participation in an Organized Criminal Group and Racketeering,
- Trafficking in Human Beings and Migrant Smuggling;
- Illicit Arms Trafficking;
- Fraud and forgery; Kidnapping,
- Illegal Restraint and Hostage-Taking;
- Robbery or Theft; Extortion;
- Insider Trading and Market Manipulation Cyber Crime Sexual Exploitation,
- Including Sexual Exploitation of Children;
- Illicit Trafficking in Stolen and Other Goods,
- Counterfeiting Currency;
- Counterfeiting and Piracy of Products;
- Murder,
- Grievous Bodily Injury;
- Environmental Crime; Piracy;

Record-Keeping Procedures

HSL shall ensure that all information obtained in the context of CDD is recorded. HSL shall 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 and 10 years for the submitted STR and CTR 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. The HSL shall maintain a comprehensive record of AML/CFT reports with respect to internal enquiries and reporting to FMU.

Internal Controls (Compliance Function, Audit Function, Employee Screening, Ongoing Training Program and Outsourcing)

HSL are expected to have systems and controls that are comprehensive and proportionate to the nature, scale and complexity of their activities and the ML/TF risks they identified. HSL should establish and maintain internal controls in relation to:

(a) compliance management arrangements;
(b) screening procedures to ensure high standards when hiring employees;
(c) an ongoing employee training programme; and
(d) an independent audit function to test the system

The Three Lines of Defense

HSL shall establish the following three lines of defense to combat ML/TF;

i. . Business unit that directs the sales force (e.g. front office, customer-facing activity, front-line and mid-line managers, who have day-to-day ownership of management of risks and controls) is the first line of defence. For each decision or approval, they need to determine and ensure that sufficient resources are provided for carrying out policies and procedures related to AML/CFT due diligence..

ii. Compliance Function: Compliance Officer, back office, internal control and risk management functions, the compliance function and human resources or technology are the second line of defence.
iii. Third the internal audit function who will periodically conduct AML/CFT audits on an Institution-wide basis and be proactive in following up their findings and recommendations

a) Compliance Function
At HSL the Compliance Officer shall be appointed who shall have the authority and ability to oversee the effectiveness of AML/CFT systems. His responsibilities shall include compliance with applicable AML/CFT legislation, reporting of suspicious and currency transactions, and providing guidance in day-to-day operations of the AML/CFT policies and procedures, including freezing of accounts/funds if subsequently identified on proscribed lists. CO shall be a person who is fit and proper to assume his role as provided in Regulation and /or guidelines

b) Audit Function
A HSL shall an Audit Officer shall be appointed who will on a regular basis, conduct an AML/CFT audit to independently evaluate the effectiveness of compliance with AML/CFT policies and procedures. The frequency of the audit should be commensurate with the HSL's nature, size, complexity, and risks identified during the risk assessments.

c) Outsourcing
HSL shall maintain policies and procedures in relation to outsourcing where they intend to outsource some of their functions. The HSL shall conduct the due diligence on the proposed service provider to whom it intends to outsource as appropriate and also ensure that the service provider ("OSP") is fit and proper to perform the activity that is being outsourced

d) Employee Screening
HSL 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. While determining whether an employee is fit and proper, the HSL may:
(1) Verify the references provided by the prospective employee at the time of recruitment
(2) Verify the employee's employment history, professional membership and qualifications
(3) Verify details of any regulatory actions or actions taken by a professional body
(4) Verify details of any criminal convictions; and
(5) Verify whether the employee has any connections with the sanctioned countries or parties.

e) Employee on going Training
HSL shall 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.

Reporting of Suspicious Transactions / Currency Transaction Report
Where a transaction is inconsistent in amount, origin, destination, or type with a customer's known, legitimate business or personal activities, the transaction shall be considered unusual, and the HSL shall put "on enquiry". Where the enquiries conducted by the HSL do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate matters to the AML/CFT CO. If the HSL decides that a disclosure should be made, the law require the HSL to report STR without delay to the FMU, in standard form as prescribed under AML Regulations.
HSL shall s also o file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above.

Targeted Financial Sanctions
The Regulations require HSL 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. HSL 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. Where there is a true match or suspicion, HSL 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.

HSL is required to submit a STR when there is an attempted transaction by any of the listed persons. HSL shall make their sanctions compliance program an integral part of their overall AML/CFT compliance program and accordingly shall have policies, procedures, systems and controls in relation to sanctions compliance. HSL shall provide adequate sanctions related training to their staff. When conducting risk assessments, HSL shall, take into account any sanctions that may apply (to customers or countries).

The obligations/ prohibitions regarding proscribed entities and persons mentioned in the sanctions 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.

The HSL shall not provide any services to proscribed/ designated entities and individuals or their associated persons as required under the Regulations. For this purpose, necessary measures should be taken including but not limited to the following controls:

(a) In case of entity accounts, it should be ensured that their beneficial owners, directors, members, trustees and authorized signatories are not linked with any proscribed/ designated entities and individuals, whether under the same name or with a different name.
(b) The association of individuals/entities with proscribed/designated entities and individuals may be determined on the basis of appropriate screening of sanctions lists, publicly known information or linkages (on the basis of Government or regulatory sources, reliable media information, etc.)
(c) While opening new accounts or extending services to customers, any similarity between the identifying information of the customer and that of proscribed/ designated entities and individuals including national identification number, address, etc. may be viewed with suspicion and properly investigated for necessary action as per requirements.
HSL shall monitor their relationships on a continuous basis and ensure that no such relationship exists. If any such relationship is found, immediate action shall be taken as per law, including reporting to the FMU.
HSL shall report to the FMU and the Commission immediately, all attempted or rejected transactions or account opening requests pertaining to proscribed/ designated entities and individuals and their associates.
HSL RPs shall maintain up to date data/MIS of all frozen assets/ funds, attempted or rejected transactions or account opening requests, and the same shall be made available to the Commission as and when required