Policy Document

Customer Due Diligence (CDD)
Anti Money Laundering (AML)
Combating Financing of Terrorism (CFT)

Version 1.3

April 2018

Table of Contents

1. Introduction

1.1. Purpose Of This Policy

The purpose of this policy is to ensure that the products and services of Kaah International Microfinance Services ("KIMS") are not used to launder the proceeds of crime and that all of KIMS's staff are aware of their obligations and the need to remain vigilant in the fight against money laundering and terrorist financing. The document also provides a framework to comply with applicable laws and regulatory guidelines especially those related to detection and reporting of suspicious activities.

For more information please contact KIMS Internal Audit Team on compliance@kimsmfi.com.

N.B.

- KIMS at present does not have a dedicated Compliance Team (Compliance Head and Senior Compliance Office) nor a dedicated Internal Audit Team. Due to the limited size of the business these roles are currently being performed by KIMS Financial Manager. It is intended that these dedicated teams and job functions will be created and posts filled during 2018.
- KIMS will be developing a Procedural Handbook for use in conjunction with this Policy.

1.2. Scope Of The Policy

This policy applies to each and every business segment and all employees of KIMS to effectively mitigate the risk of Money Laundering ("ML") and Financing Terrorism ("FT"). Financial institutions in general are prone to the risk of being misused by criminal elements for their ulterior motives. To address the risks stemming from potential misuse, this policy will be a guiding document for concerned employees towards managing the customer's risks in an effective way using the risk based approach.

KIMS will further refine its Customer Due Diligence ("CDD") process using the risk based approach, through implementation of a systematic Customer Risk Profiling under the Customer Due Diligence process, various sets of documents are formulated and provided to the branches, offices and peripherals from time to time to ensure execution of the process and identification of risks attached to each customer for effective mitigation of ML / FT risk.

Considering the huge size of informal and undocumented sector in the economy, execution of due diligence process is complex and time consuming. However, in order to follow best practice, to be in compliance with regulatory requirements and to contain the customer related risks, it has become inevitable to conduct proper due diligence of every existing and prospective customer.

1.3. Objectives

- To prevent criminal elements from using KIMS for money laundering activities.
- Ensuring that only bonafide and legitimate customers are accepted.
- Verifying the identity of customers using reliable and independent sources.
- Ongoing monitoring of customer accounts and transactions to prevent or detect potential ML / F T activities.
- Implementing Customer Due Diligence process using risk based approach.
- To effectively manage customer - driven risks by using procedures as mentioned in CDD AML & CFT Procedural Handbook.
- Managing reputational, operational, legal and concentration risks, etc.
- To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, laid down procedures and best practice.
- To comply with the applicable laws and regulatory guidelines.

1.4. Revision

The CDD, AML & CFT Policy and Procedural Handbook will be reviewed periodically every 18 months for necessary updates and to propose any required or recommended changes to the Board of Directors for their approval. The Board of Directors will authorise and issue the most up-to-date version of the policy.

KIMS will notify employees of any changes using both electronic and printed notice. Any changes to this Policy document will be kept up to date by the distribution of additional or revised individual Policies and Procedures on a regular basis. All employees must abide by the latest version of CDD, AML & CFT Policy as amended from time to time.

1.5. Overview Of Kaah International Micro Finance

Kaah International Microfinance Services (KIMS) was established in 2013, by Kaah Express Financial Services a privately-owned money transfer services company, established on February 2000 with its headquarters in Dubai Airport Free Zone. KAAH Express has licenses from different countries in North America, Europe, Africa, Asia and Australia. Kaah Express is also affiliated with both local and international financial institutions and business organisations. KIMS was registered on June, 2013 to operate as a non-banking financial institution (NBFI). As an NBFI comes under the regulatory oversight of the Central Bank of Somalia (CBS). In addition KIMS is currently seeking a specialised microfinance bank licence under the banking licensing procedures of the Central Bank of Somalia.

Kaah Express is managed by experienced individuals who have been actively involved in the remittance and financial sector for the past twenty years. Since its foundation, the company had adopted a transparent management system with full compliance to all local and international regulations. The company has also a Chief Compliance Officer and External Compliance Auditor.

As a microfinance service provider, KIMS is committed to providing affordable and efficient services to its customers. KIMS operates through Kaah Express's substantial operational infrastructure and agent network, enabling significant cost savings and rapid national reach. Moreover, this delivery model enables KIMS to expand to meet market demand much more quickly than conventional 'bricks and mortar" microfinance institutions.

Through the introduction of this new, commercially-viable model of financial access, KIMS will be able to contribute positively to its local communities. With this model emphasis must be placed on the importance of having a strong and efficient CDD, AML & CFT policy in place, and furthermore ensuring the commitment of management and employees to comply with this policy, will ensure the continuity and integrity of KIMS's operations.

KIMS provides Shariah compliant financing services including Murabaha, Ijara, deposit accounts amongst others, and will bring more products to the market in the future.

Another factor is the characteristic of the targeted clients (level of income, size of activity, nature of activity, sophistication of their operation). Given the pro-poor targeting policy of KIMS there is often a limitation on available data and some information can not be authenticated and verified easily. A high level of commitment and engagement with the community and community leaders as well as a thorough understanding of the local market is key in finding the necessary information and basics to complete customer due diligence and review to fully eliminate AM and FT risks.

1.6. KIMS approach to CDD, AML & CFT

KIMS currently runs a background check on all loan applicants/clients to confirm their identity based on the following documentation:

- Business registration documents
- Passports
- National ID, Election Card (Somaliland)
- Employment ID
- University ID/ Enrolment IDs for Students
- Drivers License
- Refugees ID (for Kismayo returnees)

KIMS also uses a personal guarantor to prove the identity of the customer.

KIMS will continue to develop and strengthen its approach to CDD, AML & CFT to ensure the efficiency and effectiveness of the procedures, AML & CFT Policy and Procedural Handbook will be developed accordingly.

2. Definitions

2.1. Money Laundering

Money Laundering is the criminal practice of processing ill-gotten gains or "dirty" money, through a series of transactions, in this way the funds are "cleaned" so that they appear to be the proceeds from legal activities, it is also the process to change the identity of illegally obtained money by using banking channel so that it appears to have originated from a legitimate source.

Stages Of Money Laundering

Money laundering can be a diverse and often complex process. The first step in the laundering process is for criminals to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity. The funds can further be transferred to other accounts, locally or internationally or use it to buy other goods or services. It eventually appears to be like legally earned money and becomes difficult to trace back to its criminal origin. The criminals can then invest or spend it or, as is often the case, use it to fund more crime.

The laundering process is often described as taking place in three stages:

(1) Placement
(2) Layering
(3) Integration.

(1) Placement

The first stage is referred to as Placement. At this stage illegal funds or assets are first brought into the financial system. When illegal funds are placed in the financial system, they become more liquid.

There are numerous Placement techniques, including the following:

- *Smurfing:* involves the deposit of small amounts of illegal cash into account(s). Typically, smurfing deposits are in small amounts in order to avoid Regulatory requirements of reporting cash transactions.
- *Alternative Remittances:* It refers to the transfer of funds through 'alternative' or illegal money transfer system. These systems are unregulated and illegal, but they are used to transfer both legitimate and illegal funds. Alternative Remittances also goes by the names of underground or parallel banking. There are very large networks of these systems in operation around the world.
- *Electronic Transfers:* In the money laundering context, an electronic transfer involves the transfer of money through electronic payment systems that do not require sending funds through a bank account. If the amount is below the CTR (Cash Transaction Reporting) limit then it will not be reported as per prevailing regulations.
- *Asset Conversion:* Asset Conversion simply involves the purchase of goods. Illegal money is converted into other assets, such as real estate, diamonds, gold and vehicles, which can then be sold and proceeds can be deposited in the account.
- *Bulk Movement:* involves the physical transportation and smuggling of cash and monetary instrument such as money orders and checks.
- *Securities Dealing:* Illegal funds are placed with securities firms which is used for buying bearer securities and other easily transferable instruments.

(2) Layering
Layering is the second stage of money laundering. In this stage illegal funds or assets are moved, dispersed and disguised to conceal their illegal origin.

There are numerous techniques and institutions that facilitate layering, including the following:

- *Offshore Banks:* Offshore Banks accept deposits from non-resident individuals and corporations. A number of countries have well-developed offshore banking sectors; in some cases, combined with loose anti-money laundering regulations.
- *Shell Corporations:* A Shell Corporation is a company that is formally established under applicable corporate laws, but does not actually conduct a business. Instead, it is used to engage in fictitious transactions or hold accounts and assets to disguise their actual ownership.
- *Trusts:* Trusts are legal arrangements for holding specified funds or assets for a specified purpose. These funds or assets are managed by a trustee for the benefit of a specified beneficiary or beneficiaries. Trusts can act as layering tools as they enable creation of false paper trails and transactions. The private nature of trusts makes them attractive to money launderers.
- *Walking Accounts:* A Walking Account is an account for which the account holder has provided standing instructions that upon receipt all funds should be immediately transferred into one or more accounts. By setting up a series of walking accounts, criminals can automatically create several layers as soon as any fund transfer occurred.
- *Intermediaries:* Lawyers, accountants and other professionals may be used as Intermediaries or middlemen between the illegal funds and the criminal. Professionals engage in transactions on behalf of a criminal client who remains anonymous. These transactions may include use of shell corporations, fictitious records and complex paper trails.

(3) Integration
Integration is the third stage of money laundering process. In this stage, illegal funds are successfully legitimised by mixing with legitimate funds in the financial system.

There are various Integration techniques, including the following:

- *Import /Export Transactions:* to bring illegal money into the criminal's country of residence, the domestic trading company will export goods to the foreign trading company on an over-invoiced basis. The illegal funds are remitted and reported as export earnings. The transaction can work in the reverse direction as well.
- *Business Recycling:* Legitimate businesses also serve as conduits for money laundering. Cash-intensive retail businesses, real estate, jewellers, and restaurants are some of the most traditional methods of laundering money. This technique combines the different stages of the money laundering process.
- *Asset Sales & Purchases:* This technique can be used directly by the criminal or in combination with shell corporations, corporate financings and other sophisticated means. The end result is that the criminal can treat the earnings from the transaction as legitimate profits from the sale of the real estate or other assets.
- *Consultants:* The use of consultants in money laundering schemes is quite common. The consultant could be fake. For example, the criminal could himself be the consultant. In this case, the criminal is channeling money back to himself. This money is declared as income from services performed and can be used as legitimate funds.
- *Credit & Debit Cards:* Credit cards are an efficient way for launderers to integrate illegal money into the financial system. By maintaining an account in an offshore jurisdiction through which payments are made, the criminal ensures there is a limited financial trail that leads to his country of residence. In the case of Debit Cards, individuals first transfer illegal funds into an offshore account and also signs up for a debit card from the bank to utilise the funds.

- *Corporate Financings:* Corporate financings are typically combined with a number of other techniques, including use of offshore banks, electronic funds transfers and shell corporations.
- The three basic stages may occur as separate and distinct phases. They may also occur simultaneously or, more commonly, may over lap. Although target clients of KIMS, because of their scale, may appear too small or of too limited sophistication to engage in these techniques, KIMS' staff should be vigilant at all times for any indication of suspicious activities that any clients might be involved in directly or indirectly and follow the proper procedures in this regards, as described in this document.

Sources Of Money Laundering

Money laundering may not just involve wealth related to Drug Trafficking/ Terrorism financing. List of crimes identified by Financial Action Task Force (FATF) as generators of criminal wealth also included:

- Facilitating illegal immigration
- Organized crime including drug trafficking and prostitution
- Embezzlement
- Bribery and kickbacks
- Illegal arms sales
- Gun running
- Smuggling (including movement of nuclear materials)
- Counterfeiting (including making of imitation and copies of original products/goods)
- Fraud, especially computer - supported fraud
- Benefiting from insider trading.
- Tax evasion
- Under and over - invoicing of trade transactions.
- Bogus trade transactions to launder money through round - tripping
- Real Estate Transactions

2.2. Terrorist Financing

Terrorist Financing can be defined as the financial support, in any form, to terrorism or of those who encourage, plan, or engage in terrorism. A terrorist group, like any other criminal organisation, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organisation.

3. Rationale for KIMS Policy for CDD, AML & CF

3.1. The Need To Combat Money Laundering & Terrorist Financing

The prevention of ML and TF from the point of view of KIMS has three dimensions:

- **Ethical:** taking part in the prevention of crime, adhering to KIMS's values, Code of Conduct and Shariah Principles.
- **Professional:** ensuring that KIMS is not involved in recycling the proceeds of crime that would call into question its reputation, integrity and, if fraud is involved, its solvency.
- **Legal:** complying with Laws and Regulations that impose a series of specific obligations on financial institutions and their employees.

The need also arises due to the severe nature of consequences of ML and TF.

Following are some examples:

- Contamination of legal financial transactions
- Threat to the functioning of economy's financial system
- Unlawful enrichment by perpetrator of crime
- Weakening of the social, collective ethical standards
- Drug trafficking, Human trafficking
- Political corruption
- Terrorism crimes cause a great deal of human misery
- Prudential risks to financial services soundness arising from these developments, in particular to the most vulnerable communities

3.2. Regulatory Oversight & Compliance Risks

KIMS has to abide by local and international regulations including Central Bank of Somalia and Central Bank of the UAE Regulations and Somalia and UAE applicable laws and also international rules and regulations to make sure it meets its obligations and requirements towards its international funders, investors and partners. The consequence of contravening the Regulations or failing to comply can be significant and include disciplinary measures, imprisonment or fine or both under local laws as well as the loss of reputation for KIMS and possible loss of support and baking from international partners.

Notwithstanding the statutory and regulatory penalties, increased vigilance by Management and staff will protect KIMS from the following risks:

Reputational risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers and business is dependent on its reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong CDD, AML & CFT policy helps to prevent a business from being used as a vehicle for illegal activities.

Operational risk: This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If CDD, AML & CFT policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business can be viewed as operationally unsound and lose the support of partners.

Legal risk: If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.

Financial risk: If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve money that the customer owes.

4. KIMS CDD, AML & CFT Policy

KIMS takes various steps to counter the menace of money laundering and terrorist financing. KIMS is stringently focusing on core compliance functions and adopts a robust policy across its network to remain complied with AML & CFT regimes in all jurisdictions.

4.1. Anti-Money Laundering and Combating Financing of Terrorism

It is the Policy of KIMS that:

- Statutory, regulatory & legal obligations to prevent ML and TF are fully complied with.
- Systems and controls are implemented and reviewed on set frequency in order to minimize the risk of the KIMS services being abused for the purposes of ML and TF.
- A money laundering risk assessment of the KIMS's services and customer base including correspondent banks and MSBs (Money Service Businesses) are undertaken and appropriate policies, procedures and due diligence controls are applied proportionate to that risk.
- KIMS would not do business with:
  - Individuals / entities subject to UN sanctions
  - Individuals / entities under OFAC or local country sanctions as applicable
  - Unauthorized money changers/prize bond dealers
  - Anonymous customers
  - Customers hiding beneficial ownership of the account
  - Client or business segment black listed by KIMS or by the Regulators (KIMS has its own internal black list. This list contains individuals/entities whom KIMS believes should not be doing business with on compliance grounds)
  - Shell Banks
  - Government officials willing to open government 's accounts in their personal names
  - Arms Dealers
- To carry out enhanced due diligence before establishing relationships with the following High risks customers
  - Trusts, NGOs, NPOs, Foundations, Welfare Association, Religious Entities, Club, Societies, Financial Institutions, Authorised Money Exchange Cos., Controversial entities, Jewellers
  - Customers using their personal accounts for business transactions
  - Any individual or entity that has caused or has been related to a credit, operational or reputational loss to KIMS
  - Politically Exposed Persons (PEPs)
  - Banking and financing facilities refused by other financial service providers
  - Institutions / Individuals whose association with KIMS could be considered controversial
  - Non-face to face / online customers
  - Correspondent Relationships
  - Private Banking Customers
  - Customers belonging to countries where CDD, AML & CFT rules are lax

- Accounts of foreign nationals belonging to sanctioned countries
- Non-resident customers
- High risk geographies
- Customers reportedly having previous unsatisfactory / suspicious social status
- Any customer relationship where the customer's conduct gives KIMS reasonable cause to believe or suspect involvement with illegal activities is required to be reported to the Regulators or relevant authorities.
- Where local regulators call for a money laundering compliance reports, KIMS Compliance Team is responsible for preparation and submission of money laundering reports to the Central Bank. Compliance Team would submit a quarterly compliance report (including significant AML/CFT issues) to KIMS Senior Compliance Officer

4.2. Customer Due Diligence

Customer Due Diligence (CDD) is closely associated with the fight against money-laundering. Supervisors around the world are increasingly recognising the importance of ensuring that their financial institutions have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, financial service providers can be exposed to reputational, operational, legal and financial risks as more prescribed above.

It is a Policy of KIMS that:

- Prior to establishing a relationship with a new customer, basic background information about the customer should be obtained, in particular, information related with customer's business and source /utilisation of funds, the expected level of activity and the reasons for starting the relationship.
- Prior to establishing relationships with correspondent banks or agents, appropriate steps must be taken to confirm the identity, integrity and due diligence procedures of those representatives or agents and, where necessary, the identities of underlying clients.
- The underlying beneficial ownership of all enterprises/businesses/companies and other legal entities with whom KIMS conduct business must be established, including the beneficial ownership of all funds or other properties that are handled by KIMS.
- Customer's profile must be updated periodically based on risk profiling of the customer. Customer activity must be monitored against a pre-determined profile, paying special attention to higher risk customers or activities.
- All new relationships should be filtered through automated solution for possible name matching with individuals / entities appearing on various negative lists maintained by KIMS. In case of exact match, relationship should be discontinued.

4.3. CDD, AML & CFT Associated Policies

Following associated policies form an integral part of the CDD, AML & CFT Policy and have been developed specifically to achieve the objectives outlined in the KIMS Policy and the regulatory requirements of the Central Bank of Somalia.

4.4. Internal controls and communication

It is a Policy of KIMS:

- To design and implement processes, systems, and controls to comply with all applicable AML & CFT laws and regulations.
- To conduct risk assessment and develop risk profiles of KIMS's customers, products & services and to apply appropriate policies and procedures to manage such risks.
- To undertake enhanced due diligence for 'High Risk' customers.
- To communicate KIMS's policies to management and staff and provide them with written procedures and control requirements to ensure ongoing compliance with AML & CFT laws and regulatory requirements.

4.5. Recognition and reporting of suspicion

It is a Policy of KIMS:

- To establish and follow procedures that requires employees to refer promptly any suspicious activity to the Compliance Team for further review and to determine whether any required reporting should be filed with the Regulators.
- To remain vigilant on unusual or suspicious transactions or other activities that appear not to make good business or economic sense, or activities that appear to be inconsistent with the given profile of the customer, including activities that may be indicative of criminal conduct, terrorism or corruption.
- To act competently and honestly when assessing information and circumstances that might give reasonable grounds to suspect ML or TF.
- To provide the Compliance Head at his /her request with access to all customer, correspondent or counterparty information that are within the possession of KIMS.
- To co-operate with law enforcement authorities in investigations concerning possible ML or TF within the confines of applicable laws, and in consultation with the Compliance Team.
- Not to alert or provide any information to any person regarding suspicion or inquiry on his or her account or transactional activities or any indication of Suspicious Transaction Reporting (STR).

4.6. Awareness raising and training

It is a Policy of KIMS:

- To ensure that the compliance officers go through the fit and proper' test. The same procedure should be applied to screen all the staff employed in areas that are relevant to the AM & CFT control environment.
- To ensure that all staff attached to the Compliance Unit should undergo periodical compliance training (two times a year) and it is also necessary to plan frequent in-house training courses to conduct case studies keeping in view live cases relating to money laundering and terrorist financing STR. Training materials will be developed by Compliance Unit in coordination with Human Resources Department, the later will keep latest version of authorized training compliance materials. Employees completing the course will be furnished with completion certificates.
- To make all management and staff aware of what is expected of them to prevent money laundering or terrorist financing and to advise them of the consequences for them and for KIMS if they fall short of that expectation.
- To provide comprehensive training through learning & development on CDD, AML & CFT to all staff members on regular basis.

- That management and staff are required to sign a form confirming they have read and understood the KIMS's CDD, AML & CFT Policy and relevant procedures. Changes made on set frequencies or on ad-hoc basis to this policy should also be communicated to the staff.

4.7. Record keeping

It is a Policy of KIMS:

- To ensure that KIMS is able to provide the basic information on clients and account holders and to reconstruct the individual transactions undertaken, at the request of the relevant authorities.
- To ensure that a database is available and all transaction are individualised and booked in the customer's account and that copies of these transactions are provided to the concerned authorities.
- To set up a files keeping system, and to instruct the respective staff to maintain correspondence, statements and contract notes on transactions in special files, in such a way to enable KIMS to respond to the relevant authorities' requests in a timely manner. In addition, the database must also contain a list of the persons who have concluded cash transaction in the amount of or more than the limit prescribed as an "indicator".

Information to be kept:

KIMS will keep the information in the system as per the following:

a. A copy of the identification in the case of transactions by individuals initialed by the concerned employee under "a true copy of the original"
b. A copy of the trade license/business registration in the case of transactions by licensed institutions/entities initialed by the concerned employee under "a true copy of the original"
c. The volume of funds flowing through the account (turn-over in and out of account).
d. The original of funds, i.e., from which banks or other financial institutions, in case of transfers.
e. The form of funds deposited or withdrawn (cash/ cheques / mobile money etc.)
f. The identity of the persons making the transaction, in case they were other than the client, account holder(s) or beneficial owners.
g. The destination of funds in case of transfers from the account
h. The type of instructions and authority regarding operating the account.

Period of Keeping Documents, Forms Records/Files:

a. In cases to which these procedures apply, records is kept and made available to Central Bank examiners and for investigation for a minimum of 5 years. This includes account - opening documents which are kept for 5 years after the closing of the account, or for whoever the regulations may impose (whichever is longer).
b. KIMS also retains documents in original where the account is open and operating / warehouse or scanned copies in the computer or stored on proper electronic storage medium.
c. If investigations relating to unusual transactions are going on, the records is retained until the Central Bank examiners or the investigating authorities declare the investigation completed and closed.

4.8. Politically Exposed Persons (PEPs)

Definition

PEPs are individuals who are or have been entrusted with prominent public functions in the country, for example Heads of State or of Government, senior politicians, senior government, judicial or military officials. Senior executives of state owned corporations, important political party officials, business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. PEPs include the following:

- Prominent public functions,
- Government ministers,
- Senior civil servants,
- Senior judicial & Military officials,
- Senior executives of state owned corporations,
- Senior political party officials.

Close family members include:

- Spouses, children, parents, siblings and may also include other blood relatives and relatives by marriage.

Closely associated persons include:

- Close business colleagues and personal advisors/ consultants to the politically exposed person as well as persons who are expected to benefit significantly by being close to such a person.

Branches are required to conduct enhanced due diligence of close family members / closely associated persons of politically exposed persons in line with the aforementioned policy references.

Policy Rationale

PEPs and related individuals can pose unique reputation and other risks, in particular:

- Some corrupt PEPs around the globe have used traditional financial products and services as safe havens for misuse of funds, illegal activities and associated practices, including money laundering;
- PEPs enjoy prominence and are therefore under continuous public spotlight. Their financial affairs are highly magnified and could easily trigger adverse publicity and franchise risks for KIMS;
- There is a growing attention worldwide to the misuse of public funds and increased reaction against corruption at high government levels;
- There is increasing responsibility and liability for financial service providers and their personnel to undertake due diligence for establishing source of wealth and investigate fund flows of PEPs.

It is a Policy of KIMS:

That relationship with PEPs would be established with the prior approval of Head of Compliance and Risk Management.

All such relationships should be classified under High Risk category for effective monitoring through automated AML solutions used by KIMS.

4.9. Correspondent Relationships / MSBs

It is a Policy of KIMS:

- To obtain sufficient information about correspondent banks /MSBs to understand the nature of their business & activities
- When considering entering into a cross - border correspondent banking relationship, banks, exchange houses/moneychangers and other financial institutions due diligence measures will be carried out. In addition, research will be conducted from publicly available information on the correspondent bank's business activities, their reputation, quality of supervision end whether the institution has been subject to a money laundering or terrorist financing investigation or any regulatory action. Prior to a relationship being established, express written approval must be obtained from concerned financial institutions' senior management.
- Special care would be taken if these financial institutions are headquartered in countries which are reported to be involved in drugs, high level of public corruption and/or criminal/ terrorist activities.
- For opening of a correspondent banking relationship, banks and other financial institutions must have measures to identify:
  - Ownership and Management Structure;
  - Major Business Activities and Customers;
  - Purpose of the Account;
  - Location;
  - Third parties that will use the account; and
  - Monitor transactions processed through the account.

All FIs relationships are subject to prior approval from Compliance Team and Board of Directors.

4.10.Automated AML solutions

It is a Policy of the KIMS:

- To make maximum use of technology and upgrade the systems and procedures in accordance with the upcoming challenges ML & TF.
- To gradually implement and use automated AML solutions across its network for effective transaction monitoring /real time filtering of payment instructions in line with the best industry practices.

4.11.Non Compliance With KIMS's CDD, AML & CFT Policy

FAILURE TO ABIDE BY THE POLICY SET BY KIMS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING WILL BE TREATED AS A DISCIPLINARY ISSUE. ANY DELIBERATE BREACH WILL BE VIEWED AS GROSS MISCONDUCT. SUCH CASES WILL BE REFERRED TO HR FOR ONWARD INITIATION OF DISCIPLINARY ACTION THAT COULD LEAD TO TERMINATION OF EMPLOYMENT AND COULD ALSO RESULT IN CRIMINAL PROSECUTION AND IMPRISONMENT FOR THE CONCERNED STAFF MEMBER.

5. Accountabilities and Responsibilities

5.1. The Board of Directors Responsibility

The Board of Directors (BOD) is responsible for:

- Ensuring that adequate systems and controls are in place to deter and recognize criminal activity, money laundering and terrorist financing.
- Seeking compliance reports from the Compliance Unit (including coverage of AML & CFT issues) on quarterly basis and taking necessary decisions required to protect KIMS from use by criminals for ML & TF activities.
- The Oversight of the adequacy of systems and controls that are in place to deter and recognize criminal activity, money laundering and terrorist financing.
- Commissioning and approving periodic and ad-hoc update of this Policy.

5.2. Management Responsibility:

The Management is responsible for:

- Ensuring that CDD, AML & CFT Policy is implemented in letter and spirit.
- Ensuring that Compliance Unit is promptly advised where there are reasonable grounds to know or suspect that transactions or instructions are linked to criminal conduct, money laundering or terrorist financing.
- Ensuring that Compliance Unit is provided with all relevant information to carry out complete assessment of underlying transaction.
- Ensuring that CDD is being carried out and following minimum steps are taken by the branches:
  a. At the time of establishing business relationship;
  b. conducting occasional transactions above US$ [3000] three thousand whether carried out in a single operation or in multiple operations that appear to be linked;
  c. carrying out occasional wire transfers (domestic / cross border) regardless of any threshold;
  d. there is suspicion of money laundering / terrorist financing; and
  e. there is a doubt about the veracity or adequacy of available identification data on the customer.
- Ensuring that Enhanced Due Diligence (EDD) is carried out for high risk relationships and following minimum steps are taken:
  a. Approval of all high risk relationships are obtained as required
  b. Names of prospective customers are screened through automated solution (e.g. WorldCheck or other similar solutions)_for possible name matching with individuals / entities appearing on various negative lists maintained by KIMS. In case of an exact match, relationship should be discontinued.
  c. Additional documentations as appropriate besides the minimum required documents
- Ensuring that Compliance Head is provided with independence and adequate resources to carry out their duties effectively.

5.3. Compliance Unit's Responsibility:

Compliance Unit is responsible for:

- Developing and maintaining policy in line with evolving statutory and regulatory obligations.
- Making use of technology and upgrading KIMS's systems and procedures in accordance with the changing compliance risks.
- Developing and ensuring that the internal procedures remain up-dated at all times. Recommendation should be put forward for BOD approval as soon as needed.
- Undertaking the required money laundering /terrorist financing risk assessment for customers, products or services.
- Monitoring and identifying transactions of suspicious nature and report to the Regulator s in a timely manner.
- Ensuring that all staff is aware of their personal obligations and adequately trained in prevention of ML & TF.
- Representing KIMS to all external agencies and any other third party enquiries in relation to money laundering prevention, investigation or compliance.
- Preparing quarterly reports on AML compliance for onward submission to the Board Audit Committee through Head of Compliance.
- Undertake an Compliance Audit on an annual basis, the final report will be submitted to the Board of Directors Compliance Committee for review and approval.
- Ensuring that all employees sign-off an undertaking confirming having read and understood KIMS's policy on CDD, AML & CFT.
- Responding promptly to any request for information made by the Regulators or law enforcement agencies.
- Take appropriate action against the staff found involved in any of such activities that comes under the domain of AML & CFT.

5.4. All Employees Responsibility:

All employees are responsible for:

- Remaining vigilant to the possibility of money laundering / terrorist financing through use of KIMS's products and services.
- Complying with all AML & CFT policies and procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Promptly reporting to Compliance Unit where they have knowledge or grounds to suspect a criminal activity or where they have suspicion of money laundering or terrorist financing whether or not they are engaged in AML & CFT monitoring activities.
- Ensuring that customer is not disclosed any information related to inquiry or filing of a suspicious activity report (STRs) or Cash Transactions Report (CTRs)
- Understanding KIMS's Policy and Procedures on CDD, AML & CFT and to sign-off on the required Form.

Employees who violate any of the Regulations or KIMS's CDD, AML & CFT policies and procedures will be subject to disciplinary action.