PEOPLE'S BANK

POLICY & PROCEDURES

ON

ANTI MONEY LAUNDERING (AML)

AND

COMBATING OF FINANCING OF TERRORISM (CFT)

DECEMBER 2019

(VERSION 1.6)

CONTENTS

		Page Nos.
1	People's Bank Policy on Anti Money Laundering and Combating of Financing of Terrorism	04-06
2	Legal Framework for Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) in Sri Lanka	07-09
3	Financial Intelligence Unit Rule No. 01 of 2016- Financial Institutions (Customer Due Diligence) Rules	10-29
4	Applicability of FIU Rule No. 01 of 2016	30-33
5	Suspicious Transaction/ Business	34-39
6	Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) – Monitoring and Controls	40-41
7	Risk Categorization Methodology	42-43
8	Risk Management	44-45
9	Identification of Beneficial Owners	46-48
10	Politically Exposed Persons	49-51
11	Glossary	52-54
12	Attachments: i. Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 1 of 2018 ii. Guidelines for Financial Institutions on Suspicious Transactions Reporting No. 6 of 2018 iii. Guidelines on Identification of beneficial Ownership for Financial Institutions, No. 4 of 2018 iv. A list of categories of customers that can be considered as PEPs v. A list of Red Flags and Indicators for suspicion	

►*Introduction*

Money Laundering and Terrorist Financing undermine confidence in the International Financial System. The challenges in the fight against Money Laundering and Terrorist Financing are vast, and potential threats exist in every corner of the world. Regulators and Law Enforcement Agencies work hard to stay ahead of increasingly sophisticated criminals seeking to exploit the Global Financial System.

We at People's Bank are committed to the fight against Money Laundering and Terrorist Financing. As a leading Bank in Sri Lanka which has more than 735 Branches and maintaining over 22 Million customer accounts and processing thousands of transactions a day, People's Bank could always be a target for would be money launderers and terrorist financiers.

We believe that no customer relationship is worth compromising our commitment to combating money laundering and terrorist financing. To fulfill this commitment, we have established an independent unit; Compliance Department headed by a Chief Compliance Officer and has taken following steps:

- ✓ Appointed a Chief Compliance Officer who also functions as the Anti Money Laundering Compliance Officer
- ✓ Train employees in Money Laundering and terrorist Financing Prevention practices and controls.
- ✓ Develop systems to capture would be money launderers and terrorist financiers.

Also the intensity and extensiveness of the risk management function of the Bank 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 Bank.

The Bank also takes appropriate steps to identify, assess and manage its money laundering and terrorist financing risks in relation to its customers, countries, geographical areas, products, services, transactions and delivery channels.

The Central Bank of Sri Lanka together with the Financial Intelligence Unit (FIU) have issued directives named Financial Institutions (Customer Due Diligence) Rules requiring Banks 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. PEOPLE'S BANK POLICY ON ANTI MONEY LAUNDERING AND COMBATTING OF FINANCING OF TERRORISM

Banks and 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 Bank 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 Bank to identify adverse conditions, if any, associated with the applicant/customer (at the time of establishing banking relationship) and guard against criminals/fraudsters making use of banking channels/services for their nefarious activities.

With the present day multifarious dimensions of deliverance of banking services and products, the need for a structured methodology for understanding customers at the time of establishing banking relationship has assumed great importance.

A few steps taken at People's Bank in this regard are

- Establishment of a Compliance Department under the Chief Compliance Officer who is dedicated to the task of overseeing People's Bank's policies, practices and procedures with regard to ML & TF.

- Establishment of a culture that values and rewards the implementation of appropriate controls and compliance procedures.

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

- The Bank relies on those closest to its customers - the local Branch Manager 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 and technology that assists the Bank in monitoring transactions for the purpose of identifying possible suspicious activities.

- The Bank will continue to update its policies and procedures that meet or exceed applicable norms in the Banking Industry both locally and globally.

- Submitting reports on AML/ CFT risk on a quarterly basis to the Board of Directors to enable the Board to take necessary steps to mitigate the risk.

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

In line with the directives received, a policy document with following sections covering various functional aspects of KYC norms and Anti Money Laundering and Combating of Financing of Terrorism (AML & CFT) measures are 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 People's Bank
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 commonly 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

Money Laundering occurs in three stages -

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.

2. LEGAL FRAMEWORK FOR ANTI MONEY LAUNDERING (AML) / COMBATING OF FINANCING OF TERRORISM (CFT) IN SRI LANKA

For several years government authorities, the Central Bank, the Financial Sector Authorities and 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 ML & TF 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 Recommendations 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 following may commit the offence of Money Laundering-

  a. 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

b. Persons 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/ Banks) which are used by criminals to launder ill gotten money.

- Following are considered as Predicate Offences

  Offences under-
  - The Poisons, Opium and dangerous Drugs Ordinance
  - Laws or Regulations relating to 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 persons
  - 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.

- The 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 persons and entities. Currently this amount is Rupees One Million (Rs. 1,000,000/-) or its equivalent.

- All suspicious transactions have to 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 an unlawful activity.

- In terms of the FTRA, institutions are required to engage in Customer Due Diligence (verifying the true identity of customers) with whom they undertake transactions and on going 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, persons 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 OF TERRORIST 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 banking 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 operation of banking 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 Bank 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 no face to face, cross- border) and
- Any other information regarding the customer.

✓ The Bank shall, using the AML system in place verify whether any prospective customer or beneficiary appears on any list of designated persons or entities issued under the regulations made in terms of United Nations Act No.45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism & terrorist financing and proliferation of weapons of mass destruction and its financing or whether such prospective customer or beneficiary acts on behalf of or under the direction of such designated persons or entities or for the benefit of such designated persons or entities .

✓ 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 Bank 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 Bank shall be affiliated and integrated with the overall risk management of the Bank.

✓ The Bank shall 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 a 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 in either internally or externally and its potential impact to the Bank
- Recent developments in written laws on money laundering and suppression of terrorist financing and its implications for the Bank.

CDD for All Customers

➢ The Bank 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 transferrable without the knowledge of the Bank and accounts that are operated and maintained with the account holder's name only.

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

- The Bank shall conduct the CDD measures specified in Rule No. 1 of 2016, on customers conducting transactions when

  a. Entering into business relationships;
  b. Providing money and currency changing business for transactions involving an amount exceeding Rs. 200,000/- or its equivalent in any foreign currency;
  c. Providing wire transfer services;
  d. Carrying out occasional transactions involving an amount exceeding Rs. 200,000/- or its equivalent in any foreign currency where the transaction is carried out in a single transaction or in multiple transactions that appear to be linked;
  e. The Bank has any suspicion that such customer is involved in money laundering or terrorist financing activities, regardless of amount; or
  f. The Bank has any doubt about the veracity or adequacy of previously obtained information.

- 1. The Bank shall-
  a. Identify its customers prior to entering into 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 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 Bank shall take enhanced CDD measures for such customer, in addition to the CDD measures stated above.

- If the customer is not a natural person, the Bank shall 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 Bank shall identify the natural persons who act on behalf of the customer and verify the identity of such persons. 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 Bank 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 Bank to satisfy itself that the Bank knows who the beneficial owner is.

- The Bank shall verify the identity of the customer and beneficial owner before or during the course of entering into 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 of the Bank and verification is not possible at the point of entering into the business relationship, the Bank may, subject to the below provision, allow its customer and beneficial owner to furnish the relevant documents subsequent to 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 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 shall be essential so as not to interrupt the normal conduct of business of the Bank; and
  c. No suspicion of money laundering or terrorist financing risk shall be involved.

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

- The Bank shall take the 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 chapter 4 of this Policy.

- If the Bank is unable to act in compliance with the above, it shall
  a. In relation to a new customer, not open the account or enter into 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 Bank 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 Bank 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.

- i. The Bank 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.

  ii. 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 Bank shall report transactions inconsistent with the rules stated in Rule No 1 of 2016 to the Chief Compliance Officer for appropriate action.

- The Bank 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 Bank 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 commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profiles and nature of transactions.

- The Bank shall increase the number and timing of controls applied and select patterns of transactions that need further examination when conducting enhanced CDD.

- The Bank shall 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 Bank may consider the following-

  a. The nature and circumstances surrounding the transaction including the significance of transaction;
  b. Any material change 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.

- The Bank shall conduct CDD on existing customer relationships at appropriate times, taking into account 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 Bank 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 Bank shall terminate conducting the CDD measures and proceed with the transaction and immediately file a suspicion transactions report.

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

- The Bank shall

  a. With regard to transactions or series of linked transactions exceeding Rs.200,000/- or its equivalent in any foreign currency conducted by occasional customers, one off customers or walk in customers conduct CDD measures and obtain copies of identification documents;
  b. With regard to occasional customers, one off customers or walk in customers who wish to purchase remittance instruments such as pay orders, drafts exceeding Rs.200,000/- or its equivalent in any foreign currency conduct CDD measures and obtain copies of identification documents;

c. With regard to all cash deposits exceeding Rs.200,000/- or its equivalent in any foreign currency made into an account separately or in aggregate by a third party customer, have on record the name, address, identification number of a valid identification document, purpose and the signature of the third party customer.

Under this rule, clerks, accountants, employees, agents or authorized persons of business places who are authorized to deal with the accounts shall not be considered as a third party.

Also, if the Bank has reasonable grounds to suspect that the transaction or series of linked transactions are suspicious or unusual, the Bank shall, obtain such information irrespective of the amount specified above.

CDD for Legal Persons and Legal Arrangements

- The Bank 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.

- In order to identify the natural person if any, who ultimately has control ownership interest in a legal person, the Bank 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 Bank shall identify the natural person who controls the legal person.

- In order to identify the beneficial owners of a legal arrangement, the Bank shall 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 persons in equivalent or similar positions.

Non Governmental Organizations, Not for Profit Organizations or Charities

- The bank shall conduct enhanced CDD measures when entering into 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. The Bank 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. The Bank 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.

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

- 1. The Bank shall review and monitor all existing relationships of a 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 Bank 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 Bank shall apply the 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 Defence has been assigned, as the case may be, shall specify the high risk countries referred above-

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

  ii. independently taking into account, 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. Upon specifying the high risk countries as specified in (ii) above the Bank shall publish the list of high risk countries in its official website.

  iv. 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 Bank shall apply appropriate counter measures, 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-

    a. 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.

Politically Exposed Persons (PEPs)

Guideline No. 3 of 2019 issued by Financial Intelligence Unit of Central Bank of Sri Lanka which shall be read together with the Financial Transactions Reporting Act No 6 of 2006 and Financial Institutions (Customer Due Diligence) Rules No 1 of 2016 provides the Banks with a set of instructions on the definition, identification, reviewing and managing the risk associated with PEPs. Accordingly the Bank has taken steps to identify and mitigate the risk associated with PEPs.

- In relation to politically exposed persons or their family members and close associates, the Bank shall-

    a. Implement appropriate internal policies, procedures and controls to determine if the customer or the beneficial owner is a politically exposed person;
    b. Obtain approval, before or after entering into the relationship from the Deputy General Manager (Channel Management) of the Bank to enter into or continue business relationships where the customer or a beneficial owner is a politically exposed person or subsequently becomes a politically exposed person;
    c. Identify, by appropriate means, the sources of funds and wealth or beneficial ownership of funds and wealth; and
    d. Conduct enhanced ongoing monitoring of business relationships with the politically exposed person.

- The Bank is aware that business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves and also that the definition is not intended to cover middle ranking or more junior officials in the foregoing categories.

Correspondence Banks

- The Bank when providing correspond banking services to respondent banks the correspondent bank shall take necessary measures to ensure that the risk of money laundering and terrorist financing through the accounts of the respondent banks are duly managed.

    Accordingly, the bank shall assess the suitability of the respondent bank by taking the following measures;

(a) gather adequate information about the respondent bank to thoroughly understand the nature of the respondent bank's business, including the following:-

(i) internal policy of the respondent bank on anti-money laundering and suppression of terrorist financing;

(ii) information about the respondent bank's management and ownership;

(iii) core business activities;

(iv) Country of geographical presence, jurisdiction or country of correspondence;

(v) Money laundering prevention and detection measures;

(vi) The purpose of the account or service;

(vii) Identity of any third party that will use the correspondent banking services (*i.e.* in case of payable through account);

(viii) The level of the regulation and supervision of banks in the country of the respondent bank.

(b) Determine from publicly available sources, the reputation of the respondent bank, and as far as practicable, the quality of supervision over the respondent bank, including facts as to whether it has been subject to money laundering or terrorist financing or regulatory action;

(c) Assess the respondent bank's anti-money laundering and suppression of terrorist financing systems and ascertain whether they are adequate and effective, having regard to the anti-money laundering and suppression of terrorism financing measures of the country or jurisdiction in which the respondent bank operates;

(d) Clearly understand and record the respective anti-money laundering and suppression of terrorist financing responsibilities of each bank; and

(e) Obtain approval of the Board of Directors or a Committee appointed by the Board of Directors of the respondent bank, before entering into new correspondent banking relationships.

- The bank shall in relation to "payable-through accounts", satisfy itself that the respondent bank-

(a) Has conducted CDD measures on its customers that have direct access to the accounts of the correspondent bank; and

(b) Is able to provide relevant CDD information upon request to the correspondent bank.

- The bank shall apply enhanced CDD measures when entering into or continuing correspondent banking relationship with banks or Financial Institutions which are located in high risk countries.

- The bank shall not enter into or continue correspondent banking relationship with a shell bank.

  When providing correspondent banking services, the bank shall take appropriate measures to satisfy itself that its respondent Financial Institutions do not permit their accounts to be used by shell banks.

Wire Transfers

- The Bank shall in processing wire transfers, take freezing action and comply with prohibitions on conducting transactions with designated persons or entities, and any other person and entity who acts on behalf of or under the direction of such designated persons or entities or for the benefit of such designated persons or entities, in terms of any regulation made under United Nations Act No.45 of 1968, giving effect to United Nations Security Council Resolutions on targeted financial sanctions related to terrorism and terrorist financing and proliferation of weapons of mass destruction and its financing or in terms of any other regulation made under the said Act giving effect to any other United Nations Security Council Resolution.

- The Bank shall preserve Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages that accompany inward remittances for a period of 12 years from the date of transaction.

- The Bank shall ensure that all cross-border wire transfers having a value more than or equal to rupees one hundred thousand or its equivalent in any foreign currency to be always accompanied with the following :-

(a) Originator information :-

  (i) name of the originator;

  (ii) originating account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction; and

  (iii) originator's address, national identity card number or any other customer identification number as applicable;

(b) beneficiary information : -

  (i) name of the beneficiary; and

  (ii) beneficiary account number where such an account is used to process the transaction or in the absence of an account, a unique transaction reference number which permits traceability of the transaction.

- Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable

within the beneficiary country and shall include the originator's account number or unique transaction reference number.

- The Bank shall verify the information pertaining to its customer where there is a suspicion of money laundering and terrorist financing risk.

- In the case of domestic wire transfers, the Bank shall ensure that the information accompanying the wire transfer includes originator information as indicated for cross-border wire transfers unless such information can be made available to the Beneficiary Financial Institution and appropriate authorities by other means.

- In the case where the information accompanying the domestic wire transfer can be made available to the Beneficiary Financial Institution and appropriate authorities by other means, the Bank shall include the account number or a unique transaction reference number, provided that any such number will permit the transaction to be traced back to the originator or the beneficiary.

  (2) The Bank shall make the information available as soon as practicable after receiving the request either from the Beneficiary Financial Institution or from the appropriate authority.

- The Bank shall maintain all originator and beneficiary information collected, in accordance with the Act.

- At instances where the requirements specified above could not be complied with the Bank shall not proceed with the wire transfer unless directed to do so by the Financial Intelligence Unit and shall consider reporting the relevant transaction as a suspicious transaction to the Financial Intelligence Unit.

Intermediary Financial Institution

- The Bank 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 Bank shall keep a record, for at least twelve years, of all the information received from the ordering Financial Institution or another Intermediary Financial Institution.

- The Bank 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 Bank 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 Bank 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 Bank 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 Bank 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; and

  (b) what is the appropriate follow up action

Money or Value Transfer Service Providers

- When conducting Money or Value Transfer Service (hereinafter referred to as "MVTS") the Bank shall maintain a current list of its agents in all countries in which the MVTS provider and its agents operate.

- The Bank if agents are used shall include them in its internal policy on Anti-money Laundering or Suppression of Terrorist Financing and monitor them in compliance with that policy.

- At instances where any amendments take place in the list of Agents those amendments will be circulated through Internal Circulars.

- The Bank shall comply with the provisions applicable for CDD in wire transfers, when operating directly or through their agents in Sri Lanka, or shall comply with similar requirements issued by a relevant authority, when operating directly or through its agents in a foreign country.

- When the Bank controls the ordering customer as well as the beneficiary customer of a wire transfer, shall –

  (a) take into account all relevant information from the ordering customer and the beneficiary customer, in order to determine whether a suspicious transaction report needs to be filed; and

  (b) file a suspicious transaction report with the Financial Intelligence Unit, on identifying a suspicious wire transfer.

- 1. The Bank shall follow special precautionary measures to make a distinction between formal money transmission services and other alternative money or value transfer

systems (ex: hundi, hawala etc.) through which funds or value are moved from one geographic location to another, through informal and unsupervised networks or mechanisms.

2. The Bank shall take reasonable measures to ascertain the sources of funds involving any such alternative money or value transfer system and file a suspicious transaction report with the Financial Intelligence Unit.

B. Account Opening Guidance

1. **Individual Customer**

(a) The following information shall be obtained:

(a1) In the case of all customers

- Full name as 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 as 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; and

(a2) In the case of non- resident customers

- The reason for opening the account in Sri Lanka
- Name, address and the copy of passport of the person or persons authorized to give instructions

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

- Copy of identification document;
- Copy of address verification document;
- Copy of the valid visa/permit in the case of accounts for non national customers.

2**. 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 the 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.

3. 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 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 as the case may be;
- 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.

4. 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 address as 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 be 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.

➢ Bank 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.

5. 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 be verified against the original

- Copy of the Trust Deed as applicable;
- Particulars of all individuals.

6. Stocks and Securities Sector specific requirements

(a) 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/ manger 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 applicant-

- 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 b submitted together with a Declaration from the Global Custodian that a custody arrangement or agreement exist between the Global Custodian and Beneficiary.

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 interview.

C. <u>General Provisions</u>

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

4. Frequently design and implement suitable training programmes for relevant employees including Board of Directors, in order 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 of the Bank and its compliance with regulatory requirements.

6. Implement group wide programmes which shall be applicable and appropriate for all branches and majority owned subsidiaries with a view of combating money laundering and terrorist financing activities and shall include following in addition to the rules set above.
   - ✓ Initiate measures and procedures for sharing information required for the purpose of conducting CDD and money laundering and terrorist financing risk management;
   - ✓ Provide information of customers, accounts and transactions and of audits, with group level compliance from all branches and subsidiaries of the financial group when necessary for implementing the suppression of money laundering terrorist financing measures and
   - ✓ Maintain adequate safeguards on the confidentiality and use of information exchanged among the branches and subsidiaries of the financial group.

7. The Bank 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.

8. The Bank 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 and
   - ✓ Monitor pre-loading of credit cards, as that may amount, inter-alia, to the abuse of credit cards, for money laundering or terrorist financing purposes, file a Suspicious Transaction Report if suspicious transactions are detected.

D. <u>Record Keeping</u>

9. The Bank shall maintain all records of transactions, both domestic and international, including the results of any analysis undertaken, such as inquiries to establish the background and purpose of complex, unusually large transactions for a minimum period of twelve years from completion of such transaction.

10. The records shall be sufficient to permit 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 so as 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 process 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 twelve years commencing from the date on which the business relationship was fulfilled or the occasional transaction was effected.

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

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

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

For the purpose of 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; and
c. Any authority receiving reports on cross border transportation of currency.

15. The Bank shall train the staff on all issues related to AML/CFT. The training shall be provided for all staff upon joining and after that once in every two years. Apart from general training provided to all staff, targeted training programs shall be conducted for specific categories of staff. Also AML/ CFT training shall be conducted for members of Board of Directors.

E. Miscellaneous

16. In the case of a prospective customer whose permanent address given in the application is at a location far away from that of the branch which receives the account opening request, the Bank shall discourage or turn down the request to open the account and shall request the prospective customer to open the account at the closest branch to the residence or business of the customer, unless an acceptable and a valid reason is given to keep in record.

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

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

19. Copies of all identification and address verification documents shall be retained in terms of the law.

20. When instructions are received from clients to transfer funds from one account to another both account numbers shall be recorded internally to aid future reference.

21. When Foreign Currency Accounts and temporary rupee accounts are opened for non-nationals/foreign passport holders who are resident in Sri Lanka, a local address shall be obtained as their permanent address during their stay in the Island. A copy of the passport, visa with validity period, foreign address and the purpose for which the account is opened shall be made available in the file. On the expiry of the visa, the account shall cease to operate unless and otherwise appropriate instructions are received. On leaving

the Island the account shall either be closed or be converted into a non-resident account. The Bank shall ensure that a valid visa is held at all times by the clients during the continuation of the account with them.

22. When Rupee Accounts are opened and maintained for non-residents (foreign passport holders), the foreign address shall be used as the permanent address and for all correspondence. The reason for choosing to open the account in a foreign jurisdiction shall be recorded in the file.

23. All cash deposits made into savings and current accounts over Rs.200,000/= by third parties shall have on record, the identity of the depositor. The required details are, the name, address, Identification number of a valid identification document, purpose and the signature. However, clerks, accountants and employees of business houses who are authorized to deal with the accounts shall not be treated as "third parties".

24. The Bank shall ensure that no Automatic Teller Machine (ATM) withdrawals exceeding the mandatory threshold are made without the expressed approval of the Bank. If regular withdrawals are made by customers in small amounts in order to circumvent the reporting limit, they shall be reported as a suspicious transaction. The Bank shall exercise due diligence to prevent any misuse of this facility. This is applicable to both rupee accounts and foreign currency accounts.

25. Accounts which record frequent transactions below the threshold limit of Rs.1,000,000/= in an attempt to circumvent the mandatory reporting requirement, shall be reported to the Chief Compliance Officer for appropriate action.

26. The Bank will ensure that account activities are consistent with the customer profile on record. Any inconsistency shall be inquired into and the correct position recorded. All unexplainable activities shall be reported to the Chief Compliance Officer for appropriate action.

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

The Guideline No.1 of 2018 issued by Financial Intelligence Unit on Money Laundering & Terrorist Financing Risk Management for Financial Institutions is attached.

4. APPLICABILITY OF FIU RULE NO. 01 OF 2016

This section of the Policy is to ensure that People's Bank has internally developed effective Anti Money Laundering and Combating of Financing of Terrorism procedures to reduce the risk of the Bank being used in money laundering transactions, in addition to the requirements of the legislation and the FIU Rule No. 1 of 2016 as set out in Chapter 3.

It is the policy of the Bank 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 Bank being unwittingly involved in the activities of third parties, who may seek to use bank facilities to hide the source of criminal funds.

As such,

- ✓ The Bank 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 banking 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.

Additionally, FIU Rule No. 01 of 2016 also provides for the update of the existing customer records in accordance with the CDD rules and acting in compliance with this rule, Regional Managers/ Department Heads are required to submit a monthly status report of same to the Compliance Department. Compliance Department shall submit a Board Paper to the Board of Directors.

Capture the information required under the rules of the Financial Intelligence Unit

In order to comply with the requirements in Direction No. 01 of 2016, it is necessary to obtain KYC Information for all Accounts opened at the branches.

The following are the broad guidelines in this regard:

1. **Individual/Joint Accounts**

   a) The individual Account opening/Mandates and information profile of the customers (KYC Form) which is prepared incorporating the basic requirements should be duly completed by the Customer/s and also 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 Manager, after perusing all account opening documents must sign the mandate certifying the accuracy of the documents obtained.

   b) The Operations Manager/ Branch Manager 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 Operations Manager/ Branch Manager.

The branch network is also required to monitor the transactions of

- high risk customers at every transaction,
- medium risk customers as and when necessary and
- low risk customers if a suspicious transaction takes place

c) The Departments/ branch network are required to retain and keep in the custody of the Bank-

- 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 document specified in Chapter 3.

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

a) The Account opening Form/Mandate and the KYC must be obtained for these customers and they should be filled 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**
02 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 have to be retained by the Bank.

d) The Operations Manager/ Branch Manager 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. This has been communicated through the Chief Compliance Officer's Circular Letter No.6552/2007 dated 4th September 2007 and Compliance Officer Circular Letter Nos. 6552/2007(1) dated 24.8.2012 and 6552/2007(2) dated 15.3.2016.

2. It is the responsibility of the Regional Managers, Branch Managers and Heads of Department to educate employees coming under their purview of the importance of KYC and CDD and the requirements on Customer Identification. Special emphasis must be made to train the Account Opening Officers in this regard. An e-learning module has been included in the Intranet of the People's Bank and all Department Heads and Branch Managers shall ensure that all operational and Front Office staff has gone through same and are familiar with the provisions therein.

3. A Certificate on Compliance with the procedures contained in this Policy; would need to be submitted by the Branch Managers to the Chief Compliance Officer, on a monthly basis.

4. The following important provisions are further highlighted:

   i) Satisfactory reference has to be obtained for all Current Accounts. For other accounts, it will be at the discretion of the Branch/ Operations Manager 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:

   The following exception procedures are laid down where compliance has not been possible, with the above.

   a) It may be acceptable to allow minor accounts to be opened pending completion of KYC requirements on documentation, within 3 months of opening the account.

   b) Where such accounts have been opened as in (a) above, they have to be recorded in a Register called the KYC Exception Register and it shall be initialed by the Branch Manager on a daily basis and on Branch inspection visits by the Regional Compliance Officer. A summary of such accounts opened with current status should be submitted to the Regional Compliance Officer on a monthly basis. The Regional Compliance Officer should collate these and submit a Quarterly Report to the Chief Compliance Officer.

   c) Outstanding KYC documentation should be obtained before the expiry of 3 months from the date of the opening of such account – in order to continue the account.

   d) Where such accounts have been opened, funds should not be paid out of the account, until such time as the KYC documentation is completed.

e) In the event the KYC cannot be successfully completed in 3 months, the account should be closed and the funds returned to the source from which they were received in the same manner the deposit was made.

iii) It shall be the duty of the In-House Auditor of each Branch to check on the status of documentation for all new accounts opened on a daily basis and enter variances and exceptions in a Register to be maintained for this purpose. This will be subjected to audit by the Internal Audit Department and the Compliance Department of the Bank

5. 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;
or

(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 Bank 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 Bank to train its officers employees and agents to recognize suspicious transactions.

The Bank has put up an AML system with rules/ scenarios to identify suspicious transactions. All alerts generated by the system shall be evaluated by the Compliance Department and if necessary forwarded to the branches for their feedback. The branches shall send their feedback to Compliance Department and the Compliance Department shall file the Suspicious Transaction report accordingly.

Whilst all unusual transactions are not automatically linked to Money Laundering, unusual transactions become suspicious if they are considered inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account.

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 particular 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 cash deposits made by an individual or a company whose normal business activities would mainly be conducted by cheques or other instruments.

2. Substantial increase in cash deposits by any customer or the Bank without an apparent cause, especially if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customers.

3. Customers who deposit Cash in numerous stages so that the amount of each deposit is small, but the total of which is equal to or exceeds the reporting threshold amount.

4. Customer accounts whose transactions, both deposits and withdrawals are mainly conducted in cash rather than in negotiable instruments (e.g. cheques, letters of credit, draft etc.) without an apparent reason.

5. Customers who constantly pay-in or deposit cash to cover requests for Bankers drafts, money transfers or other negotiable instruments without an apparent reason.

6. Customers who seek to change large quantities of lower denomination bank notes for those of higher denomination banknotes with no obvious reasons.

7. Customers who transfer large sums of money outside the country with instructions for payment in cash, and large sums transferred from outside the country in favour of non-resident customers with instructions for payment in cash.

8. Unusually large cash deposits using "ATMs" or "Cash Deposit Machines" to avoid direct contact with the employees of the relevant license, if such deposits are not consistent with the business/normal income of the concerned customers.

Suspicious Transactions using Customers' Accounts

1. 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 persons.

2. Customers who have numerous accounts and pay-in 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 banking relationships with banks which extend them facilities from time to time.

3. 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).

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

5. Paying-in large third party cheques endorsed in favour of the account holder when they do not seem to be relevant to the account holder and his nature of business.

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

7. A large number of individuals who deposit monies into the same account without an adequate explanation.

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

Suspicious Investment Related Transactions:

1. Purchasing of securities to be held by the Bank in safe custody, where this does not appear appropriate given the customer's apparent standing. (Financial income etc.)

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

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

Suspicious Transactions using Electronic Banking Services

1. When an account receives numerous small fund transfers electronically, and then the account holder carries out large transfers in the same way to another country.

2. Where a customer makes regular and large payments using different means including, electronic payments that cannot be clearly identified as bona-fide transactions, or receive regular and large payments from countries known for serious criminal activities.

3. Where transfers from abroad, received in the name of a customer of the bank or any financial institution electronically are transferred abroad in the same way without passing through an account (i.e. they are not deposited then withdrawn from the account). Such transactions should be registered in the account and should appear in the account statement.

Suspicious International Banking and Financial Transactions

1. Customers introduced by a branch outside the country, and affiliate or another bank, based in one of the countries known for the production or consumption of drugs or other serious criminal activities.

2. Building up of large balances not consistent with the known turnover of the customer's business and the subsequent transfer to account(s) held abroad.

3. Frequent requests for foreign currency drafts or other negotiable instruments, for no obvious reasons.

4. Frequent paying-in of foreign currency drafts in large amounts for no obvious reasons, particularly if originating from abroad.

Suspicious use of Letters of Credit (LC)

1. Where the applicant of LC (customer of bank) and the beneficiary of LC are same individuals/ entities.

2. Where the Bank's customer who opens these letters is the beneficiary and the owner of the shipping company.

3. Where amounts on letters of credit submitted by the customer to the bank and to the Customs/Ports/Airport authorities do not match the original.

4. Where the size of the facilities are not in line with the securities on hand, nature of business and net-worth of the customers.

5. Where such trade is not consistent with the customer's usual business.

Suspicious Loan Transactions:

1. Customers who repay classified/problem loans before the expected time and in larger amounts than anticipated.

2. Customers who request loans against assets held by the financial institutions or third party, where the origin of these assets is not known, or the assets are inconsistent with the customer's standing.

3. Non-resident individuals who request loans secured by bank guarantees issued by foreign banks where the purpose of the transaction is questionable.

4. Loan transactions against pledge of deposits with financial institutions outside the country, especially if these were in countries known for the production, processing or consumption of drugs or other criminal activities.

Recognizing & Reporting Of Suspicious Transactions

In accordance with the local and international norms it is an offence to fail to report a suspicion of Money Laundering or Terrorist Financing. Failure to report such circumstances is punishable on conviction by heavy fines and/or imprisonment.

Reporting
In the first event of your suspicion:

- The staff concerned should report the same immediately to the immediate superior to ensure that there are no known facts which would negate the suspicion.

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 law also requires the Bank 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 Bank has put in place procedures to report suspicions with supporting information,

i. Through the format issued to the branch network.
ii. Through the AML system 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 Chief Compliance Officer on receiving the Report

At the Bank,

- When the Chief Compliance Officer receives the Suspicious Transaction Report, (STR) the Chief Compliance Officer will decide whether the report gives rise to knowledge or suspicion that a customer is involved in money laundering.
- if the Chief Compliance Officer believes that the suspicions may be justified and require further investigation, must report to the Financial Intelligence Unit (FIU)

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

The employee has a duty to assist the Chief 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 are
- contains accurate information
- is timely and not delayed

The importance of timing

The Bank 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 Chief 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 Bank cannot ask the customer for an explanation, or continue to provide them with a normal customer service. But it does mean that the Bank must do so without alerting them to the fact that the Bank may or had already notified the Authorities. If customers being investigated are alerted, the Bank 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.

The Guideline No.06 of 2018 issued by Financial Intelligence Unit on Suspicious Transactions Reporting is attached.

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

CHIEF COMPLIANCE OFFICER

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

Responsibilities of the Chief Compliance Officer

- Implement Anti Money Laundering and Combating of Financing of Terrorism Policy of the Bank 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 departments/ branches 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 'recognising suspicious transactions/business')

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

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

  a) Provide feedback to staff on compliance queries.

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

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

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

Independent Compliance Testing

Bank has entrusted Regional Compliance Officers with the responsibility to test the implementation and adherence of the AML & CFT Policy of the Bank. The findings/recommendations should be reported directly to the Chief Compliance Officer. In addition the Compliance Department also carries out random assessments and reviews to verify among other things the implementation and adherence of theAML & CFT Policy in the Bank and report any non-compliances to the Board Integrated Risk Management Committee.

Record Keeping Obligations

In addition to regular bank record keeping requirements, the Anti Money Laundering and Combating of Financing of Terrorism Policy of the Bank requires that documents concerning customer identification and records relating to transactions undertaken on behalf of customers/non customers (all transactions including cash, wire transfers, purchases/sale of monetary instrument etc) be maintained as follows:

- In the case of records that were in existence on 4.8.2016- for a period of not less than ten years from that date.
- In the case of new records created after 4.8.2016- for a period of not less than twelve years from the date of creating the record.

It is also required that :

a) All anti-money laundering and combating of terrorist financing monitoring reports made by Chief 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 persons promptly on request without undue delays.

7. RISK CATEGORIZATION METHODOLOGY

From the information provided by the customer the Bank 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 customer 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 bank reference regarding the customer and the customer contact with the Bank;
- 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 updation of identification data of customer and Beneficiary owner
- Obtaining additional information on nature of business
- Obtaining information on reasons for transactions performed
- Obtaining information on source 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 Non executive –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 a large number of 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 categorised 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 Bank is poor/adverse shall be categorised as high risk.

Examples:

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

Based on the above a KYC Risk categorization Form has been prepared and this document is required to be filled by the Operations Manager/Branch Manager for all accounts opened and attached to the Account Opening Form.

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 – Annually

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

8. 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 Bank.

- By the very nature of its functioning, banks are 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 banks should know its customers, particularly their identity preferably at the time of establishing banking 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 bank against financial frauds and Money Laundering & Terrorist Financing. The bank resolves that the KYC requirements shall be realised 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 Banking 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 banks to check/reduce operational risks and also vulnerability to frauds.

- The bank 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 bank shall continue to ensure that compliance to KYC guidelines is evaluated periodically in the background of the conditions obtained in respect of the bank'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 monthly.

- The Bank 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 branches and other operational units of the Bank.

Training to Staff members (KYC/ AML/ CFT)

- The bank shall ensure that the training sessions on KYC guidelines and AML & CFT procedures are included in the Training Calendar on an ongoing basis. The Bank 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 bank's focussed endeavour to make all those concerned fully understand the rationale behind the KYC/AML & CFT procedures and implement them consistently.

- The Bank'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 detect 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 KYC/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 Branch 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 bank shall publish this Policy in the Bank's web-site and place a copy of the same in all branches/offices 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 upon 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 Bank shall endeavour to guard against denial of banking services to general public especially to those who are financially/socially under-privileged due to the implementation of Customer Acceptance Procedures on too restrictive basis.

9. IDENTIFICATION OF BENEFICIAL OWNERS

The Bank shall take steps to determine the ultimate beneficial owners of legal persons and legal arrangements and when a natural person is identified, he should be treated as the beneficial owner unless there are reasonable grounds to show that he is acting on behalf of another person or if another person is the beneficial owner of the property of the customer.

1. The Bank shall take steps to identify the beneficial owner of a legal person considering three main facts stated below and it shall not be necessary to fulfill all three factors to be a beneficial owner.

    - Who are the natural person/s who own or control more than 10% of the customer's equity?
    - Who are the natural person/s who has effective control of the Legal Person?
    - On behalf of which natural person/s is the transaction being conducted?

2. At instances where the ownership is divided among large number of individuals and the shareholding percentage of every individual is less than 10%, the Bank 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.

3. The Bank 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.

4. Bank 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.

5. The Bank shall take all reasonable measures to verify the identity of the beneficial owner/s using information obtained from reliable sources in order to obtain sufficient information to confirm who the beneficial owner/s is.

6. The identification that shall be obtained are as follows;
    - full name
    - official personal identification or any other identification number
    - permanent/ residential address

7. The Bank 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.

8. Furthermore, the Bank shall take steps to identify the beneficial owners through following means;
    - Share Register
    - Annual Returns
    - Trust Deed
    - Partnership Agreement
    - Constitution and/ or Certificate of Incorporation

- Constitution of a registered co-operative society
- Minutes of the board meetings
- Information that can be obtained by open source search or commercially available databases.
- Verification through mother company or branches, Correspondence Bank, other agents of the Bank, Corporate Registries etc. (for foreign legal persons & arrangements)
- Relevant identification information available from reliable sources such as public registers (for Companies listed in Stock Exchange)

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

10. The Bank shall review the adequacy of information in respect of beneficial owners on a annual basis through obtaining information from the existing core-banking system of the Bank.

11. 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

12. 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 relationship
- there is no suspicion of money laundering or terrorist financing risk involved
- delay will not interrupt the normal conduct of business

13. When delayed verification is allowed the Bank 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.

14. The Bank 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.

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

16. The Bank shall maintain records of identification and verification relating to beneficial ownership for a period of twelve (12) years as stated above.

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

Guidelines on Identification of Beneficial Ownership for Financial Institutions, No. 04 of 2018 are attached.

10. 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 step-children and adopted children) and their spouses;
iv. parents (including step-parents);
v. grand children and their spouses

Close associates of PEPs or their family members 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, in particular, persons acting in a financial fiduciary capacity.

Identification of PEPs

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

3. The Bank 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 Bank shall gather sufficient information to understand the particular 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 Bank shall identify the beneficial owners and take reasonable measures to verify the identity of the beneficial owners of legal persons 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 Bank shall verify if the beneficial owner is a PEP.

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

8. The Bank 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 Bank shall take steps to identify PEPs through
   a. Commercial data Bases
   b. Internally maintained data bases
   c. Publicly available registries of persons, in case of foreign PEPs
   d. Ad-hoc customer researches
   e. Self declarations obtained from customers (subject to verification)

- The Bank 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 customer's PEP status;
   d. whenever the Bank becomes aware, through any means, of the need for such an update.

- The Bank shall
    a. Obtain approval from Deputy General Manager- Channel Management 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 Bank 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.

- If the level or type of activity in the business relationship is different from what can be reasonably explained, the Bank shall conduct a further assessment to verify whether the Bank can
    a. continue with or terminate the business relationship; or
    b. should file a suspicious transaction report with FIU.

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

- When deciding to undertake a business relationship with a PEP the Bank shall ensure that the senior management involved
    a. have full knowledge and understanding of the AML or CFT internal control programs of the Bank;
    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 Bank.

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

A list of categories of customers that can be considered as PEPs and a list of Red Flags and Indicators for suspicion are attached.

GLOSSARY

Beneficiary –

A person to whom or for whose benefit the funds are sent or deposited in or paid to a Financial Institution and may include a beneficiary Financial Institution.

Beneficiary Financial Institution –

An institution which receives wire transfers from the ordering institution directly or through an intermediary institution and makes the funds available to the beneficiary customer.

Beneficial Owner –

A natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a legal person or a legal arrangement.

Board of Directors –

In relation to a Financial Institution incorporated outside Sri Lanka means the senior management authority of such Financial Institution.

Customer –

In relation to a transaction or an account includes –

(a) The person in whose name a transaction or an account is arranged, opened or undertaken;
(b) A signatory to a transaction or an account;
(c) Any person to whom a transaction has been assigned or transferred;
(d) Any person who is authorized to conduct a transaction; or
(e) Such other person as may be prescribed.

Correspondent Banking –

Provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank) including cash management (*eg:* large international banks frequently act as correspondent banks for large number of other banks around the world by providing a wide range of services such as interest-bearing accounts in a variety of currencies, international wire transfers, cheque clearing, payable-through accounts and foreign exchange services).

Close Associate Includes –

(a) A natural person having joint beneficial ownership of legal entities and legal arrangements, or any other close business relationship; and
(b) A legal person or legal arrangement whose beneficial owner is a natural person and is known to have been set up for the benefit of such person or his immediate family members.

Controlling Interest –

An interest acquired by providing more than ten percent (10%) of the capital of a Financial Institution.

Company Act –

The Companies Act No.7 of 2007.

Existing Customer –

A customer who has commenced a business relationship on or before these rules come into force.

Financial Action Task Force –

An independent inter-governmental body that develops land promotes policies to protect the global financial system against money laundering, terrorist financing and the financing for proliferation of weapons of mass destruction.

Financial Group –

A group of companies that consists of a parent company or other type of a legal person, exercising control and coordinating function over the rest of the group, for the application of group supervision under the anti-money laundering and suppression of terrorist financing policies and procedures, together with branches and subsidiaries that are subject thereto.

Finance Company –

A company licensed under the Finance Business Act No. 42 of 2011.

Immediate Family Member –

Includes the spouse, children and their spouses or partners, parents, siblings and their spouses and grandchildren and their spouses.

Intermediary Financial Institution –

An institution in a payment chain that receives and transmits a wire transfer on behalf of the Ordering Financial Institution and the beneficiary institution, or another intermediary institution.

Legal Person –

Any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association.

Legal Arrangement –

Includes an express trust, a fiduciary account or a nominee.

Licensed Bank –

Any commercial bank and specialized bank, licensed under the Banking Act No. 30 of 1988.

Majority- owned subsidiary –

A subsidiary of a group of companies of which fifty *percent* or more of the shares of the group of companies are owned by the parent company.

MVTS –

Financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message transfer or through a clearing network to which the relevant financial service provider belongs. Transactions performed by such service may involve one or more intermediary transactions and a final payment to a third party and may include any new payment methods.

Money Laundering –

The offence of money laundering in terms of section 3 of the Prevention of Money Laundering Act, No.5 of 2006.

Ordering Financial Institution –

An institution which initiates wire transfers and transfers the funds upon receiving the request for a wire transfer on behalf of the originating customer.

Person –

A natural or legal person and includes a body of persons whether incorporated or unincorporated and a branch incorporated or established outside Sri Lanka.

Politically Exposed Person –

An individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a Head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals.

Payable through Account –

Correspondent accounts that are used directly by third parties to transact business on their own behalf.

Risk Based Approach –

In relation to the application of CDD measures to manage and mitigate money laundering and terrorist financing risks, means the use of simplified CDD measures in the case of customers with lower risk levels and the use of enhanced CDD measures in the case of customers with higher risk levels.

Shell Bank –

A bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective overall supervision. The physical presence constitutes being located within a country performing a management function with meaningful mind and the mere existence of a local agent or non-managerial staff does not constitute a physical presence.

Straight through Processing –

Payment, transactions that are conducted electronically without need for manual intervention.

Terrorist Financing –

An act constituting an offence connected with the financing of terrorism under the Convention on the Suppression of Terrorist Financing Act, No.25 of 2005.

A LIST CATEGORIES 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/Charge d'affaires/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
36 Governor / Deputy Governors / Assistant Governors and Heads and Additional Heads of Department of the Central Bank of Sri Lanka
37 Advisors to the President/ Prime Minister / Ministers/ Ministries
38 Chief of staff of presidential secretariat
39 Auditor General
40 Secretary General of Parliament
41 District Secretaries/ Government Agent and Secretaries
42 Heads and Senior Officials of Government Departments
43 Chairmen and Senior Officials of State Enterprises
44 Chairmen and Senior Officials of State Corporations / Statutory Boards/ Authorities/ Public Corporations

F.

45 Field Marshall / Admiral of the Fleet/ Marshal of the Air Force
46 Chief of Defence Staff
47 General of Sri Lanka Army/Admiral of Sri Lanka Navy/ Air Chief Marshal of Sri Lanka Air Force
48 Officers in the Rank of Lieutenant Colonel and above of Sri Lanka Army
49 Officers in the Rank of Commander and above of Sri Lanka Navy
50 Officers in the Rank of Wing Commander and above of Sri Lanka Air Force
51 Inspector General of Police
52 Police officers above the rank of Asst. Superintendent of Police

G.

53 Chairman/ members and senior officers of the Public Service Commission
54 Chairman/ members and senior officers of the National Police Commission
55 Chairman/ members and senior officers of the Human Right Commission
56 Chairman/ members and senior officers of the Commission to Investigation Allegations of Bribery or Corruption
57 Chairman/ members and senior officers of the Finance Commission
58 Chairman/ members and senior officers of the Election Commission
59 Members of Constitutional Council
60 Chairman/ members and senior officers of the Audi Service Commission
61 Chairman/ members and senior officers of the Delimitation Commission
62 Chairman/ members and senior officers of the National Procurement Commission
63 Members of Cabinet appointed committees

H.

64 Chairman, Members and senior officers of University Grant Commission
65 Chairman, members of University Councils
66 Chancellor
67 Vice Chancellor
68 Registrar of universities

FOREIGN PEPS

69 Officials of international organizations who hold or have held, in the course of the last 5 years, management positions in such organizations (directors, heads of the boards or their deputies)
70 Officials of international organization who perform or performed any other management functions on the highest level, particularly in international and intergovernmental organizations,
71 Members of international parliamentary assemblies,
72 Judges and management officials of international courts

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 with 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 owner.

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 to provide 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. The PEP is unable or reluctant to explain the reason for doing business in the country of the

FIs/DNFBs.
5. The PEP provides inaccurate or incomplete information.
6. The PEPs seeks 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 does not seem to have
ties with.
8. The PEP is or has been denied entry to the country (visa denial).
9. The 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. The PEP has a substantial authority over or access to state assets and funds, policies and
operations.
2. The PEP has control over regulatory approvals, including awarding licences and concessions.
3. The PEP has the formal or informal ability to control mechanisms established to prevent and
detected ML/TF.
4. The PEP (actively) downplays 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. The 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. The 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 Defence 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.