POLICY ON RISK BASED APPROACH FOR

ANTI MONEY LAUNDERING,

SUPPRESSION OF TERRORIST FINANCING

AND CUSTOMER DUE DILIGENCE

DFCC BANK PLC

	DFCC Bank PLC	
	Title	POLICY ON RISK BASED APPROACH FOR ANTI MONEY LAUNDERING, SUPPRESSION OF TERRORIST FINANCING AND CUSTOMER DUE DILIGENCE
	Policy Owner	Compliance Officer Date: 24.08.2018

Table of Contents

PREAMBLE

Banks and other financial institutions may be unwittingly used as intermediaries for depositing, safekeeping or transferring of funds derived from criminal activity or for the financing of terrorists. Public confidence in banks, and hence their stability can be undermined by adverse publicity as a result of inadvertent association by banks with criminals. In addition banks may lay themselves open to direct losses from fraud, either through negligence in screening undesirable customers or where integrity of their own officers have been undermined through association with criminals. Therefore, it is fundamental for banks and financial institutions to manage and mitigate these risks prudently for judicious corporate governance.

1.0

PREVENTION OF CRIMINAL USE OF THE BANKING SYSTEM FOR THE PURPOSE OF MONEY LAUNDERING AND TERRORIST FINANCING

1.1 What is Money Laundering?

There are many definitions of "money laundering". A relatively simple and non-technical definition is that it is the conversion of tainted or "dirty money" into respectable assets so as to disguise or conceal the origin of such money and to give it the appearance of having been obtained from a legitimate source. What is meant by "dirty money" is that the cash or other property is derived from a criminal activity such as drug smuggling. The scope of criminal activities for purpose of anti-money laundering control is ever expanding. The purpose of conversion is to give the appearance that the cash or such other property has been obtained from a legitimate source. As in the case of soiled or dirty clothes being laundering, there is a similar process involved in money laundering.

The process of laundering money basically goes through three stages:

- Placement- initial entry of illegally derived funds, usually in the form of cash, (may include the other sources of transactions as well) into the financial system;
- Layering – multiple transactions such as transferring funds from one account to several other accounts to conceal the origin and the movement of funds;
- Integration – making investments in assets such as real estate or expensive cars etc.

1.2 What is Terrorist Financing?

The global attention became more sharply focused on terrorism and the need to arrest it funding after the terrorist attack on the World Trade Centre on 11 September 2001 which is commonly known as 9/11 attack. Extensive action has been taken globally to freeze assets held by terrorist organizations and institute other measures required for combating the financing of terrorism.

The United Nations International Convention for suppression of Terrorist Financing defines "Terrorist Financing" as below and on the recommendation of the Financial Action Task Force, most countries including Sri Lanka use this definition.

"Any person commits an offence within the meaning of the convention if that person by any means directly or indirectly, unlawfully or willfully, 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:

1) An act which constitutes an offence within the scope of and as defined in one of the treaties of United Nations Organization

2) Any other act intend to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act , by its nature or context , is to intimidate a population or to compel a Government or an international organization to do or to abstain from doing any act"

1.3 Legislation in Sri Lanka on Anti Money Laundering (AML) and Suppression of Terrorist Financing (STF)

i. Following Acts form the body of statutes aimed at Anti Money Laundering and Suppression of Terrorist Financing in Sri Lanka. These are published in the Bank's Compliance Intranet and also could be accessed through the website of the Financial Intelligence Unit. (FIU)

- Prevention of Money Laundering Act No 05 of 2006" and amendments thereto
- Convention on the Suppression of Terrorist Financing Act No 25 of 2005
- Financial Transactions Reporting Act No 06 of 2006
- All gazettes , directions, circulars, instructions issued by the FIU from time to time

ii. Unlawful activities under the Prevention of Money Laundering Act Following actions have been identified as unlawful activities and any property derived out of proceeds of such unlawful activity is considered as laundered property.

a) Offences under Poisons, Opium and Dangerous Drugs Ordinance (Chapter 218)
b) Offences under any law or regulation for the time being in force relating to the prevention and suppression of terrorism
c) Offences under Bribery Act (Chapter 26)
d) Offences under Firearms Ordinance (Chapter 182), the Explosives Ordinance (Chapter 183) or the Offensive Weapons Act No 18 of 1966.
e) Offences under the Foreign Exchange Act :
f) Offences under an offence under section 83c of the Banking Act, No.30 of 1988;
g) Offences under any law for the time being in force relating to transnational Organized crime;
h) Offences under any law for the time being in force relating to cyber crime;
i) Offences under any law for the time being in force relating to offence against children
j) Offences under any law for the time being in force relating to offenses connected with the trafficking of persons; and
k) Offences under any other law for the time being in force which is punishable by death or with imprisonment for a term of five years or more.

Penalties

As per the Act penalty for non-compliance would be a fine not more than three times the value of the property or rigorous imprisonment for a period not less than five years and not more than twenty years.

iii. Obligation to disclose to Financial Intelligence Unit of any Money Laundering Activity It would be also an offence under the Act, if any persons do not disclose to the Financial Intelligence Unit of such knowledge or information obtained by a person in the course of any trade, business, profession or employment.

iv Powers of the Financial Intelligence Unit (FIU)[1]

a) Under the Financial Transactions Reporting Act No. 06 of 2006 Financial Intelligence Unit has been established as the regulatory agency to receive and analyze data and is empowered by the Act to facilitate the prevention, detection, investigate and prosecute over the offences of money laundering and financing terrorism.

b) Under the powers vested by the Act the FIU can require institutions to undertake due diligence measures to combat money laundering and terrorist financing.

c) FIU is empowered to carry out examinations of all institutions for the purpose of ensuring compliance with rules and regulations.

d) FIU is also empowered to impose penalties to enforce compliance or on failure to comply to requirements of the Act , that includes any regulatory measures including but not being limited to the suspension or cancellation of license

[1] FIU powers listed above is only a summary and powers of FIU do not restrict to above only

2.0 AML AND STF POLICY FOR DFCC BANK PLC

In order to protect its reputation and to meet its legal, regulatory and social obligations, it is essential that the bank takes all precautions to avoid the risk of Bank being used by Money Launderers and Terrorist Activists.

2.1 Applicability of Laws and Customer due Diligence Rules

i. All staff of the Bank shall be guided by laws and regulations in respect of AML and CFT.

ii. Bank shall take such measures as may be specified in such laws and any other Rules for the purpose of following

a) Money Laundering and Terrorist Financing Risk Management of the Bank

b) Customer Due Diligence

b. i CDD for all customers

b. ii Occasional Customers , One off Customers , Walk-in- customers and Third Party Customers

b. iii CDD for legal Persons and Legal Arrangements

b. iv Non-Governmental Organizations, Not for Profit Organizations and Charities

b. v Customers and Financial Institutions from High Risk Countries

b. vi Politically Exposed Persons

b. vii Reliance on Third Parties

c) Correspondent banking

d) Wire Transfers

d.i Ordering Financial Institution

d.ii Intermediary Financial Institution

d iii Beneficiary Financial Institution

d vi Money or Value Service

e) Record keeping

2.2 Risk Based Approach on Customer Due Diligence

In terms of Extraordinary Gazette No 1951 /13 dated 27th January 2016 on Financial Institutions Customer Due Diligence Rules (CDD) No 01 of 2016 Bank shall be adopting ‘‘Risk Based Approach’’ (RBA) for the purpose of identifying, assessing and managing money laundering and terrorist financing risks posed by its customers. This will be done by conducting ongoing customer due diligence on a risk based approach.

The RBA will focus on the following.

i. Customers

ii. Geographical areas

iii. Products

iv Services

v. Transactions

vi . Delivery channels

Bank wide risk assessment based on above carried out by the Compliance Department shall be documented and periodically reviewed. Appropriate risk assessment methods in this regard shall be prepared by the Compliance Department. A report carrying following details shall be submitted to the Board

i. Results of monitoring

ii. Details of significant risks involved either internally or externally; modus operandi and its impact or potential impact on the Bank

iii. Recent developments in written laws on AML or CFT

iv. Findings and outcomes of the transaction monitoring

v. Details of Training programs conducted to mitigate the ML/TF risk on the bank

2.3 Responsibilities of the Board and Senior Management

2.3.1 Board and Senior Management shall ;

i. Ensure that Bank takes appropriate steps to identify , asses and manage its Money Laundering and Terrorist Financing risks.

ii. Ensure that intensity and extensiveness of risk management of ML and FT shall be in compliance with "risk based approach" and be proportionate to the nature , scale and complexity of the Bank's activities.

iii. Approve and oversee compliance of internal policies on AML and CFT

iv. Ensure that they receive periodic reports of its risk assessment

v. Appoint a senior management level officer as compliance officer

vi. Ensure that compliance officer and staff of the Compliance Department has prompt access to all customer records and other information required to discharge their duties under AML and CFT

vii. Develop and implement a comprehensive employee due diligence and screening procedure for permanent, contractual and outsourced personnel

viii. Maintain an independent audit function in order to effectively assess Bank's internal policies , procedures and controls over AML and CFT

ix. Shall ensure the Compliance function is equipped with appropriate systems and resources.

x. shall ensure that Bank identify and assess and take appropriate measures to manage and mitigate ML and FT risks pertaining to following

a) new products,

b) services ,

c) new business practices ,

d) new delivery channels

e) new technology development for both new and preexisting products

2.4 Responsibilities of the Compliance Officer

As per the Financial Transaction Reporting Act No. 6 of 2006 section 14, every Institution is required to appoint a Compliance Officer who shall be responsible for ensuring the Institution's compliance with the requirement of this Act. The Board shall ensure that a dedicated compliance officer is appointed in terms of the Financial Transactions Reporting Act whose responsibilities shall be among other things;

i. Develop and enforce the bank's Anti-Money Laundering and Suppression of Terrorist Financing Policy which will include the following requirements:

(a) Customer identification requirements

(b) Record keeping and retention requirements

(c) Requirements for conducting ongoing due diligence on the business relationships and ongoing scrutiny of transactions throughout the business relationship

(d) Reporting requirements including reporting of suspicious transactions and customer transactions.

(e) Ensure requirements of screening new staff before hiring them as employees.

(f) Keep staff informed of new regulations issued in relation to AML

(g) Facilitate required staff training

(h) Monitoring of transactions

(i) Submission of regulatory returns

(j) Regulator contact point

3.0 POLICIES ON CUSTOMER DUE DILIGENCE

3.1 Bank shall not open, operate or maintain any anonymous account, any account in a false name or in the name of fictitious person or any account that is identified by a number only

3.2 Bank shall not operate and maintain accounts where the ownership is transferable without the knowledge of the Bank

3.3 Bank shall not operate and maintain accounts where the account holders name is omitted.

3.4 Bank shall maintain accounts and information that assets and liabilities of a given customer can be readily retrieved.

3.5 Bank shall not maintain accounts separately from the Bank's usual operational process, systems and procedures.

3.6 Bank shall conduct CDD measures as specified in rules issued by FIU from time to time and any other appropriate guidelines that is proportionate to the nature, scale and complexity of Bank's activities and ML and CFT risk profile

3.7 Excluded and High Risk Customers

i. Following categories of business are excluded from banks business. Bank shall not open and operate accounts for such categories

a) Persons without proper identification documents

b) Shell companies[2]

c) Front organizations /individuals[3]

d) Individuals/entities whose names appear on sanctioned lists.

ii. Following types of customer categories shall principally be treated as High Risk and shall conduct enhanced due diligence since they pose a potential high risk to the Bank in respect of AML/KYC

a) Persons engaged in gaming business such as Casinos/Night clubs

b) Persons engaged in Money exchange business

c) Persons engaged in cash incentive business such as wholesale trading/petrol sheds

d) Persons engaged in Gem and Jewels trading

e) Persons engaged in Real Estate business

f) Non Governmental Organizations / Charities /Clubs and Associations/ Trusts / Foundations

g) Non face to face customers

h) Politically exposed persons

i) High Net worth individuals[4]

[2] *A **shell financial company** is a company that does not have a physical presence in any location*

[3] *A **front organization** is any entity set up by and controlled by another organizations such as organized crime groups, banned organization*

j) Existing customers if the accounts are active , yet the entire Mandate is not with the bank

k) Customers where profile is not matching with transactions and KYC reviews has not been conducted due to any reason

l) Customers where AML system analysis as High based on different para meters

It should be noted that above is an inclusive but not exhaustive list and Branches shall contact the Compliance Officer in case of doubt as to whether any category is posing high risk.

ii Staff shall obtain pre or post approval from the CEO or in the absence of CEO from D/CEO OR COO to open accounts in case of PEPS

iii Enhanced due diligence shall include one or more of following methods

a) Gather sufficient information from public domain

b) Establish source of funds and wealth

c) Obtaining of documentary evidence in case of NGOs in respect of their projects and approval

d) Obtain documentary proof of registration /licensing/certificates in respect of business such as casinos/gem traders etc

e) Customer visits

f) Continuously monitor customer transactions

iv. Branches shall monitor customer transactions / activities / behavior continuously and shall conduct post enhanced due diligence in case if any customer is identified to be High Risk subsequent to opening of account /s.

---

[4] *High net worth shall be based on the assets, amount of deposits, wealth , turn over and general information gathered from public domain etc*

3.8 Beneficial owners, Legal Persons and Legal arrangements

If a relationship is being created for a customer who is not a natural person, Bank shall take reasonable steps to understand the ownership structure of the customer and determine the natural persons who ultimately own or control such customer.

Identification, verification, documents, delayed verification time lines and any other relevant steps that are required to be adopted with regard to beneficial ownership have to be met as required.

3.9 Continuous Customer Due Diligence

In terms of FTRA and CDD rules Bank shall carry out continuous customer due diligence to ensure that the transactions carried by the customer thorough his account are consistent with the economic profile known to the bank. In this regard Bank shall adopt a risk based approach depending on the risk category of the customer and procedural guidelines issued by the Compliance Department

3.10 Occasional Customers, One off Customers, Walk-in- Customers and Third Party Customers

Any transaction or series of linked transaction if exceeds two hundred thousand rupees or equivalent in foreign currency, conducted by any of the customers mentioned above Bank shall conduct CDD measures and obtain copies of Identifications.

3.11 NGO and Non Profit Organizations and Charities

Bank shall apply enhanced due diligence measures to NGO and Non for Profit Organizations, individuals who are authorized to operate the account with the bank.

3.12 Customers and Financial Institutions from High Risk Countries

Bank shall apply enhanced due diligence measures to customers from high risk countries. Such countries will primarily be FATF listing and depending on other ML and FT scenarios unique to such countries, based on the information in public domain Compliance Department shall time to time issue instructions in this regard.

3.13 Politically Exposed Persons

Bank shall apply enhanced due diligence measures to Politically Exposed Persons. Staff shall obtain pre or post approval from the CEO or in the absence of CEO from D/CEO OR COO to open accounts for PEPs.

3.14 Agency Functions of Money or Value Transfer Service Providers

i. Bank shall act with enhanced due diligence when entering, sending and receiving funds through money remittance services owing to its inherent risk when paying and receiving funds to/from third parties.

ii. Bank has to ensure that MTVS providers are guided by provisions of the CDD gazette in terms of wire transfers

iii. Business promotion officers shall at all times obtain the Approval/clearance of the Board, senior management and Compliance Officer before establishing relationship with any money remittance services.

iv. Business promotion officers should ensure that every precautionary measure is made to distinction between formal money transfer services and other alternative money value transfer systems through which funds or value are moved from one geographic to another, through informal and unsupervised networks or mechanisms.

v. This Policy shall be applicable to all agents and shall comply with the bank's CDD requirements when accepting cash and when making payments and respective

Procedure manuals/guidelines issued by the Bank and/or the respective money remittance service.

vi. Adequate training shall be provided to agents by the business line, on their responsibilities and all aspects regarding identification, checking and approving transactions, recording, reporting and retaining records.

3.15 Correspondent Banking Relationships

i. Staff members who are responsible for establishing and maintaining correspondent Banking relationship shall ensure adequate information is obtained from the respective entity prior to entering into relationships and / or from time to time as informed by the Compliance Officer.

ii. Staff members responsible for correspondent bank relationships shall ensure that the Bank does not undertake business with shell financial institutions[5] and ensure that no accounts for shell financial institutions are opened by the Bank.

4.0 TRAINING AND AWARENESS

4.1 Responsibility on staff Training and Awareness

i. Compliance officer shall be responsible for AML/CFT training to all staff of the Bank Including the Board, Senior Management and shall design appropriate modules and shall conduct training to all staff of the Bank, with the assistance of the Training Department of the Bank . Training will be designed on a Risk Based Approach and training department shall be informed of such categories.

i. It is the duty of the training department to maintain and retain records of training sessions including attendance records and relevant training materials.

[5] *A **shell financial institution** is a financial Institution that does not have a physical presence in any country.*

ii. Compliance Officer shall from time to time to disseminate AML related laws or changes to existing AML related policies and shall coordinate with the Operations Department and communicate procedures in respect of AML compliance.

4.2 Training and awareness methods

The Bank is vigilant in making aware of its employees on the governing regulations relating to AML/KYC. The following methods are used to train/educate the employees of the Bank in Principal.

i. Having Clear Policies , procedures on AML and dissemination

ii. Singing up of required declarations pertaining to AML

iii. Periodic class room training for target staff who will be exposed to customers and transactions

iv. Inductions for new recruits

v. E learning module based training

vi. Compliance Intranet

vii. Compliance News Letters

viii. Specific trainings by industry specialists, regulator etc.

ix. Arranging participation for external seminars , symposiums, workshops etc on AML to Compliance department staff and other staff

x. Sharing knowledge via industry associations such as Association of Compliance Officers

xi. Sub agent training either by the Compliance Department or respective business lines on AML

5.0 RISK MITIGATING ON CUSTOMER TRANSACTIONS

It is imperative that bank has in place proper controls to mitigate the AML risk exposed to the bank on customer on boarding and transaction processing. In this regard bank has in placed following controls to identify suspicious transactions and customers of negative records

5.1 Transaction Monitoring

i. Bank has established an electronic monitoring regime to identify/ track suspicious transactions and customer transaction trends to ascertain whether transactions are consistent and in line with the customers' known profile. Respective staff members are required to be well acquainted with the system.

ii AML Software is based on a rule engine which has static rules inbuilt in order to generate alters. These rules are based on various money laundering typologies experienced all over the world. During the end of the day process all transactions in the core banking system will be processed through the AML software and any transaction which is violating the rules in built will generate alters. It should be noted the violation of a rule does not necessarily imply that is a money laundering transaction. It can 99% be a common transaction. Generation of an alert on a transaction is an indication that the transaction requires further clarifications.

iii. AML software and Risk Matrixes shall be used to risk rate customers in terms of CDD gazette.

5.2 Sanction Program

The Bank is keen in managing financial crime risks that are inherent in customer relationships. Thus Bank takes mitigating efforts to gain reassurance that the risk of on-boarding and continuous transactions with customers are managed appropriately in respect of following

i. Any type of sanction that has been made into Law of the country or as issued as a directive by respective regulatory authority with specific authority to banks or that has an indirect compliance requirements

ii. Internationally Sanctioned Countries and Designated Persons by the United Nations

iii. Sanction Programs of Office of Foreign Assets Control (OFAC)

iv. Any other international sanctioned program that would have an impact on Correspondent Banking Relationships etc

In order to implement an effective sanction program Bank has subscribed to name screening data base. Bank will use following methods in screening.

i. AML Software

ii. On line licenses and Batch uploads

iii. On line Licenses Manual Process

Bank will in principal screen following categories before entering into relationships and during the relationships on a periodic basis.

i. Screen customers when entering into any relationship including (not limited) following

- Account relationships
- E Wallet Customers
- Credit card relationships
- Remittance payments (Ex; Western Union)

- Establishing and maintaining Correspondent Banking relationships

ii. Trade transactions prior to effecting a transaction

iii. All inward remittances

iv. Batch processed transactions different transaction modules , products such as Exchange House Remittances, Lanka Money Transfer system

v. Customer Transaction level screening

vi. Customer Base Periodic Checking

vii. Service Providers, Agents, Outsourced Service Providers

viii. Major Shareholders

ix. Related Parties , Key Management Personnel, All other employee categories

6.0 REPORTING REQUIREMENTS FOR SUSPICIOUS TRANSACTIONS

A suspicious transaction will often be one which is inconsistent with a customer's known legitimate business or employment or personal activities. It will be also inconsistent with normal business of similar accounts. This is the first key to recognize that a transaction or series of transactions is unusual. Where the transaction is international in nature, it needs to be reasoned out if the customer has any obvious reason for conducting business with the other country involved.

6.1 Suspicious transaction reporting procedure:

i. If a staff member suspects or has reasonable grounds to suspect or has an honest belief that the funds or proceeds of an unlawful activity or related to Terrorist Financing, it should promptly informed and send a suspicious transaction report (STR) to the Compliance Officer. Suspicious transactions shall be reported to the Compliance Officer or via e-mail or through the Phone.

ii. The Compliance Officer or designate will examine such report and where necessary call for supporting document and if the suspicion still prevails, the Compliance Officer soon as practicable, but not later than *two working days*, report the transaction or attempted transaction or the information to FIU.

6.2 Confidentiality and Non-disclosure

(i) Under no circumstances should any staff member of the bank disclose to the customer or any other person or body of persons that a disclosure has been made to the FIU or any information that will identify or is likely to identify the person who handled or reported the suspicious transaction, which will constitute an offence under the financial transaction reporting Act.

(ii) No staff member when making a suspicious report should make any false or misleading statement deliberately or make any omission from any statement thereby making it false or misleading in a material particular.

(iii) No staff member should divulge that an investigation into an offence of money laundering is being or is to be conducted.

(iv) No staff member should destroy or falsify any documents likely to be relevant to the investigation.

(v) All staff is required to co-operate with the investigations relating to money laundering by such authorities or regulations.

6.3 Personal criminal liability.

i. As per the anti-money laundering legislation in Sri Lanka, any offence under the Act will give rise to a potential personal criminal liability. Therefore strong disciplinary action will be taken against any member of staff who fails, without reasonable excuse, to make a report on a suspicious transaction as per the AML policy.

ii. Disciplinary action will also be initiated against any member of staff who blocks, or attempts to block, a report by another member of staff.

6.4 Protection of persons reporting suspicious transactions

No Civil, Criminal or disciplinary or reprisal action shall be initiated against any staff member who reports suspicious activity in good faith in terms of the Financial Transactions Reporting Act and in terms of this Policy and the confidentiality of such reporting person shall be protected

6.5 Explanatory Suspicious Transactions

i. Some of the suspicious transactions are named below. It should be noted that below instances are only stated as an explanatory note and do not encompass all suspicious transactions and staff members are strongly adviced not to limit suspicious to circumstances mentioned below

- A customer-relationship with the bank that does not appear to make economic sense, for example, a customer having a large number of accounts with the same bank, frequent transfers between different accounts or exaggeratedly high liquidity
- Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal

- Transactions that cannot be reconciled with the usual activities of the customer for example, the use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business
- Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity
- Large cash withdrawals from a previously dormant/inactive account or from an account which has just received an unexpected large credit from abroad
- Frequent address changes by customers/clients
- Client does not want correspondence sent to home address.
- Client's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact client shortly after he/she has opened an account.
- Unusual nervousness of the person conducting the transaction
- Client insists on a transaction being done quickly.
- Client appears to have recently established a series of new relationships with different financial entities.
- Client attempts to develop close rapport with staff.
- Client attempts to convince employee not to complete any documentation required for the transaction.
- Large contracts or transactions with apparently unrelated third parties, particularly from abroad
- Extensive and unnecessary foreign travel

7.0 RECORD RETENTION

To assist the authorities when investigating cases of suspected money laundering, it is essential that evidence of customer identification, address verification and all transactions is retained for at least six years. Bank shall retain prescribed records of identification, pertaining to information gathered, mandates, and documents relating to transactions for a minimum of six years.

i. Following types records /reports shall be retained for a period of at least six years after the relationship with the customer has ended.

- Identification and account opening records will be retained
- Documents verifying evidence of identity (including address)
- non-account holders following an occasional transactions or the last in a series of transactions
- Account transaction records
- every transaction undertaken for a customer
- Records relating to training internal and external,
- Records of compliance monitoring of transactions
- suspicious transaction reports
- Documentary evidence of any action taken in response to internal and external reports of suspicious transactions
- Mandatory transaction Reports (CTR, EFT – In and Out)

ii. Records will be retained in hard copy, on microfiche or computer, or other electronic format and shall be available within a reasonable time to CO and to the investigating authorities.

iii Officers responsible to retain transactions records electronically shall ensure that transactional records are not lost before the six years retention period or expires as a direct consequence of automatic data retention constraints.

iv. Where it is known that an investigation is ongoing, the relevant records will be retained until the authorities inform the bank otherwise

This policy shall replace the existing AML policy of the Bank and shall be reviewed on Annually