WACEO

DECENTRILIZED ASSET COMPANY

MODEL KNOW YOUR CUSTORMER (KYC) POLICIES

15/03/2021

TABLE OF CONTENTS

1. **The Purpose of the Policy**

The DECENTRILIZED ASSET COMPANY (the "Company") is looking to make an effective Company system of prevention and detection of money laundering, terrorism financing activities, and Sanctions.

The Company demonstrates its full commitment and support to high standards of compliance with the Anti Money Laundering/Combating the Financing of Terrorism, and Sanctions (AML/CFT/SANCTIONS) requirements by establishing a strong and comprehensive policy, procedures, processes and system for the prevention and detection of money laundering, terrorism financing activities, and Sanctions violations (the "Policy").

This policy and related procedures are subject to periodic reviews to ensure that it remains robust and complies with the regulatory requirements and the international recommendations.

2. Definitions

Money Laundering

Money Laundering is the participation in any transaction that attempts to conceal or disguise the nature or origin of funds derived from illegal activities such as, fraud, corruption, tax evasion, organized crime, or terrorism, etc.

Terrorism Financing

Terrorism Financing refers to any activity that provides funding or financial support of any kind to the terrorist activities. The funds involved may have been raised from the legitimate sources as well as from the criminal sources.

Know Your Customer (KYC)

KYC is the process of identifying the customer and verifying the identity by using reliable and independent document and information. It is regarded as the basic tool for AML/CFT/SANCTIONS and its main objective is to enable the Company to know and understand its customers better and help them manage their risks prudently. If the Company is unable to apply appropriate KYC measures due to non-furnishing of information or non-cooperation by the customer, the Company has right to consider closing the account or terminating the Companying relationship after issuing due notice to the customer explaining the reasons for taking such a decision.

Customer

Customer is any person or entity engaged in a financial transaction or activity with the Company or someone on whose behalf the financial transaction or activity is being performed. For the purpose of this policy, a customer is a person or entity, who is attached to the Company through any one or more of the following events/activities:

- Maintains an account and/or has a business relationship with the Company.
- Engaged in one or more occasional transaction.

- Involved in carrying out wire transfers.
- On whose behalf the account is maintained (i.e. beneficial owner).
- Engaged in any business or transaction in any way with the Company.

Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognized as the global anti-money laundering (AML) and Combat financing of terrorism (CFT) standard.

Customer Due Diligence (CDD)

CDD is the process through which the Company develops an understanding of the customers and the money laundering, financing terrorism, and sanctions risks that they pose to the business. CDD is the cornerstone of the AML/CFT/SANCTIONS program. It involves gathering and verifying information about a customer's identity, beneficial owners and representatives.

Simplified Customer Due Diligence (SCDD)

Simplified Customer Due Diligence is the lowest level of due diligence that can be completed to the customer. Simplified CDD is the information obtained for all customers to verify the identity of a customer and assess the risk associated with that customer. Simplified Due Diligence will be applied, where the customer is considered to present a low risk of money laundering, terrorist financing, and sanctions.

Enhanced Customer Due Diligence (ECDD)

Enhanced Customer Due Diligence is the additional information collected of the customer to provide a deeper understanding of the customer activity to mitigate associated risk. Enhanced Customer Due Diligence is required where the customer and product/services combination is considered to be of higher risk. A high risk situation is where there is an increased risk for money laundering and terrorist financing through customer profiles and way of utilization of the products and services that are being offered to them.

Beneficial Owner

The "Beneficial Owner" is the natural person who ultimately owns or controls firm and/or a person on whose behalf the transactions is being conducted, and include person or persons who exercise ultimate effective control over a juridical person.

Shell Company/Entity

Shell Companies are the financial institutions or a group of financial institutions that have no physical presence in the country of origin or establishment and/or do not fall under any scope of effective regulation and supervision.

A shell company is an entity that has no active business and usually exists only in name as a vehicle for another company's business operations. In essence, shells are corporations that exist mainly on paper, have no physical presence, employ no one and produce nothing. Although they are legal entities that do have a legitimate function in business operations, shell companies are also utilized by criminals to facilitate fraudulent activities including money laundering.

Tipping Off

Tipping off is giving an idea of or disclosing information to the customer or any other unauthorized person(s) that his/her someone's account is being monitored or considered suspicious. Tipping Off is a punishable offence.

FATCA

"FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

Payable-Through accounts

Payable-Through accounts refer to the correspondent accounts that are used directly by the third parties, generally the customer of the respondent Company, to transact business on their own behalf.

Nested Accounts

Nested account occurs when a Company/FI (third party BFI) gains access of the financial services offered by the correspondent Company by operating through the correspondent account belonging to the another Company/FI i.e. of a respondent Company/FI.

Wire Stripping

Wire stripping is the deliberate act of altering or eliminating any material information from wire payments or instructions, thereby making the payment message/instruction difficult to identify the sanctioned entity and restrict payments to and from sanctioned parties or countries.

Sanctions

A sanction is a penalty levied on another country, Companies, institutions, companies, or on individual citizens of another country. It is an instrument of foreign policy and economic pressure that can be described as a sort of carrot-and-stick approach to dealing with international trade and politics.

3. Objectives of the Policy

Primarily this policy is prepared and implemented to prevent the Company from being used for money laundering, terrorism financing activities, and evasion of Sanctions. The following are the major objectives of this policy:

- To lay down policy framework to be implemented by the Company in order to safeguard it against being used, intentionally or unintentionally, by criminal elements for money laundering, financing of terrorism, and Sanctions evasion.
- To ensure full compliance by the Company with all the applicable legal and regulatory requirements pertaining to AML/CFT/SANCTIONS.
- To provide a broad framework for formulation and implementation of procedural guidelines required for effective AML/CFT/SANCTIONS & KYC compliance.

4. Scope and Application

This policy is applicable to all branches/offices of the Company and is to be read in conjunction with related Standard Operating Procedures (SOP) and guidelines issued from time to time.

The contents of the Policy shall be subject to changes/modifications as advised by the regulators and/or the Company from time to time.

Any provision laid down in this policy will be superseded by existing or future provisions of [XXX] applicable law ("[XXX] Law").

The standards set by this policy document will apply to both new and existing business relationships and across all the branches/units of the Company. Hence, in regards to the existing business relationships as well, it is essential to initiate corrective action and customer due diligence, where necessary.

5. Compliance of KYC Policy

The Company shall ensure compliance with KYC Policy through:

1. Company shall ensure that decision-making functions of determining compliance with KYC norms are not outsourced.
2. All of the Company Divisions shall ensure compliance of KYC guidelines in their respective areas of operation, products, services, activities etc.
3. Independent evaluation of the compliance functions of the Company policies and procedures, including legal and regulatory requirements to be done by Compliance Division.
4. Internal audit system to verify the compliance with KYC/AML policies and procedures and submit quarterly audit notes and compliance to the Audit Committee. At the end of every calendar quarter, implementation and compliance of concurrent audit reports on adherence to KYC-AML guidelines at branches would be reviewed for apprising Audit Committee of Board.
5. Concurrent / internal audit to also ensure verification of compliance with KYC guidelines in system through system generated reports.

6. The implementation of KYC, AML, ATF, and Sanctions policies and guidelines thought the Company.

6. Money Laundering, Terrorism Financing, and Sanctions

6.1 Money Laundering

Money Laundering is the process used to disguise the source of money or assets derived from criminal activity. Money laundering facilitates corruption and can destabilize the economies of susceptible countries. It also comprises the integrity of legitimate financial systems and institutions, and gives organized crime the funds it needs to conduct further criminal activities. Generally, money launderers tend to seek out areas in which there is low risk of detection due to weak or ineffective AML programme. Because the objective of Money Laundering is to get the illegal funds back to the individual who generated them. Therefore, Companies have been the targets for Money Laundering.

While the techniques for laundering funds vary considerably and are often highly intricate, there are generally three stages in the process:

Stages / Process of Money Laundering

Placement: Involves placing the proceeds of crime in the financial system. It refers to the physical disposal of cash, often in the form of Company deposit, through a succession of small and anonymous transactions. The money launderers insert the illicit money into a legitimate financial institution.

Layering: This stage involves converting the proceeds of crime into another form and creating complex nature of financial transactions to disguise the audit trails and the source and the ownership of funds. (e.g. buying and selling of commodities, stocks, property etc). It involves Company to Company transfers, wire transfers, several deposits and withdrawals, purchasing high value items, etc.

Integration: In this stage the money re-enters the mainstream economy in the legitimate looking form. It involves placing the laundered proceeds back in the economy under the veil of legitimacy. It would be very difficult to trace the original source of the money if there is no proper documentation in the previous two stages of Money Laundering.

6.2 Terrorism Financing

The financing of terrorism is where funds or other property is made available, directly or indirectly, with the sole intention that the funds be used to further terrorism or to initiate terrorist acts to be carried out.

The primary goal of individuals and entities involved in the financing of Terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

6.3 Sanctions

Before opening a new Company account necessary screening will be performed so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations or whose name appears in the lists circulated by OFAC, the European Union, the United Nations Security Council (UNSC), OFAC, watch list by Interpol, and any other related list. These are done using the list/ information/ databases available on information sources/tools.

The Company shall prepare a profile for each new customer based on risk categorization, as provided subsequently in this policy. The customer profile will be a confidential document and details contained therein shall not be divulged for cross selling or any other purposes.

7. Legal Framework

7.1 International Perspective

Financial Action Task Force (FATF) 40 + IX Recommendations

The Financial Action Task Force (FATF) is an independent inter-governmental body established in 1989 by the ministers of its member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the financial system.

The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard. The FATF recognizes that the countries have diverse legal, administrative and operational standards and different financial systems, and so all cannot take identical measures to achieve the common objectives of countering the money laundering and terrorism financing threats. The FATF Recommendations, therefore, set an international standard, which countries should implement through measures adapted to their particular circumstances in order to:

- Identify the risks, and develop policies and domestic coordination.
- Pursue money laundering, terrorist financing and the financing of proliferation.
- Apply preventive measures for the financing sector and other designated sectors.
- Establish powers and responsibilities for the competent authorities and other institutional measures.
- Enhance the transparency and availability of beneficial ownership information of legal persons and arrangements.
- Facilitate international cooperation.

8. Company's Effort to combat Money Laundering, Financing of Terrorism, and Sanctions Evasion

8.1 Company's Policy on KYC, AML, CFT, and SANCTIONS

The Company's policy on Know Your Customer and AML/CFT/SANCTIONS shall apply to all the branches, units and businesses of the Company. This Policy shall be the benchmark for

the supervision of systems and procedures, controls, training and other related matters in the implementation of the KYC guidelines in the Company.

By the very nature of its functioning, the Companies are more susceptible to the risk of money laundering and the possibility of its various services being unwittingly used as conducting and cycling the ill-effects of the tainted/illegal money by the launderers. As an organization committed to the prevention of money laundering and terrorism financing activities, the Company shall take following measures:

- Develop internal procedures and technology that assists the Company in monitoring transactions for the purpose of identifying possible suspicious activities.
- The Company will continue to update policies and procedures in line with the laws, regulations and regulatory guidelines. Compliance Department will be delegated the task of overseeing the Company's policies, practices and procedures with regards to AML/CFT/SANCTIONS.
- The Company will take all reasonable steps to ensure that Customer Due Diligence information is collected and up-to-date, and that identification information is updated in the event where the Company comes to know about any changes with regards to the parties involved in the relationship.
- The Company will take reasonable steps to verify the identity of the customers, including the beneficial owners of corporate entities, and the principals behind customers acting as the agents.
- The Company shall ensure that the Internal Audit Department on periodic basis and Compliance Department randomly observe audit requirements of KYC guidelines and verification of itsimplementation at branches and other operational units of the Company.
- The Company shall not tip-off its customers regarding suspicious transactions and /or any internal/external investigation being carried on them.
- The Company shall not maintain any relationship with shell companies.
- The Company shall cooperate with any lawful request for information made by authorized government agencies/statutory bodies during their investigation.
- The Company shall ensure that the training sessions on KYC and AML/CFT/SANCTIONS procedures and guidelines are included in the Training calendar of the Company on an ongoing basis. The Company shall arrange to update and module these training sessions to make all the concerned fully understand the rationale behind the KYC and AML procedures and implement them consistently.
- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts and/or establishing any business relationship with the Company, and as well to ensure transparency, the Company shall publish this Policy in the Company's website. It will be the primary duty and responsibility of Operational Staff to educate the customers and tactfully/convincingly explain the need for customer profile and its relevance in enabling the Company/Branch to render better customer service.
- The Company shall establish clear lines of internal responsibilities and reporting.

8.2 Company's Framework of AML/CFT/SANCTIONS

The standards of KYC and AML/CFT/SANCTIONS of the Company are designed to facilitate the businesses and other support units meet their responsibilities in relation to the prevention of the activities related to money laundering, terrorist financing, and Sanctions evasion. These

standards have been designed based on the relevant acts, rules and regulations, regulatory guidelines and the Company practices on prevention of money laundering and terrorism financing activities. Further, these standards will be reviewed based on the subsequent amendments in the relevant laws, rules and regulations, regulatory guidelines and recommendations.

The Company's KYC and AML/CFT/SANCTIONS standards are based on the following 4 Pillars:

I. Customer Acceptance Policy.
II. Customer Identification Procedures.
III. Monitoring of Transactions.
IV. Risk Management.

8.2.1. Customer Acceptance Policy (CAP)

Company's Customer Acceptance Policy (CAP) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Company broadly are:

- No account shall be opened in the name altering from the primary identity document, anonymous or fictitious name(s), blank names or CIFs/accounts with numeric/alphanumeric characters only.
- Accounts/CIF shall be opened only in the name of natural and legal person/organization, the name being the same as in the primary identity document of the person/entity. Accounts may however be opened with different account titles identifying the nature/use/purpose/type/ of account at the written request of the legal person/organization with appropriate control parameters.

Minimum required information and documents i.e. proper identification and information pertaining to the prospective client shall be obtained prior to account opening or performing business relation of any kind, pursuant to [XXX] Laws, and to the product paper/policy/guidelines set forth by the Company.

- Necessary checks are done before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, or sanctioned individuals and entities, etc. No account is opened where identity of a customer/prospect matches with any person or entity in the Sanctions lists (domestic and International).
- Not to maintain account relationship or conduct any kind of Company transaction (except for deposit to the respective blacklisted customer's account) with the individuals/entities blacklisted by [XXX] authorities until release from the list.
- Not to open an account, where the staffs designated to open new accounts, find sufficient ground that the identity of the prospective customer could not be verified and/or the prospective customer is not disclosing the required identity, the reason for opening account, transaction frequency and volume, etc and any other information deemed necessary for account opening. The refusal shall be properly documented and communicated to HO AML/CFT/SANCTIONS Compliance Officer through Branch AML/CFT/SANCTIONS Compliance Officer.

Further, the Company shall freeze an existing account under the situation where the designated staff is unable to apply appropriate customer due diligence measures i.e. unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data /information furnished to the Company. Decision for closure of such accounts shall be approved by Senior Management level official under recommendation of AML/CFT/SANCTIONS Compliance Officer at HO and also after giving due notice to the customer explaining the reason for such decision. Closure of such accounts shall be informed to [XXX] authorities if applicable in written.

- The Company shall not establish any business relationship with the shell companies and the institutions that deal with shell companies. Any identified business relationship with the financial and other institutions that allow the transaction of shell Company, will be discontinued.
- The Company shall not be associated with any entity located in the jurisdictions identified by the FATF as "FATF blacklist" or those fully sanctioned by the agencies that the Company refers to like, UN, OFAC, HMT, EU etc. Further, special attention shall be given for conducting any transactions involving individuals/entities located in the jurisdictions under "FATF Grey list" and under sectoral Sanctions by the Sanctions imposing agencies. Prior approval from executive level authority within the functional structure shall be obtained for the same.
- The Company shall not offer services like payable-through accounts and nested accounts services to its respondent Company/FIs while offering correspondent Companying services to the Company and FIs.
- Implementation of CAP should not be too restrictive resulting in denial of Company services to the general public, especially those who are financially or socially disadvantaged.
- The decision to open an account for Politically Exposed Person (PEP) and Person in Influential Position (PIP) shall be approved by Senior Management Level official. Information of such account shall be provided to the AML/CFT/SANCTIONS Compliance Officer at HO.

8.2.2. Customer Identification Procedures (CIP)

Customer Identification Procedure means undertaking client due diligence measures including identifying and verifying the customer and the beneficial owner. The first requirement of knowing the customers for anti-money laundering purposes is to be satisfied that a prospective customer is who he/she claims to be. The second requirement of knowing the customer is required also to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake or any expected, or predictable pattern of transaction, which would enable the Company in risk profiling of the customer.

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information to the Company's satisfaction and also to satisfy the competent authorities that the due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

The Customer Identification procedures are to be carried out at the following stages;

- While establishing a Company relationship; onboarding of the account relationships.

- When the Company feels it is necessary to obtain additional information from the existing customers based on the conduct or behavior of the account.
- When any customer (non-account holder) conducts a transaction with the Company, greater than the thresholds specified by the regulatory.
- When Company sells third party products as agent.
- When the Company has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
- Customer identification will also be carried out in respect of non-account holders approaching Company for high value one-off transaction as well as any person or entity connected with a financial transaction which can pose significant reputational or other risks to the Company.

While identifying the natural person or legal person, the Company shall obtain the documents, data and information as prescribed in the Company's procedural guidelines. All the documents and information pertaining to the identification of the natural and legal person should be retained in a legible manner and in the managed way. The Company may deploy a specialized central unit to facilitate and streamline the customer identification process and proper recording of the customer information digitally.

8.2.2.1. Identification of Customer through e-KYC

While establishing an account based relationship with individual customer, the Company shall make necessary verification so as to ensure that only one customer identifier number is assigned to the respective customer. Biometric Based e-KYC authentication can be done by the Company for the natural person. The Company may deploy e-KYC both for online based account opening and updating the existing customer information.

Accounts opened using e-KYC, in non face to face mode are subject to the following conditions:

- There must be specific consent from the customer for authentication through OTP.
- The customer should qualify for simplified due diligence standards set by the Company. In case any terms to fulfill the simplified due diligence is breached, the account shall be ceased from withdrawal operation till the Company's customer due diligence procedures are fulfilled at least to the Basic/Standard level.
- Accounts opened using OTP based e-KYC authentication shall not be allowed for operation for more than one year within which identification as per Basic Due Diligence Procedures is to be carried out.

8.2.2.2. Customer profiling and Risk based Customer Due Diligence

(a) Company shall prepare a profile for each new customer based on risk categorization. In general, Risk categorization should take into account the following risk variables specific to a particular customer or transaction:

  - Information relating to customer's identity, social/financial status.
  - The purpose of account or business relationship.
  - Nature and size of transaction undertaken by the customer.
  - Type of product/service availed by the customer.
  - Country or the Jurisdiction where the customer or customer's business.

- Beneficial owners of the customer.
- Level of regulation or governance regime to which a customer is subjected to.
- Duration of relationship with the customer and regularity / trustworthiness of the customer.
- Knowledge of local laws, rules and regulations, structure and extent of regulatory oversight.
- Transparency and Disclosure requirements.
- Intermediaries and business partners of the customer.
- Countries National and Sectoral Risk Assessment Reports as available.
- Investigation Reports of Distinguished International organizations working in the fight against money laundering, financing of terrorism, and Sanctions evasion.

(b) Based on the above criteria, Company shall categorize its customers into low risk, medium risk and high risk category based on its assessment and risk perception of the customers, identifying transactions that fall outside the regular pattern of activity and not merely based on any group or class they belong to. The nature and extent of due diligence, may be based on the following principles:

(i) Individuals (other than High Net Worth) and entities, whose identity and source of income, can be easily identified, and customers in whose accounts the transactions conform to the known profile, is categorized as low risk. Illustrative examples include salaried employees and pensioners, people belonging to lower economic strata, government departments and government owned companies, regulators and statutory bodies, etc. Company shall perform Simplified Due diligence of low risk customer.

(ii) Customers who are likely to pose a higher than average risk are categorized as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Company shall perform Basic Due diligence of medium risk customer.

(iii) Customers requiring very high level of monitoring, e.g., those involved in cashintensive business, accountsof bullion dealers (including sub-dealers), jewelers and Politically Exposed Persons (PEPs) of domestic or foreign origin etc. are categorized as high risk. Company shall perform Enhanced Due diligence of high risk customer.

Other customers to be categorized as high risk are:

a) High net worth individuals.

b) High Cash Incentive Businesses.

c) PEPs of domestic and foreign origin; customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.

d) Non-face to face customers.

e) Those with dubious reputation as per public information available, etc.

(iv) The risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer based on various risk indicators, like, customer type, customer behavior, profession, nature and scope of business, product type, volume and nature of transaction, beneficial owners, transaction partners, etc.

(v) In addition to what has been indicated above, Company shall further define the detail procedural guidelines to take steps to identify and assess the AML/CFT/SANCTIONS risk for customers, countries and geographical areas as also for products / services / transactions / delivery channels and will frame controls and procedures to effectively manage and mitigate the risk adopting a risk-based approach.

8.2.2.3. Ongoing customer Due Diligence and periodic review

Customer Due Diligence information shall be regularly reviewed, even after the completion of account opening or the commencement of any kind of relationship with the customer. The frequency of review shall be based on the level of risk associated with the kind of relationship maintained by the customer and such review will be recorded in the concerned customer file. High risk customer relationship and transaction of high volume and close to threshold, for instance, will be reviewed at more frequent intervals than the medium and low risk relationships.

Any shortcomings in CDD information detected in the review must be regularized as soon as possible. Additional information should be taken about the existing customers where it is apparent that the existing CDD information is out of date or inadequate.

Any information on changes in nature and volume of transaction, changes in nature and scope of business operation, change in ownership and/or change in person controlling a relationship, information on identified beneficial owner, or any other identified worthy alteration can be taken as a trigger update CDD information of the customer.

Company shall not insist on the physical presence of the customer for the purpose of furnishing information or furnishing consent for authentication/verification of information supplied unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, in the course of ongoing due diligence, the documents and information of the customer obtained through any reliable means shall be acceptable.

The operating procedures framed under this policy shall summarize the CDD requirements and identification standards for the customer categories across the Company. For any customer category, whether or not specified by such guidelines, CDD requirements and identification procedures must be in line with this policy document and the regulatory guidelines.

8.2.2.4. Due Diligence of Vendors/Service Providers/Business Partners

The Company shall conduct Due Diligence of its vendors, service providers, and other business partners in alignment with the KYC norms from the perspective of AML/CFT/SANCTIONS. Appropriate measures shall be taken to ensure that the third-party relationships do not pose significant money laundering and terrorism financing risks to the Company. The procedural measures formulated under this policy shall incorporate the due diligence standards for the following third party relationships of the Company:

- Listed vendors and service providers from whom the Company makes necessary procurements, rents the space and avails services as per the Company's procurement by laws and guidelines.
- Firms, individuals, institutions and companies hired by the Company for consulting services.
- Individuals, firms, companies and organizations entered into contract by the Company for performing specific job on behalf of the Company as a third party agent and/or the business partner.
- Financial or non-financial entities that the Company establishes any kind of business relationships during its operation.

The Company shall collect information about the potential business partners through direct contact, basic internet searches and database checks, input or supervision from an independent business function of the Company and assistance from any reliable external sources if deemed necessary.

The Company shall deny maintaining any kind of relationship with the third party where:

- The party is not able to prove its legitimacy.
- The party present false, misleading or incorrect information to the Company.
- The party wants to work without a contract or with a vague contract that do not meet the minimum standards as defined by the Company.
- The party refuses or is hesitant to provide any documentation required by the Company regarding the disclosure of identity, nature and scope of its business and its beneficial owners.
- The party requests for any indirect and unusual payment or billing procedure like payment to anonymous Company account, payment through shell companies, payment through foreign Company accounts other than the country where the services are being performed, payment in high value cash or through bearer cheque, etc.
- The party in any way (directly or indirectly) is incorporated in a jurisdiction identified by FATF to be a non-cooperative jurisdiction.

8.2.2.5. Identification of PEPs (Politically Exposed Persons)

Politically Exposed Persons are individuals who are or have been entrusted with prominent public functions in a country e.g. Heads of states/Governments, senior politicians, senior government/judicial/military officers, senior executives of state owned corporations, important political party officials, etc. The Company shall have the option of establishing a relationship with PEPs provided that:

- Sufficient information including the sources of fund, family members and close relatives is obtained on the PEP.
- The identity of the person shall have been verified before accepting the PEP as a customer.
- Prior approval has been taken from Senior Management Level official for opening the account of PEP.
- Accounts of PEPs shall be subject to enhanced monitoring on an on-going basis. In the event of an existing customer or a beneficial owner with significant control of an existing account is known to be a PEP or subsequently becoming

a PEP, approval from Senior Management Level official shall be obtained to continue a business relationship.

- The account of PEPs and their family members and close relatives as far as identified, shall be subject to enhanced CDD measures including enhanced monitoring on an on-going basis.

The instructions as above shall also be applicable to any account(s) where a PEP is identified to be a significant beneficial owner.

In order to ensure that the Company's customers and prospects are adequately identified regarding whether or not he/she falls under the PEP category, the Company may develop its own list of PEPs or alternately the Company may procure/use the PEPs list databases provided by various authorized and/or dedicated vendor from among those providing service in the [XXX] market.

Delisting of PEPs

For the purpose of fulfilling KYC and due diligence requirements as per this policy, any individual identified to be a PEP shall remain as PEP at least for the period of 5 years from the complete release of the prominent position. Thereafter the Company shall have the authority to release any individual from the PEPs list depending upon the current profile of the person and significance of the person to remain as a PEP. Compliance Officer and/or the officials designated by the Compliance Officer of the Company shall have the authorities to decide on whether or not any person shall remain to be identified as PEP after release from a prominent position as defined through National AML legislations.

8.2.2.6. Identification of Sanctioned Entity

The Company shall adopt appropriate measures to monitor effectively the compliance with AML legislation, rules and regulations governing the freezing of funds and assets of the sanctioned person/entity, specifically the Sanctions list of individuals and entities circulated by the UNSCR, OFAC, EU, and HMT. The Company shall ensure effective implementation of a dedicated Sanctions list databases from the dedicated service provider so as to ensure that no relationship is being maintained with any sanctioned entity.

Any prospect customer or the customer before onboarding or during ongoing due diligence or initiating cross border transactions including wire transfers, should be scrutinized against the Sanctions list databases maintained by the Company.

Any customer/prospects of the Company if identified/suspected to be a sanctioned entity, shall be reported to the [XXX] authorities through Compliance Officer pursuant to [XXX] Laws, by freezing of funds and postponing any relationship with the Company until further instruction from the regulator.

8.2.2.7. Adverse Media Screening

Adverse media screening, also known as negative news screening, involves searching for negative news about a person or business i.e. the interrogation of public data sources and third-party data sources for negative news or broadcasts associated with an individual or company,

for proactive customer risk management in terms of mitigating the risk of money laundering and terrorism financing. The adverse media screening shall include the following:

- All the prospects and existing customer shall be subject to screening against the adverse media screening databases and public data sources.
- The Company may procure and implement a dedicated adverse media screening tool and databases from the authorized vendors/third-party from among those available in [XXX].
- The screening results shall be reviewed in order to confirm the matches.
- If the matches are confirmed, the customer shall be assigned a high risk rating depending on the nature of adversity. Further, the account may even be debit restricted, if deemed necessary, and the report of same shall be submitted to the [XXX] authorities.
- In case of confirmed prospects, the Company may turn down the request to maintain any kind of relationship with such, depending on the adversity of the new.
- Compliance Officer and/or designated officer shall extend necessary coordination to the screening units where adversities have been escalated for further clarification and further course of action.

8.2.2.8. Identification of Beneficial Owners

When a customer is acting (or appears to be acting) on behalf of others, sufficient evidences on identification of both the parties (i.e. agent and the principal agent) must be obtained. The Company shall take all reasonable steps to verify the beneficial owner of the customer account and/or business relationship. Where the customer is a legal person, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridic al person, has/have a controlling ownership interest or who exercise control through other means that may include right to appoint directors or to control management or policy decisions through voting agreements, shareholders agreements, etc.

The Company shall identify and obtain KYC information of the beneficial owners where;

- The beneficial owner is the relevant natural person holding 10 percent or more shares or has obtained voting right.
- The beneficial owner is the relevant natural person who holds the position of senior management official in an organization/institution.

The Following measures shall be considered for identification of a Beneficial owner:

a) Obtain relevant information from the customer or obtain self declaration of the customer.
b) Publicly available information regarding the customer.
c) Analyzing the information available in social media.
d) Obtain Information from the Legal records maintained as per prevailing laws.
e) Available Databases of business and profession.
f) Obtain information from the related government organization if needed.

Where the customer is a trust or similar type of organization, the identification of beneficial owner(s) shall be the identification of the author of the trust, the trustee, director, the beneficiaries and any other natural person exercising ultimate effec tive control over the trust through a chain of control or ownership.

Where the customer or the beneficial owner is the company listed on a stock exchange, or is a subsidiary of such company, or is foreign company listed in stock exchange being regulated by the regulatory authority of the country known to have adequately implemented the international standards on money laundering and terrorism financing, it is not necessary to identify and verify the identity of any shareholder or the beneficial owner of suc h companies. Documents and all the records related to the beneficial owners shall be kept safe for the period of 5 years from the date of termination of relationship or transaction.

8.2.2.9. Identification in Wire Transfers

Wire transfers are used as an expeditious method for transferring funds between Company accounts. As wire transfers do not involve actual movement of currency, they are considered as a rapid method for transferring value from one location to another. Prior to initiating wire transfers of any amount in any currency, the Company shall obtain following information at minimum, with the customer.

- Originator's Name.
- Originator's Account number or in case of non account holder, a separate transaction identification code.
- Originator's address or birth date and birth place or citizenship number or national identity card number or customer identification number.
- Beneficiary's name and account number or in case of non account holder, a separate transaction identification code of the beneficiary.
- Any other information as specified by the regulatory authorities.

Inter-Company transfers and settlements where both the originator and beneficiary are Company and financial institutions would be exempted from the above documentation requirements.
Wire transfer is an instantaneous and preferred route for transfer of funds and hence, there is a need for preventing launderers and criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse.

The Company shall retain basic information about the originator of the wire transfers as stated above and make available to the appropriate law enforcement and prosecutorial authorities when asked for in order to assist them in detecting, investigating, prosecuting launderers and criminals and tracing their assets.

The Company shall perform name or Sanctions screening of the customer and all related parties to the wire transfer transactions as well as Sanctions screening of the payments or swift messages related to the trade finance transactions.

The Company shall ensure that wire stripping activities are not being conducted in the transfer messages/payments such that full compliance is been ensured to block payments linked with the sanctioned individuals, entities and countries. Resubmission of any transaction previously rejected due to any concerns over Sanctions, shall be denied and records of such transactions rejected and any attempts of resubmission, shall be maintained by the concerned department. Necessary control mechanism and approaches shall be formulated to ensure that wire stripping activities are prevented.

The Company shall obtain true identity of the beneficiary while making payment of the wire transfers. All the wire transfers must be accompanied by accurate and meaningful originator and beneficiary information.

The Company shall retain in record all the information and document related to wire transfers at least for 5 years from the date of transaction. Where the staff, initiating the wire transfer has reason to believe that a customer is intentionally structuring the wire transfers to below threshold limits to several or same beneficiaries in order to avoid documentation or reporting requirement, the Company shall insist on complete originator and beneficiary identification before effecting the transfer. Where the customer is not cooperative, the Company shall make necessary efforts to establish the identity and report suspicious transaction report to [XXX] authorities if applicable.

8.2.2.10. Identification in Cross border Correspondent Companying

Correspondent Companying is the provision of Companying services by one Company (correspondent Company) to another Company (the respondent Company).

Following measures shall be taken by the Company while maintaining cross border correspondent Companying relationship.

- Correspondent Companying relationship shall be established only after the approval of Senior Management Level official.
- The Company should be satisfied that the respondent Company has verified the identity of the customers having direct access to the accounts and is undertaking ongoing due diligence measures so as to ensure that the respondent Company is able to provide the relevant customer identification data immediately on request.
- The Company shall not establish correspondent Companying relationship with 'shell Companys' and shall further ensure that the respondent Company do not allow the operation of accounts by the shell Company.
- The Company shall ensure that the respondent Companys have adequately in place the anti money laundering policies and procedures and apply adequate due diligence procedures for transactions conducted through the correspondent accounts.
- On the basis of publicly available information, the Company shall be familiar with the reputation of respondent Company, its supervision standards, and should identify whether or not the respondent Company has been under investigation and/or regulatory action in regards to money laundering and financing of terrorism activities. The information in this regard shall be properly maintained in the respondent Company profile.
- Correspondent Company Services of the Company shall be restricted of any payable-through services and nested services for direct access by the customer or the underlying third party of the respondent Company/FIs.

8.2.3. Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC/AML/CFT/SANCTIONS procedures. The Company will exercise ongoing due diligence with respect to every customer and closely examine the transactions to ensure that they are consistent with the customer's profile and sources of funds as per extant instructions. The ongoing due diligence is based on the following principles:

a) The extent of monitoring depends on the risk category of the account. High risk accounts have to be subjected to more intensified monitoring.

b) Company will pay particular attention to the following types of transactions:

i. Large and complex transactions, and those with unusual patterns, which have no apparent economic rationale or legitimate purpose.
ii. Transactions which exceed the thresholds prescribed for specific categories of accounts.
iii. Transactions involving large amounts of cash inconsistent with the normal and expected activity of the customer.
iv. High account turnover inconsistent with the size of the balance maintained.

c) Company shall closely monitor the transactions in accounts of individuals or firms. In the accounts where there are multiple small deposits (generally in cash) and multiple withdrawal (generally in cash) near to the threshold amount defined by regulator across the country in one Company account, the operations in such accounts will be analyzed and in case any unusual operations or suspicious transactions are noticed in the accounts, the matter will be immediately reported to [XXX] authorities if applicable pursuant to [XXX] Law. The Company shall implement a dedicated Monitoring Software for automated monitoring of customer transactions in order to identify the transactions of suspicious nature.

d) Special attention shall be given to business relationships and transactions with persons from or in countries identified by FATF to insufficiently apply the FATF recommendations or identified to be non-cooperative in the fight against money laundering and financing of terrorism. Also, special attention shall be giving to persons, countries, companies, and institutions subject to Sanctions.

8.2.4. Internal Control and Risk Management

Company will exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with its knowledge about the clients, their business and risk profile and where necessary, the source of funds. Company shall also ensure that, before launching of new products and services or modifying the existing features, formulation and implementation of necessary procedures and guidelines, reasonable measures are being taken to identify and assess money laundering and terrorism financing risks being posed by the products and services and its inbuilt features, nature of transactions and delivery channels, procedural guidelines, etc under concurrence from Compliance and Corporate Governance Department to manage and mitigate the identified risks and comply with the KYC, and AML/CFT/SANCTIONS legislations.

8.2.4.1 Internal control system

8.2.4.1.1 AML/CFT/SANCTIONS unit and AML Compliance Officer

The Company shall have a separate AML/CFT/SANCTIONS unit headed by the Compliance Officer designated by the Company pursuant to the AML/CFT/SANCTIONS regulatory guidelines who will directly report all the matters on AML/CFT/SANCTIONS to the Board committee in charge of this matters. The Company will assign the responsibility of the AML/CFT/SANCTIONScompliance Officer to the Managerial level staff at Head Office to function as a focal point for implementation and compliance of this Policy and guidelines

formulated to execute this Policy in practice. The Compliance officer designated by the Company in this regard will have overall responsibility for maintaining oversight and coordinating with various divisions/departments in the implementation of KYC and AML/CFT/SANCTIONS policy. However, primary responsibility of ensuring implementation of this policy and related guidelines will be vested with the respective Branches/Divisions. Branch AML Compliance officer would ensure proper implementation and reporting, as per provisions of this policy, to the Compliance officer at Head office, that will be the Head of Compliance and Corporate Governance Department, who will be responsible for following major duties though are not limited and to comply/get it complied with all the regulatory provisions and legal KYC and AML/CFT/SANCTIONS standards:

- Overall monitoring of the implementation of the Company's KYC and AML/CFT/SANCTIONS policy.
- Ensuring that proper KYC mechanism is implemented pursuant to applicable laws and regulations.
- Ensuring that records are kept properly in regard to KYC and AML/CFT/SANCTIONS Policy of the Company.
- Monitoring and reporting of transactions, and sharing of information, as required under the law.
- Interaction with the Company AML/CFT/SANCTIONS Compliance Officers at branches for ensuring full compliance with the Policy.
- Timely submission of Threshold Transaction Reports (TTRs) and Suspicious Transaction Reports (STRs) to [XXX] authorities if applicable.
- Maintaining Liaison with the government agencies, regulating authority, Companys and other institutions, which are involved in AML/CFT/SANCTIONS.
- Ensuring submission of periodical reports to the Executive Management/AML/CFT/SANCTIONS Committee/Board.
- Train/Educate staffs on KYC and AML/CFT/SANCTIONS compliance issues through dissemination of relevant specified guidelines and circulars, rules, regulations, notices, standards, manuals, internal codes of conduct.

The reporting line of authority for issues pertaining to KYC and AML/CFT/SANCTIONS compliance shall be to the Chief Compliance Officer and Legal Counsel, by the Compliance Officers that manage all the request from the Company. The CEO or President of the Company shall receive a weekly briefing of the ongoing compliance matters in the Company.

Head of AML/CFT/SANCTIONS Department, the Compliance officer, shall be responsible for the general oversight of the Company's KYC and AML/CFT/SANCTIONS Policy, effectiveness of control, monitoring and reporting procedures and to establish and maintain adequate arrangements for training on KYC and AML/CFT/SANCTIONS. The obligations of the AML/CFT/SANCTIONS Compliance Officer is as follows:

1. Function as focal point to perform tasks in accordance with [XXX] Law, these Rules and the Directives.
2. Cause to maintain secure record of transaction.
3. Provide information about suspicious or other necessary transaction to the [XXX] authorities through letter or electronic means of communication like fax and email.
4. Provide information about transaction of the branch offices to the other Company Units and to [XXX] authorities in a regular basis if applicable.

If applicable pursuant to [XXX] law, the details of AML/CFT/SANCTIONS Compliance Officer including name, designation, address, qualification, contact number, email etc. shall be furnished to [XXX] authorities and information regarding the change in AML Compliance Officer and details thereof shall also be furnished to the [XXX] authorities.

AML/CFT/SANCTIONS Unit at Central Level:

AML/CFT/SANCTIONS at Central level shall reside within the AML/CFT/SANCTIONS department at Head Office. Monitoring and analysis of AML/CFT/SANCTIONS alerts, including the Sanctions information in SWIFT's Sanction Screening Portal, shall be done at the centralized AML/CFT/SANCTIONS on a daily basis. Makers/checkers at the centralized AML/CFT/SANCTIONS Unit will analyze alerts pertaining to their respective assigned branches on day to day basis and will close the alerts after thorough analysis of the transactions/alerts and ensure that all the transactions are genuine in nature and match with the business profile of the customer known to the Company. STRs on all suspicious transactions shall be put up to the AML/CFT/SANCTIONS Officer immediately for recommendation and further approval and onwards submitted to the [XXX] authorities through the Compliance Officer if applicable.

8.2.4.1.2 Branch AML/CFT/SANCTIONS Compliance Reporting Officer

AML/CFT/SANCTIONS Compliance Officer at HO will have overall responsibility of maintaining oversight and coordinating with various divisions/departments in the implementation of KYC and AML/CFT/SANCTIONS policy. However, primary responsibility of ensuring implementation of KYC and AML/CFT/SANCTIONS policy and related guidelines/procedures will be vested with the respective branch/division. For this purpose, a staff will be designated from each branch as Branch AML/CFT/SANCTIONS Compliance Officer who would ensure proper implementation and reporting, pursuant to the provisions of this Policy, to the AML/CFT/SANCTION Compliance Officer at HO. Where separate Branch AML/CFT/SANCTIONS Compliance Officer is not designated, the Operation Officer, or the staff officiating the said position will be assuming the responsibilities of the Branch AML/CFT/SANCTIONS Compliance Officer. The Branch AML/CFT/SANCTIONS Compliance Officer shall have a direct reporting line to the AML/CFT/SANCTIONS Compliance Officer at Head Office for all KYC and AML/CFT/SANCTIONS related issues.

8.2.4.1.3 Internal Audit Department

Company has entrusted Internal Audit Department with the responsibility to test the implementation and adherence of Company's KYC and AML/CFT/SANCTIONS policy and procedures. As a part of the Internal Audit Plan, the Company's Internal Audit will provide an independent evaluation of implementation status of KYC and AML/CFT/SANCTIONS policy including legal and regulatory requirements. Internal Auditor shall specifically check and verify the application of KYC and AML/CFT/SANCTIONS procedures at the branches and comment on the lapses observed in this regards. The findings/recommendations should be reported directly to the Compliance officer and the Audit Committee.

9. Reporting Requirements to [XXX] Authorities

9.1 Reporting of Suspicious Transaction

Whilst all unusual transactions are not automatically linked to AML/CFT/SANCTIONS, unusual transactions become suspicious if they are considered inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account. The suspicious transaction or activity shall be reported to [XXX] authorities if applicable, as soon as possible within 3 days of the detection of suspicion. Compliance Officer and/or the designated officer shall ensure that the Suspicious Transaction/Activities Reports are duly submitted to [XXX] authorities in digital form as well, through goAML application.

A key to recognizing suspicious transactions is to know enough about the customer to recognize that a transaction, or series of transaction, is unusual for that particular customer. So, any transaction that has a reasonable ground to arouse suspicion that the proceeds may be of illegitimate activity, may be applied in illegitimate activity or do not seem to have any rational and lawful purpose can be taken as suspicious transaction. Further, suspicion can also be roused by the behavior or identity of the customer. For such account activity/transaction or observation, the Company shall file the Suspicious Transaction Report (STR) to [XXX] authorities if applicable at the earliest as per the regulatory requirement in the prescribed format. The Company shall not put any restriction on operation of account where an STR has been reported.

Appropriate internal record of the STR been filed will be maintained for necessary references and undertakings. Also, even if a transaction/activity is been found to be satisfactory after proper analysis, thus not requiring to raise STR, the same shall be recorded appropriately.

Some of the areas, but certainly not all, where staff should remain vigilant to possible money laundering situation are suspicious cash transactions, suspicious transaction using customers' accounts, suspicious transactions using electronic Company services, suspicious use of letter of credit, suspicious loan transactions, etc. The fact that any of the suspicion do occur in any of the areas, does not necessarily lead to the conclusion that money laundering, financing terrorism, and Sanctions evasion has taken place, but they could well raise the need for further investigation on the transaction/activity.

The Company shall extend full cooperation for any lawful request made by government agencies, and other regulatory bodies, during their investigation into money laundering, financing terrorism, and Sanctions evasion without "tipping-off" the customer, unless is required by applicable [XXX] law.

No information regarding the customer collected through CDD shall be disclosed to the unauthorized person/organization including the Company staffs and/or family members and friends, in any means, except to the agency, organization or official(s) legally mandated to receive such information.

The detailed procedures for the reporting of suspicious transaction shall be as described in the procedural guidelines for suspicious transaction reporting framed under this Policy. The copies of disclosures made to the authorities shall be retained, together with the record of all other related documents including the inquiries undertaken in regards to the submitted record. Similarly, appropriate records shall be retained regarding the non disclosure of any internal

records to the authorities to demonstrate that at the time there was insufficient justification for making such a disclosure.

The Company shall extend full and prompt cooperation to all the legal requests to provide customer information to the authorities, necessary to assist their investigations in regards to money laundering, terrorism financing, and Sanctions. Under no circumstances should the customer or any other unauthorized parties be informed regarding the making of such disclosure by the Company, as such notifications may compromise on an existing or potential investigation by the authorities unless is authorized by [XXX] law.

10. Training and Awareness

Relevant laws, regulations, policies and procedures, and other informative and educative materials shall be communicated to all the employees of the Company so that they are adequately aware of the regulatory requirements as well as the internal policies and procedures regarding the KYC and AML/CFT/SANCTIONS. The Company shall also provide training to all the relevant departments and employees of the Company that manage information relating to AML/CFT/SANCTIONS.

The main purpose of AML/CFT/SANCTIONS training is to ensure that the employees are aware of the risk of ML/FT/SANCTIONS faced by the Company and how they should respond when confronted with such risks. Training will be provided on AML/CFT/SANCTIONS legislation, AML/CFT/SANCTIONS policies, procedures and controls on regular basis and all the information regarding the training shall be recorded appropriately.

The Company shall assess the learning requirement to the BOD members due to changes in acts, policies, procedures related to AML/CFT/SANCTIONS and develop learning and development program to the Board members, executive management and major stakeholders of the Company in coordination with internal /external expert, and other institutions.

11. Recruitment/Hiring of Employees

Keeping in mind that KYC norms/ AML standards / CFT measures / applicable Sanctions have been prescribed to ensure that offenders are not allowed to misuse Company channels, the Company will put in place necessary and adequate screening mechanism to know its Employee as an integral part of recruitment/hiring process of its personnel. Company shall regularly update the Employee information and their details as part of Know Your Employee (KYE).

All employees will be educated that in case, if any loss occur to a customer because of lawful submission of information to the [XXX] Authorities by the Company or its staff, none of the officials of the Company will be liable for the same. However, in case of failure to report any suspicious activities, the Company could be subject to sanctions by [XXX] authorities.

12. Secrecy of Information

Any staffs or authorities of the Company shall not disclose any of the reports, documents, records, details or information that have been prepared pursuant to the requirements of AML/CFT/SANCTIONS legislation, rules, regulations, directives and guidelines, to the customer or to any other unauthorized person/agent unless the disclosure/act has been required for fulfillment of the responsibilities as per the provisions stated by [XXX] Law, rules and

directives. In case the disclosures have identified to be made against the AML and Sanctions legislations and this policy, the person shall be subject to disciplinary action as per the Company's rule.

Information collected from the customers for the purpose of opening of account and/or satisfying the KYC requirements shall be treated as confidential and details thereof shall not be divulged for any purpose to the unauthorized person/entity without the express permission of the customer, unless disclosure is mandatory by law.

13. Retention of Record

Adequate records of identification, address verification, account opening and transactions will be retained for the prescribed period enabling to provide a clear audit trail in the event of need and investigation. Following documents and details will be retained, for the period as prescribed by law/policy after the business relationship has ended.

- Documents relating to the identification and verification of customer and related beneficial owner.
- Documents relating to national and international transaction.
- Documents relating to attempted transaction and business relationship.
- Records relating to suspicious transaction report.
- Records of employee code of conduct and trainings in regards to KYC and AML/CFT/SANCTIONS.

All the documents pertaining to the prevention of Money Laundering, Combating Financing Terrorism, and Sanctions including monitoring reports made by the Compliance Officer and the action taken as a consequence, records showing the dates of KYC, AML/CFT/SANCTIONS training and the names and acknowledgement of the staffs receiving the training shall be retained for the period as prescribed by [XXX] law. All records maintained should be available to the authorized persons promptly on request without any undue delays.

14. Employees' Code of Conduct

Staff will maintain a code of conduct in regards to KYC, AML/CFT/SANCTIONS by taking into account the following standards:

- The Company might inform in some cases the customers about the suspicion of their nature of transaction.
- The Company staff shall not talk/disclose about ongoing investigation of suspicious transaction or about customer's activity with other employees or friends or family members.
- The Company staff will comply with the instruction given in accordance to the Company Policies by the competent authority and immediate supervisor or line manager/s.

The Company staff will be liable to cooperate with the competent authorities during the process of investigation. All the employees of the Company shall make necessary declarations and ensure full compliance with the Company's Employees' code of ethics and other applicable policies.

15. Roles and Responsibilities

15.1 Roles and Responsibilities of BOD

The Board of Directors or applicable body within the Company shall be responsable for:

- To review and approve this Policy document on KYC and AML/CFT/SANCTIONS and its subsequent amendments from time to time.
- To review the reports submitted by the Compliance Officer through CEO, with respect to the Company's compliance with legislation and other requirements contained therein and provide directions to the Company Management as required.
- To discuss on setting up and improving mechanism to prevent customer's suspicious and abnormal transaction or money laundering based on the report submitted by the Compliance Officer, at least on quarterly basis, and make necessary arrangements to this effect.
- To review the status of implementation of AML/CFT/SANCTIONS [XXX] Laws, and the provisions contained in the directives, circulars and guidelines issued by regulatory bodies at least on quarterly basis and furnish the review report on the implementation of the directives to [XXX] authorities if appliable on half yearly basis.

15.2 Roles and Responsibilities of CEO and the Chief Compliance Officer

The Chief Compliance Officer and the CEO of the Company shall be responsible to review on quarterly basis as to whether or not the provisions of the of AML/CFT/SANCTIONS [XXX] Laws. Further, a brief summary relating to this shall also be disclosed in the annual report of the Company.

The Chief Executive Officer will be responsible for reviewing and approving the controlling, monitoring and reporting procedures formulated for the effective implementation of this Policy on KYC and AML/CFT/SANCTIONS.

16. Review and Amendments of the Policy

This policy shall be reviewed annually. Any amendments, if deemed necessary, to this Policy shall be approved by the BOD, except specifically mentioned in this policy. In case any confusion in the interpretation of this policy arises, the matter shall be referred to the BOD through AML Committee and the decision made therein, shall be the final and binding.

17. Power to formulate appropriate operating procedures

Appropriate guidelines, manuals and other operating procedures required for effective implementation of the provisions laid down in this Policy, will be approved by the CEO and the same shall be furnished to the BOD for information. Such procedures and supplementary guidelines shall be construed as the part of this Policy and shall be read in conjunction with the provisions contained in this Policy.

18. Applicable Laws

This Policy shall be read in conjunction with the applicable laws of [XXX] relating to AML/CFT/SANCTIONS, [XXX] Law Directives on KYC, Sanctions, and AML, Unified Directives issued by [XXX] Authorities, Suspicious Transaction Reporting Guidelines, Threshold Transaction Reporting Guidelines, and directives, circulars, rules and regulations issued pursuant to [XXX] Law, and other relevant act/rules/guidelines issued by other competent/regulatory authorities from time to time. If any provision contained herein this policy and procedures formulated within the scope of this policy contradict with the changing regulatory provisions in the scope of AML/CFT/SANCTIONS, the existing regulatory provisions will prevail and the provisions herein shall be deemed as void to the extent of contradiction.

19. Introduction of New Technologies

The Company shall pay special attention to any AML/CFT/SANCTIONS, threats that may arise from new or developing technologies that might favor anonymity, and take measures, if needed, to prevent its use in money laundering, Sanctions, and CFT schemes.