POLICY ON RISK BASED APPROACH FOR ANTI MONEY LAUNDERING, SUPPRESSION OF TERRORIST FINANCING AND CUSTOMER DUE DILIGENCE

Version 2.0

Version	Date Approved by the Board Integrated Risk Management Committee	Modification Summary
1.0	05th June 2018	Previous AML Policy of the Bank was replaced with the new version that included the Risk Based Approach on Anti Money Laundering , Suppression of Terrorist Financing and Customer Due Diligence
2.0	04th June 2019	Annual Review – No Changes
2.0	July 2020	Previous Policy on Risk Based Approach for Anti Money Laundering, Suppression of Terrorist Financing and Customer Due Diligence – Version 2.0 was replaced with the following new additions. i. Amended the Predicated Offenses List in line with the Amendment No 40 of 2011 to the Prevention of Money Laundering Act No 05 of 2006 ii. Inclusion of PEP identification categories in line with Guideline No. 03 of 2019 issued by the Financial Intelligence Unit iii. Inclusion of procedure to be followed on Non -face to face customers
3.0	14th October 2021	The Policy has been amended with the following to provide better clarity. i. Inclusions were made covering Standards, Legislation and Regulatory requirement ii. Inclusions on fines and penalties imposing to the bank and to the Employees iii. Inclusion on the Compliance Structure in the three lines of Defense Model iv. Responsibility of all Staff on AML/STF v. Process on Annual Review of the PEP Customers vi. New additions on the High Risk Customers vii. Manual transactions monitoring based on exceptional reports.
4.0	13th October 2022	The Policy has been amended with the following to provide better clarity. i. Inclusions were made covering requirement on the New Financial Crime Management System ii. Inclusions were made covering Standards, Legislation and Regulatory requirement

5.0	17th May 2023	The Policy has been amended with the following. i. Amending the AML policy, on timing of the screening of the existing customer database from quarterly basis to as and when a designated list is published and existing customer base to be screened once in two weeks. ii. Inclusions were made to the Bank's policy to exclude some categories from entering into financial relationships. Accordingly the Bank will not enter into financial relationships with the individuals with matching NICs to fraudulent NICs published by the Department of Persons Registration (DRP) and individuals and entities engaged in scams as identified and communicated by the director FIU with the Compliance Officer of the Bank. iii. The approving authority to onboard a customer was changed from CEO to COO.

Table of contents

Glossary

AML	Anti Money Laundering
STF	Suppression of Terrorist Financing
FATF	Financial Action Task Force
PMLA	Prevention of Anti Money Laundering Act No 05 of 2006
FTRA	Financial Transactions Reporting Act No 06 of 2006
FIU	Financial Intelligence Unit
RBA	Risk Based Approach
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
PEP	Politically Exposed Person
NGO	Non Governmental Organization
NPO	Non Profit Organization
UBO	Ultimate Beneficial Owner
MTVS	Money or Value Transfer Service Providers
STR	Suspicious Transaction Report
FCM	Financial Crime Mitigation System
RMA	Relationship Management Application

Preamble

Banks and other financial institutions may be used as intermediaries for depositing, safekeeping or transferring of funds derived from criminal activity or financing terrorism. Public confidence in banks' stability can be undermined by adverse publicity as a result of inadvertent association with criminals/terrorists.

Therefore, absence of sound policies, guidelines and practices of managing Money Laundering and Terrorist Financing may expose the banks to serious risks.

Recent developments, including robust enforcement actions taken by regulators, corresponding direct and indirect costs incurred by banks due to their lack of diligence have highlighted those risks associated with the failures.

In addition to incurring fines and sanctions by regulators, could result in significant indirect financial costs to banks through the termination of wholesale funding and facilities, claims against the bank, investigation costs, asset seizures and freezes and loan losses.

Therefore, it is of paramount importance that the Bank's Policy of Risk Management on AML/STF is set to be in line with the internationally accepted best practices as well as the domestic legislative and regulatory framework.

DFCC is committed to the highest standards of anti-money laundering compliance within the bank and it's a mandatory requirement for all the employees to adhere to standards and procedures described in the Policy Manual to prevent the use of DFCC's products, services and operations for money laundering and terrorist financing purposes.

In line with above, DFCC has adopted an Anti Money Laundering, Suppression of Terrorist Financing and Customer Due Diligence Policy Manual which provides the basis for all employees to comply with all relevant requirements in this area and assists employees in preserving the good name and reputation of Bank.

This Policy manual is a high level guide and sets out the relevant areas that employees of the Bank need to be aware of at all times. This Policy Manual is issued to enable employees to obtain a basic guidance on Anti Money Laundering/Terrorist Financing and should be read and understood in Conjunction with the other relevant and applicable circulars, instructions and guidance notes issued by the Compliance department from time to time.

1.0 Prevention of criminal use of the banking system for the purpose of money laundering and terrorist financing

i. What is Money Laundering?

There are many definitions of "money laundering". A relatively simple and non-technical definition is that 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 derived from a criminal activity such as drug smuggling, corruption. The scope of criminal activities for money laundering 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.

ii. 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 financing of terrorism.

Given below is the definition for "Terrorist Financing"' used by Sri Lanka as recommended by Financial Action Task Force (FATF) and used by the United Nations International Convention for Suppression of Terrorist Financing.

"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***"

iii. Applicable Standards, Legislation and Regulatory Structure

a. International Best Practices:

- **Recommendations of the Financial Action Task Force (FATF)**

The Financial Action Task Force (FATF) which is an inter-governmental body which develops international standards to combat money laundering and terrorist financing issued forty (40) recommendations in 2012 setting the international standards that constitute the basic framework for preventing, detecting and suppressing both money laundering and the financing of terrorism and proliferation.

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

i. Following Acts form judicious framework on 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 amendment Act, bearing No. 40 of 2011 (PMLA)**
- **Convention on the Suppression of Terrorist Financing Act No 25 of 2005 and amendment Acts bearing No. 41 of 2011 and No. 3 of 2013 (CSTF)**
- **Financial Transactions Reporting Act No 06 of 2006 (FTRA)**
- **All gazettes , directions, circulars, instructions issued by the FIU from time to time**

iv. Significant Obligations arising on the Bank

a. Prevention of Money Laundering Act (PMLA)

i. Section 03 of the PMLA -The offence of Money Laundering is defined as "*receiving, possessing, concealing, investing, depositing or bringing into Sri Lanka, transferring out*

of Sri Lanka or engaging in any other manner in any transaction, in relation to any property derived or realized directly or indirectly from "Unlawful Activity" or proceeds of "Unlawful Activity". "

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.

ii. Section 05 of the PMLA

If any person do not disclose to the FIU, knowledge or information obtained by a person in the course of any trade, business, profession or employment on any Money Laundering Activity also an offence under the Act.

Penalty for non compliances would be a fine not exceeding Rs. 50,000 or to imprisonment of either description for a period not exceeding six months or to both such fine and imprisonment.

iii. Unlawful Activities (Predicated offences under the Prevention of Money Laundering Act *Refer Annexure I of this Policy)*

If any Bank Employee has knowledge or reasons to believe that funds in any account or any transction is connected with any of the activities given in the list , such knowledge shall be disclosed to the Compliance Officer immediately

iv. Freezing Orders

Section 7- A Police Officer not below the rank of Superintendent of Police or an Assistant Superintendent (in the absence of SP) of Police may issue an Freezing Order prohibiting any transaction (any account/ property /investment) which may have been used or which may be intended to be used in connection with offence

Freezing Order shall be in force for a period of 7 days and will be extended through a court order.

As per the Section 7 (3)of the Act , if any person who acts in contravention of a **Freezing Order** issued, shall be guilty of an offence subject to the following fines and penalties .

- Fine not exceeding Rs. 100,000 or one and a half times the value of the money in such account, property or investment, or
- To imprisonment of either description for a period not exceeding one year or to both such fine and imprisonment.

Bank staff shall not at any given time allow withdrawing any money or facilitating any transaction in line with above section.
Any attempts to violate such freezing orders by the customer or any other staff member should be informed to the CO immediately

b. Convention on the Suppression of Terrorist Financing Act

The Convention on the Suppression of Terrorist Financing Act (CSTFA) . No.25 of 2005 was enacted to give effect to Sri Lanka's obligations under "***International Convention for the Suppression of Terrorist Financing adopted by the United Nations General Assembly, dated 10/01/2000***" **and was further amended under Act No. 41 of 2011.**

In terms of the Act, the provision or collection of funds for use in terrorist activity with the knowledge or belief that such funds that could be used for financing a terrorist activity is an offence

The Act prohibits the financing of terrorist acts, terrorists and terrorist organizations. Further the CSTFA has provisions for freezing of terrorist financing related assets and forfeiture of such assets.

In many respects terrorist financing is the mirror image of money laundering. In one there is an effort to take bad money and make it good and in the other there is an effort to use good money for bad purposes.

Employees should therefore remain alert to all possible money laundering or terrorist financing situations so as to prevent the products, services and operations of DFCC being exploited. Further if any suspicious transactions are noted, same to be reported to the Compliance Officer as per the procedures detailed in this policy Manual.

c. Financial Transaction Reporting Act (FTRA) No.6 Of 2006

Section 5-Bank shall conduct ongoing due diligence on the business relationship with its customer.

Further ongoing scrutiny of any transaction undertaken throughout the course of the business relationship with a customer to ensure that any transaction that is being conducted is consistent with the Banks' knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds,

Section 9 – Further under the FTRA, no person should divulge that an investigation into an offence of money laundering is being or is to be conducted.

Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is acceptable as it forms an integral part of the KYC program. Such enquiries should not give rise to tipping off.

Section 15 (2) -As per the powers vested under Section 15 (2) of the FTRA, the Financial Intelligence Unit (FIU) may direct the Banks not to proceed with any transactions or attempted transaction excluding credit transactions in respect of accounts (including safe boxes/safe deposit lockers), transactions, CDS accounts or any other business relationships including remittances, maintained by certain individuals/entities.

Section 19- Failure to conform to the requirements in the Act, the Bank shall be liable to a penalty as may be prescribed taking into consideration the nature and gravity of relevant non-compliance: Provided however such penalty shall not exceed a sum of Rs.1 Mn in any given case.

Further, failure to comply with the requirement in the Act will lead to Suspension of the Institution from carrying out business or the cancellation of license and will negatively impact on Bank reputation.

Financial Intelligence Unit (FIU)[1]

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

b) Require institutions to undertake due diligence measures to combat money laundering and terrorist financing.

c) Carry out examinations of all institutions for the purpose of ensuring compliance with rules and regulations.

d) Empowered to impose penalties to enforce compliance or on failure to comply requirements of the Act, that includes any regulatory measures including but notbeing limited to suspension or cancellation of license.

e) FIU has powers to issue Rules , Guidelines , Circulars ect

As part of its anti-money laundering and suppression of terrorist financing program of the bank, Refer Annexure II for the applicable rules as of date:

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

2.0 AML and STF Program of the Bank

DFCC Bank attributes the highest importance to prevent the Bank from being utilized as a conduit and/or to be directly or indirectly be used for financial crime purposes by its customers. This Policy is a high-level guide and all employees of the Bank need to be aware of the contents of same.

i. The Compliance Structure in the three line of Defense Model

Compliance Risk is the Risk arising due to non-Compliance with applicable Laws, Regulations and standards including internal policies. Compliance risks may arise in the form of Regulatory, legal, financial and reputational risk.

Bank has a three line of defense mechanism in order to facilitate the management of Compliance Risk and Compliance Department is positioned as the second line of defense in the three lines of defense frame work of the Bank. The Internal Audit Departments acts as the third lines of defense by carrying out periodic evaluations of the effectiveness of compliance with AML/CFT policies and procedures.

ii. Applicability of Laws and Customer Due Diligence Rules

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

ii. Bank shall take measures as specified in laws and any other Rules for the purpose of complying with following;

iii. Money Laundering and Terrorist Financing Risk Management of the Bank

iv. Customer Due Diligence for all customers and transactions. (Customers shall include regular account holders as well as Occasional Customers, One-off Customers, Walk-in- customers and Third Party Customers, legal Persons, Legal Arrangements and third parties, who are connected customers on transactions carried out with correspondent banks, wire transfers.)

iii. Risk Based Approach on Customer Due Diligence

a. Critical elements on Risk Assessment

In terms of Extraordinary Gazette No 1951 /13 dated 27th January 2016 on Financial Institutions Customer Due Diligence Rules (CDD) No 01 of 2016 and Circular No 1/18 with reference 037/05/002/0018/017 dated 11th January 2018, Bank shall be adopting "Risk Based Approach" (RBA) for the purpose of identifying, assessing and managing money laundering, terrorist financing risks

pertaining to the Bank. The Bank's RBA shall be proportionate to the nature, scale and complexity of the Bank's activities, customer profile and money laundering, terrorist financing risk posed to the Bank on its day to day operations.

Business lines of the Bank shall primarily assess the AML/STF risk, when entering into and continuation of relationships, conducting transactions based on the criteria given below.

i. Customers (Type and Business of the customer)
ii. Countries or geographical areas
iii. Products
iv. Services
v. Transactions
vi. Delivery channels

b. Bank wide AML/STF risk assessment

Bank wide risk assessment based on above elements, will be carried out by Compliance Department. Appropriate risk assessment methods, risk matrices, processes and systems shall be developed by Compliance Department towards this purpose and shall be reviewed periodically to ensure adequacy. Results of the risk assessment shall be documented and presented to the Board, annually.

Risk assessment report presented to the Board shall encompass the following at minimum,

i. Bank's AML/STF exposure in terms of criteria given in above
ii. Findings and outcomes of the transaction monitoring
iii. Details of significant risks involved either internally or externally; modus operandi and its impact or potential impact on the Bank
iv. Recent developments in written laws on AML and STF
v. Details of Training programs conducted to mitigate the Money Laundering and Terrorist Financing risk on the bank

iv. Responsibilities of the Board on AML/STF

Board shall;

i. Understand the legal regime and regulatory environment governing the Anti Money Laundering Laws and Suppression of Terrorist Financing.

ii. Approve internal policy of Anti Money Laundering and Suppression of Terrorist Financing.

iii. Ensure that Bank takes appropriate steps to identify, assess and manage its Money Laundering and Terrorist Financing Risks.

iv. Appoint a Senior Management level officer as the Compliance Officer, who shall be responsible for ensuring Bank's compliance with the requirements of the AML/STF rules.

v. Ensure that the Board receives timely reports of Bank's risk assessment on money laundering and terrorist financing risk profiles, effectiveness, and risk control and mitigation measures.

vi. Ensure that Compliance Officer and staff of the Compliance Department have prompt access to all customer records and other information required to discharge their duties under AML and STF.

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

viii. Ensure the Compliance function is equipped with appropriate systems and resources.

v. Responsibilities of the Senior Management

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

ii. Ensure that the Compliance officer or any other person authorized to assist the Compliance officer has prompt access to all customer records and other relevant information which may be required to discharge the duties of the Compliance function.

iii. Ensure developing and implementing of comprehensive employee due diligence and screening procedure.

iv. Support the Compliance Officer to implement suitable training for employees including Board of Directors.

v. Ensure that Bank identify, 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 new and existing products

vi. Responsibilities of the Compliance Officer

In terms of the Financial Transaction Reporting Act No. 6 of 2006 section 14, Compliance Officer's responsibilities shall primarily be to develop and enforce the Bank's Anti-Money Laundering and Suppression of Terrorist Financing Policy, which will include the following;

(a) Customer identification requirements

(b) Record keeping and retention requirements

(c) Requirements for conducting ongoing due diligence on 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 Board, Management & the staff informed of new regulations issued in relation to AML/STF

(g) Conduct required staff training

(h) Monitoring of transactions

(i) Implement process and systems to enforce effective transaction screening process

(j) Submission of regulatory returns

(k) Act as a Regulatory contact point

(l) Provide timely information to the Board/BIRMC and to the Management on the status of AML/STF risk of the Bank for their appraisal.

vii. Responsibility of all Staff

- All employee of the Bank is responsible to ensure the prevention of money laundering and suppression of terrorist financing on a day to day basis and to ensure the implementation and monitoring of procedures and controls that meet the requirements of this policy and

related policies and guidelines issued by the Compliance Department.

- Staff members who become aware of breaches of this policy shall raise/escalate such breaches through the procedure laid down in the Bank Whistle Blowing Policy

- Most of the provisions in this Policy Manual as well as the other Guidelines issued by the Compliance Department involve detailed and/or technical requirements. Any employee requiring clarification regarding any matter in this Policy Manual or concerning any other money laundering or terrorist financing matter, or wishing to provide feedback or suggestions for updates to the Manual, should contact Compliance Officer of the Bank:

3.0 Policies on Customer Due Diligence

Bank shall develop and implement clear customer acceptance policies and procedures to identify the types of customers that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment. Such policies and procedures should require basic due diligence for all customers and commensurate due diligence as the level of risk associated with the customer. For proven lower risk situations, simplified measures may be permitted to the extent given by CDD rules. Where the risks are higher, the bank should take enhanced measures to mitigate and manage those risks.

Bank's basic customer acceptance policy is set forth below. Detailed procedures relating to CDD shall be communicated as required time to time in respective manuals, guidelines and instructions.

i. 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.

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

iii. Bank shall not operate and maintain accounts where the account holder's name is omitted.

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

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

vi. 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.

vii. Bank shall not enter into relationship with certain business categories. Further, Bank shall conduct Enhanced Due Diligence when entering into relationship with High Risk Customer categories.

Refer Annex III of the Policy for Excluded and High Risk Customer Categories and EDD measures

viii. Beneficial owners, Legal Persons and Legal arrangements

If a relationship is being created for a customer who is not a natural person (legal person and legal arrangement), the 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 in line with CDD rules on beneficial ownership should be complied.

ix. Customer Risk Assessment at the time of client on- boarding

In terms of Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 by Gazette Extraordinary No 1951/13, dated January 27, 2016, bank shall take appropriate steps to identify, access and manage its money laundering and terrorist financing risk in relation to its customers.

In line with the above guideline, it is a requirement of Account Opening Officers/ Relationship Managers to assess the customer in order to identify Money Laundering and Terrorist Financing (ML/TF) risk at the time of client on boarding.

Account Opening Officers/ Relationship Managers should be mindful that the risk profile of a customer is variable and will depend on several risk factors as detailed below.

- Customer Type
- Occupation/Business
- Jurisdiction/ Geographic Area
- Products /Services
- Delivery Channels
- Expected Turnovers
- Source of funds
- Identification of Ultimate Beneficial owners
- PEP Status.

In order to comply with the above requirement, ML/TF Risk Assessment on customers should be conducted based on the above parameters at customer level (CIF) which has been developed through KC+ Module of the Financial Crime Mitigation System (FCM).

x. 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. In principle, CDD review of a customer shall be conducted based on the below given periodicity.

Customer Risk Category	CDD frequency
High Risk	Annually
Medium Risk	Every three years
Low Risk	Every Five years

Based on Risk Category allocated to each customer, risk assessment shall be periodically reviewed by the respective branch as per the mentioned period.

xi. CCTV Operations for AML/CFT Purposes

The Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021 has issued pursuant to section 15(I)(j) of the Financial Transactions Reporting Act, No. 06 of 2006 and the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016.

In terms of the Guideline No 02 of 2021, the Bank has developed a CCTV Policy and CCTV Procedure Manual ensures to mitigate risk of money laundering and terrorist financing risk of the bank. As part of bank's anti-money laundering and suppression of terrorist financing program, the bank shall comply with these two manuals/policy on CCTV Operations.

xii. Guidelines for Financial Institution on Keeping Accounts reported in Suspicious Transaction Reports. Under surveillance, No 01 of 2022.

In terms of FIU Guideline No 01 of 2022, The bank is required to closely monitor the reported

accounts informed by the FIU to be Kept Under Surveillance (KUS), for a period of three months, unless specified otherwise and submit a report to the FIU within three working days from the end of the period of three months or the end of the specified period on whether the reported suspicious transactions are continuing or not. Reporting circumstances are below.

- Customer Requests to close the reported accounts
- Significant deposits/withdrawals to/from the reported account not in line with the declared profile
- Change in the transaction pattern/emergency of new trends
- Change of the ownership/control of the reported account
- Significant changes in KYC/CDD details

xiii. 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.

xiv. NGO and Non Profit Organizations and Charities

Bank shall apply enhanced due diligence measures to NGO, NPO and Charities. CDD should also be conducted on office bearers and authorized signatories of the entity.

xv. Non -face to face customers

A non-face-to-face transaction is where a transaction occurs without a customer having to be physically present. As such Bank shall apply enhanced due diligence measures and risk profiling on customer considering the products, transactions or delivery channels of the non face to face customer. Further Bank shall have in place proper customer verification mechanism process in line with the given regulation as applicable.

Non face to face customer on boarding shall have proper control to mitigate fraud risk, laundering risk and terrorist financing Risk.

xvi. 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 decided based on FATF listing, depending on other ML and FT scenarios unique to such countries and information through public domain. Compliance Department shall time to time issue instructions in this regard.

xvii. Politically Exposed Persons

Bank shall apply enhanced due diligence measures to Politically Exposed Persons. Bank will adopt the Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by the Financial Intelligence Unit on 01st October 2019 for identification of PEPs. In terms of Section 08, 09 and 10 of the guideline Bank will consider following categories as PEPs

- Domestic PEPs: individuals who are entrusted with prominent public functions in Sri Lanka.
- Foreign PEPs: individuals who are entrusted with prominent public functions by a foreign country.
- International organization PEPs: persons who are entrusted with a prominent function by an international organization.
- Immediate Family members: individuals who are related to a PEP either directly (on grounds of consanguinity) or through marriage or similar (civil) forms of partnership.
- Close associates: individuals who are closely connected to PEP, either socially or professionally.
- immediate family members of PEPs include any of the following relations:

  i. spouse (current and past);
  ii. siblings, (including half-siblings) and their spouses;
  iii. children (including step-children and adopted children) and their spouses;
  iv. parents (including step-parents);
  v. grand children and their spouses.

- Close associates of PEPs or their family members includes;

  i. a natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship with any person identified in FIU guidelines 7 or 9 on PEPs
  ii. a legal person or legal arrangement whose beneficial owner is a natural person and is known to have been set up for the benefit of such person or his immediate family members identified in FIU guidelines 7 and 9 on PEPs
  iii. a PEP's widely- and publicly-known close business colleagues or personal advisors, in particular, persons acting in a financial fiduciary capacity.

Bank will also adopt the Non-Exhaustive List Categories of Customers that can be considered as PEPs mentioned ANNEXURE A to the above FIU Guideline on PEPs.

Officers are required to obtain prior approval from the Chief Operating Officer (COO) or in the absence of COO from Vice President - Branch Operations be for entering in to relationship with PEPs. In order to get the COOs approval the branch should first get the Compliance clearance and then Branch Operation's clearance to be obtained.

In case of entering into relationship the status of PEP is not identified due to whatsoever reason or the customer becomes a PEP subsequently to entering into relationship, respective Branch or Relationship Manager shall obtain post approval from COO and in the absence of COO from Vice President - Branch Operations for continuation of the relationship.

Account officer shall ensure to tag the PEP customer in the T24 at the time of on boarding the PEP customer.

Annual Review of the PEP Customers: In terms of the regulation No. 03 of 2019, PEPs shall be subject to annual reviewed and Enhanced Due Diligence (EDD) shall be carried out by the RM/Branches. Relevant Branches /RMs are required to carry out PEP annual reviews on the standard format shared by Compliance Department.

xviii. Agency Functions of Money or Value Transfer Service Providers(MVT'S)

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.

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

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.

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.

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.

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.

xix. Correspondent Banking Relationships

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.

Staff members responsible for correspondent bank relationships shall ensure that the Bank does not undertake business with shell financial institutions[2] and ensure that no accounts for shell financial institutions are opened by the Bank.

Staff members should ensure to conduct annual reviews on the correspondent banks & RMAs.

xx. Trade Finance

Trade-based Money Laundering and Terrorist Financing usually involve invoice manipulation and uses trade finance routes and commodities to avoid financial transparency, laws and regulations. The use of these Trade facilities such as Letters of Credit and other contingency facilities need to be reviewed from time to time by the Trade and relevant Relationship/Branch staff.
Further Trade Transactions are screened against "World Check" (a database consisting of high risk individuals and institutions worldwide) to ensure that transactions with sanctioned countries, vessels, individuals and entities are effectively captured.

All trade facilities/services shall only be offered to customers who maintain accounts with the Bank and whose KYC is in place and subject to Enhance Due Diligence.CDD reviews as per the policy of the Bank to be conducted on all such customers.

xxi. Treasury Dealings

With regard to dealings in Forex, money market, bonds, securities, precious metals etc. The Bank staff should ensure that the counter-parties are adherence to AML/CFT guidelines to prevent transactions with non-Compliant.

xxii. Wire Transfer services /Remittances

Extra vigilance is required by the Bank when facilitating money transmission services and other money or value transfer systems through, which the funds or values are moved from one geographic location to another.

This is required in order to ascertain the sources of such funds and the legitimacy of the transaction/s.

Further, Wire Transactions are screened against "World Check" (a database consisting of high risk individuals and institutions worldwide) through FCM to ensure that transactions with sanctioned countries are effectively captured.

All Wire transfer services shall only be offered to customers who maintain accounts with the Bank and whose KYC is in place and subject to Enhance Due Diligence

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

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. Compliance officer shall conduct training to all staff of the Bank, with the assistance of bank's Training Department. Training will be designed on a Risk Based Approach and training department shall be informed of such categories.

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

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

iv. Staff should follow mandated training programs on AML/STF.

5.0 Risk Mitigating on Customer Transactions

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

i. Transaction Monitoring

Ongoing Monitoring:

The Bank and its employees are required to monitor transactions to determine if any particular transaction is suspicious in nature and may be related to money laundering or terrorist financing activities. The extent of the monitoring will be determined on a risk based approach. Ongoing monitoring is an important part of the Bank's anti- money laundering and suppression of terrorist financing program.

Post transaction AML Monitoring

a) Transaction monitoring system (AML Software)

Bank's Post Transaction Monitoring will be conducted through FCM system which shall be implemented to automatically analyze data via post transaction monitoring rules.
The FCM system covers all accounts of the Bank's customers and transactions. Alerts will be generated daily, weekly and monthly and are used to analyze transaction trends and identify unusual transactions and business relationships.

b) Manual transactions monitoring based on exceptional reports other than FCM.

Further manual transactions monitoring process is being carried out by the compliance staff on an daily basis, based on the system generated Reports. The transactions monitored may include the following.

- All transaction report
- CDM Cash Deposit, CEFT transfers,
- Online Banking transaction report
- Wire transfers,
- PEP transactions,

ii. Sanction Program

The Bank is keen in managing financial crime risks that are inherent in customer relationships. Thus the Bank takes efforts to gain reassurance that the risks 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 (UNSC) and EU

iii. Sanction Programs of Office of Foreign Assets Control (OFAC) and UK sanctions regimes

iv. Any other international sanctioned program that would have an impact on Correspondent Banking Relationships as decided by the Compliance Officer time to time

The bank has implemented a new Financial Crime Mitigation System (FCM) for sanctioned screening purposes to ensure full compliance with CDD Rule No. 01 of 2016. FCM system is integrated with the " World Check" (a database consisting of high risk individuals and institutions worldwide), FIU blacklists / watch lists, the LTTE list and the Al Qaida, Taliban lists.

The Bank does not carry out business with sanctioned individuals and entities.

Refer Annexure IV for details on customer screening

6.0 Reporting requirements for Suspicious Transactions

A suspicious transaction will often be inconsistent with a customer's known legitimate business or employment or personal activities. It will also be inconsistent with normal business of similar accounts.

Refer annexure V for examples of suspicious transactions

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 a suspicious transaction report (STR) should be sent 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. Suspicious transactions reporting procedure is detailed in the AML Manual.

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 FTRA.

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.

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.

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.

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.

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 FTRA and in terms of this Policy and the confidentiality of such reporting person shall be protected

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 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
    - Documents verifying evidence of identity (including address)
    - Non-account holders identifications
    - 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 Compliance Officer 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 be reviewed on annually.

Annexure

Annexure 1

Predicated offences under the Prevention of Money Laundering Act

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 section 83c of the Banking Act, No.30 of 1988;
f) Offences under any law for the time being in force relating to transnational Organized crime;
g) Offences under any law for the time being in force relating to cyber crime;
h) Offences under any law for the time being in force relating to offence against children
i) any written law for the time being in force relating to offences connected with the trafficking or smuggling of persons;"
j) the Customs Ordinance (Chapter 235) and any Regulation, Rule or Order made there under;
k) the Excise Ordinance (Chapter 52) and any Regulation, Rule or Order made there under
l) the Payment Devices Frauds Act, No. 30 of 2006 and any Regulation, Rule or Order made there under;
m) the National Environmental Act, No. 47 of 1980 and any Regulation, Rule or Order made there under;
n) an offence under any other written law for the time being in force which is punishable by death or with imprisonment for a term five years or more:
o) an act committed within any jurisdiction outside Sri Lanka, which would either constitute an offence in that jurisdiction or which would if committed in Sri Lanka amount to an unlawful activity within the meaning of this Act.

Annexure 11

Rules, Guidelines, Circulars issued by the FIU

i. Extraordinary Gazette No 1437/24, March 23 of 2006 - Establishment of the Financial Intelligence Unit (FIU)
ii. Extraordinary Gazette No 1555/9, June 25 of 2008 – the requirement under Section 6 (b) to report to the Financial Intelligence Unit every cash and electronic fund transfer made at the request of a customer, where the amount of such transfer exceeds Rupees One Million (Rs. 1,000,000) or its equivalent in any foreign currency.
iii. Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 by Gazette Extraordinary No 1951/13, dated January 27, 2016.
iv. Guidelines for Financial Institutions on Suspicious Transactions Reporting, No 06 of 2018
v. Guidelines for Financial Institutions on Identification of Beneficial Ownership, No. 04 of 2018
vi. Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by the Financial Intelligence Unit on 01st October 2019 for identification of PEPs.
vii. Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 03 of 2020
viii. Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021
ix. Guidelines for Financial Institution on Keeping Accounts reported in Suspicious Transaction Reports. Under surveillance, No 01 of 2022.

Annexure III

Excluded Customer categories

Bank shall not open and operate accounts for following categories of business.

a) Persons without proper identification documents
b) Shell companies[1]
c) Front organizations /individuals[1]
d) Individuals/entities whose names appear on sanctioned lists.
e) The individuals with matching NICs to fraudulent NICs published by the Department of Persons Registration (DRP).
f) Individuals and entities identified as engaged in SCAMs as identified and communicated by the director FIU with the Compliance Officer of the Bank.

High Risk Customer Categories

Following types of customer categories shall principally be treated as High Risk and respective Branch Managers/Relationship Mangers who are directly responsible to maintain the relationship with the particular customer shall conduct enhanced due diligence since they pose a potential high risk to the Bank in respect of AML and STF

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/ pharmacies/ clothing/ vehicle sales
d) Persons engaged in Gem and Jewels trading
e) Persons engaged in Real Estate business
f) Non Governmental Organizations /Non Profit Organizations/ Charities /Clubs and Associations/ Trusts / Foundations
g) Non face to face customers
h) Politically exposed persons
i) High Net worth individuals[1]
j) Existing customers if the accounts are active , yet the proper documentation of CDD is not with the bank
k) Customers where profile is not matching with transactions and CDD reviews has not been conducted
l) Customers in High Risk Jurisdictions
m) Correspondent Banking Relationships
n) Treasury Dealings customers
o) Trade Finance Business
p) Persons engaged in Wire Transfers

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

Enhanced Due Diligence for high risk customers shall include one or more of following methods

a) Gather sufficient information from public domain and/or through customer interviews
b) Establish source of funds and wealth with documentary evidence such as audited or management accounts of business , CRIB reports
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

- 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.

Annexure IV

Bank's Sanction Program will consist of;

i. Financial Crime Management System (FCM)
ii. On line Licenses Manual Process

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

- **Through FCM system**

PART 1 - Transaction Alert Manager

1. The screening will be conducted on a real time basis for the
   i. New customer on boarding / Existing customer amendments
   ii. Inward and Outward Remittances
   iii. Inward and Outward RTGS
   iv. Trade Transactions (Import LC , Export LC, Import Collection Bills , Import Shipping Guaran tees , Export Collection Bills,Export LC Amendments , Import LC amendments)
   v. Local Drafts issuances and collections
   vi. Foreign Drafts issuances and collections (Foreign clearing & Local clearing)

2. Post Transaction monitoring will be conducted for the CEFTS, SLIPS and LMT transaction types.

PART 1 - CIF Alert Manager

Apart from that the Bank will be conducting a screening for the entire customer base (Existing Customers) on fortnightly basis and when the sanction lists are published. The newly on boarded customers will be screened against the configured sanctioned lists on an incremental basis too.

- **On line Licenses Manual Process**

ii. Remittance payments (Ex; Western Union, Lanka Money Transfer System (LMT))
iii. Correspondent Banks
iv. Products such as Exchange HouseRemittances, Lanka Money Transfer system
v. Service Providers, Agents, Outsourced Service Providers
vi. Major Shareholders
vii. Related Parties , Key Management Personnel, all other employee categories

Annexure V

Examples for suspicious transactions

- 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