AML/CDD/CFT POLICY

For Prevention of Money Laundering/Terrorist Financing

HBL UAE

Owner:
HBL UAE COMPLIANCE
Revision Date:
February 2014
Slogan for HBL

‘Compliance is My Responsibility’
## Contents

**Introduction** ................................................................................................................................. 4

1 **METHODOLOGY** .......................................................................................................................... 6

1.1 **Objectives of AML/CDD/CFT Policy** ...................................................................................... 6

1.2 **Scope** ........................................................................................................................................ 6

1.3 **Money Laundering** ................................................................................................................... 6

1.4 **Stages of Money Laundering** ..................................................................................................... 6

1.5 **Sources of money laundering:** .................................................................................................. 9

1.6 **Terrorist Financing** .................................................................................................................. 10

1.7 **The need to combat Money Laundering (ML) and Terrorist Financing (TF)** ..................... 11

1.8 **Regulatory Oversight & Compliance Risks** ............................................................................ 10

2 **LEGAL/ REGULATORY OBLIGATIONS** ..................................................................................... 13

2.1 **Legal/ Regulatory Obligations** .................................................................................................. 13

2.2 **Regulatory Obligations** ........................................................................................................... 13

2.3 **Offences and Penalties (Key elements)** .................................................................................. 14

3 **THE BANK’S POLICY for AML/CDD/CFT** ............................................................................. 17

3.1 **AML/CFT** ............................................................................................................................... 17

3.2 **CDD** ....................................................................................................................................... 18

3.3 **AML/ CDD/CFT ASSOCIATED POLICIES** ........................................................................ 18

3.3.1 **Internal controls and communication** ................................................................................ 19

3.3.2 **Recognition and reporting of suspicion** ............................................................................. 19

3.3.3 **Awareness raising and training** ........................................................................................ 19

3.3.4 **Record keeping** .................................................................................................................. 20

3.3.5 **Bank’s’ policy on Foreign politically exposed persons (FPEPs)** .................................... 21

3.3.6 **Bank’s policy on Correspondent Relationships/MSBs.** ................................................... 21

3.3.7 **Use of Automated AML solutions** .................................................................................... 21

3.4 **Non Compliance with Bank’s AML/CDD/CFT Policy** .......................................................... 23

3.5 **accountabilities and responsibilities** ...................................................................................... 23

3.5.1 **The Board is Responsible for:** ............................................................................................ 23

3.5.2 **Management is Responsible for:** ......................................................................................... 23
INTRODUCTION

Habib Bank (‘the Bank’) is a pioneer financial institution of Pakistan, having largest domestic network of branches, a well-known brand locally with a substantial international presence.

To protect itself from the increasing danger of organized criminal activity and money laundering, it is essential for the Bank to have a clearly laid down “Anti-Money Laundering” (AML)/“Customer Due Diligence” (CDD)/‘Counter Financing of Terrorism (CFT) Policy to ensure that the Bank remains protected from the menace of money laundering and is not used by existing &/or prospective customers for any criminal activity.
METHODOLOGY
1 METHODOLOGY

1.1 OBJECTIVES OF AML/CDD/CFT POLICY

The objective of this policy is to ensure that the products and services of the Bank are not used to launder the proceeds of crime and that all of the Bank’s staff is aware of their obligations and the need to remain vigilant in the fight against money laundering/terrorist financing. The document also provides a framework to comply with applicable laws, Regulatory guidelines specially related with detection and reporting of suspicious activities.

In case of any clarification contact Head of Compliance Gulf at Regional Office Dubai complianceuae@hbl.ae

1.2 SCOPE

Our coverage will include:

- Central Bank of the UAE Regulations 24/2000, subsequent amendments and changes.
- FATF 40 Recommendations
- International Standards and guidelines, including Basel and Regulatory sanctions as applicable.
- Union Law No. (10) of 1980 and the provisions contained in Part Three: “Organization of Banking and Finance”, Chapter Two, Section Five “Supervision” and namely Article 94.

1.3 MONEY LAUNDERING

Definition:
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.

1.4 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 funded more crime.

The laundering process is often described as taking place in three stages:-
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
- Alternative Remittances
- Electronic Transfers
- Asset Conversion
- Bulk Movement
- Securities Dealing

**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
- Shell Corporations
- Trusts
- Walking Accounts
- Intermediaries

**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 legitimized by mixing with legitimate funds in the financial system.

There are various Integration techniques, including the following:

- Import /Export Transactions
- Business Recycling
- Asset Sales & Purchases
- Consultants
- Credit & Debit Cards
- Corporate Financings

**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.
Business Recycling: Legitimate businesses also serve as conduits for money laundering. Cash-intensive retail businesses, real estate, jewelers, 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.

Debit Cards: Individuals first transfer illegal funds into an offshore account and also signs up for a debit card from the bank to utilize 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 overlap.

1.5. 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:

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

1.6. 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 organization, builds and maintains an infrastructure to develop sources of funds and channel them to those who provide materials and or services to the terrorist organization.

1.7. THE NEED TO COMBAT MONEY LAUNDERING (ML) AND TERRORIST FINANCING (TF)

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

- **Ethical** - taking part in the prevention of crime.
- **Professional** - ensuring that the Bank 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:

- Unexplained changes in supply and demand for money,
- Volatility of capital flows and exchange rates due to un-anticipated cross border asset transfers,
- Contamination of legal financial transactions,
- Threat to the functioning of economy’s financial system,
- Systemic risk,
- Unlawful enrichment by perpetrator of crime,
- Dampening effect on foreign direct investment,
- 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 bank soundness arising from these developments.

1.8. REGULATORY OVERSIGHT & COMPLIANCE RISKS

HBL has used Central Bank of the UAE Regulations 24/2000, subsequent amendments/changes and UAE applicable laws, to formulate its own AML/CDD/CFT Policy. 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 the bank.

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

- Reputational
• Operational
• Legal
• Financial

Reputational risk: The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependent on 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 AML/CDD/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 AML/CDD/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.

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.
LEGAL AND REGULATORY OBLIGATIONS
2 LEGAL/REGULATORY OBLIGATIONS

2.1 LEGAL OBLIGATIONS

The bank is obligated to comply with the requirements of the UAE AML Laws applicable to Banks and Union Law No. (10) Of 1980 and the provisions contained in Part Three: “Organization of Banking and Finance”, Chapter Two, Section Five “Supervision” and namely Article 94.

2.2 REGULATORY OBLIGATIONS

HBL UAE is committed to comply with Central Bank of the UAE Regulations 24 of 2000 and subsequent changes and amendments.

The Board of Directors of the Central Bank has decided to implement the procedures, which reflect the Forty Recommendations relating to stopping financing of terrorism issued by the Financial Action Task Force (FATF) established by countries of the Group of Seven (G7), and to provide support to international efforts to combat possible money laundering taking advantage of the excellent banking and financial infrastructure available in the UAE.

In compliance with Article (22) of Central Bank of the UAE Regulations #24/2000 HBL UAE would adopt only these procedures and immediately stop the practice of applying any internal procedures or compliance with regulations of any foreign country in this regard.

The Bank itself has similar obligations.

It is a regulatory requirement for an institution to have in place policy and procedures to combat money laundering/terrorist financing. These procedures as a minimum must include:

- Setup a compliance unit with a full time Head
- The verification of new client identification, CDD (Know Your Customer) profiling, update customer’s information and record at reasonable interval.
- Risk-based controls
- Awareness raising and training of staff members.
- Recognition and reporting suspicions of money laundering/terrorist financing.
- Retention of records.
- Independent testing (internal/external Audits);

It is a criminal offence if management or staff:

1. Acquire proceeds of a crime or assist anyone whom they know or suspect has committed, or benefited from any criminal conduct. (Acquire, Possess & Assist)
2. Prejudice an investigation by informing the subject of a suspicion, or any third party that a disclosure has been made either internally or externally, or that the authorities may act or propose to act or investigate. (Tip Off)
3. Acquire knowledge or a suspicion, or has reasonable grounds to know or suspect, that benefit has been gained from criminal conduct or that the proceeds of crime have been laundered, and have not reported the same as soon as possible. Bank staff negligent in this respect would liable for prosecution. (Failure to Report)

4. Have not implemented effective systems, controls and procedures to guard against money laundering. (Systems & Controls)

2.3 OFFENCES AND PENALTIES (KEY ELEMENTS)

Federal Law No (4) of 2002 Regarding Criminalization of Money Laundering
Chapter Three Penalties

Article (13)

Whoever commits any of the acts set out in Clause (1) of Article (2) of this law, shall be punished by imprisonment for a term not exceeding seven years, or by a fine not exceeding AED 300,000 (UAE dirhams three hundred thousand) and not less than AED 30,000 (UAE dirhams thirty thousands), in addition to confiscation of the Proceeds, or the equivalent thereof, if such Proceeds were wholly or partially converted into, or combined with, other Property derived from lawful sources.

Article (14)

Whoever violates the provisions of Article (3) of this law shall be punished by a fine not less than AED 300,000 (UAE dirhams three hundred thousand), and not exceeding AED 1,000,000 (UAE dirhams one million), in addition to confiscation of the Proceeds, or Property of value equivalent thereto, or the equivalent of those Proceeds, if the latter were wholly or partially converted into, or combined with other property derived from lawful sources.

Article (15)

Chairmen, directors, managers and employees of Financial Institutions or Other Financial, Commercial and Economic Establishments who know of, yet fail to report to the Unit stated in Article (7) hereof any act that occurred within their establishments and was related to the Money Laundering offence, shall be punished by imprisonment or by a fine not exceeding AED 100,000 (UAE dirhams hundred thousand) and not less than AED 10,000 (UAE dirhams ten thousand) or by both penalties.

Article (16)

Whoever informs any person that his transactions are being scrutinized for possible involvement in suspicious operations, or that security authorities or other competent authorities are investigating his possible involvement in suspicious operations, shall be punished by imprisonment for a term not exceeding one year, or by a fine not exceeding AED 50,000 (UAE dirhams fifty thousand) and not less than AED 5,000 (UAE dirhams five thousands) or by both penalties.

Article (17)

The maximum penalty prescribed for false notification shall be imposed on whoever notifies the competent authorities, in bad faith, of the commission of the Money Laundering offence, with intent to cause damage to another person.

Article (18)
Whoever violates provisions of Article (6) hereof shall be punished by a fine of not less than AED 2,000 (UAE dirhams two thousand) and not exceeding AED 10,000 (AED ten thousand). Amounts that arise from such violation shall be attached, and unless proven to be associated with another offence, shall be released only by a Public Prosecution Order.

Article (19)

Whoever violates any of the other provisions herein shall be punished by imprisonment or by fine not exceeding AED 100,000 and not less than AED 10,000.

Article (20)

Financial Institutions and Other Financial, Commercial and Economic Establishments, as well as their directors, employees and authorized representatives shall be immune from any criminal, civil or administrative liability, which may result from providing required information, or breaking a restriction imposed by a legislative, contractual, regulatory or administrative provision, for safeguarding confidentiality, unless such reporting was proved to have been done in bad faith.

Staff Training:

The Compliance Officer in each bank, moneychanger or any other financial institutions should provide training to staff responsible for receiving cash or overseeing accounts and their reports, on all matters pertaining to money laundering. The training should be in line with the responsibilities undertaken by the employees who should always exercise utmost prudence.

The Central Bank shall direct banks with regard to methods of training to be applied, as well as holding workshops to train on methods of combating money laundering. All financial institutions should send their concerned staff to benefit from such programs.
THE BANK’S POLICY FOR AML/CDD/CFT
3 THE BANK’S POLICY FOR AML/CDD/CFT

Keeping in view of Global threat, the bank has taken various steps to counter the menace of money laundering and terrorist financing. The bank is stringently focusing on core Compliance functions and has adopted a robust Policy across HBL network to remain complied with AML/CFT regimes in all jurisdictions.

3.1 AML/CFT

It is the Policy of HBL 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 Bank's services being abused for the purposes of ML and TF.
- A money laundering risk assessment of the Bank’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.
- The bank 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 the Bank or by the Regulators.
  - Shell Banks & off shore corporate clients
  - Government officials willing to open government’s accounts in their personal names.

- To carry out enhanced due diligence before establishing relationships with the following High risks customers
  - Politically Exposed Persons (PEPs)
  - Correspondent Relationships
  - Customers using their personal accounts for business transactions
  - Private Banking Customers
  - Institutions / Individuals whose association with HBL could be considered controversial
  - Any individual or entity that has caused or has been related to a credit, operational or reputational loss to HBL
  - Banking facilities refused by other banks
  - Customers belonging to countries where AML/CDD/CFT rules are lax
  - Non-face to face / on-line customers,
  - Accounts of foreign nationals belonging to sanctioned countries
  - Walk in customers
  - Non-resident customers
Customers in cash based business
- High risk geographies
- Customers reportedly having previous unsatisfactory / suspicious social status
- Any customer relationship where the customer's conduct gives the Bank reasonable cause to believe or suspect involvement with illegal activities is required to be reported to the Regulators or relevant authorities.
- In countries where local regulators call for a money laundering compliance reports, Compliance Unit is responsible for preparation and submission of money laundering reports to Central Bank. Compliance Unit would submit a quarterly compliance report (including significant AML/CFT issues) to Chief Compliance Officer.

3.2 CDD

CDD is closely associated with the fight against money-laundering. Supervisors around the world are increasingly recognizing the importance of ensuring that their banks 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, banks can be exposed to reputational, operational, legal and financial risks

**It is a Policy of the Bank 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/utilization of funds, the expected level of activity and the reasons for opening the account.
- 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 companies and other legal entities with whom the bank conduct business must be established, including the beneficial ownership of all funds or other properties that are handled by the Bank.
- 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 the bank. In case of exact match, relationship should be discontinued.

3.3 AML/ CDD/CFT ASSOCIATED POLICIES

Following associated policies form an integral part of the AML/CDD/CFT Policy and have been developed specifically to achieve the objectives outlined in the Bank’s Policy and the regulatory requirements of the State Bank of Pakistan/Financial Monitoring Unit.
3.3.1 Internal controls and communication

It is a Policy of the Bank:

- 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 the Bank’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 Bank’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.

3.3.2 Recognition and reporting of suspicion

It is a Policy of the Bank:

- To establish and follow procedures that requires employees to refer promptly any suspicious activity to Compliance Unit for further review and to determine whether STR 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 Compliance Head at his/her request with access to all customer, correspondent or counterparty information that are within the possession of the bank.
- To co-operate with law enforcement authorities in investigations concerning possible ML or TF within the confines of applicable laws, and in consultation with Compliance Unit.
- 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 being reported to the Regulators.

3.3.3 Awareness raising and training

It is a Policy of the Bank:

- 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 AMUCFT control environment;
- All staff attached to the Compliance department should undergo periodical training 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 STRs.
• 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 the Bank if they fall short of that expectation.

• To provide comprehensive training through L&D on AML/CDD/CFT to all staff members on regular basis

• That Management and staff are required to sign a memorandum confirming they have read and understood the Bank's AML/CDD/CFT policy and relevant procedures. Changes made on set frequencies or on adhoc basis to this policy should also be communicated to the staff.

3.3.4 Record keeping

It is a Policy of the Bank:

a. To ensure that bank is able to provide the basic information on the account holder and to reconstruct the individual transactions undertaken, at the request of the relevant authorities.

b. To ensure that a database is available and all transaction are individualized and booked in the customer’s account and that copies of these transactions are provided to the concerned authorities.

c. 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 the bank 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 on “indicator” Information:-

Keep the information in the system relates to the following:-

a. A copy of the passport 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 in the case of transactions by institutions initialed by the concerned employee under “a true copy of the original”

c. The volume of funds flowing through the account (turn-over in the 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, etc.)

f. The identity of the persons making the transaction, in case they were other than the 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:**

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 (Code of Commercial Practice: Article 32).

Bank also retains documents in original where the account is open and operating/warehouse or scanned copies in the computer or stored on microfilm.

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.

### 3.3.5 Bank’s’ policy on Foreign politically exposed persons (FPEPs)

**Definition**

FPEPs are individuals who are or have been entrusted with prominent public functions in a foreign 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. FPEPs 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**

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

- Some corrupt FPEPs around the globe have used traditional banking products and services as safe havens for misuse of funds, illegal activities and associated practices, including money laundering;
• FPEPs 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 the Bank;
• 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 banks and bank personnel to undertake due diligence for establishing source of wealth and investigate fund flows of FPEPs.

It is a Policy of the Bank:
• That relationship with FPEPs would be established with the prior approval of Head of Compliance and RGM.
• All such relationships should be classified under High Risk category for effective monitoring through automated AML solutions used by the bank.

3.3.6 Bank’s’ policy on Correspondent Relationships / MSBs

It is a Policy of the Bank:
• 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 FID/ Global Compliance.

3.3.7 Use of automated AML solutions
It is a Policy of the Bank:

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

3.4 NON COMPLIANCE WITH BANK’S AML/CDD/CFT POLICY

Failure to abide by the Policy set by the Bank 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.

3.5 ACCOUNTABILITIES AND RESPONSIBILITIES

3.5.1 The Board 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 through BAC from the CCO (including coverage of AML/CFT issues) on quarterly basis and taking necessary decisions required to protect the bank 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.

3.5.2 Management is Responsible for:

- Ensuring that AML/CDD/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 are 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 rupees one million 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 EDD is being 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 filtered through automated solution for possible name matching with individuals / entities appearing on various negative lists maintained by the bank. 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.

3.5.3 Compliance is Responsible for:

- Developing and maintaining policy in line with evolving statutory and regulatory obligations.
- Making use of technology and upgrading Bank’s systems and procedures in accordance with the changing compliance risks.
- Undertaking the required money laundering /terrorist financing risk assessment for customers, products or services.
- Developing and ensuring that the internal procedures remain up-dated at all times.
- Monitoring and Identifying transactions of suspicious nature and report to the Regulators in a timely manner.
- Ensuring that staff is aware of their personal obligations and adequately trained in prevention of ML/TF.
- Representing the Bank 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 Chief Compliance.
- Ensuring that all employees sign-off an undertaking confirming having read and understood Bank’s policy on AML/CDD/CFT.
- Responding promptly to any request for information made by the Regulators or law enforcement agencies.
- Take appropriate action against the staff found involve in any of such activities that comes under the domain of AML / CFT

3.5.4 All Employees are Responsible for:

- Remaining vigilant to the possibility of money laundering / terrorist financing through use of bank’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 the customer is not disclosed any information related to inquiry or filing of a suspicious activity report (STRs) or Cash Transactions Report (CTRs)

• Understanding Bank’s Policy and Procedures on AML/CDD/CFT and to sign-off on the required Form.

Employees who violate any of the Regulations or the Bank’s AML/CDD/CFT policies and procedures will be subject to disciplinary action.
ABBREVIATIONS USED IN AML/CDD/CFT POLICY

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFT</td>
<td>Counter Financing of Terrorism</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>CCO</td>
<td>Chief Compliance Officer</td>
</tr>
<tr>
<td>MLRO</td>
<td>Money Laundering Reporting Officer</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>PEPs</td>
<td>Politically Exposed Person</td>
</tr>
<tr>
<td>BOD</td>
<td>Board of Directors</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>MSB</td>
<td>Money Service Business</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>EDD</td>
<td>Enhanced Due Diligence</td>
</tr>
</tbody>
</table>