Anti Money Laundering & Counter Terror Financing Policy

I. PURPOSE OF Anti Money Laundering & Counter Terror Financing Policy (the **"Policy"**)

Company Food and Logistics Private Limited, its subsidiaries/affiliates (collectively referred to as the **"Company"**) are committed to conducting its business ethically in accordance with all applicable laws and regulations and enhance its reputation in the market. This Policy formalizes Company's approach to the identification, mitigation and management of the risk that Company's products and services might be involved in the facilitation of money laundering or the financing of terrorism. The Policy is global in nature and outlines standards to meet regulatory and ethical obligations in the economies in which Company does its business. This contributes to the stability, integrity and strength of its financial system and protects Company from reputational damage and regulatory action. The Policy is subject to regular review to ensure it remains consistent with regulator expectations and industry standards. The core principles for the management of Money Laundering & Terror Financing risks are as given underneath.

Core Principles:

Company opposes the crimes of money laundering and/or terrorist financing and maintains a framework to identify and mitigate the risk that its products and services could be used for the aforementioned purposes.

Company will report any activity it detects, which is suspicious and may involve potential money laundering and/or terrorism financing, to the applicable regulator.

Company will comply with the anti-money laundering laws and counter-terror financing laws and the relevant rules and regulations formulated thereunder of the countries where Company has place of business through which Company provides products or services or has operations or other places where Company provides products or services or has operations

Company will endeavour to provide its products and services only for legitimate purposes to stakeholders whose identities have been reasonable ascertained by Company.

Company will take reasonable steps to ensure that sufficient funding and resources are available for the implementation and performance of activities required by Company's anti-money laundering (**"AML"**) and counter-terrorist financing ("**CTF"**) program.

Company's employees are required to attend AML/CTF training on quarterly basis and screening to understand their obligations under the relevant laws, rules, regulations and sanction compliance.

Company will monitor its investors and all its stakeholders and their transactions, and its employees, consistent with the level of money laundering and terrorist financing risk they represent. Company will manage new and revised changes to Company's products, business processes and systems to ensure that money laundering and terrorist financing risks are identified and managed.

Company will follow all Know Your Customer (**"KYC**") policies and procedures relevant to the regions in which it operates.

II. DEFINITIONS & INTERPRETATION

Prevention of Money Laundering Act, 2002 (PMLA):PMLA provides the key legislative framework for the prosecution of money laundering. The primary legal authority responsible for investigating and prosecuting money laundering offences under PMLA at the national level is the Directorate of Enforcement (ED), under the aegis of the Department of Revenue, Ministry of Finance. In addition to the above, regulators such as the Reserve Bank of India ("**RBI**"), Securities & Exchange Board of India ("**SEBI**") and the Insurance Regulatory & Development Authority of India (IRDAI) are empowered to deal with issues relating to money laundering activities and lay down guidelines on anti-money laundering (AML) standards. These guidelines, read with PMLA and the relevant rules and regulations formulated under the PMLA, form the core of the legal framework for AML law and enforcement in India.

Money Laundering (ML): ML is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin. More precisely, it may encompass three distinct, alternative areas - the conversion or transfer, knowing that such property is the proceeds of crime, the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime and the acquisition, possession or use of property, knowing, at the time of the receipt, that such property is the proceeds of crime. Under PMLA, the term "property" means any property or assets of any description, whether corporeal or incorporeal, movable or immovable, tangible or intangible; includes deeds and instruments evidencing title to, or interest in, such property or assets, wherever located; and covers property of any kind used in the commission of an offence under PMLA or any of the scheduled offences. By the very nature of its definition, ML involves obtaining/deriving proceeds arising from the commission of a criminal offence. Criminal activities, such as drug trafficking, smuggling, human trafficking, corruption and others, tend to generate large amounts of profits for the individuals or groups carrying out the criminal act and in order to benefit freely from the proceeds of their crime, they conceal the illicit origin of these funds.

Terrorism Financing (TF): TF involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, a person commits the crime of financing of terrorism if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an offense within the scope of the International Convention for the Suppression of the Financing of Terrorism. The primary goal of individuals or 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.

Corporate Criminal Liability: Under PMLA, both natural and legal persons may be prosecuted for the offence of money laundering. Section 70 of PMLA recognises corporate criminal liability; it states that where a company contravenes PMLA or its rules, every person who was in charge of or responsible for the actions/business of the company at the time of the contravention was committed, as well as the company, shall be deemed guilty and liable to be proceeded against under PMLA. Hence, in addition to the liability accruing on natural persons for contravention of PMLA and the rules formulated thereunder (**"PML Rules"**), other legal entities may also attract liability and can be fined for such contraventions. However, as per the proviso to Section 70, the person who was in charge of or responsible for the actions/business of the company at the time the contravention was committed may contend in their defence, and prove that such contravention took place without their knowledge/despite all due diligence. A company may be prosecuted irrespective of whether the prosecution/conviction is contingent on the prosecution or conviction of any individual.

Penalty: Under PMLA, fines ranging from INR 10,000 to 100,000 for each failure can be imposed on legal entities who qualify as Reporting Entities, if they fail to maintain records or supply relevant information in the prescribed manner under PMLA and the PML Rules. Although PMLA and the PML Rules do not provide for the revocation of licences of Reporting Entities, regulators such as Reserve Bank of India and Securities and Exchange Board of India regulating the Reporting Entities may take such actions based on their circulars relating to KYC and AML. Properties that are derived or obtained, directly or indirectly, by any person as a result of criminal activities relating to a scheduled offence are subject to attachment/confiscation under PMLA.

Due Diligence: Reporting Entities are required to verify the client's identity at the time of commencement of an account-based relationship with the client including the beneficial ownership, if applicable, or while carrying out a transaction of an amount equal to or exceeding INR 1,00,000, whether conducted as a single transaction or several transactions that appear to be connected or while carrying out any international money transfer operations.

Clients Due Diligence (CDD): Stakeholders for the purpose of this Policy includes customers, clients, partners, investors, shareholders, vendors and business stakeholders. Any of the methods applied by criminals to launder money or finance terrorism involve the use of the financial system to transfer funds. The application of strict due diligence and a high degree of transparency is crucial to fight ML and the TF effectively. Due diligence will be applied upon establishment of a business relationship or in preparation of a (i) specific cash transactions in excess of a certain amount, (ii) suspicious activity report/suspicious

transaction report. It will also be applied whenever there is any suspected ML or TF activities. The basic steps of due diligence are the appropriate identification of a stakeholder and/or beneficial owner, the verification of the identity of the stakeholder or beneficial owner, as well as the collection of information on the stakeholder's purpose and nature of the business relationship.

for high-risk customers, i.e. those for whom the sources of funds are not clear, need to be specifically dealt, on a case to case basis. These include non-resident customers, high-net-worth individuals, trusts, charities, non-governmental organisations ("**NGO"**), not-for profit organisations ("**NPO**") and organisations receiving donations (NPOs and NGOs promoted by the United Nations or its agencies may be classified as low-risk customers), companies with close family shareholding or beneficial ownership, firms with "sleeping partners", politically exposed persons of foreign origin, customers who are their close relatives and accounts of which they are the ultimate beneficial owner and non-face-to-face customers and those with dubious reputations as per publicly available information.

Politically Exposed Persons (PEPs): PEPs mean the individuals who are or have been entrusted with prominent public functions e.g., Heads of States/Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

Suspicious Transaction: The PML Rules mandate the reporting of those transactions, including an attempted transaction, whether or not made in cash, which to a person acting in good faith give rise to a reasonable ground of suspicion that the transactions may involve the proceeds of a scheduled offence specified in the schedule to PMLA, regardless of the value involved, appear to be made in circumstances of unusual or unjustified complexity, appear to have no economic rationale or bona fide purpose or give rise to a reasonable ground of suspicion that the transactions may involve the financing of activities relating to terrorism. Furthermore, for reporting suspicious transactions, apart from "transactions integrally connected", "transactions remotely connected or related" must also be considered by the Reporting Entities.

Record Keeping or Reporting Large Currency Transactions: Under the PML Rules, the records maintained must contain information including the nature of the transactions, the amount of the transaction and the currency in which it was denominated, the date on which the transaction was conducted and the parties to the transaction, to enable the Reporting Entity to reconstruct individual transactions.

Beneficial Owner: PMLA defines "beneficial owner" as an individual who ultimately owns and controls a Reporting Entity's client or the person on whose behalf a transaction is being conducted, which includes a person who exercises ultimate effective control over a juridical person. Under PMLA and the PML Rules, it is the responsibility of a Reporting Entity to identify and maintain records of documents evidencing the identities of its clients and beneficial owners, and to file a copy of the records with the Central KYC Records Registry. These records must be maintained for a period of five years after the business relationship between a client and the Reporting Entity has ended or the account has been closed, whichever is later. Additionally, the Reporting Entity is required to take enhanced due diligence steps to examine ownership prior to the commencement of specified transactions. Pursuant to the RBI Master Direction and SEBI AML Guidelines, all records, memoranda and clarifications sought in relation to relevant transactions should be made available to the auditors, RBI, SEBI, Financial Intelligence Unit and any other relevant authorities during the audit or inspection, or as and when required. Further, as per Section 90 of the Companies Act, 2013 (**"CA 2013"**) a company shall maintain a register of significant beneficial owners which must be open to inspection by any member of the company. The competent authorities at the RoC have access to the information recorded. Further, the CA 2013 also provides that the Central Government may at any time appoint inspectors to investigate a company's real ownership.

Reporting Entities: PMLA lays down the broad framework for AML compliance requirements applicable to banking companies, financial institutions, intermediaries and persons carrying out a designated business or profession (collectively, "**Reporting Entities**"). Pursuant to PMLA and the PML Rules, Reporting Entities are required to undertake certain AML measures that include, inter alia, customer identification, estimated date of delivery, customer acceptance, maintenance of records, and tracking and reporting of certain types of transactions. Reporting Entities must ensure implementation of PMLA provisions, including operational instructions issued from time to time. "Reporting Entities" include person(s) carrying out certain designated business or profession, as the Central Government may designate by notification. There are no specific AML

requirements applicable to persons engaged in international trade or to persons of certain geographical areas.

III. Applicability under PMLA

Company does not fall specifically under the gambit of 'Reporting Entities', however, Company ethos will be to follow the provisions of PMLA and other associated and connected laws and regulations, in letter and spirit so that any cash transactions of the value of more than Rs 10 Lacs or its equivalent in foreign currency and all series of cash transactions integrally connected to each other which have been valued below Rs 10 Lacs or its equivalent in foreign currency where such series of transactions take place within one calendar month, will be treated as 'Suspicious Transactions'. All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place will also be treated as 'Suspicious Transactions'.

Company will designate an officer as 'Principal Officer[1]' who would be responsible for ensuring compliance of the provisions of the PMLA. The Chief Executive Officer (CEO) and/or Chief Financial Officer (CFO) is nominated as Principal Officer.

IV. Compliance to PMLA

The checklist for compliance as per PMLA as applicable is as below will be taken as guideline by the Principal Officer:

a. One Time/Periodical Compliances: This policy framework on AML measures is put into place as approved by board of directors of Company and Mr. Srikanth Gandini, Chief Financial Officer appointed as 'Principal Officer'. A proper record of transactions will be maintained and preserved. An internal mechanism will be ensured for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities and for the purpose of satisfactory audit trail.
b. Stakeholders Due Diligence: Records of the identity of stakeholders will be maintained along with sufficient information in order to identify persons who beneficially own or control various accounts. Identify beneficial ownership and control, i.e. which individuals own or control the stakeholders and/or the person on whose behalf a transaction is being conducted. Stakeholders Due Diligence will be conducted on a risk sensitive basis depending on the type of stakeholders business relationship.
c. Monitoring of Transactions: Regular monitoring of transactions will be done for ensuring effectiveness of the AML procedures. Special attention will be given to all complex, unusually large transactions/patterns which appear to have no economic purpose.
d. Suspicious Transaction Monitoring and Reporting: Transaction of suspicious nature will be monitored and reported to the higher authorities. CDD process will be revisited when there are suspicions of money laundering or financing of terrorism.
e. Training to Staff and Hiring Policies: Adequate training to persons specifically dealing with such matters and in general it would be ensured that all staff members understand these provisions. Awareness and vigilance to guard against ML,TF and sanctions compliance will be developed. Adequate screening procedures, as determined by the board of directors of Company will be implemented to ensure high standards in relation to sanctions compliance when hiring employees.
f. Audit/Testing of AML Program: Audit will be conducted annually to test AML Programme adequacy to meet the compliance requirements. This audit will be conducted under an independent third party.

V. INTERNAL POLICIES, PROCEDURES, AND CONTROLS

Policies and procedures set under this Policy shall cover:

a. Communication of policies relating to prevention of ML and TF and sanctions compliance to all management and relevant staff;
b. Stakeholders due diligence measures, including requirements for proper identification;
c. Maintenance of records;

[1] Note to Company: The Compliance Officer can be designated as Principal Officer.

d. Compliance with relevant statutory and regulatory requirements;
e. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information, if required;
f. Role of internal audit or compliance function to ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF and sanctions compliance, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of stakeholders and other such factors. Internal audit/inspection shall verify compliance at least on an annual basis. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects.

g. This Policy should be reviewed from time to time to conform with the PMLA and PML Rules.

VI. KNOW YOUR CLIENT (KYC) NORMS

Client Due Diligence Process will involve:

a. Policy for acceptance of clients

b. Procedure for identifying the clients

c. Transaction monitoring and reporting especially suspicious

KYC norms will be laid down to include:

a. Where a stakeholder is a person, the steps to be taken to identify the stakeholder and its beneficial owner(s) and to take all reasonable measures to verify his/her identity to their satisfaction so as to establish the beneficial ownership.

b. Where the stakeholders is a company, it shall submit one certified copy of the following documents:
    i. Certificate of incorporation;
    ii. Memorandum and Articles of Association;
    iii. Resolution from the board of directors of Company and power of attorney granted to its managers, officers or employees to transact on its behalf;
    iv. An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
c. No client will be allowed the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.
d. While implementing the KYC norms on juridical person company shall verify that any person purporting to act on behalf of such stakeholders is so authorised and verify the identity of that person.
e. At any point of time, where company is no longer satisfied about the true identity and the transaction made by the stakeholders, a Suspicious Transaction Report should be initiated.

VII. SIMPLIFIED DUE DILIGENCE (SDD)

SDD should be resorted to for amounts not exceeding INR 10,000/ for an accounts based relationship, wherein any of the identification documents like passport, driving licence, proof of possession of Aadhaar number, Voter's Identity Card, PAN card, job card issued by NREGA duly signed by an officer of the State Government, letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government are sufficient. SDD measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher-risk scenarios apply, based on the Risk Assessment/categorization.

VIII. ENHANCED DUE DILIGENCE (EDD)

Where the risks of money laundering or terrorist financing are higher, company will be required to conduct enhanced due diligence measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Conducting enhanced due diligence should not be limited to merely documenting income proofs. It would mean having measures and procedures which are more rigorous and robust than that of normal KYC. These measures should be commensurate to the risk. While it is not exhaustive, the following are some of the reasonable measures in carrying out enhanced due diligence:

a. More frequent review of the stakeholders' profile/transactions
b. Application of additional measures including gathering information from publicly available sources
c. Review of the proposal/contract by a senior officials.
d. Measures so laid down should be such that it would satisfy competent authorities (regulatory/enforcement authorities), if need be at a future date, that due diligence was in fact observed in compliance with the guidelines and the PMLA.
e. Company shall increase the future monitoring of the business relationship with the stakeholders, including greater scrutiny or transactions where any specified transaction or series of specified transactions undertaken by a stakeholder is considered suspicious or likely to involve proceeds of crime.

XII. RISK ASSESSMENT/ CATEGORIZATION

Company shall carry out ML and TF risk assessment (including sanctions compliance assessment) exercise periodically at least once in a year to identify, assess, document and take effective measures to mitigate its ML and TF risk for clients, stakeholders or geographic areas, products, services, services, nature, volume of transactions or delivery channels etc. Risk assessment so carried out be documented, consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied, be kept up to date; and be available to competent authorities and self-regulating bodies. As part of the risk assessment, company will classify the stakeholders into high risk and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence. For the high risk profiles, like for stakeholders who are non-residents, high net worth individuals, trusts, charities, NGO's and organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, PEPs, and those with dubious reputation as per available public information who need higher due diligence, KYC and other procedures should ensure higher verification and counter checks.

XIII. CONTRACTS WITH PEPs

Company shall devise procedure to ensure that proposals for contracts with high risk stakeholders are concluded only after approval of legal department and senior management officials. Proposals of PEPs will be specifically approved at director level. If any existing stakeholder subsequently becomes or found to be PEP, senior management should be informed on this business relationship and apply enhanced due diligence measures on such relationship.

XIII. NEW BUSINESS PRACTICES/DEVELOPMENTS

Company shall pay special attention to ML threats that may arise from development of new products, new business practices including new delivery mechanisms or use of new or developing technologies for both new and pre-existing products. Special attention should especially, be paid to the 'non-face-to-face' business relationships brought into effect through these methods. The extent of verification in respect of such 'non face-to-face' stakeholders will depend on the risk profile of the product and that of the stakeholders. Company shall have in place procedures to manage specific increased risks associated with such relationships e.g. verification of details of the stakeholders through on-site visits.

XIV. IMPLEMENTATION OF SECTION 51A OF THE UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967 (UAPA)

The company will not enter into a contract with a stakeholders whose identity matches with any person in the (i) UN sanction list, (ii) Office of Foreign Assets and Control and/or other relevant sanction list with banned entities and those reported to have links with terrorists or terrorist organizations. Company shall periodically check the respective websites of MHA (Ministry of Home Affairs), Office of Foreign Assets and Control and/or organisations of other relevant jurisdictions for updated list of banned entities.

XV. CONTRACTS EMANATING FROM COUNTRIES IDENTIFIED AS DEFICIENT IN AML/CFT REGIME

Company is required to conduct EDD while taking risk exposure to individuals/entities connected with countries identified by Financial Action Task Force (**"FATF")** as having deficiencies in their AML/CFT regime. Additionally, the Company is required to pay special attention to business relationships and transactions, especially those which do not have apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined and written findings have to be maintained for assisting competent authorities. Company needs to go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF recommendations while using the FATF public statements. Similar measures should be taken on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption).

XVI. REPORTING OBLIGATIONS

Principal Officer will ensure record of all transactions including, the record of all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency, all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency, all transactions involving receipts by non-profit organisations of value more than INR 10,00,000 or its equivalent in foreign currency, all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions, all suspicious transactions whether or not made in cash and by way of deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or travellers cheques, or transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to nostro and vostro accounts, or any other mode in whatsoever name it is referred to, credits or debits into or from any non-monetary accounts such as demat account, security account in any currency, money transfer or remittances in favour of own stakeholders or non-stakeholders from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by payment orders, cashiers cheques, demand drafts, telegraphic or wire transfers or electronic remittances or transfers, internet transfers, automated clearing house remittances, lock box driven transfers or remittances, remittances for credit or loading to electronic cards, or any other mode of money transfer by whatsoever name it is called; loans and advances including credit or loan substitutes, investments and contingent liability by way of subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitised participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or purchase and negotiation of bills, cheques and other instruments, foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support, collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to, all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency

where either the origin or destination of fund is in India, all purchase and sale by any person of immovable property valued at INR 50,00,000 or more that is registered by the reporting entity, as the case may be.

XVII. RECORD KEEPING

Principal Officer or other connected persons are required to maintain the information/records of types of all transactions under PMLA as well as those relating to the verification of identity of stakeholders for a period of five years. Such records must be sufficient to permit reconstruction of individual transactions including the amounts and types of currency involved, if any, so as to provide, if necessary, evidence for prosecution of criminal activity. In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. The records referred shall contain all necessary information specified by the Regulator to permit reconstruction of individual transaction, including the nature of the transactions, the amount of the transaction and the currency in which it was denominated, the date on which the transaction was conducted and the parties to the transaction. The Principal Officer shall maintain a record of (i) all the breaches under the applicable laws exceeding [●] and (ii) training to the employees with respect to this policy.

XIX. EXEMPTIONS/ RELAXATION

Notwithstanding the standards mentioned for SDD of these guidelines, the company may avail different exemptions/ relaxations from the stipulated KYC norms in certain conditions, such as for continued operation of accounts of existing stakeholders of not more than aggregate premium of INR 50,000/- in a financial year. However, the exemptions/relaxations are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific higher-risk scenarios apply, basis the risk assessment/categorization policy of the insurers. Illustrative list of suspicious transactions is as under:

a. Stakeholders insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information;
b. Frequent cancellation by stakeholders;
c. Assignments to unrelated parties without valid consideration;
d. Request for purchase beyond apparent need;
e. Documentation from a place where he does not reside or is not employed;
f. Frequent request for change in addresses;
g. Overpayment with a request for a refund of the amount overpaid;
h. Media reports about a stakeholders;
i. Information sought by Enforcement agencies;
j. Unusual termination of contracts;
k. Borrowings/ seeking loans

The list is only illustrative and not exhaustive.

XX. PERIODIC REVIEW AND EVALUATION

Audit committee will monitor the effectiveness and review the implementation of this Policy, considering its suitability, adequacy and effectiveness. Company reserves the right to vary and/or amend the terms of this Policy from time to time. The Company shall refresh the KYC process periodically as per the directions of the board of directors of the Company.

XXI. CONCLUSION

An effective anti-money laundering/counter financing of terrorism framework must address both risk issues - it must prevent, detect and punish illegal funds entering the financial system and the funding of terrorist individuals, organizations and/or activities. AML and CFT strategies converge and they aim at attacking the criminal or terrorist organization through its financial activities, and use the financial trail to identify the various components of the criminal or terrorist network. This implies to put in place mechanisms to read all financial transactions, and to detect suspicious financial transfers. Company will ensure that regular compliance reviews and independent audits of AML/CTF program and procedure documents and execution

against established standards will be carried out. Company will create a robust AML/CTF training program to educate employees in implementing and maintaining AML/CTF program and in relation to sanctions compliance. All employees will undergo initial AML/CTF and sanction compliance training when they join Company. In addition, there will also be ongoing training requirements for all employees. Company's Management will ensure that it follows all applicable laws, rules and regulations.

This Policy is also required to be operated in coordination of the Anti Corruption policy as both are linked in numerous ways, and especially in recommendations that promote, in general, transparency, integrity and accountability. Corruption is also a source of ML as it generates large amounts of proceeds to be laundered. Corruption may also enable the commission of a ML offense and hinder its detection, since it can obstruct the effective implementation of a country's judicial, law enforcement and legislative frameworks. When authorities are empowered to investigate and prosecute corruption-related money laundering they can trace, seize and confiscate property that is the proceeds of corruption and engage in related international cooperation. When corruption is a predicate offense for money laundering, AML preventive measures can also be more effectively leveraged to combat corruption.