HORIZON SECURITIES LIMITED

DOCUMENT IDENTIFICATION INFORMATION	
Document Name:	**ANTI MONEY LAUNDERING POLICY AND KYC/CDD**
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**

ANTI MONEY LAUNDERING AND KYC/CDD POLICY

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 ML and TF control processes and procedures, not only as a principle of good governance but also as an essential tool to avoid involvement in ML and TF. 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 earned 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 polices 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 and compliance framework suitable to its business, and in particular, in detecting and reporting suspicious activities.

The policies and procedures to combat the money laundering cover:-

- Prevention of Money Laundering
- Obligation of RP in Establishing an Effective AML /CFT Governance and Compliance Regime
- Program and Systems to prevent ML and TF
- The Three Lines of Defense
- Monitoring AML/CFT Systems and Controls
- Documentation and Reporting
- New Products and Technologies
- Cross-border Correspondent Relationship
- Customer Due Diligence
- On-going Monitoring of Business Relationships
- Simplified Due Diligence Measures ("SDD")
- Enhanced CDD Measures ("EDD")
- Politically Exposed Persons (PEPs)
- Record-Keeping Procedures
- Internal Controls (Audit Function, outsourcing, employee Screening and Training)
- Reporting of Suspicious Transactions / Currency Transaction Report
- Implementation of UN Security Council Resolutions

- Risk Assessment and Applying a Risk Based Approach

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 RP 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 must 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: -

i. Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities, including all applicable sanctions lists;
ii. Policies and procedures to undertake a Risk Based Approach ("RBA");
iii. Internal policies, procedures and controls to combat ML/TF, including appropriate risk management arrangements;
iv. Customer due diligence measures;
v. Record keeping procedures;
vi. Group-wide AML/CFT programs
vii. An audit function to test the AML/CFT system;
viii. Screening procedures to ensure high standards when hiring employees; and
ix. An appropriate employee-training program.

The Three Lines of Defense
HSL shall d establish the following three lines of defense to combat ML/TF;

i. First the business units (e.g. front office, customer-facing activity): They should know and carry out the AML/CFT due diligence related policies and procedures and be allotted sufficient resources to do this effectively.
ii. Second the Compliance Officer, the compliance function and human resources or technology. CO must have the authority and ability to oversee the effectiveness of HSL' AML/CFT systems, compliance with applicable AML/CFT legislation and provide guidance in day-to-day operations of the AML/CFT policies and procedures.
iii. 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.

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

New Products and Technologies
HSL shall have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing

products 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 must be fed into the HSL' business risk assessment.

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.

Customer Due Diligence

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 is the beneficial owner), 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 3), including, where necessary, the source of funds. HSL shall conduct CDD 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

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 e are in line with its expectation and use the information as a basis for ongoing monitoring. The Regulations require HSL to identify and verify the identity of any person that is purpose purporting to act on behalf of the customer

("authorized person"). The HSL should also verify whether that authorized person is properly authorized to act on behalf of the customer. HSL shall conduct CDD on the authorized person(s) using the same standards that are applicable to a customer. Additionally, HSL shall ascertain the reason for such authorization and obtain a copy of the authorization document. HSL may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service.

The purpose of the requirements set out regarding the identification and verification of the applicant and the beneficial owner is twofold: first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the applicant to be able to properly assess the potential ML/TF risks associated with the business relationship; and second, to take appropriate steps to mitigate the risks. In this context, HSL should identify the customer and verify its identity. The type of information that would normally be needed to perform this function should be as specified in Annexure 1 of the Regulations.

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) Timing of Verification

The best time to undertake verification is prior to entry into the business relationship or conducting a transaction. However, as provided in the Regulations HSL may complete verification after the establishment of the business relationship

b) Existing Customers

At HSL it is required to apply CDD measures to existing customers on the basis of materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

c) Tipping-off & Reporting

Therefore, if HSL form a suspicion of ML/TF while conducting CDD or ongoing CDD, they should 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

applicant/customer, it may choose not to pursue that process, and should file a STR. HSL should ensure that their employees are aware of, and sensitive to, these issues when conducting CDD or ongoing CDD.

d) No Simplified Due Diligence for Higher-Risk Scenarios
HSL should not adopt simplified due diligence measures where the ML/TF risks are high. HSL shall identify risks and have regard to the risk analysis in determining the level of due diligence.

On-going Monitoring of Business Relationships
HSL shall conduct ongoing monitoring of their business relationship with their customers which includes scrutinizing the transactions undertaken throughout the course of the business relationship with a customer. HSL shall develop and apply written policies and procedures for taking reasonable measures to ensure that documents, data or information collected during the "Identification" process are kept up-to-date and relevant by undertaking routine reviews of existing records. HSL shall consider updating customer CDD records as a part its periodic reviews (within the timeframes set by the HSL based on the level of risk posed by the customer) or on the occurrence of a triggering material change event, whichever is earlier. HSL shall be vigilant for any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts.

Simplified Due Diligence Measures ("SDD")
HSL may conduct SDD in case of lower risks identified by the HSL. However, the HSL 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, HSL should pay particular attention to the level of risk assigned to the relevant sector, type of customer or activity. Where an HSL 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.

Enhanced CDD Measures ("EDD")
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.

For enhanced CDD measures that could be applied for high-risk business relationships include:

(1) Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
(2) Updating more regularly the identification data of applicant/customer and beneficial owner.
(3) Obtaining additional information on the intended nature of the business relationship.
(4) Obtaining additional information on the source of funds or source of wealth of the applicant/customer.

(5) Obtaining additional information on the reasons for intended or performed transactions.
(6) Obtaining the approval of senior management to commence or continue the business relationship.
(7) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

a) High-Risk Countries
HSL should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

Politically Exposed Persons (PEPs)
HSL are encouraged to be vigilant in relation to PEPs from all jurisdictions, who are seeking to establish business relationships. HSL should, in relation to PEPs, in addition to performing normal due diligence measures:

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

HSL should obtain senior management approval to continue a business relationship once a customer or beneficial owner is found to be, or subsequently becomes, a PEP. HSL shall take a risk based approach to determine the nature and extent of EDD where the ML/TF risks are high. In assessing the ML/TF risks of a PEP, the HSL shall consider factors such as whether the customer who is a PEP:

(1) Is from a high risk country;
(2) Has prominent public functions in sectors known to be exposed to corruption;
(3) Has business interests that can cause conflict of interests (with the position held).

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. 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.

Internal Controls (Audit Function, outsourcing, employee Screening and Training)

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:

(1) an audit function to test the AML/CFT systems, policies and procedures;
(2) outsourcing arrangements;
(3) employee screening procedures to ensure high standards when hiring employees; and
(4) an appropriate employee training program.

ii. The type and extent of measures to be taken should be appropriate to the ML/TF risks, and to the size of the HSL

a) Audit Function
A HSL sshall 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.

b) Outsourcing
HSL should 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

c) 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.

d) Employee 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 must be considered unusual, and the HSL should 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 2008. HSL is also obligated to file Currency Transaction Report (CTR), for a cash-based transaction involving payment, receipt, or transfer of Rs. 2 million and above. HSL is required to report total number of STRs filed to the Commission on bi-annual basis within seven days of close of each half year. The CO should ensure prompt reporting in this regard.

Sanctions Compliance- Implementation of UN Security Council Resolutions

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 should 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 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.

Risk Assessment and Applying a Risk Based Approach
HSL will carryout ML/TF risk assessment and apply RBA to prevent or mitigate ML and TF. The process of ML/TF risk assessment has four stages:-

1) Identifying the area of the business operations susceptible to ML/TF
HSL will understand, identify and assess the inherent ML/TF risks posed by its customer base, products and services offered, delivery channels and the jurisdictions within which it or its customers do business, and any other relevant risk category. At HSL ML/TF risks will be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk for determining the overall risk classification (e.g. high, medium or low). HSL shall make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, HSL shall take into consideration the relevance of different risk factors in the context of a particular customer relationship.

2) Conducting an analysis in order to assess the likelihood and impact of ML/TF;
The HSL will assesse/ analyze the ML/TF risks as a combination of the likelihood that the risks will occur and the impact of cost or damages if the risks occur. This impact can consist of financial loss to the HSL from the crime, monitory penalties from regulatory authorities or the process of enhanced mitigation measures. It can also include reputational damages to the business or the entity itself. The analysis of certain risk categories and their combination is specific for each HSL so that the conclusion on the total risk level must be based on the relevant information available. For the analysis, the HSL will identify the likelihood that these types or categories of risk will be misused for ML and/or for TF purposes. This likelihood is for instance high, if it can occur several times per year, medium if it can occur once per year and low if it is unlikely, but not possible.

3) Managing the risks;

(a)Risk Tolerance
Risk tolerance is the amount of risk that the HSL will be willing and able to accept. HSL shall establish their risk tolerance HSL not to accept or maintain that particular type of customer(s) if it it determines that the risks associated with that client exceed its risk tolerance., HSL will ensure that the risk mitigation measures for the the risks if the risks associated with a particular type of customer are within the bounds of HSL ’s risk tolerance.

(b)Risk Mitigation
HSL shall have have appropriate policies, procedures and controls to manage and mitigate effectively the inherent risks that it has have identified, including the national risks. It will monitor the implementation of those controls and enhance them, if necessary. The policies, controls and procedures should be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with legal and regulatory requirements.

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

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

4) Evaluating Residual Risk and Comparing with the Risk Tolerance

Subsequent to establishing the risk mitigation measures, HSL shall devaluate their residual risk, the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the HSL overall risk tolerance. Where the HSL will find that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high-risks, the HSL shall enhance the risk mitigation measures that are in place.