POLICY & PROCEDURES

ON

ANTI MONEY LAUNDERING(AML) AND COMBATING OF FINANCING OF TERRORISM (CFT)

Responsible Officer
Compliance Officer

Approvals and Sign Off

Version	Change	Approved By	Date
1.0	Implemented	Board of Directors	22.11.2022
2.0	Policy for AML/CFT (reviewed)	Board of Directors	12.12.2023
3.0	Reviewed -AML/CFT Template	Board of Directors	18.11.2024
4.0	Reviewed	Board of Directors	28.04.2025

Contents

12.Introduction

The objective of KYC guidelines is to prevent institution from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. Apart from this, the institution realizes the need for a well-defined customer acceptance, customer care and customer severance policy to ensure prompt and inclusive services to all customers within the prescribed regulatory framework as well as defined processes of the institution. In this regard, Itis the paramount duty and responsibility of the institution to know and understand its customers fully in terms of identity and activity to the extent of establishing the correctness/genuineness of the credentials for extending better Customer Service.

This exercise also helps the institution to identify adverse conditions, if any, associated with the applicant/customer (at the time of establishing relationship) and guard against criminals/fraudsters making use of product channels/services for their nefarious activities. With the present-day multifarious dimensions of delivery of services and products, the need for a structured methodology for understanding customers at the time of establishing relationship has assumed a great importance.

Also, the intensity and extensiveness of the risk management function of the institution operates in compliance with the Risk Based Approach and proportionate to the nature, scale and complexity of the activities and money laundering and terrorist financing risk profile of the institution.

The Central Bank of Sri Lanka together with the Financial Intelligence Unit (FIU) have issued directives named Financial Institutions (Customer Due Diligence) Rules requiring financial institution to follow certain laid down procedures for opening accounts, maintenance of accounts and monitoring transactions of a suspicious nature.

This Anti Money Laundering (AML) and Combating of Financing of Terrorism (CFT) Policy is prepared based on the said rules issued by the Financial Intelligence Unit of Central Bank of Sri Lanka.

1. NATIONAL SAVINGS BANK -FUND MANAGEMENT DIVISION

POLICY ON ANTI MONEY LAUNDERING AND COMBATTING OF THE FINANCING OF TERRORISM

Financial Institutions have to take steps to combat the risks of money laundering and Terrorist Financing (ML & TF) in order to assist regulators in their fight against ML & TF.

It is the paramount duty and responsibility of the NSB Fund Management to know and understand its customers fully in terms of identity and activity to the extent of establishing the correctness/genuineness of the credentials for extending better Customer Service.

This exercise also helps the NSB Fund Management (NSBFMC) to identify adverse conditions, if any, associated with the applicant/customer (at the time of establishing relationship) and guard against criminals/fraudsters making use the channels/services for their nefarious activities. With the present-day multifarious dimensions of deliverance of services and products, the need for a structured methodology for understanding customers at the time of establishing relationship has assumed great importance.

The following steps taken at NSBFMC in this regard are

- Establishment of a Compliance Department under the Compliance Officer who is dedicated to the task of overseeing institution's policies, practices, and procedures regarding ML & TF.

- Use of independent compliance, audit, and risk management functions to help evaluate the NSBFMC compliance with applicable ML & TF laws, rules and regulations.

- The Institution relies on those closest to its customers - the Front Office to provide guidance and understand fully with whom we are doing business with – "Know Your Customer" (KYC) and to ensure that the business we conduct on behalf of our customers is proper.

- Development of internal procedures that assists the NSBFMC in monitoring transactions for the purpose of identifying possible suspicious activities.

- Recognizes and is aware that preventing ML & TF and adhering to KYC principles is an ongoing process that involves constant diligence and the difficulties faced when the NSBF tries to keep pace with the ever more sophisticated schemes employed by criminals.

- Continue to update its policies and procedures that meet or exceed applicable norms in the industry both locally and globally.

In line with the directives received, a policy document with the following sections covering various functional aspects of KYC norms and AML measures is set out herein.

a) What is Money Laundering and Terrorist Financing

b) The Sri Lankan Legislation

c) Know Your Customer (KYC) and Customer Due Diligence (CDD), based on the Financial Institutions (Customer Due Diligence) Rule No. 1 of 2016 issued by the Central Bank of Sri Lanka.

d) Applicability of the Directive at NSB Fund Management

e) Identifying and reporting Suspicious Transactions

f) Risk Management and Monitoring Controls

g) Beneficial Owners

h) Politically Exposed Persons

A. What is Money Laundering?

Definition of "Money Laundering"

Various definitions are given to the term "Money Laundering". Set out below are two of the most used ones.

Definition 1 "The process of converting cash or other property which is derived from criminal activity so as to give it the appearance of having been obtained from a legitimate source"

Definition 2 "The process by which criminals seek to disguise the illicit nature of their proceeds by introducing them into the stream of legitimate commerce and finance

B) The Process of Money Laundering

In the process of Money Laundering, there are, theoretically four factors that are common to Money Laundering operations.

a) The real source of criminal money must be concealed and will not be done with public knowledge.
b) The form in which money is held must be changed in order to hide identity.
c) The trail of transaction must be obscured to defeat any attempted follow-up by law enforcement agencies.
d) The launderer must maintain constant control on the monies as he cannot legally declare any theft of such money.

C. Stages of Money Laundering

- **Stage 1- Placement**

Placement means the consolidation and placement of different proceeds of criminal money in the financial system through different sources or smuggling them out of the country. The objective of the launderer is to remove the proceeds of the illegal transaction to another location without detection and to transform them into transferable assets.

- **Stage 2 - Layering**

The Launderer by moving the money through many accounts, through different countries and through dummy companies creates complex layers of transactions to disguise the trail and provide anonymity. This process will distance his deeds from his gains and obliterate the path of movement of funds.

- **Stage 3 - Integration**

Once the money has been cleaned through the first two processes, "washed" or "cleaned" funds are brought back into circulation.

D. What is Terrorist Financing?

The United Nations International Convention for Suppression of Terrorist Financing defines Terrorist Financing in under mentioned manner in its article-2 and also the recommendation of the Financial Action Task Force (FATF) gives the same definition. Most countries including Sri Lanka use this definition.

Article 2

1. Any person commits an offence within the meaning of the Convention if that person by any means, directly or indirectly, unlawfully and willfully provides or collects funds or property with the intention that such funds or property should be used or in the knowledge that they are to be used or having reason to believe that they are likely to be used, in full or in part, in order to commit:

a) an act which constitutes an offence within the scope of or within the definition of any one of the Treaties listed in the Convention on the Suppression of Terrorist Financing Act; or

b) any other act intended 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 or otherwise and 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; or

c) Any terrorist act.

02. LEGAL FRAMEWORK FOR ANTI MONEY LAUNDERING (AML) / COMBATING OF FINANCING OF TERRORISM (CFT) INSRI LANKA

For several years government authorities, the Central Bank, the Financial Sector Authorities, Legal and Law Enforcement Authorities, have worked together with international experts to formulate the necessary AML/CFT legal framework for Sri Lanka. The Central Bank played a major role in these deliberations not only because it is the institution at the helm of the financial sector, but also because one of its core objectives is the preservation of financial system stability which could be threatened by Money Laundering activities. The first piece of legislation, the Convention on the Suppression of Terrorist Financing Act, No.25 of 2005 became law on 8th August 2005.The other two laws, the Prevention of Money Laundering Act No.5 of 2006 and the Financial Transactions Reporting Act. No.6 of 2006 became law on 6th March 2006. All three Acts were prepared in line with the 40 Recommendations for Prevention of Money Laundering and 9 Special Recommendations for combating the financing of terrorism provided in the Financial Action Task Force (FATF), and therefore Sri Lanka is compliant with the requirements of the FATF. Convention on the Suppression of Terrorist Financing Act, No.25 of 2005 was amended in 2011 by Convention on the Suppression of Terrorist Financing (Amendment) Act, No.41 of 2011 and Convention on the Suppression of Terrorist Financing (Amendment) Act, No.03 of 2013 while Prevention of Money Laundering Act No.5 of 2006 was amended by Prevention of Money Laundering (Amendment) Act No.40 of 2011. Some of the main features of these three Acts are given below.

A) PREVENTION OF MONEY LAUNDERING ACT (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".

- ✓ Any movable or immovable property acquired by a person which cannot be part of the known income or receipts of a person or money/ property to which his known

income and receipts have been converted, is deemed to have been derived directly or indirectly from unlawful activity, in terms of the PMLA.

- ✓ PMLA has provisions for a police officer not below the rank of Assistant Superintendent of Police to issue an order prohibiting any transaction in relation to any account, property or investment which may have been used or which may be used in connection with the offence of Money Laundering for a specific period which may be extended by the High Court, if necessary, in order to prevent further acts being committed in relation to the offence.

- ✓ Under PMLA the following may commit the offence of Money Laundering-

- ✓ Persons who commit or have been concerned in the commission of predicate offences, and thereby come into possession or control of property derived directly or indirectly from the commission of such predicate offences

- ✓ People who receive possess or come into control of property derived directly or indirectly from the commission of predicate offences, knowing or having reason to believe the true nature of such property (to this group belong persons employed at Financial Institutions which are used by criminals to launder ill gotten money.

The following are considered as Predicate Offences

- ✓ Offences under- - The Poisons, Opium, and dangerous Drugs Ordinance
- ✓ Laws or Regulations relating to the prevention and suppression of terrorism
- ✓ The Bribery Act - Firearms Ordinance, Explosives Ordinance, Offensive Weapons Act etc.
- ✓ Laws relating to cyber crimes
- ✓ Laws relating to offences against children
- ✓ Laws relating to offences against trafficking of people

- ✓ Any law punishable with death or imprisonment of seven years or more, whether committed within or outside Sri Lanka.

In terms of the PMLA Money Laundering is liable to a penalty of not less than the value of the property involved in the offence and not more than thrice this value and a term of **imprisonment of not less than 5 years and not more than 20 years or both to such fine and imprisonment.**

- Property derived from an offence of Money Laundering is forfeited to the State free of encumbrances in terms of the PMLA.

- PMLA makes "tipping-off" (pre warning suspects of impending action against them) an offence.

- The extradition law applies to the offence of Money Laundering.

B) FINANCIAL TRANSACTIONS REPORTING ACT NO.6 OF 2006 (FTRA)

- ✓ FTRA provides for the setting up of a Financial Intelligence Unit (FIU) as a national central agency to receive analyses and disseminate information relating to Money Laundering and Financing of Terrorism.

- ✓ FTRA obliges institutions, to report to the FIU Cash Transactions and Electronic Fund Transfers above a value prescribed by an Order published in the Gazette. The term "Institutions" covers a wide array of people and entities. Currently this amount **is Rupees One Million (Rs. 1,000,000/-) or its equivalent.**

- ✓ All suspicious transactions must be reported by institutions to the FIU irrespective of their magnitude.

- ✓ FTRA requires an institution covered by the Act to appoint a Senior Officer as the Compliance Officer who would be responsible for the institution's compliance with the Act.

- ✓ The FTRA also requires Supervisory Authorities of Institutions and Auditors to make a Suspicious Transaction Report if they have information which gives them reasonable grounds to suspect that a transaction is related to money laundering or financing of terrorism

- ✓ Supervisory Authorities are required by the FTRA to examine whether institutions supervised by them comply with the provisions of the FTRA and to report instances of non-compliance to the FIU. Further, they are also required to co-operate with law enforcement agencies and the FIU in any investigation, prosecution or proceeding relating to any act constituting unlawful activity.

- ✓ In terms of the FTRA, institutions are required to engage in Customer Due Diligence (verifying the identity of customers) with whom they undertake transactions and ongoing Customer Due Diligence with customers with whom they have a business relationship.

- ✓ The opening and operating of numbered accounts and accounts under a fictitious name are an offence under the FTRA.

- ✓ FTRA makes "tipping-off" an offence (e.g. pre-warning a suspect of an impending investigation).

- ✓ In terms of the FTRA, people making reports under the Act are protected from civil or criminal liability.

- ✓ The FIU with Ministerial approval may exchange information with other FIUs or Supervisory Authorities of a Foreign State.

C. CONVENTION ON THE SUPPRESSION OFTERRORIST FINANCING ACT NO.25 OF 2005 AS AMENDED BY ACT NO. 41 OF 2011

On 10th January 2000, Sri Lanka became a signatory to the International Convention for the Suppression of Terrorist Financing adopted by the United Nations General Assembly on 10/01/2000 and ratified the same on 8/9/2000. The Convention on the Suppression of Terrorist Financing Act No.25 of 2005 was enacted to give effect to Sri Lanka's obligations under this Convention and further amended under Act No. 41 0f 2011 and Act No. 3 of 2013.

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

- The penalty for an offence under the Act is a term of imprisonment between 15-20 years and/ or a fine.

- On indictment of a person for an offence under the Act, all funds collected in contravention of the Act will be frozen (if lying in a bank account) or seized (if held in the control of any person or institution other than a bank).

- On the conviction of a person for an offence under the Act, all funds collected in contravention of the Act are forfeited to the State.

- The extradition law applies to the offence of financing of terrorism

3. FINANCIAL INTELLIGENCE UNIT RULE NO.1 OF 2016 – FINANCIAL INSTITUTIONS (CUSTOMER DUE DILIGENCE) RULES

Introduction Public confidence in financial institutions, and hence their stability, is enhanced by sound financial practices that reduce financial risks to their operations. Money laundering and terrorist financing can harm the soundness of a country's financial system, as well as the stability of individual financial institutions, in multiple ways. Customer identification and due diligence procedures also known as "Know Your Customer" (KYC) rules, are part of an effective Anti-Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) regime. These rules are not only consistent with, but also enhance the safe and sound operations and other types of financial institutions. While preparing operational guidelines on customer identification and due diligence procedures, financial institutions are advised to treat the information collected from the customer for the purpose of opening of accounts, as confidential and not divulge any details thereof for cross-selling or for any other purpose, and that the information sought is relevant to the perceived risk, is not intrusive and is in conformity with the rules issued hereunder. These rules are issued under Section 2 of the Financial Transactions Reporting Act No.6 of 2006 and any contravention of, or non-compliance with the same will be liable to the penalties under the relevant provisions of the Act.

A. Provisions on Money Laundering and Terrorist Financing Risk Management Rules

As required by the above rules the institution shall

- ✓ **Conduct following processes in assessing money laundering and terrorist financing risks**:

- Documenting the risk assessments and findings

- Considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied

- Keeping the assessment up to date through a periodic review and

- Having appropriate mechanisms to provide risk assessment information to the supervisory authority.

✓ **Have proper risk control and mitigation measures including**

- Internal policies, controls, and procedures to manage and mitigate money laundering and terrorist financing risks that have been identified.

- Management Information systems that provide reliable data on the quantity and nature of Money Laundering/ Terrorist Financing risks and effectiveness with which risks are being mitigated.

- Monitor the implementation of those policies, controls, procedures and enhance them if necessary and

- Take appropriate measures to manage and mitigate the risks, based on the risk-based approach.

✓ **Conduct risk profiling on the customers considering**

- Risk level according to customer category (resident or non- resident, occasional or one off, legal persons, politically exposed persons and customers engaged in different types of occupations)
- Geographical location of business or country of origin of the customer

- Products, services, transactions or delivery channels of the customer (cash based, face to face or not face to face, cross- border) and

- Any other information regarding the customer.

- ✓ The risk control and mitigation measures implemented shall be commensurate with the risk level of a particular customer as identified based on risk profiling.

- ✓ After the initial acceptance of a customer, the institution shall regularly review and update the risk profile of the customer based on his level of money laundering and terrorist financing risk.

- ✓ The money laundering and terrorist financing risk management of the NSBFMC shall be affiliated and integrated with the overall risk management.

- ✓ Provide a report of its risk assessment, money laundering and terrorist financing risk profile and the effectiveness of its risk control and mitigation measures to the **Board of Directors on monthly basis**. This report shall include

- Results of monitoring activities carried out for combating money laundering or terrorist financing risks.

- Details of recent significant risks involved either internally or externally and its potential impact to the Institution.

- Recent developments in written laws on money laundering and suppression of terrorist financing and its implications for the Institution.

CDD for All Customers

- ✓ The Institution shall not open, operate or maintain any anonymous account, any account in a false name or in the name of a fictitious person or any account that is identified by a number only (hereinafter referred to as numbered accounts)

Numbered accounts include accounts where the ownership is transferable without the knowledge of the institution and accounts that are operated and maintained with the account holder's name only

- ✓ The Institution shall maintain accounts in such a manner that the assets and liabilities of a given customer can be readily retrieved. Accordingly, the Institution shall not maintain accounts separately from the usual operational process, systems or procedures.

- ✓ Conduct the CDD measures specified in Rule No. 1 of 2016, on customers conducting transactions when

a. Entering business relationships

b. Providing wire transfer services

c. The Institution has any suspicion that such customer is involved in money laundering or terrorist financing activities, regardless of amount

e. The Institution has no doubt about the veracity or adequacy of previously obtained information.

1. The Institution shall-

a. Identify its customers prior to entering business relationships

b. Obtain the information specified in Rule No. 1 of 2016, verify such information, as applicable and record same for the purpose of identifying and initial risk profiling of customers, at the minimum.

c. Obtain the following information for the purpose of conducting CDD, at minimum:

i. Purpose of the account

ii. Sources of earning

iii. Expected monthly turnover

iv. Expected mode of transactions

v. Expected type of counterparties (if applicable)

2. If any customer is rated as a customer posing a high risk, the Institution shall take enhanced CDD measures for such customers, in addition to the CDD measures stated above

- If the customer is not a natural person, take reasonable measures to understand the ownership and control structure of the customer and determine the natural persons who ultimately own or control the customer.

- If one or more natural persons are acting on behalf of a customer, the Institution shall identify the natural persons who act on behalf of the customer and verify the identity of such people. The authority of such person to act on behalf of the customer shall be verified through documentary evidence including specimen signatures of the persons so authorized.

- If there is a beneficial owner, the Institution shall obtain information to identify and take reasonable measures to verify the identity of the beneficial owner of the customer using relevant information or data obtained from a reliable source,

adequate for the Institution to satisfy itself that the institution knows who the beneficial owner is.

- The Institution shall verify the identity of the customer and beneficial owner before or during entering a business relationship with or conducting a transaction for an occasional customer.

- Provided however, where the risk level of the customer is low as per the risk profile and verification is not possible at the point of entering into the business relationship, the Institution may, subject to the below provision, allow its customer and beneficial owner to furnish the relevant documents after entering into the business relationship and subsequently complete the verification (this shall be called as "delayed verification")

- In any case where the delayed verification is allowed the following conditions shall be satisfied:

a. Verification shall be completed as soon as it is reasonably practicable but not later than 14 working days from the date of opening the account

b. The delay should be essential so as not to interrupt the normal conduct of business of the Institution and

c. No suspicion of money laundering or terrorist financing risk shall be involved

- ✓ To mitigate the risk of delayed verification, the Institution shall adopt risk management procedures relating to the condition under which the customer may utilize the business relationship prior to verification.

- ✓ The Institution shall take measures to manage the risk of delayed verification which may include limiting the number, type and amount of transactions that can be performed, as stated in this Policy.

- ✓ If the Institution is unable to act in compliance with the above, it shall

a. In relation to a new customer, not open the account or enter the business relationship or perform the transaction; or

b. In relation to an existing customer, terminate the business relationship with such customer and consider filing a suspicious transaction report in relation to the customer.

- ✓ The Institution shall not, under any circumstances, establish a business relationship or conduct any transaction with a customer with high money laundering and terrorist financing risk, prior to verifying the identity of the customer and beneficial owner.

- ✓ The Institution shall monitor all business relationships with a customer on an ongoing basis to ensure that the transactions are consistent with the economic profile, risk profile and where appropriate the sources of earning of the customer.

- ✓ The institution shall obtain information and examine the background and purpose of all complex, unusually large transactions and all unusual patterns of transactions, which have no apparent economic or prima facie lawful purpose.

- ✓ The background and purpose of such transactions shall be inquired into, and findings shall be kept in record with a view to making such information available to the relevant competent authority when required and to make suspicious transaction reports.
- ✓ The NSBFMC shall report transactions inconsistent with the rules stated in Rule No 1 of 2016 to the Compliance Officer for appropriate action.

- ✓ The Institution shall periodically review the adequacy of customer information obtained in respect of customers and beneficial owners and ensure that the information is kept up to date, particularly for higher risk categories of customers.

The review period and procedure shall be decided by the institution from time to time as appropriate and shall be decided on a risk-based approach.

- ✓ The frequency of the ongoing CDD or enhanced ongoing CDD shall be commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profiles and nature of transactions.
- ✓ Increase the number and timing of controls applied and select patterns of transactions that need further examination when conducting enhanced CDD.

- ✓ Perform such CDD measures as may be appropriate to the existing customers based on its own assessment of materiality and risk but without compromise on the identity and verification requirements. In assessing the materiality and risk of an existing customer, the Institution may consider the following-

a. The nature and circumstances surrounding the transaction including the significance of transaction.

b. Any material changes in the way the account or business relationship is operated or

c. The insufficiency of information held on the customer or change in the information of the customer.

- ✓ NSBFMC shall conduct CDD on existing customer relationships ongoing considering whether and when CDD measures have previously been conducted and the adequacy of data obtained.

- ✓ If an existing customer provides unsatisfactory information relating to CDD, the relationship with such customer shall be treated as a relationship posing a high risk and be subjected to enhanced CDD measures.

- ✓ If the NSBFMC forms a suspicion of money laundering or terrorist financing risk relating to a customer and it reasonably believes that conducting the process of CDD measures would tip off the customer, the Institution shall terminate conducting the CDD measures and proceed with the transaction and immediately file a suspicion transactions report.

CDD for Legal Persons and Legal Arrangements

The Institution shall in the case of a customer that is a legal person or legal arrangement.

a. Understand the nature of the business of the customer, its ownership and control structure

b. Identify and verify the customer in terms of the requirements set out below.

- ➢ To identify the natural person if any, who ultimately has control ownership interest in a legal person, the Institution shall at the minimum obtain and take reasonable measures to verify the following-

a. Identity of all Directors and Shareholders with equity interest of more than 10% with the requirement imposed on the legal person to inform of any change in such Directors and Shareholders.

b. If there is a doubt as to whether the person with the controlling ownership, interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person, if any, exercising control of the legal person or arrangement through independent sources.

c. Authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise.

d. Where no natural person is identified under the preceding provisions, the identity of the relevant natural persons who hold the positions of senior management.

e. When a legal person's controlling interest is vested with another legal person, the Institution shall identify the natural person who controls the legal person.

To identify the beneficial owners of a legal arrangement, obtain and take reasonable measures to verify the following-

a) For Trusts, the identities of the author of the Trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the Trust (including those who control through the chain of control or ownership); or

b) For other types of legal arrangements, the identities of people in equivalent or similar positions.

Non -Government Organization Not for Profit Organizations or Charities

The NSBFMC shall conduct enhanced CDD measures when entering a relationship with a Non-Governmental Organization (NGO) or a Non-Profit Organization (NPO) and Charities to ensure that their accounts are used for legitimate purposes and the transactions are commensurate with the declared objectives and purposes.

1. NSBFMC shall open accounts in the name of the relevant NGO, NPO or Charity as per title given in the constituent document thereof.

2. The individuals who are authorized to operate the account and members of their governing bodies shall also be subject to enhanced CDD measures.

3. NSBFMC shall ensure that the persons stated in (2) above are not affiliated with any entity or person designated as a prescribed entity or person, whether under the same name or a different name.

NSBFMC shall not allow personal accounts of the members of the governing bodies of an NGO, NPO or Charity to be used for charity purposes or collection of donations.

1. The Institution shall review and monitor all existing relationships of an NGO, NPO or Charity to ensure that those organizations, their authorized signatories, members of their governing bodies and the beneficial owners are not linked with any entity or person designated as a prescribed entity or person, either under the same name or a different name.

2. In case of any suspicion on similarity in names, the institution shall file a Suspicious Transaction Report or take other legal action or take both steps.

Customers and Financial Institutions from High-Risk Countries

1. The institution shall apply enhanced CDD measures to business relationships and transactions to customers and Financial Institutions from high-risk countries

2. The Secretary to the Ministry of the Minister to whom the subject of Foreign Affairs has been assigned or the subject of Defense has been assigned shall specify the high-risk countries

i. based on the Financial Action Task Force listing; or

II. independently considering, the existence of strategic deficiencies in anti-money laundering and combating of financing of terrorism policies and not making sufficient progress in addressing those deficiencies in those countries.

III. The type of enhanced measures applied under (i) above shall be effective and correspond to the nature of risk.

➢ In addition to enhanced CDD measures, the institution shall apply appropriate counter measures, such as follows, for countries specified in the list of high-risk countries referred to in (ii) above, corresponding to the nature of risk of listed high-risk countries.

Limiting business relationships or financial transactions with identified countries or persons located in the country concerned.

b. Review and amend or, if necessary, terminate, correspondent banking relationships with Financial Institutions in the country concerned.

c. Conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the Financial Institution or financial group, located in the country concerned; and

d. Conduct any other measures as may be specified by the Financial Intelligence Unit.

Intermediary Financial Institution

The institution when involved in wire transfers as an Intermediary Financial Institution shall ensure that for cross-border wire transfers, all originator and beneficiary information that accompanies a wire transfer is retained with the wire transfer message.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross- border wire transfer from remaining with a related domestic wire **transfer, the institution shall keep a record, for at least six years, of all the information received from the ordering Financial Institution or another** Intermediary Financial Institution.

The institution shall take reasonable measures, which are consistent with straight- through processing to identify cross-border wire transfers that lack the required originator information or required beneficiary information.

The institution shall have risk-based internal policies and procedures for determining-

(a) when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and
(b) What is the appropriate follow up action?

Beneficiary Financial Institution

¬ The institution shall take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

¬ For cross-border wire transfers of rupees one hundred thousand or above or its equivalent in any foreign currency, the institution shall verify the identity of the beneficiary and maintain the information in accordance with the Act if the identity has not been previously verified.

¬ The institution shall have risk-based internal policies and procedures for determining

(a) when to execute, reject or suspend a wire transfer with insufficient, originator or beneficiary information

(b) what is the appropriate follow up action

1. **Individual Customer**

(a) The following information shall be obtained:

(a1) In the case of all customers

- Full name appearing in the identification document.
- Official personal identification or any other identification document that bears a photograph of the customer (ex: National Identity Card, valid Passport, or valid driving license)

Permanent address appearing on the identification document. If residential address differs from the permanent address residential address shall be supported by a utility bill not over three months old or any other reliable proof of residence. Utility bills are to be specified as electricity bill, water bill and fixed line telephone operator's bill. **No post box number shall be accepted except for state owned enterprises. In the case of "C/O",** property owner's consent and other relevant address verification documents are required to be obtained.

- Telephone number, fax number, and e-mail address
- Date of birth
- Nationality

- Occupation, business, public position held, and the name of employer and geographical areas involved
- Purpose of which the account is opened
- Expected turnover/ volume of business
- Expected mode of transactions
- Satisfactory reference as applicable

Documents required for Account opening – Individual Clients

Individual Registration

Application for Real Time SMS/Email Notification

Indemnity for Email/Fax – Individual clients

Standard Services Agreement (SSA)

Master Repurchase Agreement (MRA)

Customer Agreement of Government Securities (CAGS)

Documents Required for Corporate Client Registration

Account Opening – Corporate Clients

Annexure – Corporate Registration

Indemnity for Email/Fax – Corporate Clients

Application for Real Time SMS/Email Notification

Standard Services Agreement (SSA)

Master Repurchase Agreement (MRA)

Customer Agreement of Government Securities (CAGS)

Certified Copy of Name Change Certificate (if applicable)

Board Resolution

DOCUMENTS TO BE SUBMITTED For Account Opening

- Certified copy of Certificate of Incorporation
- Up-to-date certified copy of Memorandum & Articles of Association
- Duly certified true copy of the Board resolution certifying that it is duly adopted at a duly constituted meeting of the Directors of the Company
- The Board Resolution should include the following information:
    1. Board of Director's authorization to open an account with NSBFMC.
    2. Authorized signatory list for operating instructions etc.

Proprietorship/ Partnership Accounts.

(a) The following information shall be obtained

- Full names of the partners or proprietors as appearing in the business registration document
- Nature of the business
- Registered address or the principal place of business
- Identification details of the proprietor/ partners as in the case of individual accounts
- Contact telephone or fax number
- Income Tax file number
- The extent of ownership controls
- Other connected business interests

(b) The following documents shall be obtained (each copy shall be verified against the original)

- Copy of the business registration document
- Proprietors' information/ Partnership Deed
- Copy of identification and address verification documents.

Corporation/ Limited Liability Company

(a) The following information shall be obtained

• Registered name and the Business Registration Number of the institution.
• Nature and purpose of business.
• Registered address of principal place of business.
• Mailing address, if any.
• Telephone/ Fax/ email.
• Income Tax file number.
• Bank references (if applicable)
• Identification of all Directors as in the case of individual customers.
• List of major shareholders with equity interest of more than ten percent.
• List of subsidiaries and affiliates.
• Details and the names of the signatories**.**

In the case of companies listed on the Stock Exchange of Sri Lanka licensed under the Securities and Exchange commission of Sri Lanka Act No. 36 of 1987 or any other stock exchange subject to disclosure requirements ensuring adequate transparency of the beneficial ownership, the Bank may use the information available from reliable sources to identify the Directors and major shareholders.

(b) The following documents shall be obtained (each copy shall be verified against the original)

• Copy of the Certificate of Incorporation.

• Copy of Form 40 (Registration of an existing company) or Form 1 (Registration of a company) under the Companies Act and Articles of Association.

• Board Resolution authorizing the opening of the account.

• Copy of form 20 (change of Directors/ Secretary and particulars of Directors/ Secretary) under the Companies Act.

Copy of form 13 – changing of Registered address

• Copy of form 44 (full address of the registered or principal office of a company incorporated outside Sri Lanka and its principal place of business established in Sri Lanka) under the Companies Act.

• Copy of Form 45 List and particulars of directors of a company incorporated outside Sri Lanka with a place of business established in Sri Lanka) under the Companies Act.

• Copy of the Board of Investment Agreement if a Board of Investment approved company.

• Copy of the export Development Board (EDB) approved letter, if EDB approved company.

• Copy of the certificate to commence business, if a public quoted company.

• Name of the person or persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board resolution.

• Latest audited accounts if available.

The above documents shall apply to a company registered abroad as well. The non-documentary method in the absence of the above documents would entail a search at the Credit Information Bureau (CRIB), bank references, site visits and visiting the business website of the customer.

Clubs, Societies, Charities, Associations and Non-Governmental Organization

Clubs, Societies, Charities, Associations and Non-Governmental Organization

(a) **The following information shall be obtained**

• Registered name and the registration number of the institution.
Registered addresses appearing in the Charter, Constitution etc.
• Identification of at least two office bearers, signatories, administrators' members of the governing body or committee or any other person who has control and influence over the operations of the entity as in the case of individual accounts
• Committee or Board Resolution authorizing the account opening.
• The source and level of income funding.
• Other connected institutions/ associates/ organizations.
• Telephone/ facsimile number/ email address

(b) **The following documents shall be obtained and verified against the original**
• Copy of the registration document/ Constitution/ Charter etc.
• Board Resolution authorizing the account opening.
• Names of the persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board/ Committee Resolution

➢ Accounts for charitable and aid organizations and Non-Government Organizations (NGO)s should be opened only with the registration of the regulatory authority empowered to regulate charitable and aid organizations, non-governmental organizations and non-profit organizations.

for the time being and with other appropriate credentials. Due regard should be paid to specific directions governing their operations i.e. issued by the Department of Bank Supervision and Department of Supervision of Non-Bank Financial Institutions of the Central Bank and the Director- Department of Foreign Exchange

Trusts Nominees and Fiduciary Accounts

(a) The following information shall be obtained

• Identification of all trustees, settlers, grantors and beneficiaries in case of trust as in the case of individual accounts.
• Whether the customer is acting as a 'front' or acting as a trustee, nominee or other intermediary.

(b) The following documents shall be obtained and verified against the original
• Copy of the Trust Deed as applicable.
• Particulars of all individuals.

Stocks and Securities Sector specific requirements

The following information shall be obtained from the Funds approved by the Securities and Exchange Commission of Sri Lanka

• Name of the Fund.
• Purpose of the fund.
• Place of establishment of the Fund.
• Details (name, address, description etc.) of the Trustee/ Manger of the Fund.
• If the Trustee/ manager is a company, date of incorporation, place of incorporation, registered address of such trustee/ Manager.
• Copies of the document relating to the establishment and management of the fund. (ex: prospectus, Trust Deed, Management Agreement, Bankers Agreement, Auditors agreement);
• Copy of the letter of approval of the fund issued by the supervisory authority of the relevant country.
• Copy/ copies of the relevant Custody/ Agreement.
• Details of beneficiaries.

(b) Certification requirement All supporting documents to be submitted to Central Depository System shall be certified, attested or authenticated by the person specified in (A) or (B) below for the purpose of validating the applicant

(A) For non-resident applicants-

• By the Company Registrar or similar authority.

• By a Sri Lankan Diplomatic Officer or Sri Lankan Consular Officer in the country where the documents were originally issued.

• By a Solicitor, an Attorney-at-Law, a Notary Public practicing in the country where the applicant resides.

• By the Custodian Bank.

• By the Global Custodian (the Custodian Bank shall certify the authenticity of the signature of the Global Guardian) or

• By a Broker.

(**B) For resident applicants**-

• By the Registrar of Companies or the Company Secretary (applicable in respect of corporate bodies);

• By an Attorney-at- Law or a Notary Public.

• By a Broker; or

• By the Custodian Bank.

The person certifying shall place the signature, full name, address, contact telephone number and the official seal (Not applicable for Brokers, Custodian Banks and Global Custodians) Where the application is titled in the name of the 'Registered Holder/ Global Custodian/ Beneficiary' and forwarded through a Custodian Bank, a copy of the SWIFT message or similar document issued by the Global Custodian instructing the local Custodian bank to open the account on behalf of the Beneficiary company shall be submitted together with a Declaration from the Global Custodian that a custody.

The examples quoted above are not the only possibilities. In particular jurisdictions there may be other documents of an equivalent nature which may be produced as satisfactory

evidence of customers' identity. The Bank should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interviews.

Non-Face to Face

In pursuant with section 15(1) of the Financial Transactions Reporting Act No. 6 of 2006, the Financial Intelligence Unit of Central Bank of Sri Lanka has issued Guideline No. 3 of 2020 on Non-Face to Face Customer Identification and Verification. In compliance with these Guidelines which must be read with Financial Transactions Reporting Act No. 6 of 2006 and Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 which are detailed above, the institution has adopted following process to open accounts of non-face to face customers.

1. The institution shall act in compliance with the requirements stated in Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 and shall follow the alternate methods introduced by Guideline No. 3 of 2020 to verify the identity document and the address.

2. The institution shall follow safe and trustworthy methods to obtain identification information such as

- electronic forms,
- mobile app,
- video conferencing,
- secure email,
- registered post etc.

and shall not use agents, third party service providers acting as agents, third party financial institutions, designated non finance businesses to collect identification information. Also, steps should be taken by the institution to obtain high quality still images of the customer, ID documents and address verification documents.

3. Also, steps shall be taken to obtain the quality images of passport.

4. The electronic interface provided by the Department of Registration of Persons shall be used by the institution to independently verify the identity of the customer.

5. Verify and authenticate the identity of the customer through the link provided by the Department of Registration of Persons and video calls before entering a relationship with a customer non-face to face.

6. When the identity cannot be verified or authenticated the institution shall not enter a business relationship with a customer or process transactions on behalf of a customer.

7. Address of the customer shall be verified through the information available in the customer's identity obtained through the electronic interface of the Department of Registration of Persons.

8. At instances where the address differs from the information obtained through the electronic interface provided by Department of Registration of Persons, follow the guidelines give in the Financial Institutions (Customer Due Diligence) Rules in verifying the address of the customer.

9. The institution shall not open accounts or establish relationships with customers non face to face,

a. When the customer uses any other identification document other than National Identity Card.

b. When high quality interactive real time video of the customer cannot be obtained.

c. When high quality data and still images of the customer identity document cannot be obtained.

d. When identity documents appear damaged or degraded to the point, they are no longer fit for the purpose of identification;

e. When identity documents appear altered, security features cannot be validated, or the integrity of the document is suspected.

f. When the customer refuses or is unable to comply with the established procedure of the institution.

g. At instances where the institution is not able to fully execute the established procedure due to a system failure.

h. When the electronic interface of the Department of Registration of Persons does not show the existence of the National Identity Card.

i. When the details of customer identity do not match with the details obtained through the electronic interface of the Department of Registration of Persons.

j. When the photograph of the National Identity Card produced by the customer does not match with the imagery obtained from the Department of Registration of Persons.

k. When the customer appears to have intentionally modified his appearance to disable the institution to identify and verify the customer to fully complete the established-on boarding procedure.

10. Risk categorization of the customer identified as non-face to face subject to enhanced due diligence till the customers are able to present their original identifications to the institution to enable the institution to verify and make a copy thereof.

11. The risk status of the customers shall be maintained taking into consideration the risk of the jurisdiction where the customer resides.

12. The institution shall take steps to file a Suspicious Transaction Report with the Financial Intelligence Unit at instances such as impersonation, forwarding forged documents, forged, or altered National Identity Cards or address verification documents,

altered images, spoofing, reluctance to corporate or provide additional information for verification, discrepancies in information provided or when suspicious behaviors are noted.

Foreign Investors and Non-Resident Sri Lankans

Guidelines Procedures to Participating Agents on the purchase and sale of Treasury bills and Treasury bonds issued by the Government of Sri Lanka to foreign investors and non-resident Sri Lankans

1. General

1.1. Eligible Investors

Persons who are eligible to maintain INWARD INVESTMENT ACCOUNT (IIA) in terms of Foreign Exchange (Opening and Maintenance of Accounts for the purpose of engaging in Capital Transactions) Regulations No. 2 of 2017 or any subsequent amendment thereto are eligible to invest in Treasury bills or Treasury bonds.

Only the following categories of investors are eligible to invest in Treasury bills and Treasury bonds issued by the Government of Sri Lanka under this category:

(a) A non- national resident in or outside Sri Lanka.

(b) A non-national of Sri Lankan origin, who is a resident outside Sri Lanka

(c) A Sri Lankan citizen, resident outside Sri Lanka.

(d) A Company incorporated outside Sri Lanka.

(e) Country and Regional Funds, Mutual Funds, Unit Trusts, and other Institutional investors who are established outside Sri Lanka.

(I) An administrator or executor of the estate of a deceased person, who maintained an Inward Investment Account with that authorized dealer until the completion of the administration of the deceased

person's estate.

(g) A receiver of liquidator of a Company that maintained an Inward Investment Account with that authorized dealer until proceedings are concluded.

(h) Any other person or category of person who may be authorized by the Central Bank from time to time.

All participating agents are required to adhere to the standard "Know Your Customer" (KYC) verification requirements when entertaining requests for investments.

1.2. Limit on Treasury bill and Treasury bond Investment

The total investment permitted to eligible investors in Treasury bills and Treasury bonds should not exceed the threshold limit approved by the Monetary Board of the Central Bank of Sri Lanka. (Subject to the Clause 2.3 below).

1.3. Tenure of Treasury bills and Treasury bonds

Foreign investors and non-resident Sri Lankans referred to in 1.1 above (hereinafter referred to as 'eligible investors') are permitted to purchase or sell Treasury bills and Treasury bonds with any maturity period.

1.4. Registration

Participating agents shall be responsible for registering details of their investors at the Central Depository System (CDS) maintained by the Public Debt Department (PDD) of the Central Bank of Sri Lanka (CBSL) in terms of the Lanka Settle System Rules.

CDS will inform the account holders in following instances.

(a) A monthly statement confirming the transactions that have taken place / recorded during the month.

(b) A semiannual statement of the outstanding balance of the account

(c) A monthly statement of maturity proceeds/interest payments made to the account. The statements will be addressed directly to the investor, as registered in the CDS.

2. Sales Procedure

Eligible investors are permitted to purchase or sell Treasury bills and Treasury bonds issued by the Government of Sri Lanka.

2.1. To affect the transactions in accordance with instructions received from the eligible investors, participating agents shall ensure that such transactions are within the legal requirements and do not breach the System Rules applicable to LankaSettle and any other guidelines issued by PDD and the Department of Foreign Exchange (DFE) of CBSL.

2.2. Foreign exchange brought into the country for the purchase of Treasury bills and Treasury bonds and proceeds realized on a sale/maturity of Treasury bills and Treasury bonds and coupon payments or any income realized by way of capital gain shall be routed through an IIA opened or already maintained with a Licensed Commercial Bank in the name of the eligible investor.

2.3. Before confirmation of the sale, participating agents shall be responsible for inquiring from PDD of CBSL the leeway available in the specified Treasury bill and Treasury bond limit permitted for eligible investors to invest in Treasury bills and Treasury bonds. PDD shall be informed by fax/e-mail once the deal is confirmed.

2.4. Participating agents shall be responsible for creating investor accounts promptly for their investors in the CDS and the transactions should be recorded according to the Lanka Settle System Rules.

3. Fund Transfers

When an eligible investor buys Treasury bills and Treasury bonds from the primary market, proceeds should be remitted from the HA of the eligible investors to the relevant Primary Dealer (PD) and PD should remit the proceeds of the Treasury bi1[s and Treasury bonds to CBSL's Real Time Gross Settlement System (RTGS) Account. When an eligible investor purchases/sells Treasury bills and Treasury bonds in the secondary market, the investor/participating agent shall arrange with the Licensed Commercial Bank (LCB) who maintains the IIA to transfer respective Rupee amounts to the relevant party on behalf of the investor.

4. Payment of Coupon and Maturity Proceeds

4.1. Maturity proceeds on Treasury bills and Treasury bonds, and coupon payments on Treasury bonds shall be payable in Rupees by the PDD of CBSL on behalf of the Government of Sri Lanka through RTGS to the respective participating agents on the respective dates. Such participating agents are responsible to transfer the respective payments to the IIA of account holders with proceeds value on the same day.

4.2. If the maturity date or the coupon payment date falls on a day which is not a business day for the banks in Sri Lanka, the payment of maturity proceeds shall be made on the business day prior to the due date in respect of a Treasury bill and the maturity proceeds and/or coupon payment shall be made on the business day after the due date in respect of a Treasury bond.

5. Repatriation

All proceeds received by sale or maturing of Treasury bills and Treasury bonds and coupon payments on Treasury bonds shall be fully repatriable.

6. **Joint Holdings**

Treasury bills and Treasury bonds may be held jointly by eligible investors. Payment of maturity proceeds and coupons shall be credited to IIA/IIAs of joint holders, based on the agreement between LCB which maintains the IIA and joint holders.

General Provisions

1. The institution is required to appoint a senior management level officer as the Compliance Officer, who shall be responsible for ensuring the institution's compliance with the requirements of the Act and the above-mentioned Rules.

2. Ensure that the Chief Compliance Officer or any other person authorized to assists him or act on behalf of him has prompt access to all customer records and other relevant information which may be required to discharge their functions.

3. Develop and implement a comprehensive employee due diligence and screening procedure to be carried out at the time **of appointing or hiring of all employees** whether permanent, contractual or outsourced. Hence. All employees details mentioned in the above categories to be forwarded to the Compliance Division for due diligence and screening procedures before appointing or hiring to the institution.

4. Frequently design and implement suitable training programmers for relevant employees including Board of Directors, to effectively implement the regulatory requirements and internal policies and procedures relating to money laundering and terrorist financing risk management.

5. Maintain an independent audit function in compliance with the Code of Corporate Governance issued by the Central Bank of Sri Lanka that is adequately resourced and able to regularly assess the effectiveness of the internal policies procedures and controls and its compliance with regulatory requirements.

6. The institution shall identify and assess money laundering and terrorist financing risks that may arise in relation to the development of new products and new business practices including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

7. The institution shall
   - Undertake the risk assessments prior to the launch or use of new products and technologies

   - Take appropriate measures to manage and mitigate the risks which may arise in relation to the development of new products and new business practices

C. Record Keeping

8. a) Records of transactions and of correspondence relating to transactions and records of all reports furnished to the Financial Intelligence Unit for a **period of six years** from the date of the transaction, correspondence or the furnishing of the report, as the case may be; and.

   c) records of identity obtained in terms of section 2 for a period of six years from the date of closure of the account or cessation of the business relationship, as the case may be
   d) unless directions have been issued by the Financial Intelligence Unit that such records or correspondence should be retained for a longer period, in which case the records or correspondence should be retained for such longer period.

10. The records shall be sufficient to permit the reconstruction of individual transactions including the nature and date of the transactions, the type and amount of currency involved and the type and identifying number of any account involved in the transactions to be produced in a court of law, when necessary, as evidence. The transaction records may be maintained in document form, by electronic means, on microfilm or in any other form that may be admissible as evidence in a court of law.

11. The records of identification data obtained through CDD processes such as copies of identification documents, account opening forms, know your customer related documents, verification documents and other documents along with records of account files and business correspondence, shall be maintained for a minimum period of **six years commencing from the date o**n which the business relationship was fulfilled, or the occasional transaction was affected.

12. The records shall be maintained up to date and kept in original or copies with the attestation of the institution.

13. The institution shall retain the above records for a longer period if transactions, customers, or accounts are involved in litigation or required to be produced by a court of law or before any other appropriate authority.

14. The institution should ensure that all CDD information and transaction records are available immediately to relevant domestic authority and Financial Intelligence Unit.

For this rule relevant domestic authority means-

a. Any public authority (including a supervisory authority established as independent non-governmental authority with statutory powers) with designated responsibilities for prevention of money laundering and suppression of terrorist financing.

b. Any authority that performs the function of investigating and prosecuting money laundering and terrorist financing associated offences and seizing or freezing and confiscating assets relating to such offences

D. Miscellaneous

15. Where two or more CD accounts are opened in the institution by one customer, the institution shall record the specific purpose for which such accounts are opened, in order to enable ongoing CDD of all accounts.

17. Unless and until adequate identity of the prospective client is obtained no account should be opened. If any discrepancy in information is detected subsequently the account should be suspended until the veracity of such information is confirmed.

18. Copies of all identification and address verification documents should be retained in terms of the law.

19. Accounts which record frequent transactions of the threshold limit of Rs.1,000,000/= to circumvent the mandatory reporting requirement, should be reported to the institution's Compliance Officer for appropriate action.

22. The institution must ensure that accounting activities are consistent with the customer profile on record. Any inconsistency should be inquired into, and the correct position recorded. All unexplainable activities should be reported to the Compliance Officer for appropriate action.

23. When applications for opening of accounts are received by mail or e-mail, due care should be exercised to record the identity of the client prior to opening the accounts or activating them. In no case should the institution short-circuit the required identity procedures just because the prospective client is unable to present himself in person.

04.APPLICABILITY OF FIU RULE NO.01 OF 2016

This section of the Policy is to ensure that the ***NSB Fund Management*** has internally developed effective Anti-Money Laundering and Combating of Financing of Terrorism procedures to reduce the risk of the institution being used in money laundering transactions, in addition to the requirements of the legislation and the FIU Rule No. 1 of 2016.
It is the policy of the institution to prevent the use of its facilities for the laundering of money derived from criminal activities. All Employees must be alert to the possibility of the institution being unwittingly involved in the activities of third parties, who may seek to use facilities to hide the source of criminal funds.

As such,

- The institution has formulated this Policy which is approved by the Board of Directors prepared subject to the written laws in force for the time being, on anti-money laundering and suppression of terrorist financing
- The area of coverage of this Policy among other things, include risk assessment procedures, CDD measures, manner of record retention, handling correspondent services, handling wire transfers, the detection and internal reporting procedure of unusual and suspicious transactions and the obligation to report suspicious transactions to the Financial Intelligence Unit
- Detailed procedures and controls have been developed in compliance with this Policy. Circulars are issued from time to time setting out the new standards and requirements of Know your Customer and Customer Due Diligence concept

Capture the information required under the rules of the Financial Intelligence Unit
The following are the broad guidelines in this regard:

1. Individual/Joint Accounts

a. The individual investment Accounts and information profile of the customers (KYC Form) which is prepared incorporating the basic requirements should be duly completed by the Customer/s and signed by them as being correct. An authorized officer must put his signature in this document to certify that the information was provided in his/her presence and the Officer, after perusing all account opening documents, must sign the mandate certifying the accuracy of the documents obtained.

b. Authorized Officer should also fill out the Risk Categorization form as a means of assessing the risk of Money Laundering/Terrorist Financing before the end of each working day for accounts opened on a particular date. This is the responsibility of the Head of the unit.

The institution is also required to monitor the transactions of

- high risk customers for every transaction
- medium risk customers considering transaction pattern
- low risk customers if a suspicious transaction takes place.

C). The institution is required to keep and keep in the custody of the customer-

- A photocopy of the identification document
- A copy of the Address Verification Document, in the event, the current address of the customer differs from that of the Identification Document
- Any other additional documents.

2. Proprietorship/Partnership/Company/Trust/NGO/Charitable Organization/Club/ Society etc.

a) The CD Account opening Form/Mandate and the KYC must be obtained for these customers and they should be filled in by the Customer and signed by the Delegated Representative of the Customer as being correct.

b) Additionally, for

i) Companies

Each Director should complete an individual profile of the customer (KYC) form in addition to the KYC form for the company.

ii) **Proprietor/Partnership**

An individual profile of the customer (KYC) form in addition to the KYC form for the proprietor/partnership.

iii)**Trusts**

Each Trustee should complete an individual profile of the customer (KYC) form

iv) **NGOs/Charities/Clubs/Societies/Other**

office bearers who are the authorized signatories of the entity to complete individual profile of the customer (KYC) form

c) Copies of all documents as applicable as set out in this Policy must be retained by the institution.

c) Head of the Unit should also fill out the Risk Categorization form as a means of assessing the risk of Money Laundering/ Terrorist Financing before the end of each working day for accounts opened on a particular date.

General Guidelines

1. All staff members are required to comply with the FIU directives on Know Your Customer (KYC) and Customer Due Diligence (CDD) at all times.
2. It is the responsibility of the Heads of Department to educate employees under their purview of the importance of KYC and CDD and the requirements on Customer

Identification. Special emphasis must be put on training the Account Opening Officers in this regard. And all Department Heads and Head of the unit shall ensure that all operational and Front Office staff has gone through same and are familiar with the provisions therein.

3. The following important provisions are further highlighted.

i) Satisfactory reference must be obtained for all other accounts; it will be at the discretion of the Head of the unit on a Risk Assessment Basis.

ii)No account should be opened, unless and until proper identification and information pertaining to a prospective client is obtained, except as follows:

05. SUSPICIOUS TRANSACTION/BUSINESS

As per Section 7 of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA);

"Where an Institution –

(a) has reasonable grounds to suspect that any transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence

(b)has information that it suspects may be relevant – (i) to an act preparatory to an offence under the provisions of the Convention on the Suppression of Financing of Terrorism Act, No. 25 of 2005; (ii) to an investigation or prosecution of a person or persons for an act constituting an unlawful activity, or may otherwise be of assistance in the enforcement of the Money Laundering Act, No. 05 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005,

the Institution shall, as soon as practicable, after forming that suspicion or receiving the information, **but no later than two working days there from, report the transaction** or attempted transaction or the information to the Financial Intelligence Unit".

Also, under section 14(1)(b)(iv) of the Act the Institution has to establish and maintain procedures and systems to implement the reporting requirement under Section 7 of the FTRA. Further, Section 14 (1) (d) requires the institution to train its officers, employees and agents to recognize suspicious transactions.

Screening Process

The Customer Screening process should be conducted by the Front Office Staff for new and existing customers using the following list generated by the Compliance Department.

UNSCR List

When customer on bordering, screening the customer

https://www.opensanctions.org/search

Internal Data base

List of Designated UNSCR – \\10.1.7.80\User Share\DESIGNATED LIST

Sanction Screening solution -Compass

Log in to the AML system by using 10.1.45.203:8080/Compass/login from any browser.

PEP

When customer on bordering

\\10.1.7.11\User Share\DESIGNATED LIST ,PEP and other FIU Notices\PEP\2024

https://www.opensanctions.org/search

All alerts informed by the unit shall be evaluated by the Compliance Department and if necessary, forwarded to the related unit for their feedback. The unit shall send their feedback to the Compliance Department and the Compliance Department shall file the Suspicious Transaction report accordingly.

The following are some –

but certainly not all areas where staff should remain vigilant to possible Money Laundering situations. The fact that any of the following do occur does not necessarily lead to a conclusion that Money laundering has taken place, but they could well raise the need for further enquiry. A key to recognizing suspicious transactions is to know enough about the customer to recognize that a transaction, or series of transactions, is unusual for that customer. While the following provide some examples, recognizing suspicious transactions is a matter of good sense and attention to detail.

Suspicious Cash Transactions

1. Unusually large investment is made by an individual or a company whose normal business activity would mainly be conducted by cheques or other instruments.

2. Customers who maintain a number of trustee or customers' accounts which are not required by the type of business they conduct particularly, if there were transactions which contain names of unknown people.

3. Customers who have numerous accounts and pay large amounts of cash to each of these accounts, whereby the total of credits is a large amount except, for institutions which maintain these accounts for relationships with the institution which extend them facilities from time to time.

4.Any individual or company whose account shows virtually no normal personal banking or business-related activates but is used to receive or disburse large sums which have no obvious purpose or for a purpose not related to the account holder and/or his business (e.g., substantial turn-over in the account).

5.Customers who have accounts with several Financial Institutions within the same locality and who transfer the balances of those accounts to one account, then transfer the consolidated amount to a person abroad.

6.Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received unexpectedly large sums of money from abroad.

Many individuals who invest in money into the same account without an adequate explanation.

Suspicious Transactions using Customers' Accounts

1. Customers who maintain several trustee or customers' accounts which are not required by the type of business they conduct particularly if there were transactions which contain the names of unknown people.

2. Any individual or company whose account shows virtually no normal personal business-related activates but is used to receive or disburse large sums which have no obvious purpose or for a purpose not related to the account holder and/or his business (e.g. substantial turnover in the account).

3. Customers who have accounts with several investment companies within the same locality and who transfer the balances of those accounts to one account, then transfer the consolidated amount to a person abroad.

4. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received unexpectedly large sums of money from abroad.

6. Many individuals who deposit monies into the same account without an adequate explanation.

8. Unusually large investment in the accounts of a jewelry shop whose accounts have never witnessed such deposits particularly if a large part of these deposits is in cash.

Suspicious Investment Related Transactions:

1. Individual or commercial institutions which bring in large sums of money to invest in foreign currencies or securities, where the size of transactions is not consistent with the income of the concerned individual or commercial institutions.

2. Buying or selling securities with no justifiable purpose or in circumstances, which appear unusual.

Scams

1. A local person establishes a relationship on behalf of a third party, maybe a foreigner.

2. The accounts are operated by a third party or a foreigner(s).

3. Often customers' use of forged /stolen NICs to establish business relationships.

4. The customer's company name is very similar to a very well-known, global company name, but not quite the same (e.g., P&G Printing, GE Electricians, Amazing Books)

5. The customer's company name or email address is not available on the internet.

6. The individual who operates the account(s) hardly visits a branch.

7. The account holder cannot be contacted: the correspondence sent to the customer repeatedly returned as undeliverable despite having an active account with ongoing transactions.

8. Frequent third-party deposits but depositors identify themselves in the deposit slip or in the remarks in an online transfer using their names and NICs.

9.An inquiry or a complaint from a third party regarding the account stating that the account holder is collecting funds.

Possible Drug Trafficking Related Transactions:

A. Suspicions based on profile mismatches:

i. The number, frequency and volume of transactions do not match with the declared profile or the source of income of the customer.

ii. Abnormal transaction pattern in accounts related high risk business categories for drug trafficking such as pharmaceutical drugs.

iii. Unusual patterns of transactions while the customer is engaged into cash-sensitive businesses or occupations.

iv. Rapid upward movement in turnover values in the accounts with unmatched clarifications given by the customer (financial activity not commensurate with the stated business of the customer/ occupation of the depositing individuals/ stated purpose at the account opening stage/ declared monthly income/ expected monthly turnover values).

B. Irregularities in volumes, turnovers, and account balances:

i. Accounts with high aggregate values of rupee deposits but with low account balances (e.g., frequent cash deposits followed by immediate withdrawals).

ii. High frequency of credit transactions with low volumes followed by immediate withdrawals.

ii. Sudden increases in volumes/frequency of transactions while customer is not willing to provide a valid explanation or inability to contact the customer through the given means of contacts.

C. Involvement of 3rd Parties into account operations:

i. Newly opened accounts seem to be controlled by a third party, including account opening documents/forms completed in different handwriting and/or the customer is not sure about the information given such as contact details (e.g., mobile number, address, etc.)

ii. Accounts seem to be operated on instructions of a third party residing inside/outside of the country (e.g., instances where the customer is not sure about the information provided at the account opening or transactions taken place in the account, etc.)

iii. Frequent transactions with third parties engaged in businesses where the value could not be precisely defined (e.g., Gem business)

D. Fund movements/transactions using non-face-to-face methods:

i. Transactions are mostly executed through non-face-to-face channels such as ATM, CRM/CDM deposits/withdrawals, CEFT transactions.

ii. Students/young people who maintain highly operated accounts while engaging in online activity related businesses (e.g., Finance trading, crypto currency transactions).

E. Period of relationship with the institution:

i. Accounts maintained for a short period of time (less than one year) with high volumes/frequency of transactions.

ii. Account holder requests to close the account without giving a reasonable explanation when institution inquired about the unusually high volumes/frequency of transactions.

F. Negative media news, 3rd party complaints or such other information:

i. Accounts/persons that could be linked with negative local or foreign media news/ organized drug related crime activities or listed persons by foreign authorities due to drug trafficking such as OFAC Designated Narcotics Trafficker Kingpins.

Red Flags on Identification of Suspicious Transactions relating to Bribery and/or Corruption

A. Transactions incompatible with the known profile of the customer:

i. The customer is a Politically Exposed Person (PEP) and maintains an account/account with high volumes of transactions or high frequency of transactions.

ii. A customer who is a salaried employee of a public entity, or a private business and transactions of the account do not tally with the possible level of income of such a salaried employee.

iii. An account transacting with large/one-off payments or frequent small/medium amounts in contradiction to the declared profile of the customer. (Bribes can be of varying values and may carry narrations or be exhibited as compensation, commission, bonus, returns, donation, incentive, entertainment, gift, etc.)

iv. Inability or reluctance to provide evidence to prove the given occupation or involvement with a given business.

v. Customer is a low-income profile with a high volume of transactions: e.g., a laborer receiving frequent small to medium amounts of deposits from different parties (these types of transactions may be relating to daily commissions from different businesses such

as renting out of properties which could be collected to an account maintained by a low-profile individual and then pass to a higher official of a public/private institution)

B. Customer is unable/not willing to provide an explanation on unusual transactions:

i. The customer is getting a large amount of one-time investment, but unable to explain or provide proof of funds.

ii. When inquired about an unusual transaction, the customer is not willing to provide a response and/or customer could not be contacted directly through the given means of contacts. Instead, a family member could provide different responses.

C. Operation of business transactions through personal accounts:

Instead of maintaining a business current or savings account, the customer conducts transactions linked to his/her business via a personal account.

ii. An employee of a company deposits funds relating to his/her employment to his/her personal account (personal accounts are normally used to facilitate bribery and/or corruption to conceal its nature, and to avoid scrutiny).

iii. The customer is an agent of a business and invest monthly his/her agency service into his/her personal account.

D. Irregularities in transaction volume, frequency, or turnovers:

i. unexpected repayments for his/her Reverse Repo settlement or other liabilities.

ii. A sudden transaction or payment to an individual, group of individuals or entity known for a widespread corruption activity.

v. Full settlement of liabilities, sudden acquisition of assets with unidentifiable sources of funds.

E. Customer is into high-risk industries/business for money laundering/terrorist financing or related crimes:

i. Customer operating in an industry reputed for bribery and/or corruption. (As per recent publications about the economic status of the country, several industries have been identified to induce bribery and/or corruption)

ii. Customer maintaining unprofessional and unhealthy relationships with stakeholders such as employees, suppliers, customers, regulators, etc. (regulatory requirements on start-ups and operations, receiving generous services from suppliers, retention of customers even after offering low quality services)

iii. Customer transacting with individuals or companies bearing characteristics such as poor business conduct, weak procedures, lack of ethics, negative reputation, improper payment practices, and ongoing court proceedings.

F. Transactions from/to tax havens and/or high-risk countries:

i. Customer transacting with a country with high corruption as per global indices such as the Corruption Perceptions Index or designated as tax havens.

ii. The account is funded by sources of higher-risk countries as identified by the FATF under its categories of countries with deficiencies in their ML/TF controls.

G. Suspicions due to adverse news media:

i. Adverse local or foreign news relating to bribery and/or corruption regarding the customer (Sources may include Paradise Papers, Pandora Papers, Panama Papers, etc.).

ii. 3rd party information on possible links to corruption.

iii. An account holder getting frequent, unusual deposits into his/her investment account while he/she is an employee of a public/private entity or an official of an authority known for corruption and fraud.

H. When the beneficial ownership of a legal person/arrangement is not clear:

i. Complex, non-compliant, unethical businesses, and corporate structures with unclear details about beneficial ownership (mostly, bribery and/or corruption transactions are indirect, employing multiple personnel, agents, subsidiaries, contractors making the entire process cumbersome).

ii. The customer is not able to provide proof of documents to establish the ownership of the company.

Reporting In the first event of your suspicion

- The staff concerned should report the same immediately to the ***Manager Front Office to*** ensure that there are no known facts which would negate the suspicion. Manager, Front ***Office should report the same immediately to the Compliance Officer***.

How to report a Suspicious Transaction

To reiterate, the law requires employees to report any reasonable suspicion that they may have about a customer or his/her transactions. The origin of these assets is not known, or the assets are inconsistent with the customer's standing.

The law also requires the institution to have appropriate effective reporting procedures and systems in place to implement the reporting requirement. It also requires that all employees follow these procedures using them correctly as they are intended to be used.

Reporting procedures

Good reporting procedures and their correct use are designed to ensure that, when a suspicious transaction has been identified -

 the suspected customer or any other related person is not alerted

 the matter is dealt with quickly and professionally

- the external authorities are notified and provided with the necessary records, if appropriate

The institution has put in place procedures to report suspicions with supporting information, through the Compliance Department put in place to monitor suspicious activities.

Awareness has been made among the employees to ensure that the supporting information sent is relevant to the suspicion so that it is passed on to the Financial Intelligence Unit (FIU).

Role of the Compliance Officer on receiving the Report

At the Institution

- ✓ When the Compliance Officer receives the Suspicious Transaction Report, (STR) the Compliance Officer will decide whether the report gives rise to knowledge or suspicion that a customer is involved in money laundering.

- ✓ If the Compliance Officer believes that the suspicions may be justified and require further investigation, must report to the Financial Intelligence Unit (FIU) .

- ✓ The institution may make further enquiries within the parameters of its own records, but it does not need to carry out more detailed criminal investigations.

- ✓ The employee has a duty to assist the Compliance Officer in reporting the complaint to the FIU effectively, by making sure that the information provided

- ✓ describes why there are reasonable grounds for suspicion and what they contains accurate information is timely and not delayed

The importance of timing

The institution is aware that,

- ✓ It is very important that there is no delay in reporting, and it is the duty of all employees to report suspicion as soon as they have established reasonable grounds and collected the relevant supporting material.

- ✓ The consequences of not reporting suspicions immediately to the Compliance Officer could be serious for the employee involved and may include individual fines, imprisonment, or both as set out in the legislation.

- ✓ Under no circumstances should the customer know that they have been reported for the activity, or that an investigation is underway or may be underway.

- ✓ The above does not mean that the institution cannot ask the customer for an explanation or continue to provide them with normal customer service. But it does mean that the institution must do so without alerting them to the fact that the institution may or had already notified the Authorities. If customers being investigated are alerted, the institution could be blamed for tipping them off, which is a criminal offence for the individual who alerted the customer to the existence of an actual or potential investigation.

- ✓ As required by Law, suspicious transactions should be submitted to Financial Intelligence Unit (FIU) as soon as practicably possible but **no later than two working days of formation of suspicion.**

06.COMMUNICATING THE SUSPENSION ORDER BY THE FIU.

a) The FIU may communicate the suspension order by email/ telephone/ any other mode of communication which will be followed up in **writing within 24** hours. The written order will be addressed to the Chief Executive Officer/ Managing Director of the FI with a copy to the compliance officer appointed under Section14 of the FTRA, or to any officer of the FI who is informed by the FI to the FIU as acting on behalf of the compliance officer, during any period of absence of the compliance officer.

b) The suspension order may be issued,

i. against an individual by his/her name and/or with reference to the National Identity Card (NIC) number and/or passport number and/or driving license number,

ii. against an entity identified by name and/or by business registration number,

iii. for specific account or transaction, where such account or transaction is identified by account number or by relevant reference number

c) The suspension order will be effective from the initial date it is communicated (via telephone/mail/letter) to the FI **up to 7 calendar days.**

d) The order will provide instructions to the FI, requiring the FI not to proceed with any transactions 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 entity/individual.

Communicating the Extension order by the FIU

a) Upon expiry of 7 calendar days, if any suspension order is extended by the High Court of the Western Province holden in Colombo in terms of the provisions of Section 15 (3) of the FTRA (hereinafter referred to as the Extension Order), the FIU will communicate to the FI, by telephone/email followed up in writing, the following.

i. accounts (including safe boxes/safe deposit lockers), transactions, CDS accounts or any other business relationship including remittances, subject to extension

ii. the date until when the Extension Order is effective

b) The communication by the FIU on the Extension Order will be addressed to the Chief Executive Officer/ Managing Director of the FI with a copy to the compliance officer appointed under Section 14 of the FTRA, or to any officer of the FI who is informed by the FI to the FIU as acting on behalf of the compliance officer, during any period of absence of the compliance officer.

c) The Extension Order will require FI not to proceed with any transactions excluding credit transactions with respect to accounts (including safe boxes/safe deposit lockers), transactions, CDS accounts or any other business relationship including remittances specified under the Extension order until the date specified in the order and communicated to the FI.

Responsibilities of the Financial Institution with respect to suspension and extension orders

a) The Financial Institution should,

i. Immediately acknowledge the suspension orders by way of an email to the FIU.

ii. Confirm the suspension order with details of **all business relationships** maintained along with the balances available as at the date of suspension, immediately to the FIU.

iii. FI is required to report **all business relationships** maintained by the concerned individual/entity including any business relationship connected with the individual/entity (e.g. Joint holder/guardian of a minor, sole proprietorship/partner etc.) to the FIU under (ii) above without any discretion. When FI confirms connected business relationships the nature of connection to concerned individual/entity has to be specified.

iv. If any FI fails to confirm to the FIU on any business relationship with the concerned individual/entity **within 5 calendar days after communicating** the suspension order, it is considered that there is no business relationship between the FI and the individual/entity subject to suspension.

v. If any business relationship has commenced by the subject individual using any other identification number other than NIC No., such as driving license/ passport number, necessary steps should be taken to identify the NIC No. of the relevant individual ensuring all business relationships with him/her have been captured.

vi. Ensure that for individuals, if the suspension order has been issued under the old NIC No. the availability of business relationships should be checked with the new NIC No. and vice versa.

vii. Ensure that all information confirmed to the FIU relating to suspension and extension orders is complete and accurate.

viii. Ensure that the Institution Automated system will reflect suspension and extension order restricting any transactions (excluding credit transactions) into suspended accounts (including safe boxes/safe deposit lockers), transactions, CDS accounts or any other business relationship.

ix. Ensure communication of the **suspension order to all relevant staff within the institution without delay.**

xi. Provide instructions to relevant staff on dealing with requests by customers, if any, whose accounts are subject to suspension.

xii. Provide instructions to relevant staff on dealing with requests by customers, if any, whose accounts are subject to suspension.

xiii. Acknowledge and confirm the extension order with the balance available as at the date of extension immediately to the FIU.

xiv. Obtain confirmation from **the FIU before releasing any suspended account**.

b) If any suspended account is receiving salary/pension relating to the customer, that facts req**uired to be notified to the FIU along with suspension confirmation.**

c) Transactions in suspended accounts:

During the period of suspension of transactions, FIs should not allow any transaction (including any statutory payments, standing orders, etc.) except for credit transactions into a suspended account. Any debit transaction, whether it is statutory or otherwise, should be communicated by the FI to the FIU**, and should await the High Court order permitting such transaction prior to debiting the suspended account.**

d) Communicating the suspension order to customers:

The FI may inform the customer about the suspension of his/her transactions **only upon an inquiry** by the customer and in the same manner the inquiry is made. **In relation to the initial seven-day suspension,** FI may inform the customer funds/ accounts/ transactions have been suspended by the FIU under the FTRA. FI is not required to provide a reason for such action by the FIU to the customer. In relation to extension of suspension, FI **may inform the customer that funds/accounts/ transactions have been suspended as per an order of the High Court of the Western Province holden in Colombo**. The FI required it to take necessary steps to ensure that Section 9 of the FTRA is not violated during the communication process.

e) Every individual and institution subjected to a suspension order should be considered as of high-risk customers on all occasions in implementing the requirements under the

provisions of the FTRA and CDD rules and any other rules and regulations issued under the FTRA.

f) Future transactions with customers whose accounts are subject to suspension: The FTRA does not prohibit FIs from establishing new business relationships with customers whose transactions are under suspension. However, the fact that the customer's previous transactions were subject to suspension under the FTRA is required to be reflected in the customer's risk profile as high risk, and due consideration should be given to the risk entailing the new business relationship proposed to be entered in to with the customer by conducting enhanced due diligence. Further, the FI is advised to keep the FIU informed about such new business relationships as appropriate.

g) FIs should include written procedures in dealing with suspension orders into institution's AML/CFT policy to address the matters highlighted above.

h). Conduct audits from time to time to ensure that due procedure is being followed, and corrective measures are taken to eliminate weaknesses in the systems.

Further information requested on Suspicious Transaction Reports (STRs)

The institution is required to adhere to the following specified time periods when submitting additional information requests on STRs.

- For '**Extremely Urgent** 'information requests-provide information within **24 hours or as specified in the request.**
- For '**Urgent' information requests** – provide information within **three working days from the date of the letter.**
- For **other information** requests, provide information **within two weeks from the** date of the letter.

07. ANTI MONEY LAUNDERING (AML) – COMBATING OF FINANCING OF TERRORISM (CFT) MONITORING AND CONTROLS

COMPLIANCE OFFICER

Financial Institution has designated the responsibility to control and monitor AML and CFT issues within the institution to an independent staff designated as "Compliance Officer" with reporting line directly to the Board Integrated Risk Management Committee.

Responsibilities of the Compliance Officer

- Implement Anti Money Laundering and Combating of Financing of Terrorism Policy of the institution in line with the requirements and update AML & CFT Policy on an ongoing basis in line with local and international requirements.

-Train staff and create awareness on Anti Money Laundering and Combating of Financing of Terrorism requirements.

-Ensure that all staff conduct their business in accordance with the spirit of the AML & CFT Policy.

- Monitor the day-to-day operations to detect unusual customer activity (as mentioned above under section 'recognizing suspicious transactions/business')

- Put in place, policies, procedures, and systems to ensure that the institution will not be used by the money launderers or terrorist financiers.

- Serve as a contact point in the institution for compliance issues:

  a) Provide feedback to staff on compliance queries.

  b) Receive internal suspicious transactions report from staff, analyze and investigate the same and liaise with the Financial Intelligence Unit.

  c) Take reasonable steps to acquire relevant information from customers or other sources.

d) Report all suspicious money laundering and terrorist financing transactions to Financial Intelligence Unit (FIU) .

Independent Compliance Testing

The institution has entrusted the Compliance Officer with the responsibility to test the implementation and adherence of the AML & CFT Policy of the institution. In addition, the Compliance Department also carries out random assessments and reviews to verify among other things the implementation and adherence of the AML& CFT Policy in the institution and report any non-compliances to the Board Integrated Risk Management Committee.

Record Keeping Obligations

In addition to regular institution record keeping requirements, the Anti Money Laundering and Combating of Financing of Terrorism Policy of the institution requires that documents concerning customer identification and records relating to transactions undertaken on behalf of customers/noncustomers to be maintained for the period of six years.

It is also required that

a) All anti-money laundering and combating of terrorist financing monitoring reports made by Compliance Officer and records of consideration on those reports and of any action taken consequently including reporting done to management/auditors/regulators be maintained as stated above for future reviews.

b) Records showing the dates of anti-money laundering and combating of terrorist financing training and the names and acknowledgement of the staff receiving the training be also maintained as stated above.

All records maintained should be available to authorized people promptly on request without undue delays and ***Board Secretary shall retain the Board Minutes regarding AML/CFT issues for the period of six years.***

Some of the questions that the narrative should attempt to answer, if possible, include:

What is the nature of suspicion?

• What offenses may have been committed?

•What transactions, attempted transactions, behaviors, facts, belief and circumstances are involved and relevant to the suspicion?

• Who are the natural and legal people involved?

• Who are the beneficial owners?

• What are their identifiers such as names, ID numbers, registration numbers, etc.?

• What are their addresses?

• What are their occupations or lines/types of business?

• Who are their employers?

• What political exposure do they have, if any?

• How are they connected with each other and with the transactions?

• What were their roles in the transactions?

• What property is involved?

• What is the nature and disposition and estimated value of involved property?

• When and where did the transactions or attempted transactions or behaviors occur?

• How, if at all, do the timing or location of the transactions contribute to the institution's suspicion?

• Why do these facts and circumstances support the suspicion?

• How was the suspicion formed?

• What triggers or indicators are present?

• What actions have been taken?

• What related STRs have the institution already submitted?

• What red flags are present?

• What deviations from expected activities have taken place?

Accuracy:

It is imperative that the information provided in the report is accurate. This is particularly true for identifiers such as names, **ID numbers, registration numbers, etc**. **All spellings**

and transcriptions of identifiers should be double checked. A single inaccurate digit in a passport number or an NIC, or a misplaced or transposed character in a name, can make the difference between a successful and an unsuccessful analysis. Identifiers for legal entities (e.g. company / business registration number, registered name of company) should be identical in every respect to those found on the official registration documents.

Submission of Supporting Documents

The institution is required to submit relevant supporting documents along with the STR. If the institution is unable to submit the supporting documents via GO AML, the institution should submit the relevant supporting documents through email and/or along with the signed hard copy of the STR. In such cases, the institution should mention in GO AML that additional supporting documents are submitted via email or through post**.**

Supporting documents should support rather than replace the STR contents, including the narrative. It is not acceptable to only refer to a supporting document in the narrative when information from the supporting document can be directly included in the narrative.

Confidentiality

As per the Section 9 of the FTRA Financial Institutions are not allowed to inform any person, including the customer, about the contents of an STR and even that the Financial Institution has filed such a report to the FIU.

As per Rule 46 of the Financial Institutions Customer Due Diligence Rule, No. 1 of 2016, where a Financial Institution forms a suspicion of money laundering or terrorist financing risk relating to a customer and where the Financial Institution reasonably believes that conducting the process of CDD measures would tip off the customer, then the Financial Institution should terminate conducting the CDD measures and proceed with the transaction and immediately file an STR.

Breach of Confidentiality

If any customer is being tipped off about the reporting of STRs by any officer of the institution it would consider as a violation under the FTRA Section 9 and 10. This is described as the offence of ***'tipping off' and is an offence punishable with a fine not exceeding five hundred thousand rupees or imprisonment of either description for a term not exceeding two years, or to both such fine and imprisonment***.

Protection for Persons Reporting STRs 28. As per Section 12 of the FTRA: No civil, criminal or disciplinary proceedings shall lie against — (a) a such Institution, an auditor or supervisory authority of an Institution ; or (b) a director, partner, an officer, employee or agent acting in the course of that person's employment or agency of an Institution, firm of auditors or of a supervisory authority, in relation to any action by the Institution, the firm of auditors or the supervisory authority or a director, partner, officer, employee or agent of such Institution, firm or authority, carried out in terms of the FTRA in good faith or in compliance with regulations made under this Act or rules or directions given by the Financial Intelligence Unit in terms of the FTRA.

Failure to Report STRs

If a Financial Institution fails to submit STRs when reasonable grounds exist to suspect that a transaction is related to money laundering or terrorist financing, such is considered ***as non-compliance with the FTRA. As per Section 19 of the FTRA such non-compliances are liable to penalties up to one million rupees (Rs. 1,000,000.00) or double this for subsequent failures to report***.

Should a reporting entity continue a business relationship with a customer about whom an STR has been reported?

The FTRA does not prohibit Financial Institutions from continuing business relationships with customers about whom STRs has been reported or suspicion has been formed. Especially Financial Institution's behavior toward the customer should not amount to any tipping off subject to the provisions of the Section 3 of the FTRA.

Obligations of Financial Institutions which has submitted an STR in relation to a customer and is continuing the business relationship

After the submission of an initial STR, the Financial Institution should continue to comply with all relevant provisions of the FTRA in all future dealings with that customer, which may include a requirement to submit additional STRs /information on further suspicions identified / further developments.

Further Information Requests

Where the FIU has requested further information regarding any STR, the Financial Institution should take all necessary measures to provide such information promptly to the FIU.

08. RISK CATEGORIZATION METHODOLOGY

From the information provided by the customer the institution should be able to make an initial assessment of a customer's risk profile and accordingly special attention needs to be focused on those customers identified thereby as having a higher risk profile. Enhanced Due Diligence (EDD) must be paid on those customers and in order to carry out EDD additional inquiries should be made, and information should be obtained in respect of those customers including the following: -

- Evidence of an individual's permanent address sought through independent verification by field visits
- Personal reference (i.e. by an existing customer of the same institution)
- Prior institution reference regarding the customer and the customer contact with the institution
- The customer's source of wealth
- Verification of details relating to employment, public position held (previous/present), if any, supplied by the customer.

- Obtaining & verifying additional information on the customer such as details of occupation, volume of assets, information available in public data- bases, internet search, etc.)
- Regular updating of identification data of customer and Beneficiary owner
- obtaining additional information on the nature of business
- Obtaining information on reasons for transactions performed
- Obtaining information on sources of funds/ wealth of the customer
- obtaining the approval of Senior Management.

A. Low Risk

Individuals and entities whose identities and sources of wealth can easily be identified and in whose accounts, transactions by and large conform to the known profile, shall be categorized under Low Risk.

Example:

Student/Housewife/Pensioner
Employee Nonexecutive –Government
Employee – Non-executive -Private
Public Limited Liability Company
Business – Individual
Club/Society/Association
Educational Institution
Self-Employed - Professional
Self-Employed - Business
Other Individuals

B. Medium Risk

Individuals and entities whose accounts reflect a large volume of turnover or many high value transactions in the estimation of a branch, taking into account the relevant factors such as the nature of business, source of funds, profile, market reports etc. shall be categorized under Medium Risk.

In these cases, upon seeking clarification satisfactory responses shall be forthcoming from the customers.

Example:

Employee-Executive-Government
Lawyer & Accountant
Government Institution
Private Limited Liability Company
Business-Proprietor/Partnership

C. High Risk

Individuals and entities whose public image profile in terms of the KYC and AML in the estimation of the financial institution is poor/adverse shall be categorized as high risk.

Examples:

PEPs
NGOs
Offshore/Non-Resident Company
Foreign Citizen
Share & Stockbrokers
Investing/Administering/managing public funds
Restaurant/Bar/Casino/Gambling House/Night Club
Importer/Dealers in 2nd hand motor vehicles

How does the institution change the risk categorization when a customer's risk level changes?

Under normal circumstances the risk status of customers, shall be evaluated and updated based on the risk status as follows.

a. Low Risk Customers – Once in every three years

b. Medium Risk Customers – Once in every two years

c. High Risk Customers – Ongoing monitoring (high risk customers who make new investments with the NSB FMC)

But at instances where the status of the customer changes, the institution shall take steps to evaluate and change the customer risk rate accordingly.

When a customer's risk level changes, the institution typically updates the risk categorization through a **risk review and reassessment process**.

1. **Triggering Event or Periodic Review**:
    - A change in customer behavior (e.g., unusual transactions, change in occupation,)
    - Periodic reviews based on the customer's risk level
2. **Review and Assessment**:
    - The institution reevaluates the customer's profile, including updated KYC (Know Your Customer) information, transaction history, or sanctions hits.
    - The customer's activity is assessed against the institution's risk rating criteria.
3. **Re-Risk Rating**:
    - Based on the reassessment, the customer's risk level is updated in the system (e.g., from low to medium, or medium to high).
4. **Internal Approvals**:
    - **Changes in risk category may require approval *from compliance or senior management, especially for upgrades to high risk.***
    -

5. **System Update and Documentation**:
    - The new risk level is recorded in the institution's customer due diligence system.
    - All relevant documentation supporting the change is stored for audit and regulatory purposes.
6. **Enhanced Due Diligence (if required)**:
    - If the customer is now high-risk, enhanced due diligence (EDD) measures are implemented (e.g., more frequent reviews, stricter monitoring).

09. RISK MANAGEMENT

- This Policy document shall be the benchmark for the supervision of systems and procedures, controls, training, and other related matters in the implementation of AML & CFT guidelines in the institution.

- By the very nature of its functioning, institution is more susceptible to the risk of Money Laundering & Terrorist Financing and the possibility of its various services being unwittingly used as conducting and cycling the ill-effects of the tainted/illegal money by the financial launderers. In this context it is imperative that the institution should know its customers, particularly their identity, preferably at the time of establishing a relationship since the incidence or risk factor begins at this point of time-itself.

- The front office functionaries (Counter Staff) at the operational points are vested with greater responsibility of effectively administering KYC procedures to protect the institution against financial frauds and Money Laundering & Terrorist Financing. The institution resolves that the KYC requirements shall be realized

without inconveniencing the customer and rather it shall be through convincing them that it is well intended in their long-term interest and in the interest of the institution Community and the Regulator.

- Identifying/handling the transactions which are of a suspicious nature, and the procedure that has to be followed when the KYC cannot be completed, have been defined and set out in the previous chapters.

- The operational staff shall continue to be trained on an on-going basis on the basic requirement of proper, - Customer identification or KYC - Maintenance of records of transactions and identification - Listing and submission of details of large value currency transactions reports which will certainly help institutions to check/reduce operational risks and vulnerability to frauds.

- The institution shall administer Anti Money Laundering & Combating of Financing of Terrorism measure keeping in view the risk involved in a transaction, account, or business relationship for the existing and new customers.

- The institution shall continue to ensure that compliance to KYC guidelines is evaluated periodically in the background of the conditions obtained in respect of the institution's Policies, system and Procedures, Legal and Regulatory requirements. Compliance Report on the implementation of KYC guidelines shall continue to be placed at the Board of Directors.
- The institution shall ensure that the Internal Audit Department regularly/periodically and the Compliance Department randomly observe audit requirements of KYC guidelines and verification of its implementation at operational units of the institute

10.CCTV Operations

To enhance operational risk management and safeguard the institution being abused for money laundering and financing of terrorism, the institution shall have in place a fully operational robust CCTV system.

The institution should ensure that CCTV cameras are installed at appropriate locations with adequate lighting in a manner that the camera is able to clearly capture, monitor and record the relevant areas where business operations take place.

The CCTV systems should be aligned in a manner and at an angle as to obtain a complete and unimpeded view of the areas where business operations are taking place and the institution shall ensure that the CCTV system is not interfered by internal or external lighting, glare, or any other object.

The institution shall ensure that all images captured visible, recognizable, and clear with the capability of identifying the features of the individuals separately. High quality digital equipment with capabilities such as easy viewing, recording and retrieval of high-quality images shall be used by the institution.

11.Training to Staff members (AML/ CFT)

- The institution should ensure that the training sessions on AML & CFT procedures are included in the Training Calendar on an ongoing basis. The institution shall arrange to update and modulate these training sessions to the requirements of front-line staff, compliance staff and counter-staff dealing with new customers. It shall be the institution's focused endeavor to make all those concerned fully understand the rationale behind the AML & CFT procedures and implement them consistently.

- The institution's operational staff shall continue to have the conviction to educate and impress the customers that the KYC guidelines are meant for good understanding and for better deliverance of customer service as also for weeding - out the fraudsters in the initial stage itself.

- Transaction monitoring with a view to detecting suspicious cases is the most crucial problem that any comprehensive Anti-Money Laundering and Combating Financing of Terrorism measures must address. This fact is effectively taken care of by the structured methodology for implementing AML & CFT procedures which eventually tend to emit warning signals wherever required and the sustained functional commitment to these procedures in their day-to-day work will enable desk officials to pick up the adverse signals for reporting to the Manager through STR Reports.

Customer Education

- In order to educate customers on KYC requirements and the need for seeking certain personal information from the customers/applicants for opening accounts and also to ensure transparency, the institution shall publish this AML Policy in the web-site and place a copy of the same in branch for the reference by user Public.

- It is the duty and responsibility of Operational Staff to educate the customers and tactfully/convincingly explain the need for customer profile and its relevance in the present adverse conditions of Money Laundering, Terrorist Financing etc. The customers shall be impressed by the fact that the profile format enables the branch to render better Customer Service.

- An initial resistance by the customers to fill up the exhaustive customer profile format is an expected initial response, and it is foreseen as a temporary phenomenon only. The expected resistance could be overcome if the background could be explained to the customers so that the required information can be gathered.

- The institution shall endeavor to guard against denial of institution services to public especially to those who are financially/socially under-privileged due to the implementation of Customer Acceptance Procedures on too restrictive basis

12. IDENTIFICATION OF BENEFICIAL OWNERSHIP

In the process of identifying beneficial owner(s) of a legal person, the institution has to consider three main elements:

a) Which natural person(s) owns or controls more than ten percent (10%) of the customer's equity?
b) Which natural person(s) has "effective control" of the legal person?
c) On behalf of which natural person(s) the transaction is being conducted?

Figure 1: Simple Indirect Shareholding

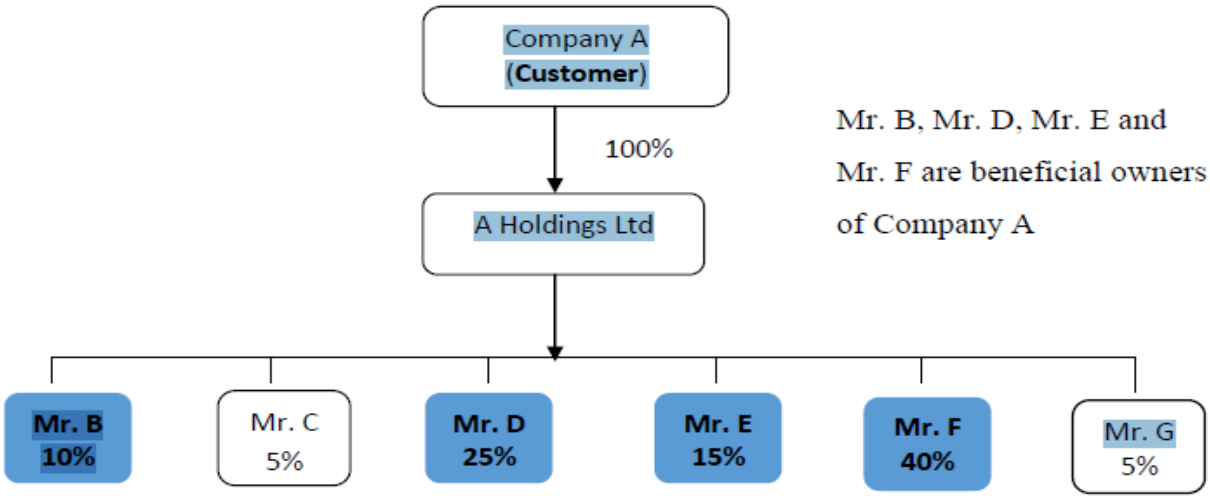
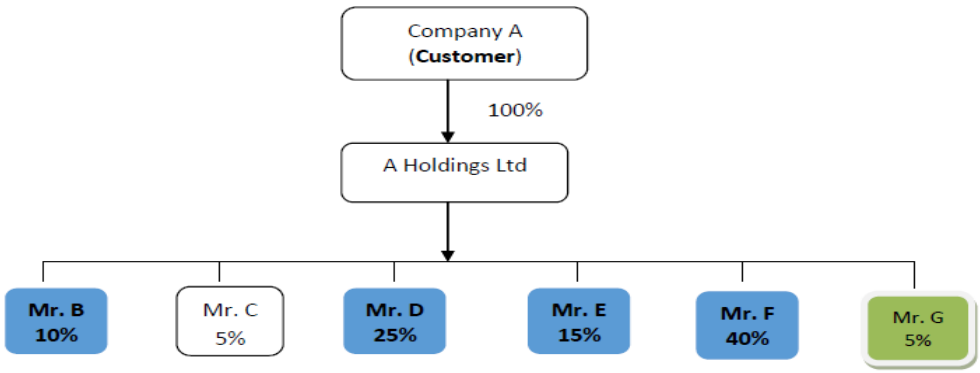


Figure 4: Effective Control



Mr. G is the managing director of the ABC Bank, which is the main financing source of company A. In such a situation even if Mr. G holds less than ten percent (10%) of Company A, he has effective control over company A through ABC Bank and should be considered as a beneficial owner through effective control.

At instances where the ownership is divided among large number of individuals and the shareholding percentage of every individual is less than 10%, the institution shall take steps to verify the status of Beneficial Ownership by verifying the person/s who hold the Effective Control of the Legal Person or Legal Entity or verifying the person on whose behalf a transaction is being conducted.

The institution shall take steps to obtain and verify information on Trusts including the identities of the author of the Trust, the trustees the beneficiary or class of beneficiary and any other natural person, exercising ultimate effective control over the Trust.

The Financial Institution shall obtain documents pertaining to

Trust (Deed of Trust, Instrument of Trust, Trust Declaration, etc.) and shall verify the provisions provided in the documents within the context of the laws through independent means.

The institution shall take all reasonable measures to verify the identity of the

owner/s using information obtained from reliable sources in order to obtain sufficient information to confirm who the beneficial owner/s is.

The identification that shall be obtained are as follows

- Full name
- Official personal identification or any other identification number
- Permanent/ residential address

The Financial Institution shall verify the identity of the beneficial owner before or during the course of entering into a business relationship with or conducting a transaction for an occasional customer.

For the verification of beneficial ownership, some of the documentation that institutions can rely on may include (but not limited to) the following:

a) Share register

b) Annual Returns

c) Trust deed

d) Partnership agreement

e) The constitution and/or certificate of incorporation for an incorporated association

f) The constitution of a registered co-operative society

g) Minutes of the board of directors' meetings

h) Information available through open-source search or commercially available databases.

The institution should not establish a business relationship or conduct any transaction with a customer who poses a high money laundering and terrorist financing risk, prior to verifying the identity of the beneficial owner.

At instances where a beneficial owner is not available & individual person existing control over the customer is not available, the institution shall identify natural persons holding senior management positions as beneficial owners.

The institution shall review the adequacy of information in respect of beneficial owners on a annual basis through obtaining information from the existing system of the institution.

The review of beneficial ownership shall take place if any material/ significant change as stated below takes place in the customer.

- A public company is taken private
- A shareholder or a group of shareholders takes effective control of voting shares

- A new partner is added, or an existing partner is removed
- Change in management positions
- New trustees are appointed
- A Trust is dissolved
- A new account is opened for the same customer
- Transactions are attempted that are inconsistent with customer profile

A delayed verification is permitted to be carried out to verify the identity of beneficial owners when

- Risk level of the customer is low & verification is not possible at the point of entering into the business
- there is no suspicion of money laundering or terrorist financing risk involved
- Delay will not interrupt the normal conduct of business

When delayed verification is allowed the institution should carry out risk management procedures such as, limiting the number, put in restrictions on types and/ or amounts of transactions, monitoring large or complex transactions etc.

The institution shall not establish a business relationship or conduct any transaction with a ***customer who poses a high money laundering and terrorist financing risk prior to verifying the identity of the beneficial owner.***

The institution shall not conduct any business relationship with any customer who is not able to comply with the above provisions.

The institution shall maintain records of identification and verification relating to beneficial ownership for a period of six years as stated above.

The institution shall identify if the beneficial owner is a Politically Exposed Person (PEP) & will consider such relationships as high risk and conduct enhanced due diligence

13. POLITICALLY EXPOSED PERSONS

Definition

A Politically Exposed Person (PEP) is defined as an individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization. This includes

- a Head of a State or a Government
- a Politician
- a Senior Government Officer
- a Judicial Officer or Military Officer
- a Senior Executive of a State-Owned Corporation/Government or Autonomous body

The above definition does not include middle ranking or junior ranking individuals but is applicable to family members and close associates of PEPs.

Immediate family members of PEPs include

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

Close associates of PEPs or their family members include

i. a natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship with a PEP

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 a PEP or his immediate family members

iii. a PEP's widely- and publicly known close business colleagues or personal advisors' persons acting in a financial fiduciary capacity

Identification of PEPs

1. The institution shall implement appropriate internal policies, procedures and controls to determine if the customer or the beneficial owner is a PEP and also to carry out periodic reviews on existing PEPs to ensure that all information available are up to date.

2. The institution shall not identify middle ranking or junior individuals as PEPs but shall take steps to identify middle ranking and junior officials who act on behalf of a PEP to circumvent AML/CFT controls.

3. The institution shall take necessary steps to gather information on foreign public officials

at account opening and when existing foreign customers become PEPs.

4. In case the customer is determined to be a domestic/international organization PEP, the institution shall gather sufficient information to understand the characteristics of the public functions that the PEP has been entrusted with and, in the case of an international organization, the business model of that organization.

Beneficial Owners

5. The institution shall identify the beneficial owners and take reasonable measures to verify the identity of the beneficial owners of legal people and arrangements whose ultimate beneficial owners or controllers or their family members or associates are PEPs.

6. If there are reasonable grounds to believe that a beneficial owner is a PEP, the institution shall verify if the beneficial owner is a PEP.

7. The institution shall inquire about the reason for a person purporting to act on behalf of a beneficial owner to determine whether the beneficial owner of the customer or client is PEP.

8. The institution shall apply all the requirements applicable to a PEP for: a) a person who is acting on behalf of a PEP, or b) a customer or beneficial owner of a customer who is identified as a family member or close associate of a PEP.

Methods to identify PEPs

The institution shall take steps to identify PEPs through

a. Commercial data Bases

b. Internally maintained databases

c. Publicly available registries of people, in case of foreign PEPs

d. Ad-hoc customer research

e. Self-declarations obtained from customers (subject to verification)

 The institution shall take steps to monitor non-PEP accounts based on risk, for a change in the customer status/profile or account activity and update customer information accordingly at instances such as

a. when a customer spontaneously submits a new declaration of political exposure

b. when ongoing monitoring reveals activities or information that deviate significantly from the customer and/or account profile in a manner that suggests previously unknown political exposure

c. when an election is held that affects any of the customers' PEP status

d. whenever the institution becomes aware, through any means, of the need for such an update.

The institution shall

a. **Obtain approval from Chief Manager prior to entering** into a new business relationship with a PEP or continuing an existing relationship
b. Identify the source of funds and wealth by appropriate means.
c. Perform enhanced ongoing monitoring of the business relationship.

- ✓ The institution shall take reasonable measures to establish the source of wealth and the source of funds of PEPs to monitor the ongoing due diligence process effectively and ensure that the level and type of transactions are consistent with the source of wealth and source of funds of the PEP.

- ✓ PEP accounts are treated as High Risk in the customer risk profiling mechanism, and they are subject to frequent periodic reviews.

The institution shall evaluate the status of PEPs annually and take decisions on customers who are no longer coming under the purview of PEP, taking into consideration the level of influence that the customer could exercise and whether the previous and current functions are linked in any manner.

The institution shall ensure that the senior management of the institution are aware of relationships with PEPs and that the institution does not undertake business relationships with PEPs in the absence of adequate controls by senior management.

e) When deciding to undertake a business relationship with a PEP the institution shall ensure that the senior management involved

a. has full knowledge and understanding of the AML or CFT internal control programs of the institution.

b. have a strong understanding of the potential or existing client's or customer's ML or TF risk profile; and

c. have active involvement in the approval process of the AML /CFT policies and procedures of the institution.

The institution shall maintain the records identification and verification information relating to PEPs as per the record keeping procedures applicable to the institution.

A LIST CATEGORY OF CUSTOMERS THAT CAN BE CONSIDERED AS PEPS

DOMESTIC PEPS

A.

1 The President

2 The Prime Minister

3 The Speaker and the Deputy Speaker of the Parliament

4 Cabinet Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers

5 Members of Parliament

6 Leaders of Political Parties

B.

7 Governors of Provinces

8 Chief Ministers of Provinces

9 Mayor, Chairman of Municipal Councils

10 Chairman of Provincial Councils

11 Members of Municipal Councils/ Provincial Councils / Local Government Bodies

12 Commissioners/ Secretaries to Municipal Councils/ Provincial Councils / Local Government Bodies

C.

13 Chief Justice

14 Attorney General

15 Judges of Supreme Court

16 Judges of the Court of Appeal

17 Solicitor General of the Attorney General's Department

18 Judges of High Courts/Provincial High Courts

19 Judges of District Courts

20 Judges of Magistrate Courts

21 Registrar of Supreme Court

22 Registrar of the Court of Appeal

23 Registrars of Judges of High Courts/Provincial High Courts

24 Registrars of District Courts

25 Registrars of Magistrate Courts

D.

26 Ambassadors /High Commissioners

27 Consul-General/ Deputy Head of Mission/Charged affairs/Honorary Consul

28 Ministers plenipotentiary and Envoys Extraordinary

29 Representatives of UN agencies and Heads of other international organizations

E.

30 Secretary/ Senior Additional Secretaries/ Additional Secretaries to the President

31 Secretary/ Senior Additional Secretaries/ Additional Secretaries to the Prime Minister

32 Secretary /Senior Additional Secretaries/ Additional Secretaries to the Cabinet of Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers

33 Deputy Secretary to the Treasury

34 Secretary/ Senior Additional Secretaries /Additional Secretaries/ Deputy Secretaries to Ministries 35 Members of the Monetary Board

35Governor / Deputy Governors / Assistant Governors and Heads and Additional Heads of Department of the Central Bank of Sri Lanka

36 Advisors to the President/ Prime Minister / Ministers/ Ministries

37 Chief of staff of presidential secretariat

38 Auditor General

39 Secretary General of Parliament

40 District Secretaries/ Government Agent and Secretaries

41 Heads and Senior Officials of Government Departments

42 Chairmen and Senior Officials of State Enterprises

43 Chairmen and Senior Officials of State Corporations / Statutory Boards/ Authorities/ Public Corporations

F.

44 Field Marshall / Admiral of the Fleet/ Marshal of the Air Force

45 Chief of Defense Staff

46 General of Sri Lanka Army/Admiral of Sri Lanka Navy/ Air Chief Marshal of Sri Lanka Air Force

47 Officers in the Rank of Lieutenant Colonel and above of Sri Lanka Army

48 Officers in the Rank of Commander and above of Sri Lanka Navy

49 Officers in the Rank of Wing Commander and above of Sri Lanka Air Force

50 Inspector General of Police

51 Police officers above the rank of Asst. Superintendent of Police

G.

52 Chairman/ members and senior officers of the Public Service Commission

53 Chairman/ members and senior officers of the National Police Commission

54 Chairman/ members and senior officers of the Human Right Commission

55Chairman/ members and senior officers of the Commission to Investigation Allegations of Bribery or Corruption

56 Chairman/ members and senior officers of the Finance Commission

57 Chairman/ members and senior officers of the Election Commission

58 Members of Constitutional Council

59 Chairman/ members and senior officers of the Audi Service Commission

60 Chairman/ members and senior officers of the Delimitation Commission

61 Chairman/ members and senior officers of the National Procurement Commission

62 Members of Cabinet appointed committees

H.

63 Chairman, Members and senior officers of University Grant Commission

64 Chairman, members of University Councils

65 Chancellor

66 Vice Chancellor

67 Registrar of universities

FOREIGN PEPS

68. Officials of international organizations who hold or have held, during the last 5years, management positions in such organizations (directors, heads of the boards or their deputies)

69. Officials of international organization who performs or performed any other management functions on the highest level, particularly in international and intergovernmental organizations

70. Members of international parliamentary assemblies

71. Judges and management officials of international courts

14.A LIST OF RED FLAGS AND INDICATORS FOR SUSPICION

A.

PEPs attempting to shield their identity

1. Use of corporate vehicles (legal entities and legal arrangements) to obscure
   i) ownership,
   ii) involved industries or
   iii) countries.

2. Use of corporate vehicles without valid business reason.

3. Use of intermediaries when this does not match normal business practices or when this seems to be used to shield identity of PEP.

4. Use of family members or close associates as legal owners.

B.

Red flags and indicators relating to the PEP and his behavior

1. The PEP makes inquiries about the institution's AML policy or PEP policy.
2. The PEP seems generally uncomfortable providing information about source of wealth or source of funds.
3. The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries.
4. PEP is unable or reluctant to explain the reason for doing business in the country of the FIs/DNFBs.
5. PEP provides inaccurate or incomplete information.
6. The PEPs seek to make use of the services of a FIs/ DNFBs that would normally not cater to foreign or high value clients.

7. Funds are repeatedly moved to and from countries to which the PEPs do not seem to have ties with.
8. The PEP is or has been denied entry to the country (visa denial).
9. PEP is from a country that prohibits or restricts its/certain citizens to hold accounts or own certain property in a foreign country.

C.

PEP's position or involvement in businesses:

1. PEP has substantial authority over or access to state assets and funds, policies and operations.
2. PEP has control over regulatory approvals, including awarding licences and concessions.
3. PEP has the formal or informal ability to control mechanisms established to prevent and detect ML/TF.
4. The PEP (actively) downplays the importance of his/her public function, or the public function he is relates to associated with.
5. The PEP does not reveal all positions (including those that are ex officio).
6. PEP has access to, control or influence over, government or corporate accounts.
7. The PEP (partially) owns or controls FIs/ DNFBs, either privately, or ex officio.
8. PEP (partially) owns or controls the FIs/ DNFBP (either privately or ex officio) that is a counter part or a correspondent in a transaction. 9. The PEP is a director or beneficial owner of a legal entity that is a client of a FIs/DNFB.

D.

Red flags and indicators relating to the industry/sector with which the PEP is involved

1. Arms trade and Defense industry.
2. Banking and finance.
3. Businesses active in government procurement, i.e., those whose business is selling to government or state agencies.

4. Construction and (large) infrastructure.
5. Development and other types of assistance.
6. Human health activities.
7. Privatization.
8. Provision of public goods, utilities.

15.Breach of policy

Failure to abide by the institution AML /CFT policy leads to loss of confidence in the institution's integrity and fair dealing, severe impact on the institution shareholders, customers, and the relevant regulatory bodies, and market, and significant adverse publicity and reputational damage, even if no law was broken. As a result, management will take appropriate corrective action in the scope of laws, policies, and procedures when breaches of laws, rules and standards are identified that might include "Disciplinary Action

Staff members who become aware of breaches of this policy shall raise/escalate such breaches through the procedure laid down in the institution Code of Conduct.

16.Review of Policy

The Policy shall be reviewed as and when required or **once a year** to suit the needs of the NSBFMC and to comply with revised guidelines issued by the Regulator from time to time

Annex 1

Unique Identification Numbers (UINs) for each category of Investors

Type of Depositor	Type of Identification Document/Number to be Produced
Individuals	
Sri Lankan citizens	National Identity Card (NIC) and NIC Number **<u>Alternative documents</u>** Licensed banks and licensed finance companies can use a depositor's driving license or passport, which includes the NIC number, to open accounts. However, ***it is mandatory for these institutions to record the NIC number*** as the unique identification number of the depositor.
Sri Lankan Citizen (residing outside Sri Lanka/ Permanent Resident holders/Temporary Resident holders), Sri Lankan Dual Citizens (residing in or outside Sri Lanka)	NIC and NIC Number **<u>Exceptional circumstances</u>** The Sri Lankan Passport Number can be used only in the following instances when the NIC is not available, (a) the NIC has been temporarily surrendered by a depositor (b) a Sri Lankan is living overseas (c) the depositor left Sri Lanka prior to becoming a major and does not have an NIC In such scenarios, depositors are instructed to obtain their NICs as early as possible and update the same in the systems of licensed banks and licensed finance companies
Non-Sri Lankan citizens Includes - Foreign Nationals of Sri Lankan	Foreign Passport and Passport Number

origin (residing outside Sri Lanka), Foreign Nationals on temporary visit to Sri Lanka or intending to visit Sri Lanka and Foreign Diplomats.	
Minor Depositors (until obtaining the NIC	Birth Certificate: To record the Date of Birth followed by the Birth Certificate Number as the identification number until obtaining the NIC
Institutions	
Companies registered under the Companies Act	Company Registration Certificate and Company Registration Number
Non-Governmental Organizations	Registration Certificate issued by the National Secretariat for Non-Governmental Organizations and relevant Registration Number
Institutions registered under divisional/local government bodies such as Proprietorships/ Partnerships/Joint Ventures, etc.	Business Registration Certificate and Business Registration Number
An entity incorporated by an Act of Parliament	A copy of the initial Act of Parliament: To record the initial Act Number followed by Year of Incorporation
All other entities such as Clubs, Associations, Societies, etc.	Registration Certificate obtained from the relevant Authorities and relevant Registration Number. Alternative for unregistered entities Identification number obtained under the International Transaction Reporting System through a licensed bank is permitted to be recorded as the unique identification number for that specific entity

ANNEX 2

List High Risk Countries

- Myanmar (Burma)
- Nigeria
- Turkmenistan
- Ukraine
- Guatemala
- Cook Islands
- St Vincent &The Grenadines
- Russia
- Angola
- Zimbabwe
- Afghanistan
- Cuba
- Iraq
- Libya
- Azerbaijan
- Moldova
- Kazakhstan
- Georgia
- Uzbekistan
- Belarus
- Armenia
- Kyrgyzstan
- Tajikistan