POLICY AND PROCEDURES

"ANTI-MONEY LAUNDERING, COMBATING THE FINANCING OF TERRORISM AND COUNTERING PROLIFERATION FINANCING"

ZILLION CAPITAL SECURITIES (PVT) LIMITED

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

A. INTRODUCTION, PURPOSE AND SCOPE

i. 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. These policy and procedures require ZILLION CAPITAL SECURITIES (PVT) LIMITED ("the Company") 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.

ii. These policy and procedures also intends to assist the Company in complying with the Regulatory requirements. These policy and procedures supplement the Regulations and the AML/CFT/CPF regime by requiring the Company to apply AML/CFT/CPF measures, develop an effective AML/CFT/CPF risk assessment and compliance framework suitable to its business, and in particular, in detecting and reporting suspicious activities.

B. OBLIGATION OF THE COMPANY IN ESTABLISHING AN EFFECTIVE AML/CFT/CPF GOVERNANCE AND COMPLIANCE REGIME

i. It is the obligation of the Company to establish an effective AML/CFT/CPF regime to deter criminals from using the Company as a platform for ML or TF purposes, and to develop a comprehensive AML/CFT/CPF compliance program to comply with the relevant and applicable laws and obligations.

ii. These policy and the procedures and controls prescribed are approved by the Board of Directors and senior management of the Company.

iii. This policy will be reviewed at regular intervals and on need basis to ensure it reflects any legislative changes. All such changes in the policy and procedures shall be approved by the BODs. Approval and minutes of the meeting in which approval was obtained shall be recorded in writing.

SECTION 2: RISK BASED ASSESSMENT (RBA) AND MITIGATION

C. RISK BASED ASSESSMENT ('RBA'), IT'S DOCUMENTATION AND REPORTING

i. The Company must conduct and document its RBA. Conduct and documentation of the assessment results should enable the company to demonstrate:

   a. Risk assessment process including how the Company assesses ML/TF risks;
   b. Details of the implementation of appropriate systems and procedures, including due diligence requirements, in light of its risk assessment;
   c. How it monitors and, as necessary, improves the effectiveness of its systems and procedures; and
   d. The arrangements for reporting to senior management on the results of ML/TF risk assessments and the implementation of its ML/TF risk mitigation systems and control processes.

ii. The company shall take enhanced measures to manage and mitigate the risks where higher risks are identified. The company may take simplified measures to manage and mitigate risks, if lower risks have been identified. Simplified measures should not be permitted whenever there is a suspicion of ML/TF.

iii. It shall be noted that the ML/TF risk assessment is not a one-time exercise and therefore, the company must ensure that ML/TF risk management processes are kept under regular review which is at least annually.

iv. The management should identify and assess the ML and TF risk (also review the program's adequacy) that may arise in the development of new products, businesses and practices, including new delivery mechanism, and the use of new and pre-existent technology. Prior to the launch or use of product, practice or technology, shall undertake the risk assessment and take appropriate measures to manage and mitigate the risks.

v. The Company should categorize its own overall entity level risk as high, medium or low based on the result of risk assessment and any other risk assessment publicly available or provided by the Commission;

vi. The Company on the basis of the assessment should be able to provide information to the Commission.

vii. The Company should be able to demonstrate the adequacy of its assessment, management and mitigation of ML/TF risks; its customer acceptance policy; its 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/CPF. The company shall maintain Risk Assessment Tables (see Annexure 1) and AML/CFT/CPF Compliance Assessment Template (see Annexure 2) within the period as required by the Commission from time to time. At present the Company shall ensure meticulous compliance with the Commission's S.R.O. 920 (I)/2020 dated; 28 September, 2020.

viii. Detailed guidance and requirements of Risk based Assessment is enclosed as Annexure 3 to this policy.

SECTION 3: CUSTOMER DUE DILIGENCE

D. CUSTOMER DUE DILIGENCE

i. The Company shall ensure it take steps to know its customers. No anonymous accounts or accounts in fictitious names shall be kept and or operated. The company 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. The identity of the customer shall be verified using reliable and independent documents, data and information as set out in Annexure 5.

ii. The Company shall categorize each customer's risk depending upon the outcome of the CDD process.

iii. Where the customer is represented by an authorized agent or representative, the Company shall:

a. shall ascertain the reason for such authorization and obtain a copy of the authorization document
b. identify every person who acts on behalf of the customer,
c. verify the identity of that person in using reliable and independent documents, data and information as set out in Annexure 5; and
d. Verify the authority of that person to act on behalf of the customer.

iv. The Company shall also identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner by using reliable and independent document, data or sources of information as set out in Annexure 5, such that the company is satisfied that it knows who the beneficial owner is.

v. The company shall ensure that the purpose and intended nature of the proposed business relationship or transaction is understood. The company 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.

vi. For customers that are legal persons or legal arrangements, the company shall identify the customer and verify its identity by obtaining the following information in addition to the information required in Annexure 5:

a. name, legal form and proof of existence;
b. the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; and
c. the address of the registered office and, if different, a principal place of business.

For customers that are legal persons or legal arrangements, the company should understand the nature of the customer's business and its ownership and control structure.

vii. For customers that are legal persons, the company shall identify and take reasonable measures to verify the identity of beneficial owners by:

a. identifying the natural person(s) (if any) who ultimately has a controlling ownership interest (as defined under relevant laws) in a legal person; and
b. to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and
c. where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

viii. For customers that are legal arrangements, the company shall identify and take reasonable measures to verify the identity of beneficial owners as follows:

a. for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership);
b. for waqfs and other types of legal arrangements, the identity of persons in equivalent or similar positions as specified in (a).

c. Where any of the persons specified in (a) or (b) is a legal person or arrangement, the identity of the beneficial owner of that legal person or arrangement shall be identified.

ix. The Company shall identify the customer and beneficial owner before establishing a business relationship or during the course of establishing a business relationship.

x. The Company may complete verification of a customer or beneficial owner's identity after the establishment of the business relationship, provided that-

a. this occurs as soon as reasonably practicable;
b. this is essential not to interrupt the normal conduct of business; and
c. the ML/TF risks are low.

The types of circumstances where the company permits completion of verification after the establishment of the business relationship may include situations where;

a. it is required to perform transactions very rapidly, according to the market conditions
b. Performance of the transaction may be required before verification of identity is completed.

Transactions such as above can only be performed subject to the approval of the CEO. Verification, once begun, should normally be pursued either to a satisfactory conclusion or to the point of refusal. If an applicant does not pursue an application, the staff could consider that this in itself is suspicious, and they should evaluate whether a STR to FMU is required.

xi. The Company shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

xii. If the company has any reason to believe that any customer has been refused facilities by another brokerage house/regulated entity 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.

xiii. The Company shall maintain details of all accounts which have been refused by them as per the format enclosed in Addendum 1.

xiv. Company shall maintain details of all complaints received with regards to AML as per the format enclosed in Addendum 2.

E. ON-GOING MONITORING

i. Once the identification procedures have been completed and the business relationship is established, the company shall monitor the conduct of the relationship to ensure that it is consistent with the nature of business stated when the relationship/account was operated. The company shall conduct ongoing monitoring of their business relationship with their customers. Ongoing monitoring helps to keep the due diligence information up-to-date and reviewing/adjusting the risk profiles of the customers, where necessary.

ii. Company shall conduct ongoing due diligence on the business relationship, including:

a. scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, their business and risk profile, including where necessary, the source of funds. For this purpose, the company shall ensure that client's deposit and net investment may be gauged against their profile (such monitoring serves as enhanced due diligence on pre transaction basis).

b. Obtaining information and examining, as far as possible, the background and purpose of all complex and unusual transactions which have no apparent economic or visible lawful purpose. The background and purpose of these transactions shall be inquired and findings shall be documented with a view of making this information available to the relevant competent authorities when required. In addition to the above, customers' profiles should be revised keeping in view the CDD and basis of revision shall be documented.

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

iii. In addition to the above on-going monitoring measures, the company shall consider updating customer CDD records as a part its periodic reviews (i.e. annually) 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 changes to the way that the account usually operates;
b. Where it comes to the attention of the company that it lacks sufficient or significant information on that 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. There is a suspicion of ML/TF. Annexure 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF, that will help recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered.

Examples of the above circumstances include:

a. New products or services being entered into;
b. A significant increase in a customer's deposit;
c. A person has just been designated as a PEP;
d. The nature, volume or size of transactions changes.

F. SUSPICIOUS TRANSACTIONS REPORTING (STRS)/ CURRENCY TRANSACTIONS REPORTING (CTRS)

i. A suspicious activity will often be one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of account. 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 company should put "on enquiry". The company shall also pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

ii. The Company shall comply with the provisions of the AML Act and rules, regulations and directives issued thereunder for reporting suspicious transactions/currency transactions in the context of money laundering or financing of terrorism

iii. The company shall conduct CDD and 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 company's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds. The company shall enhance its scrutiny level in the following instances as they may prompt filing of STR:

a. There is a suspicion of ML/TF. Annexure 4 gives some examples of potentially suspicious activities or "red flags" for ML/TF, that will help recognize possible ML/TF schemes and may warrant additional scrutiny, when encountered. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny will assist in determining whether the activity is unusual or suspicious or one for which there does not appear to be a reasonable business or legal purpose; or
b. There are doubts as to the veracity or adequacy of the previously obtained customer identification information. The Company shall take steps to ensure that all relevant information is obtained as quickly as possible
c. CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of offences and crimes related to ML/TF, the company should not voluntarily agree to open accounts with such customers*
d. there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile
e. the company is unable to complete and comply with CDD requirements as specified in this policy**

* In such situations, the company should file an STR with the FMU and ensure that the customer is not informed, even indirectly, that an STR has been, is being or shall be filed.

** The company shall not operate the account, commence a business relationship, or perform the transaction. If the business relationship has already been established, the company shall terminate the relationship. Additionally, the company shall consider making a STR to the FMU.

iv. In case of suspicion of ML/TF,:

a. The Company should seek to identify and verify the identity of the customer and the beneficial owner(s), irrespective of any specified threshold; and
b. Where the enquiries conducted by the company do not provide a satisfactory explanation of the transaction, it may be concluded that there are grounds for suspicion requiring disclosure and escalate the matter to the AML/CFT CO and
c. Where a customer is hesitant/fails to provide adequate documentation (including the identity of any beneficial owners or controllers), consideration should be given to filing a STR. Also, where an attempted transaction gives rise to knowledge or suspicion of ML/TF that attempted transaction should be reported to the FMU, in accordance with this policy.
d. The basis of deciding whether an STR is being filed or not, shall be documented and kept on record together with all internal findings and analysis done in relation to a suspicion irrespective of the fact that transaction is subsequently reported or not.
e. In addition to reporting the suspicious activity, the company shall ensure that appropriate action is taken to adequately mitigate the risk of the company being used for criminal activities. This may include a review of either the risk classification of the

customer or account or of the entire relationship itself. Appropriate action shall be to escalate the matter to CEO to determine how to handle the relationship, taking into account any other relevant factors, such as cooperation with law enforcement agencies or the FMU.

Where the company files STR with respect to a customer with whom it has an existing business relationship, and if the company considers it appropriate to retain the customer, then the company shall:-

1. substantiate and document the reasons for retaining the customer; and
2. subject the business relationship to proportionate risk mitigation measures, including enhanced ongoing monitoring.

f. The Law prohibits tipping-off. However, a risk exists that customers could be unintentionally tipped off when the company 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. Therefore, if the company 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 company 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. All concerned employees should be aware of, and sensitive to, these issues when conducting CDD or ongoing CDD

v. Enquiries regarding complex, unusual large transactions, and unusual patterns of transactions, their background, and their result should be properly documented, and made available to the relevant authorities upon request.

vi. The company 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. However, for the sake of clarity, the company shall not accept any cash based transaction and or any transaction involving wire transfer/fund transfer to and from a foreign jurisdiction.

vii. If the company decides that a disclosure should be made, the law require the company to report STR promptly (without delay) to the FMU, in standard form as prescribed under AML Regulations 2008. The STR prescribed reporting form can be found on FMU website through the link http://www.fmu.gov.pk/docs/AML_Regulations-2008.pdf.

viii. The company shall report total number of STRs filed to the Commission on biannual basis within seven days of close of each half year. The CO should ensure prompt reporting in this regard.

ix. The company shall should maintain register of all reports made to the FMU. Such registers should contain details of:
   a. the date of the report;
   b. the person who made the report;
   c. the person(s) to whom the report was forwarded; and
   d. Reference by which supporting evidence is identifiable.

G. EXISTING CUSTOMER

i. The Company shall apply CDD requirement to its existing customers on the basis of materiality and risk and should conduct due diligence on existing relations at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

ii. For existing customers who opened accounts with old NICs, the company shall ensure that attested copies of identity documents shall be present in the company's record. The Company 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 or biometric verification, the block from the accounts shall be removed.

iii. For customers whose accounts are dormant or in-operative, withdrawals shall not be allowed until the account is activated on the request of the customer. For activation, the Company 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 requirements. **Dormant or in-operative account"** means the account in which no transaction or activity or financial service has been extended by the regulated person from last three (3) years;

H. ENHANCED DUE DILIGENCE

i. The Company shall apply EDD where a customer presents high risk of ML/TF including but not limited to the following circumstances:

   a. business relationships and transactions with natural and legal persons when the ML/TF risks are higher;
   b. business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF;
   c. PEPs and their close associates and family members.

ii. Examples of enhanced CDD measures that could be applied for high-risk business relationships include:

   a. Obtaining additional information on the applicant/customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.).
   b. Updating more regularly the identification data of applicant/customer and beneficial owner.
   c. Obtaining additional information on the intended nature of the business relationship.
   d. Obtaining additional information on the source of funds or source of wealth of the applicant/customer.
   e. Obtaining additional information on the reasons for intended or performed transactions.
   f. Obtaining the approval of senior management to commence or continue the business relationship as per the format enclosed as Addendum 3.
   g. 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.
   h. Monitoring of the net investment of the clients as per Addendum 4 on monthly basis to also help in identifying any STR.

iii. In case of accounts where the accountholder has instructed the company not to issue any correspondence to the accountholder's address, such accounts do carry additional risk to the company, and due caution shall be exercised as a result.

I. POLITICALLY EXPOSED PERSONS (PEP)

i. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose the company to significant reputational and/or legal risk. Such persons, commonly referred to as 'politically exposed persons' (PEPs) includes heads of state, ministers, influential public officials, judges and military commanders and includes their family members and close associates.

ii. "close associate" of a PEP means—

   a. an individual known to have joint beneficial ownership of a legal person or a legal arrangement or any other close business relations with a PEP;
   b. any individual(s) who have beneficial ownership of a legal person or a legal arrangement which is known to have been set up for the benefit of a PEP;
   c. an individual who is reasonably known to be closely connected with the PEP for any other reason, including socially or professionally.

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

iv. The company shall ensure that it determines if a customer or a beneficial owner is a PEP or a close associate or family member of a PEP, both prior to establishing a business relationship or conducting a transaction, and periodically throughout the course of business relationship. The Company shall apply, at minimum the following EDD measures:

   a. obtain approval from senior management (refer Addendum 3) 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;
   b. 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; and
   c. 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.

v. The company shall take a risk based approach to determine the nature and extent of EDD in assessing the ML/TF risks of a PEP. The company shall consider factors such as whether the customer who is a PEP:

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

vi. The other red flags that the company shall consider include:

   a. The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries;
   b. Funds are repeatedly moved to and from countries to which the PEP does not seem to have ties;

c. A PEP uses multiple bank accounts for no apparent commercial or other reason;
d. The PEP is from a country that prohibits or restricts certain citizens from holding accounts or owning certain property in a foreign country.

vii. The company 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:

a. the level of (informal) influence that the individual could still exercise; and
b. 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).

J. COUNTER MEASURES AGAINST HIGH RISK COUNTRIES

i. Certain countries associated with crimes pose a higher potential risk to the company (reputational risk and legal risk). Company should exercise additional caution and conduct enhanced due diligence on individuals and/or entities based in high-risk countries.

ii. Caution should also be exercised in respect of the acceptance of certified documentation from individuals/entities based in high-risk countries/territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability. In addition, the Company shall apply the countermeasures including but not limited to, enhance due diligence proportionate to the risk as indicated by the Federal Government, pursuant to recommendations by the National Executive Committee and when called upon to do so by the FATF.

iii. The company shall consult publicly available information to ensure that they are aware of the high-risk countries/territories including sanctions issued by the UN, the FATF high risk and non-cooperative jurisdictions (www.fatf-gafi.org), and Transparency international corruption perception index (www.transparency.org)

K. SIMPLIFIED DUE DILIGENCE

i. The company may apply SDD only where low risk is identified through adequate analysis and risk assessment and any other risk assessment publicly available or provided by the Commission and commensurate with the lower risk factors.

ii. The decision to rate a customer as low risk shall be justified in writing by the Company.

iii. SDD measures 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 transactions, based on a reasonable monetary threshold as prescribed or as set out by the Commission;
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.

iv. Simplified CDD shall not be permitted whenever there is a suspicion of money laundering or terrorist financing.

L. TARGETED FINANCIAL SANCTIONS (OBLIGATION)

i. The company shall undertake TFS obligations under the United Nations (Security Council) Act 1948 and/or Anti-Terrorism Act 1997 and any regulations made there under.

ii. The company shall have mechanisms, processes and procedures in an automated manner for screening and monitoring customers, potential customers and beneficial owners/associates of customers to detect any matches or potential matches with the stated designated/proscribed persons in the SROs and notifications issued by MoFA, under United Nations (Security Council) Act 1948 or intimation from NACTA/ Law Enforcement Agencies/ Home Departments of Provinces/Ministry of Interior regarding additions, deletions and updates in list/SRO under the Anti- Terrorism Act, 1997.

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

iv. If during the process of screening or monitoring of customers or potential customers the company finds a positive or potential match, it shall immediately:

   a. Freeze the relevant funds and assets without delay the customer's fund/ policy or block the transaction, without prior notice if it is an existing customer in accordance with the respective SRO.
   b. Lodge a STR with the FMU, and simultaneously
   c. prohibit from making any funds or other assets, economic resources, or financial or other related services and funds in accordance with the respective SRO
   d. Reject the transaction or attempted transaction or the customer, if the relationship has not commenced.
   e. Notify SECP and the Ministry of Foreign Affairs in case that person is designated under United Nations Security Council Resolutions or the National Counter Terrorism Authority ("NACTA") in case that person is Proscribed under the Anti-Terrorism Act, 1997.

v. The company shall implement any other obligation under the AML Act 2010, United Nations (Security Council) Act 1948 and Anti-Terrorism Act 1997 and any regulations made there under.

vi. Compliance report on Statutory Regulatory Orders issued by the Ministry of Foreign Affairs under United Nations (Security Council) Act, 1948 or intimation from National Counter Terrorism Authority/Law Enforcement Agencies/Home Departments of Provinces/Ministry of Interior regarding updates in the list of proscribed person(s)/entity(ies) under the Anti-Terrorism Act, 1997, shall be submitted to the Commission within forty eight (48) hours of receiving the same in the manner as may be instructed from time to time by the Commission

vii. The Company shall comply with the requirements of Red Flags/ indicators for identification of persons or entities suspected to be acting on behalf of or at the direction of designated/proscribed individuals or entities as detailed in Annexure 4.

viii. The Company is prohibited, on an ongoing basis, from providing any financial services 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 company shall monitor its business relationships with the entities and individuals on a continuous basis and ensure that no such relationship exists directly or indirectly, through ultimate control of an account and where any such relationship is found, the Company shall take immediate action as per law, including reporting to the FMU.

Explanation:- expression associates means persons and entities acting on behalf of, or at the direction, or for the benefit, of proscribed/ designated entities and individuals that may be determined on the basis of appropriate screening of sanctions lists, disclosed nominee/beneficiary information, publicly known information, Government or regulatory sources or reliable media information, etc

ix. The sanctions compliance program shall be an integral part of the overall AML/CFT/CPF compliance program.

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

xi. The company shall keep track of all the applicable sanctions, and where the sanction lists are updated, shall ensure that existing customers are not listed. The Company shall maintain list of all SROs as per format given in Addendum 5.

xii. Results of the screening (manual and or system based) shall be maintained which shall depict the results of the screening. The same shall be reviewed by the compliance officer and reported to the CEO and BODs on immediate basis and monthly basis, respectively.

The compliance office shall document the results of the screening with regard to screening performed against

- "Al-Qaida and Taliban related entities/individuals mentioned in the UNSC Consolidated List" as per Addendum 6 and
- "proscribed persons/organizations list of UN /NACTA" Addendum 7.

xiii. The company shall ensure that while screening the list of client against the sanctioned list, the client list shall include details including but not to be limited to
- Main account holder
- All joint account holders
- Nominees
- Major shareholders of legal clients (excluding listed companies)
- Board of Directors
- Trustees
- Authorized signatories
- Office bearers.

SECTION 4: COMPLIANCE PROGRAM

M. COMPLIANCE PROGRAM

i. In order to implement compliance program, the Company shall implement the following internal policies, procedures and controls:

a. compliance management arrangements, including the appointment of a compliance officer at the management level, as the individual responsible for the Company's

compliance with these Regulations, the AML Act and other directions and guidelines issued under the aforementioned regulations and laws;

b. screening procedures when hiring employees to ensure the integrity and conduct, skills, and expertise of such employees to carry out their functions effectively;
c. an ongoing employee training program; and
d. an independent audit function to test the system.

ii. For the serial no. i (a) above, the company shall ensure that the compliance officer:

a. reports directly to the board of directors or chief executive officer or committee;
b. has timely access to all customer records and other relevant information which they may require to discharge their functions, as well as any other persons appointed to assist the compliance officer;
c. has sufficient resources, including time and support staff;
d. be responsible for the areas including, but not limited to-

i. ensuring that the internal policies, procedures and controls for prevention of ML/TF are approved by the board of directors of the Company and are effectively implemented;
ii. monitoring, reviewing and updating AML/CFT/CPF policies and procedures, of the Company;
iii. providing assistance in compliance to other departments and branches of the Company;
iv. timely submission of accurate data/ returns as required under the applicable laws;
v. monitoring and timely reporting of Suspicious and Currency Transactions to FMU; and
vi. ensures regular audits of the AML/CFT/CPF program;
vii. maintains various logs, as necessary, which should include logs with respect to declined business, politically exposed person ("PEPs"), and requests from Commission, FMU and Law Enforcement Agencies ("LEAs") particularly in relation to investigations; and
viii. Responds promptly to requests for information by the SECP/Law enforcement agency.
ix. Provides guidance in day-to-day operations of the AML/CFT/CPF policies and procedures.
x. Is entrusted with other responsibilities as the company may deem necessary in order to ensure compliance with the regulatory requirements.

The compliance officer shall also refer all the Rules, Regulations, notices and directives issued by the competent authority along with the policy and procedures and in particular Annexure 2 (AML/CFT/CPF Compliance Assessment Checklist) as manual to ensure compliance with the applicable regulatory requirements.

SECTION 5: AML/CFT/CPF SYSTEMS AND CONTROLS

N. MONITORING AML/CFT/CPF SYSTEMS AND CONTROLS

i. The management shall utilize back office software as well, to ensure to monitor the risks identified and assessed as they may change or evolve over time due to certain changes in risk factors, which may include changes in customer conduct, development of new technologies, new embargoes and new sanctions. The management shall update the back office as appropriate to suit the change in risks.

ii. The company shall assess the effectiveness of its risk mitigation procedures and controls, and identify areas for improvement, where needed. For this purpose, the company shall consider monitoring following aspects:
   a. the ability to identify changes in a customer profile or transaction activity/behavior, which come to light in the normal course of business;
   b. the potential for abuse of products and services by reviewing ways in which different products and services may be used for ML/TF purposes, and how these ways may change;
   c. the adequacy of employee training and awareness;
   d. the adequacy of internal coordination mechanisms i.e., between AML/CFT/CPF compliance and other functions/areas;
   e. the compliance arrangements (such as internal audit);
   f. Changes in relevant laws or regulatory requirements; and
   g. Changes in the risk profile of countries to which the company or its customers are exposed to.

iii. For an effective monitoring of accounts, the same shall be achieved through a combination of computerized and through corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, effective monitoring mechanism.

iv. The Company shall ensure that it maintains programs and systems to prevent, detect and report ML/TF. The systems should be commensurate to the size of the business and nature of the company and the ML/TF risks to which it is exposed and should include:
   a. Adequate systems to identify and assess ML/TF risks relating to persons, countries and activities which should include checks against all applicable sanctions lists;
   b. procedures to undertake a Risk Based Approach (“RBA”);
   c. procedures and controls to combat ML/TF, including appropriate risk management arrangements;
   d. Customer due diligence measures;
   e. Record keeping procedures;
   f. An audit function to test the AML/CFT/CPF system;
   g. Screening procedures to ensure high standards when hiring employees; and
   h. An appropriate employee-training program.

v. It shall be the responsibility of the senior management to ensure that appropriate systems are in place to prevent and report ML/TF and that the company is in compliance with the applicable legislative and regulatory obligations and this policy.

O. THE THREE LINES OF DEFENSE

i. The Company shall ensure that the following three lines of defense to combat ML/TF remains established at all material times;

   a. Business units (e.g. front office, customer-facing activity):

   Business units should know and carry out the AML/CFT/CPF due diligence related policies and procedures.

As part of first line of defense, this policy shall be communicated to all employees. Further, clear description for employees of their obligations and instructions shall be provided. The employees shall ensure that they follow the procedures for detecting, monitoring and reporting suspicious transactions.

b. Compliance function:

Compliance function shall function in the manner as explained in section "M" of the Policy.

c. Internal Audit Function:

Internal audit, the third line of defense, should periodically conduct AML/CFT/CPF audits on company level and be proactive in following up their findings and recommendations.

P. INTERNAL CONTROLS (AUDIT FUNCTION, EMPLOYEE SCREENING AND TRAINING)

i. The company shall maintain internal controls and policies (appropriate to the ML/TF risks, and to the size of the company) in relation to:
   a. an audit function to test the AML/CFT/CPF systems, policies and procedures;
   b. employee screening procedures to ensure high standards when hiring employees; and
   c. An appropriate employee training program.

a) Audit Function

i. The company should, on annual basis, conduct an AML/CFT/CPF audit to independently evaluate the effectiveness of compliance with AML/CFT/CPF policies and procedures. The frequency of the audit shall be revisited after the evaluation of the risks identified during the risk assessments. The AML/CFT/CPF audits should be conducted to assess the AML/CFT/CPF systems which include:

   a. test the overall integrity and effectiveness of the AML/CFT/CPF systems and Controls;
   b. assess the adequacy of internal policies and procedures in addressing identified risks, including;
      (a) CDD measures;
      (b) Record keeping and retention;
      (c) Transaction monitoring; assess compliance with the relevant laws and regulations;
   c. test transactions in all areas of the company, with emphasis on high–risk areas, products and services;
   d. assess employees' knowledge of the laws, regulations, guidance, and policies & procedures and their effectiveness in implementing policies and procedures;
   e. assess the adequacy, accuracy and completeness of training programs;
   f. assess the effectiveness of compliance oversight and quality control including parameters for automatic alerts (if any), and

g. assess the adequacy of the company's process of identifying suspicious activity including screening sanctions lists.

b) Employee Screening

i. The company shall should maintain adequate 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 particular risks associated with the individual positions.

ii. Employee screening should be conducted at the time of recruitment and where a suspicion has arisen as to the conduct of the employee.

iii. The company 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 company 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.

c) Employee Training

i. The company 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.

ii. 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 in the company's business operations or customer base.

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

iv. Staff should be aware on the AML/CFT/CPF 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.

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

vi. The company shall obtain an undertaking from their staff members (both new and existing) confirming that they have attended the training on AML/CFT/CPF matters, read the company's AML/CFT/CPF manuals, policies and procedures, and understand the AML/CFT/CPF obligations under the relevant legislation. Undertaking with regard to the reading and understanding of the company's AML/CFT/CPF manuals, policies and procedures, and understand the AML/CFT/CPF obligations under the relevant legislation shall be obtained as per Addendum 8.

vii. 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 suspicious about a customer's activities, and actions to be taken when a transaction is considered to be suspicious.

viii. 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.

ix. 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.

x. Record with regard to training obtained from outside the company shall be maintained as per the format given in Addendum 9, whereas, record of all internal trainings shall be maintained as per the format given in Addendum 10.

SECTION 6: RECORD KEEPING

Q. RECORD KEEPING

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

   a. recording the documents the company is provided with when verifying the identity of the customer or the beneficial owner, and
   b. Transcription into the company's own IT systems of the relevant CDD information contained in such documents or obtained by other means.

ii. Where there has been a report of a suspicious activity or the company 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.

iii. The company shall keep and maintain all record related to STRs and CTRs filed by it for a period of at least 10 years after reporting of transaction.

iv. The company shall maintain, for at least 5 years after termination, all necessary records on transactions (obtained through CDD process including copies of identification documents, account opening forms, Know Your Customer forms, verification documents, other documents and result of any analysis along with records of account files and business correspondence) 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.

v. 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 negative verification(refer Addendum 1)

SECTION 7: ANNEXURES (ENCLOSED SEPARATELY)

I. AML/CFT/CPF ASSESSMENT

II. AML/CFT/CPF COMPLIANCE ASSESSMENT

III. RISK BASED ASSESSMENT

IV. ML/TF WARNING SIGNS/ RED FLAGS

V. IDENTIFICATION AND VERIFICATION OF CUSTOMER