Policy on Anti Money Laundering (AML), Countering To Financing of Terrorism (CFT) and Proliferation Financing (CPF)

(Reviewed on December 2025)

Contents

Policy on Anti Money Laundering (AML), Countering to Financing of Terrorism (CFT) and Proliferation Financing (CPF)

1. Introduction

Anti- Money Laundering (AML), Countering of Financing Terrorism (CFT) and Countering of Proliferation Financing (CPF) policy is structured to guide and support for preventing from money laundering, countering of financing to terrorism and countering of proliferation financing at providing financial services throughout its day-to-day operations as well. Pradeshiya Sanwardhana Bank, since it's a Licensed Specialized Bank with a state ownership, it becomes a key responsibility of fencing for money laundering to support for the well-being of society and within the financial industry while ensuring the safeguard the customers, corporate image and reputation of the Bank.

The policy will cover the following key areas to ensure the clear guide to implement Anti money laundering and fencing to prevent from financing to terrorism.

- ✓ Establishing of a methodology for Identifying and concentrate on the victim of money laundering and augment using the banking industry for its prevalent.
- ✓ Make comprehensive awareness on money laundering which may experience in the market and to introduce efforts can be taken through staff individually and as collective efforts to AML within the Bank.
- ✓ Understanding of the guidelines and rules introduced by legal and regulatory bodies to act against Money Laundering and terrorists financing mainly using CDD and KYC regulations for a broader customer risk assessment.
- ✓ Developing and Placing Anti Money Laundering procedures, regulations, and legal surroundings for combating money laundering within the organization in each level.
- ✓ Starting the process of identifying the Suspicious Transactions comprehensive screening process and financing to promote the reporting process enable to mitigate risk incurred on money laundering.
- ✓ Screening the customers, including beneficial owners' information at the time of customer onboarding against Sanctions Lists. As well as build up procedure to prohibited or restrict the transaction.
- ✓ Structuring of strategic approach and implementation process on anti-money laundering against money laundering; to comply with minimizing of risk involves in the industry.

- ✓ Strengthening of reporting process under Financial Transaction Reporting Act to ensure the review the transactions described in AML act.

2. Purpose & Objective of the Policy

In the highly volatile banking environment, intensified by rapid technological advancements, it is essential for the institution to establish a structured and effective process for assessing its AML/CFT/CPF framework. The primary objective of this policy is to ensure that the institution maintains a robust, comprehensive, and adaptive system for detecting, preventing, and mitigating illicit financial activities.

- **Establish a Robust Compliance Mechanism:** To implement and maintain a formal mechanism capable of detecting, preventing, and addressing money laundering (ML), terrorism financing (TF), and proliferation financing (PF) schemes, particularly those of increasing complexity and sophistication.

- **Ensure Senior Management Oversight and Accountability:** To clearly define and embed the responsibility of Key Management and the Board in providing adequate resources, oversight, and strategic attention to the effective execution of the Anti-Money Laundering (AML) process.

- **Foster Organization-Wide Understanding and Compliance:** To develop and maintain a thorough understanding among all staff layers (including operational teams) regarding ML/TF activities, associated risks in the financial market, and the regulatory obligations introduced by the Central Bank of Sri Lanka (CBSL) Financial Intelligence Unit (FIU) as preventive measures.

- **Ensure Accurate and Timely Regulatory Reporting:** To develop and enforce a standardized process for the regular, complete, and accurate submission of all required financial transaction reports to the regulator.

- **Mitigate Institutional ML/TF/PF Risk:** To cultivate a comprehensive, bank-wide environment for risk management that effectively combats money laundering and terrorist/proliferation financing across all business units, thereby mitigating risks allied to illicit finance.

- **Mandate Strict Customer Due Diligence (CDD):** To establish an organizational structure and process that rigorously adheres to Know Your Customer (KYC) and

Customer Due Diligence (CDD) regulations, providing a strong defense against ML/TF/PF activities.

- **Implement Continuous Sanctions Screening:** To ensure mandatory and timely screening of all relevant sanction lists (both domestic and international) at critical intervals, including during the initial customer onboarding process and upon any subsequent list updates.

Ensure Board of Directors and entire staff are responsible and being bounded at performing as on the directions at the process of combatting on money laundering, prevention from financing to terrorist and prevention to proliferation financing.

3. Money Laundering, Terrorist Financing, and Proliferation Financing

3.1. Background

Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) represent critical global threats. These activities are fundamentally interrelated, collectively constituting a form of financial terrorism that provides the essential funding mechanisms for serious organized and transactional crime worldwide.

3.2. The Global Threat

Illicit actors—ranging from individuals to complex organized criminal groups—engage in a spectrum of offensive activities, including drug trafficking, extortion, insider trading, corruption, and illegal gambling. The success of these activities relies on their ability to utilize the global financial system, including the banking industry and other financial institutions, to disguise the origins of illegally obtained proceeds. Whether knowingly or unknowingly, financial organizations are vulnerable to being exploited to facilitate the legitimization of these funds, thereby enhancing and sustaining criminal and terrorist enterprises over time.

3.3. The Process of Money Laundering (ML)

Money laundering is the process used to make funds generated through illegal activities appear to have originated from legitimate sources. It involves obscuring the source, ownership, and movement of these illicit proceeds, typically through a multi-stage process (Placement, Layering, and Integration) that introduces the funds into the financial system and

moves them through numerous accounts to create confusion and distance from the original crime.

3.4. The Motivations for Illicit Financial Activity

The growth and sophistication of ML, TF, and PF are driven by several financial and strategic benefits for the criminal organizations, including:

- Tax and Regulatory Evasion: Circumventing formal tax obligations, regulatory requirements, and established barriers of organized, legal processes.
- Legal Barrier Avoidance: Bypassing authorized business licensing and legal scrutiny applicable to legitimate transactions.
- Facilitating Illicit Transfers: Enabling the furtive and illegal transfer of funds between individuals or organized groups involved in unlawful endeavors, operating entirely outside legal channels.
- Supporting Criminal and Destructive Acts: Providing financial support for a variety of criminal enterprises, including drug trafficking, dealing in weapons, organized abuse, and various forms of terrorist and extremist activities.
- Securing Legal Form: Ensuring that the ultimate proceeds of crime are "cleaned" and provided with a legal appearance, thus protecting the perpetrators from detection and asset seizure.

4. Definitions

4.1. Money Laundering (ML)

Money Laundering is defined as the process of disguising the source of money generated through illegal activities so that it resembles legitimate income. In the context of the banking and financial industries, it is often understood as the manipulation of financial transactions to facilitate illegal and unauthorized business transactions.

The process involves the breaking up of large amounts of cash into smaller transactions, changing its form through investments or deposits into bank accounts, and moving the money through seemingly legitimate businesses to reintegrate it into the mainstream economy.

4.2. Terrorist Financing (TF)

Terrorist Financing is the act of providing financial support to terrorists or terrorist organizations to enable them to carry out terrorist acts. This can involve funds sourced from both illegal activities (similar to ML) and legitimate sources (e.g., charitable donations, business profits), making the detection of TF uniquely challenging.

4.3. Proliferation Financing (PF)

Proliferation Financing refers to the act of providing funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery. PF is specifically targeted by international sanctions regimes designed to prevent the catastrophic use of Weapons of Mass Destruction (WMD).

5. The Social Conflict and the Indispensable Role of AML/CFT

5.1. The Destabilizing Social Conflict of Illicit Finance

Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) are highly organized, transnational criminal processes that pose a direct, existential threat to the integrity of global society and governance. Illicit funds sustain sophisticated criminal networks engaged in heinous acts, including terrorism, drug trafficking, child abuse, and large-scale fraud. Furthermore, these funds corrupt legitimate commerce by financing enterprises that—despite holding licenses and appearing reputable—deal in goods like prohibited chemicals or harmful products, posing severe risks to public safety.

This corruption is facilitated by the exploitation of the global financial system. Trillions in illicit assets are moved across borders through complex schemes where payments often circulate between interconnected organizations with the same underlying beneficial ownership. Financial institutions are thus unwittingly or unwillingly used as "bill settlers" for criminal enterprises, eroding public trust and diverting capital from productive economic use.

5.2. Mandatory Importance of Anti-Money Laundering (AML) Procedures

The scale of this threat mandates a global, organized response. International bodies like the International Monetary Fund (IMF) and the Financial Action Task Force (FATF) have established a framework—the revised FATF 40 Recommendations—to combat ML and CFT.

5.3. Core Responsibility of the Bank

A financial institution must act as the essential gatekeeper against illicit finance. This is executed through:

- **Strict Regulatory Implementation:** Adhering to all directives from the Financial Intelligence Unit (FIU) and other regulators.
- **Enforcing KYC/CDD:** Structuring the organization to ensure the rigorous application of Know Your Customer (KYC) and Customer Due Diligence (CDD) as fundamental preventive measures.
- **Accountability**: Ensuring that Key Management and all staff are fully responsible and legally bounded to the precise performance of these regulations across all bank operations.

Aspect	Importance of AML Policy to the Bank
Social	Safeguards the well-being of society by controlling illegal activities, subjecting those involved in ML/TF/PF to legal action, and establishing them as criminal offenses.
Reputational	Protects the reputation, image, and integrity of the bank from being corrupted, ensuring it remains an uncompromised entity within the financial market.
Legal/Regulatory	Establishes a clear, enforceable legal setup to create barriers against money laundering, ensuring the bank cannot avoid accountability under local and international legal networks.
Operational/Customer Safety	Ensures the safety of the bank and its legitimate customers from becoming victims of financial crime, while enabling the effective monitoring and countering of suspicious transactions made through bank accounts.

6. Laws, Rules and Regulations Applicable In AML/CFT/CPF and Sanction Screening.

Under measures taken to control money laundering activities of the world. Internationally developed preventive measures have been launched against ML. It has passed the resolutions for AML procedures which each and every country has to follow and perform according to those requirements which consider as international regulations. 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 confined with the requirements of the FATF. Further, 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.

In addition to above key acts and regulations, following guideline, Press Release and regulations introduce by FIU & DBS of CBSL may supported to enhance AML process.

- Customer Due Diligence Rule NO.1 OF 2016 – Extraordinary Gazette No.1951/13 on 27/01/2016 & Amendments to the Financial Institutions (Customer Due Diligence) Rule No.01 of 2016 - Extraordinary Gazette No.2092/02 on 08/10/2018.
- Guideline on AML/CFT Compliance Obligations for Money or Value Transfer Service providers, No.01 of 2017
- Guideline on Beneficial Ownership No 04 of 2018
- Guidelines on Money Laundering & Terrorist Financing Risk Management of Financial Institutions, No. 01 of 2018
- Guidelines on Suspicious Transactions Reporting, No. 06 of 2018
- Guideline on identification of Political Exposed Person, No.03 of 2019
- Circular No; 03/2020 issued by the FIU - Financial Institutions are advised to be vigilant to emerging Money Laundering/ Terrorist Financing risks
- Guideline No. 03/2020 issued by the FIU -Revised Guidelines for Non-Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 3 of 2020
- Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021
- Circular No. 04/2021 issued by the FIU - Deposits Made Under The Finance Act, No. 18 of 2021
- Circular No.02 /2022 – Further Information requested on suspicious Transaction Reports (STRs)
- Regulations made in terms of United Nations Act No.45 of 1968, with respect to any designated list.

- Sanitized Report of the Second National Risk Assessment (NRA) on ML/TF (2021/ 2022)
- National Policy on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) of Sri Lanka (2023–2028)
- Consumer Protection Regulation Rile No 01 of 2023
- Companies (Amendment) Act No.12 of 2025

7. Regulations against Terrorist Financing

Similar to the Anti-Money Laundering Act No 05 of 2006 is also passed by the parliament of Sri Lanka to control of supporting and contributing to terrorist financing or such transactions in this nature and it denotes various precaution actions to be followed in controlling measures of terrorist financing. Operational procedures of Anti Money Laundering have to develop within the bank. Since we are a bank expanded its branch network at everywhere and involving in banking operations with various kinds of people involving in business activities in various nature.

Banks may follow the recommendations of Financial Action Task Force (FATF) which are gazette by Ministry of External Affairs on 31st May 2012 (Extra ordinary Gazette No 1760/40).

Accordingly, the PSB is in line with the direction for

- Reporting on prescribed transactions on freezing funds.
- Freezing on accounts identified by United Nations Security Council.
- Maintain records and reports on accounts / transactions follow directions issued by Financial Intelligence Unit of the Central Bank of Sri Lanka.
- Follow directions issued by Financial Intelligence Units & Department of the bank supervision of the Central Bank of Sri Lanka.

8. Major Consistence on Act.

8.1. Prevention Of Money Laundering Act (PMLA) - No.5 Of 2006

Following specific areas are being covered in the Act.

- 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 Act.
- 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.
- Laws relating to offences against transnational organized crime (2006 No.05)

- Laws relating to offences against Exchange Control Act (2006 No.05)

c) 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.

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

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

f) The extradition law applies to the offence of Money Laundering

8.2. Financial Transactions Reporting Act- No.6 Of 2006- (FTRA)

Following specific areas are being covered in the Act.

- Financial Intelligence Unit (FIU) will play the role of national central agency to receive analyses and disseminate information relating to Money Laundering and Financing of Terrorism.
- Bank may oblige and responsible to report following reports on half month basis to the FIU on follow.
    i. Report on Cash Transactions (Rs. over one million)
    ii. Report on Electronic Fund Transfers (Rs. over one million)
- Suspicious transactions made by customers have to be reported by institutions to the FIU irrespective of their magnitude which are identified within the operations of the Bank.
- Senior Officer as the Compliance Officer who would be responsible for the institution's compliance with the Act.
- 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.

- Bank is required to engage in Customer Due Diligence (verifying the true identity of customers) with whom they undertake transactions and ongoing Customer Due Diligence with customers with whom they have a business relationship.
- Maintaining of numbered accounts and accounts under a fictitious name by bank becoming offensive 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.
- 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.

8.3. Convention On the Suppression of Terrorist Financing Act. No.25 Of 2005 as Amended by Act No. 41 of 2011 and Act No. 3 of 2013.

Major concentrations of the Act;

- 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).
- Conviction of a person for an offence under the Act, all funds collected in contravention of the Act is forfeited to the State.
- The extradition law applies to the offence of financing terrorism.

9. Customer Due Diligence (CDD) Rule No.1 of 2016 - Financial Institutions

9.1.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.

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

<u>As required by the above rules the Bank shall</u>

- Conduct following processes in assessing money laundering and terrorist financing risks:
  a. Documenting the risk assessments and findings
  b. Considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied
  c. Keeping the assessment up to date through a periodic review and
  d. Having appropriate mechanisms to provide risk assessment information to the supervisory authority.

- Have proper risk control and mitigation measures including
  a. Internal policies, controls and procedures to manage and mitigate money laundering and terrorist financing risks that have been identified.
  b. 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.
  c. Monitor the implementation of those policies, controls, procedures and enhance them if necessary and
  d. Take appropriate measures to manage and mitigate the risks, based on the risk-based approach.

- Conduct risk profiling on the customers considering
  a. 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)
  b. Geographical location of business or country of origin of the customer
  c. products, services, transactions, or delivery channels of the customer (cash based, face to face or no face to face, cross- border) and
  d. 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.

  a. Screening of new customers (at the time of customer onboarding) against the consolidated list of designated persons and associates, to make sure no such persons are becoming customers of the institutions.
  b. Screening of the entire customer database as and when update notifications are issued by the FIU

c. Identify the beneficiaries and/or beneficial owners of their accounts/transactions to ensure that no designated persons and associates are beneficiaries and/or beneficial owners of the funds, accounts or other assets. Bank are required to be able to demonstrate reasonable efforts have been made to verify the beneficiaries of the funds, accounts or other assets.

- 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/ Board Integrated Risk Management Committee on a annually basis. This report shall include

a. Money laundering (ML) and Terrorist Financing (TF) risk profile
b. Results of monitoring activities carried out for combating money laundering or terrorist financing risks (The effectiveness, of risk control and mitigation measures)
c. Details of recent significant risks involved in either internally or externally and its potential impact to the Bank
d. Recent developments in written laws on money laundering and suppression of terrorist financing and its implications for the Bank.

<u>CDD for All Customers</u>

- 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 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.

I). 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).

II). 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 detail verification which may include limiting the number, type and amount of transactions that can be performed.
- 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.
- 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 be commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profiles and nature of transactions.
- 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.

9.3. Occasional Customers, one off Customers, Walk in Customers and Third - Party Customers

I). 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 customer or walk in customers conduct CDD measures and obtain copies of identification documents.
b) With regard to occasional customers, one off customer 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.

9.4.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-

- Identity and assess of all Directors and Shareholders with equity interest of more than 10% to check the beneficial ownership of the company.
- Authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise;
- In any case of a natural person who is identified under the preceding provisions, who hold the positions of Key Management it may obtain the approval of the higher authority of the Bank.
- 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.

9.5.Non -Governmental Organizations/ Not for Profit Organizations / Charities

- Enhanced CDD measures may be taken 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.
- 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.
- 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.

9.6. Wire Transfers & Freezing of accounts with the UNSCR.

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.

9.7. Wire Transfers

- 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.
- 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 legal 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.

9.8.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.

9.9.Money or Value Transfer Service Providers (MVTS)

- The bank shall endeavor to identify, as far as practicable, beneficial ownership of funds transferred, and be mindful of series of linked transactions, if any
- The absence of required information on the originator or the beneficiary should be considered as a factor in assessing whether a transaction involving electronic funds or wire transfer is suspicious and whether it is required to be reported to the FIU.
- The bank shall maintain and update a list of its agents, sub-agents and/or merchants within Sri Lanka or outside Sri Lanka (if any) and provide access to such lists to the FIU on request.
- The bank shall have in place an adequate management information system (MIS), either electronically or manually, to complement its CDD process. The MIS is required to provide timely information on a regular basis to enable the reporting institution to detect irregularity of transactions and/or any suspicious activity
- The bank should not misuse any innovation by way of technological advancements provided for the benefit of their customers where such misuse shall amount to a violation of KYC/CDD practices, and any rule issued by the FIU
- 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.
- The Bank is required to establish employee/agent/sub-agent/merchant assessment system and screening procedures that are commensurate with the size of its operations and the risk exposure of the reporting institutions to ML/TF activities.

9.10. Customers and Financial Institutions from High-Risk Countries

- The bank shall apply the enhanced CDD measures to business relationships and transactions to customers and Financial Institutions from high risk countries.
- The bank shall apply appropriate counter measures,as follows, for countries specified in the list of high risk countries referred to The Secretary to the Ministry of the Minister to whom the subject of Foreign Affairs , 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 measure as may be specified by the Financial Intelligence Unit**.**

10. Politically Exposed Persons (PEPs)

Guideline No. 03 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.

10.1. Regulatory Definition

An individual who is entrusted with prominent public function either domestically or by a foreign country, or in an international organization and includes

i. A Head of a State or a Government
ii. A Politician
iii. A Senior Government Officer, Judicial Officer or Military Officer
iv. A Senior Executive of a State-Owned Corporation/ Government or Autonomous Body
v. Family members and close associates of the above stated PEPs.

10.2. Regulatory Descriptions of PEPs

a) Domestic PEPs:

Individuals who are entrusted with prominent public functions in Sri Lanka.

b) Foreign PEPs:

Individuals who are entrusted with prominent public functions by a foreign country.

c) International Organization PEPs:

Persons who are entrusted with a prominent function by an international organization.

d) Immediate Family Members:

Individuals who are related to a PEP either directly or through marriage or similar forms of partnerships. This includes

- Spouse (current and past)
- Siblings (including half siblings and their spouses)
- Children (including stepchildren and adopted children) and their spouses
- Parents (including stepparents)
- Grand children and their spouses

e) Close Associates:

Individuals who are closely connected to PEPs either socially or professionally. This includes,

- A natural person having joint beneficial ownership of legal entities and legal arrangements or any other close business relationship with a PEP
- A legal person or a legal arrangement whose beneficial owner is a PEP or an immediate family member or a close associate is a PEP.
- A publicly and widely known close business colleagues or personal advisors (especially those who are acting in a financial fiduciary capacity) of PEPs.

f) Procedure adopted at the Bank

i) Identification of PEPs

Acting in compliance with the regulatory framework it is proposed to consider following Persons/ Institutions as PEPs:

1. Local PEPs

i. External (Not in the Bank)

- Present and former Presidents of the country
- Present and former Prime Ministers of the country
- Members of Parliament including Speaker and Deputy Speaker
- Members of Provincial Councils (including Governors of the Provinces), Members of Pradeshiya Saba and Members of Municipal Councils.
- Leader, Secretary and Treasurer of all Political Parties

- Central Bank of Sri Lanka – Governor, Senior Deputy Governor, Deputy Governors and Assistant Governors and Heads and Additional Heads of the Departments.
- Auditor General's Department – Auditor General, Additional Auditor
- General and Assistant Auditor Generals.
- Diplomatic representatives of the government serving in foreign countries.
- Members of Monetary Board.
- Government appointed Commissions – Chairman, Members and Senior Officers.
- Senior Government Officials:
- Government Departments – Director / Commissioner and above.
- Corporations – General Manager and above.
- Ministries – Additional Secretary and above.
- State Owned Enterprises – Head and Deputy Head of the entity.
- Statutory Boards – Head and Deputy Head of the entity.

ii. Judicial Officers

- All judges.
- Attorney General (AG).
- Solicitor General and Additional Solicitor General of the AG's Department.
- Registrars of Courts.

iii. Military Officers

- Sri Lanka Army – Lieutenant Colonel and above.
- Sri Lanka Air Force – Wing Commander and above.
- Sri Lanka Navy – Commander and above.
- Sri Lanka Police – ASP and above.

iv. Personal Secretaries, Coordinating Secretaries, Senior additional secretaries,

- Personal Relationship Officers and Media Secretaries to the President, Prime Minister and Cabinet Ministers; Personal and Coordinating Secretaries to Deputy/State/Provincial Council Ministers.
- Immediate family members and close associates of PEPs as detailed in the FIU Guideline.
- A private company where a PEP is a director or a significant shareholder.
- Other Business concerns (Proprietorships, Partnerships) in which a PEP has a material interest/control.
- Any other person, who, in the opinion of the Bank should be categorized as a PEP based on information available in the public domain.

v. Internal PEPs (In the Bank)

- The Employees of the Bank, who are performing executive functions of the Bank and are
- considered as Key Management Persons (KMPs) as per the Banking Act Determination No. 1 of 2019 shall be considered as Internal PEPs of the Bank.
- Though the KMPs shall be categorized as Internal PEPs
- The necessity of obtaining the approval of General Manager and Deputy General Manager -Operation and bank support service to open an account at the Bank shall not be applicable to Internal PEPs.
- The Chief Executive Officer/ General Manager shall have the authority to approve or reject the facilities applied by Internal PEPs.

2. Foreign PEPs

- Heads of Foreign States or Governments.
- Judges and Management Officials of International Courts, Judicial or Military officials.
- Heads/ Deputies/ Directors etc. of International Organizations.

- Members of international parliamentary assemblies.

ii) Duration of Treating a Person as a PEP

- Members of Parliament/ Provincial Councils/ Pradeshiya Saba/ Municipal Councils immediate family members and close associates- as PEPs for lifetime
- Government/ Judicial/ Military officers, immediate family members and close associates- as PEPs only during the time they hold their offices and for a further period of six months after removal from office.
- Members, immediate family members and close associates of Government appointed Commissions/ Boards/ Corporations- as PEPs only during the time they hold their offices and for a further period of six months after removal from office.

iii) Ways of PEP Identification

PEPs shall be identified based on the customer self-declaration, information available in the PEP lists internally maintained at the Bank, information available in public domain and information available in the global watch lists**.**

iv) Banking Relationships with PEPs

a) Opening New Accounts

The Bank has put in place a due diligence process on conducting banking relations with PEPs and as per the due diligence process

The approval of the Senior Management (General Manager and Deputy General Manager- Operation and bank support service) should be obtained to open a new account for a PEP.

Source of funds and wealth is identified through appropriate means

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

b) Granting Facilities

Credit facilities to PEPs (Member of Parliament , Member of Provincial councils including ministers, Mayors and Chairman of the Pradeeshiya Saba) shall be granted with the prior approval of the Board of Directors.

c) General Provisions

i. In accordance with the due diligence process implemented at the Bank all essential information such as principal occupation or employment, source of income, purpose of opening the account etc. shall be obtained to identify the customer.

ii. Though middle ranking and junior individuals are not considered as PEPs, the Bank shall take measures to identify middle ranking or junior officials who act on behalf of PEPs to circumvent AML/CFT controls.

iii. The Bank shall use the self-declaration, information available in public domain, information available in global watch lists, institutional websites etc. to identify international PEPs.

iv. In order to identify the customers who have become PEPs after opening accounts with the Bank measures shall be taken to monitor non-PEP accounts at instances where

- a customer updates the Bank with information on his political exposure
- ongoing monitoring reveals activities or information that suggests previously unknown political exposure
- an election is held which effects any of the customer's PEP status
- the Bank becomes aware of the need of such an update

v. If the Bank is of the opinion that the type of activities taking place in the account are not reasonable, when compared with the source of funds/ wealth, steps shall be taken to conduct a further assessment and a decision will be taken on continuation or termination of the business relationship and filing a suspicious transaction report with FIU the findings of the assessment.

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

- Bank may establish a procedure to controls to determine if the customer or the beneficial owner is a politically exposed person;
- Obtain approval, before or after entering into the relationship from the General Manager, 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;

- Identify, by appropriate means, the sources of funds and wealth or beneficial ownership of funds and wealth; and
- Conduct enhanced ongoing monitoring of business relationships with the politically exposed person. The bank is aware that the Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves.

11. Beneficial Ownership

11.1. Companies (Amendment) Act No.12 of 2025

Section 130A . (1) Every company incorporated or registered under this Act or any former written law relating to companies (under this heading referred to as the "company") shall, at the time of incorporation or within twenty working days of the issue of any shares or transfer of shares, give notice to the Registrar in the prescribed form of-

a. the full names and previous full names (if any) as appearing in the identification document of beneficial owners of the company;
b. the dates and places of birth, nationalities, countries of residence, and the last known addresses of beneficial owners of the company;
c. the residential addresses, business addresses, email addresses, and postal addresses of beneficial owners of the company;
d. the National Identity Card numbers, Tax Identification Numbers, or passport numbers and the countries of issuance of beneficial owners of the company;
e. the contact details of beneficial owners of the company; and
f. a full statement describing the nature and the extent of the beneficial ownership.

Section 130C . (1) A company shall appoint, in a prescribed manner a natural person residing in Sri Lanka as the authorised person who is –responsible for the safe keeping of the register of the beneficial owners of the company; and

authorised by the company to make the details of the beneficial owners of the company recorded in terms of section 130A available to the person or authority specified in section 130B.

(2) The company shall disclose the details of the authorised person referred to in subsection (1) at the time of incorporation and any subsequent changes to such authorised person in a form as may be prescribed.

(3) Every company incorporated or registered under the Companies Act, No. 07 of 2007 or any former written law relating to companies shall, within a period of three months from the date of operation of the Companies (Amendment) Act, No. 12 of 2025, disclose the details of the authorised person referred to in subsection (1).

Section 130. I The Minister may make regulations in respect of all or any of the following matters: -

a) maintenance of the register of beneficial ownership of the company;
b) reporting of an acquisition of beneficial ownership of the company; and
c) for obtaining details relating to beneficial ownership of the company.

11.2. Guideline on Beneficial Ownership No 04 of 2018

As per the Guideline on Beneficial Ownership No 04 of 2018, Bank shall take steps to determine the ultimate beneficial owners of legal persons and legal arrangements and has identified that if a customer is a natural person; 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.

a) The Bank shall take steps to identify the beneficial owner of a legal person considering three main facts “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”.
b) 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.
c) The Bank shall take steps to obtain and verify information on trusts including the identities of the author of the trust, the trust is, the beneficiary or class of beneficiary and any other natural person, exercising ultimate effective control over the trust.

d) 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.

e) 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.

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

g) 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

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

   a. Risk level of the customer is low & verification is not possible at the point of entering into the business relationship
   b. There is no suspicion of money laundering or terrorist financing risk involved
   c. Delay will not interrupt the normal conduct of business

i) 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.

j) 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

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

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

m) 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.

n) 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.
- The identification that shall be obtained are as follows;
  - i) full name
  - ii) official personal identification or any other identification number
  - iii) permanent/ residential address
- 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.
- Furthermore, the Bank shall take steps to identify the beneficial owners through following means;
  - iv) Share Register
  - v) Annual Returns
  - vi) Trust Deed
  - vii) Partnership Agreement
  - viii) Constitution and/ or Certificate of Incorporation
  - ix) Constitution of a registered co-operative society
  - x) Minutes of the board meetings
  - xi) Information that can be obtained by open-source search or commercially available databases.
  - xii) Verification through mother company or branches, Correspondence Bank, other agents of the Bank, Corporate Registries etc. (for foreign legal persons & arrangements)
  - xiii) Relevant identification information available from reliable sources such as public registers (for Companies listed in Stock Exchange)

o) 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.

p) The Bank shall review the adequacy of information in respect of beneficial owners according to the risk status of the customer, through obtaining information from the existing core-banking system of the Bank.

q) In addition, 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

r) 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

s) 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.

12. Using New Technologies

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.

<u>The Bank shall,</u>

a) Undertake the risk assessments prior to the launch or use of new products, practices and technologies;
b) 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
c) Not permit pre-loading of credit cards, as that may amount, inter-alia, to the abuse of credit cards, for money laundering and terrorist financing purposes, file a Suspicious Transaction Report if suspicious transactions are detected.

13. Accounts Opening Guideline Introduce by FIU

Bank may adhere with the Guideline introduced by FIU as on the Gazette dated 2016.01.27 at accounts opening to collect relevant information belongs to following Individual and legal persons.

13.1. Face to Face

13.1.1. Individual Customer

a) The following information shall be obtained:
   a. In the case of all customers
      i) Full name as appearing in the identification document;
      ii) 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.
      iii) Telephone number, fax number, and e-mail address;
      iv) Date of birth;
      v) Nationality;
      vi) Occupation, business , public position held and the name of employer and geographical areas involved;
      vii) Purpose of which the account is opened;
      viii) Expected turnover/ volume of business;
      ix) Expected mode of transactions;

x) Satisfactory reference as applicable; and

b. In the case of non- resident customers

i) The reason for opening the account in Sri Lanka

ii) 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)

i) Copy of identification document;

ii) Copy of address verification document;

iii) Copy of the valid visa/permit in the case of accounts for non-national customers.

According to Banking Act No 07 of 2022 issued on 29.08.2022 on Mandatory Recording of the unique Identification Number of Depositors, states that following accepted document/identification number should be used for opening the individual accounts

Type of Depositor	**Type of Identification Number**
Sri Lankan Citizen	National Identity Card (NIC) Number (For open the account Driving License and Passport can be used. However, it is compulsory to insert NIC number in the banks system)
Sri Lankan Citizen (Residing outside Sri Lanka/PR Holders/TR Holders Sri Lankan Dual Citizen (Residing in SL) Sri Lankan Dual Citizen (Residing Outside Sri Lanka)	National Identity Card (NIC) Number. (Sri Lankan Passport number can be used only when NIC number temporally surrendered by a Depositor.
Non-Sri Lankan Citizen	Foreign Passport Number. (Including Foreign National of Sri Lankan origin, Foreign Nationals on temporally visit to Sri Lanka or intending to visit Sri Lanka, Foreign Diplomat.
Minor Depositors	Date of Birth+ Birth Certificate Number Eg: Date of Birth-2005.01.07 Birth Certificate Number -0325

	Unique Identification Number (UIN)= 200501010325

13.1.2. 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

13.1.3. 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.
- Beneficial Ownership Certificate

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.

13.1.4. 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.

13.1.5. Trusts Nominees and Fiduciary Account

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

According to Banking Act No 07 of 2022 issued on 29.08.2022 on Mandatory Recording of the unique Identification Number of Depositors, states that following accepted document/identification number should be used for opening the institutional accounts.

Institutions	**Type of Identification Number**
Company Registered under Company Act	Company Registration Number.
Non-Governmental Organization	Registration number used by the National Secretariat for Non-Governmental Organization
Institute registered under Divisional/Local Government Bodies such as Proprietorships/Partnerships/Joint Ventures	Business Registration Number.
All Other Entities	Registration Number issued by relevant authorities.

13.1.6. 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.

13.2. Non-Face to Face

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

above, the Bank has adopted following process to open accounts of non-face to face customers.

a. The Bank shall act in compliance with the requirements stated in Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 and shall follow the alternate methods introduced by Guideline No. 3 of 2020 to verify the identity document and the address.
b. The Bank shall follow safe and trustworthy methods to obtain identification information such as
    - Electronic forms,
    - Mobile app,
    - Video conferencing,
    - Secure email,
    - Kiosks (ATMs, CDMs),
    - Registered post etc.

    and shall not use agents, third party service providers acting as agents, third party financial institutions, designated non finance businesses to collect identification information. Also, steps shall be taken by the Bank to obtain high quality still images of the customer, ID documents and address verification documents.
c. Also steps shall be taken to obtain the quality images of passport
d. The electronic interface provided by Department of Registration of Persons shall be used by the Bank to independently verify the identity of the customer.
e. The Bank shall verify and authenticate the identity of the customer through the link provided by the Department of Registration of Persons and video calls before entering into a relationship with a customer non face to face.
f. When the identity cannot be verified or authenticated the Bank shall not enter into a business relationship with a customer or process transactions on behalf of a customer.
g. Address of the customer shall be verified through the information available in the customer's identity obtained through the electronic interface of the Department of Registration of Persons.
h. At instances where the address differs from the information obtained through the electronic interface provided by Department of Registration of Persons, the Bank shall

follow the guidelines give in the Financial Institutions (Customer Due Diligence) Rules in verifying the address of the customer.

i. The Bank shall not open accounts or establish relationships with customers non face to face,

- When the customer uses any other identification document other than National Identity Card;
- When high quality interactive real time video of the customer cannot be obtained;
- When high quality data and still images of the customer identity document cannot be obtained;
- When identity documents appear damaged or degraded to the point the they are no longer fit for the purpose of identification;
- When identity documents appear altered, security features cannot be validated, or the integrity of the document is suspected;
- When the customer refuses or unable to comply with the established procedure of the Bank.
- At instances where the Bank is not in a position to fully execute the established procedure due to a system failure.
- When the electronic interface of the Department of Registration of Persons does not show the existence of the National Identity Card.
- When the details of customer identity do not match with the details obtained through the electronic interface of the Department of Registration of Persons;
- When the photograph of the National Identity Card produced by the customer does not match with the imagery obtained from the Department of Registration of Persons.
- When the customer appears to have intentionally modified his appearance to disable the bank to identify and verify the customer to fully complete the established on boarding procedure.

j. The customers identified non face to face shall be categorized as High Risk and as such shall be subject to enhanced due diligence till the customers are in a position to present their original identifications to the Bank to enable the Bank to verify and make a copy thereof.

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

l. The Bank shall take steps to file a Suspicious Transaction Report with Financial Intelligence Unit at instances such as impersonation, forwarding forged documents, forged, or altered National Identity Cards or address verification documents, altered images, spoofing, reluctance to corporate or provide additional information for verification, discrepancies in information provided or when suspicious behaviors are noted.

In order to comply with the requirements in Direction No. 01 of 2016, it is necessary to take action at the opening the accounts.

The following are the broad guidelines in this regard:

13.3. 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 with coordinating the AML system of the bank. 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.

13.4. 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

Trustee, settlers/grantors and beneficiaries should complete an individual profile of the customer (KYC) form

iv. NGOs/Charities/Clubs/Societies/Other

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

c) Copies of all documents as applicable as set out in this Policy have to be retained by the Bank.

d) The authorized officer of the bank 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.

14. Sanction Screening

a) Bank shall establish a sanction screening process through AML System before entering any transaction at the customer on boarding (Ad hoc screening) and when sanction lists are updating from time to time (Scheduled Screening) as per the Regulations made in terms of United Nations Act No.45 of 1968.

b) Bank shall screen new customers and their beneficial owners or transactions at the time of on boarding against the consolidated list of designated persons, entities or counties.

(Screening of names, addresses and other details against the consolidated list of designated persons and entities published by the UN Security Council or its Committee/FIU in Sri Lanka is necessary in ensuring compliance with certain elements of targeted financial sanctions. However, the above screening would not be sufficient on its own, as targeted financial sanctions are also applicable to persons / entities acting on behalf of or at the direction of designated persons/entities. Therefore, bank shall require identifying the beneficial owners and other connected parties of their customers to the extent reasonably possible and apply the screening measures to such associates as well.)

c) Further, bank shall maintain records on beneficial owners behalf of their customers.

d) Bank shall maintain designated customer list which are regulated sanctions lists by FIU in Sri Lanka.

e) The following sanctions list to be considered at the sanction screening.

   i. Consolidated United Nations Security Council Sanctions List (UN) (UNSCRs 1267, 1718, 2231) and any other subsequent Resolutions)

   ii. FIU Sri Lanka -local list (National Level -UNSCR Regulation 1273 (2001).

f) The following customers/Countries are prohibited as per the instructions given by FIU and under regulation 4(7) of the United Nations Regulations.

   - Taliban (Islamic Emirate of Afghanistan)
   - Islamic State of Iraq and Levant (ISIL, also known as Da'esh)
   - Al-Qaida.

g) Bank shall take necessary action to report to the FIU and Defense Ministry (Competent Authority) not later than 24 hours from the time of finding such customer, if identified any customer in the sanction list and freeze such accounts immediately with informing the customer.

   (It is required to immediately freeze funds, financial assets or economic resources individuals and entities who are designated by the United Nations Security Council based on such person's/entity's connections with terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing)

h) When the Competent Authority issues an authorization to use the frozen funds for exemption conditions, bank should have release such frozen funds without delay.

15. Suspicious Transactions/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.

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 activity 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. Unusually large cash deposits using "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.
5. Multi transaction one day but conduct different branch.
6. Multi-client using the same address.

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.
5. Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received unexpected large sums of money from abroad.
6. A large number of individuals deposit monies into the same account without an adequate explanation.
7. Unusually large deposits in the accounts of a jewelry shop whose accounts have never witnessed such deposits particularly, if a large part of these deposits is in cash.

Suspicious Investment Related Transactions:

1. 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 account.
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 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.

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.

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.

16. Suspicious Transaction Reporting Procedures

Good reporting procedures and their correct implementation are designed to ensure that when a suspicious transaction is identified:

- The suspected customer or any related person is not alerted (non-tipping-off)
- The matter is addressed quickly and professionally.

- The external authorities are notified and provided with the necessary records, as appropriate.

16.1. Reporting Mechanisms

The Bank has established clear procedures for reporting suspicions, supported by relevant information, through the following channels:

A standardized reporting format issued to the branch network.

The Anti-Money Laundering (AML) system implemented to monitor suspicious activities.

Employees have been trained to ensure that the supporting information provided is relevant and sufficient for the Chief Compliance Officer to pass on to the Financial Intelligence Unit (FIU).

Role of the AML Officer

Upon receiving a Suspicious Transaction Report (STR), the AML Officer will assess whether the report indicates knowledge or suspicion that a customer is involved in money laundering.

If the AML Officer determines that the suspicions are justified and require further investigation, the AML Officer must report this to the Financial Intelligence Unit (FIU).

The Bank may conduct further inquiries utilizing its own records, but it is **not required to carry out detailed criminal investigations**.

16.2. Employee's Duty to Assist

The employee has a duty to assist the AML Officer in effectively reporting the matter to the FIU by ensuring the information provided:

- Clearly describes the reasonable grounds for suspicion
- Contains accurate and complete information.
- Is timely and submitted without delay.

16.3. The Importance of Timeliness

The Bank emphasizes the critical importance of submitting reports within 48 hours of identifying any suspicious transaction or customer.

No delay in reporting is acceptable. It is the duty of all employees to report suspicion as soon as reasonable grounds have been established and the relevant supporting material has been collected.

Failure to immediately report suspicions to the AML Officer could result in serious consequences for the employee involved, including individual fines, imprisonment, or both, as stipulated in the relevant legislation.

16.4. Tipping Off Condition

Under no circumstances must the customer be made aware that they have been reported or that an investigation is underway or may be initiated.

This does not preclude the Bank from asking the customer for an explanation or continuing to provide normal customer service. However, any interaction must be conducted without alerting them to the notification of authorities.

Alerting a customer under investigation can lead to the Bank being accused of "tipping off," which is a criminal offense for the individual who disclosed the existence of an actual or potential investigation.

As required by law, suspicious transactions must be submitted to the Financial Intelligence Unit (FIU) as soon as practicably possible, and no later than two working days (preferably 48 hours) from the formation of suspicion.

17. Risk Categorization Methodology

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

- Basic Information on the customer; -

  Bank may collect and verify 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 etc.

- Purpose of the Account.

  Bank may identify the purpose of transactions and will decide the nature of operations accordingly.

- The customer’s source of wealth/ sources of Income.
- Nature of Business and employment.

  based on the businesses it may decide the risk category together with other above components.

Customer will be graded to one of the following risk categories.

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.

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 categorized under Medium Risk.

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 categorized as high risk.

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.

18. Consistence and Implementation of AML /CFT/CPF

The AML policy is mainly constituted under the directions issued by Financial Intelligence Unit based on the Anti-Money Laundering Act no. 05 of 2006, Financial Transaction Reporting Act no. 06 of 2006 and Act no.25 of 2005 on countering to Terrorists financing. Since the Bank a state-owned Bank with a branch network, spread island wide (272), Bank has to stable a broader and recognized Anti Money Laundering procedure based on the policy to mitigate the operational, reputation and legal risks arises on money laundering. Adhering to this task, following steps can be recognized as the process of Anti Money Laundering.

Accordingly,

- ✓ Policies & procedures will be structured by the Board and will be communicated to all levels of the staff.
- ✓ A compliance officer will be appointed to monitor the regulatory compliance of the bank and also to monitor AML & CFT procedures of the bank whom is responsible to assess the level of compliance of implementation of AML/CFT process and also sufficient resources will be allocated to perform the compliance division effectively.

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 'recognizing 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)

✓A system software (AML System) had introduced by IT Division to filter and capture the suspicious transactions through day-to-day transactions of the Bank.

✓A system level process will be introduced to suspend identified suspicious transactions and also the accounts and persons identified in the sanctioned list locally or internationally.

✓A process will be introduced through the system to identify and highlight following personals.

- Directors & KMPs,
- Politically exposed persons,
- Listed persons suspended to transactions. & etc.
- Personals in the sanction list.

✓Special attention will be drawn on beneficial ownership on institutional customers/ corporate entities.

✓Bank may take actions to make awareness's to all levels of the staff include managerial groups on KYC and CDD regulations as a continuous process

- ✓The compliance team and corporate management of the Bank will assess and monitor the implementation of regulations which will be communicate / report to Board/Board sub committees.
- ✓Reporting process will be strengthening to report EFT and CTR within the given layer.
- ✓Frequent customer review mechanism will be introduced to follow up the risk assessment of high-risk groups and large exposures.

18.1.Structuring of Policies and Procedure manuals.

A comprehensive AML policy and other relevant policies related to KYC and CDD will be structured by compliance division and will be approved by Board with the recommendation of the BIRMC which will be communicated to corporate management and the contents of the policy will issue circulars to communicate to the staff. Documented to cover regulatory framework of Anti Money Laundering which will be reviewed frequently. Circulars and directions will issue to communicate the operational team.

18.2.Implementation:

Implementation will be done through awareness and with the support of the system enhancements to be used at CID and accurate customer database in the system.

18.3.Structuring the environment for enhancing the AML procedures

To be compatible with the recommendations of Financial Action Task Force bank is responsible to implement the Anti-Money Laundering (AML), Countering of Financing of Terrorism (CFT) and Countering of Proliferation financing Bank may implement the combating process Based on this Anti-Money Laundering policy, through a clear procedure enables to implementation of best practices on eliminating money laundering.

Accordingly,

i. Establishing a proper identification process on customer accounts, KYC details and the nature of transactions.
ii. Clear understanding on ownership of the transactions focusing to volume, frequency and or beneficiary level.
iii. Maintaining of adequate database on accounts (Customer Details) which are sufficient to confirm the person, risk level and sources of income & etc.
iv. Interviewing the process for realizing the nature of transactions to determine the purpose of follow up transactions whether it involves in an illegal activity or any nature of suspicious transactions and terrorist financing.

v. Establishing a clear and proper reporting requirement on Cash Transaction Report [CTR], Electronic Fund Transfer [EFT] and Suspicious Transaction Report [STR] as on the regulatory requirements determined by the Financial Intelligence Unit of the Central Bank of Sri Lanka or other regulatory bodies. Such as, Inland Revenue Department.

vi. Follow up a clear internal control and monitoring process structured on AML implementation specified to CDD and KYC regulations.

vii. Drawing more attention on Shell Bank activities and also PEPs involvements at transactions.

18.4. Issuing Circulars / Guidelines / Directions

The bank may issue the circulars on Anti Money Laundering procedure which has to follow by each and every staff member in their daily operations to get an involvement of combating to money laundering in bank as a whole.

Accordingly, while fulfill the requirement of customer service, staff may be instructed to not to contribute or support to any nature of money laundering which may unknown or invisible just in appearance.

Further, it may be included the mechanism to measure the nature of irregular transactions or fund movements. It is expected by issuing the circulars and guidance to make non following of these instructions / circulars may be counted as disciplinary misbehaves which may have considered as negligence points.

18.5. Awareness Process

With the releasing of the policy and procedures, Compliance unit of the Bank may be responsible to make proper awareness throughout the bank staff parallel with the operating instructions in addition to direct awareness of the Compliance unit. Bank may take highest attempts to aware the staff member at each level (based on the resources) to cover the requirement of Money Laundering and Anti Money Laundering. Also, staff members may expose to the external training, programs and workshops assist to mitigate risk involves in money laundering and to gain the Anti-Money Laundering procedures with the highest awareness from the external bodies and organizations. Further, awareness may continue periodically.

18.6. Proper Reporting and Regulatory Requirement

Regular Reporting.

Financial Intelligence Unit has released the instructions and guidance which are to be taken the measures of the bank. Mainly, CTR, EFT, STR and other call of information which are relevant to control Money Laundering in the country. Our responsibility is adhering and continue these reporting requirements in an understanding manner treating as a part of the service in their duties as an obligation as a citizen of the country.

18.7. Monitoring and review of operational level involvements

For a clear access to Anti Money Laundering procedures, Bank has to follow the procedures as on the guidance and circulars to meet its ultimate goal. Bank may construct a proper monitoring setup which can be observed in various angles to monitor the application of regulations (KYC & CDD regulations,) proceeding on accounts opening and continuing of Business transactions to verification documents as

follows.

i. Monitoring through various layers: Branch Manager, Assistant District Managers, District Manager, Regional General Manager and or Heads of Department.
ii. Audit, Inspections, and other visits: Conduct the Branch visits and interviews with particular officers involve in daily operations.
iii. Obtaining and reviewing data through centralized system. Such as suspicious transactions, large exposures, transactions from dormant accounts or other misuses of funds etc. Maintaining of CID and KYC information and details of financial transaction reporting.
iv. Maintaining of records and the system backups.
v. Suspension of transactions for identified persons who involved in terrorist financing, FCID [Financial Criminal Investigation Division] and or parties counted under Court orders in various sources victims.
vi. Reviewing Process

19. Deposits Made Under the Finance Act, No. 18 of 2021

If any person/entity depositing funds under the Finance Act, No. 18 of 2021, through a bank is required to comply with the requirements imposed under Financial Transactions Reporting Act, No. 6 of 2006 and any regulations, rules, directives, guidelines issued there under. In addition, when a customer makes a deposit under the above scheme, the deposit slip must state that such "deposit is made under the Finance Act, No. 18 of 2021".

20. CCTV Operations for AML/CFT Purposes, (FIU Guideline No. 2 of 2021)

These Guidelines issued by FIU along with the Rules, No. 01 of 2016, issued by Gazette Extraordinary No. 1951/13, dated January 27, 2016 (hereinafter referred to as CDD Rules). More specifically, these Guidelines should be referred together with Rules 7 and 11 of the CDD Rules, to take measures specified therein for the purpose of having proper risk control and mitigation measures by having internal policies, controls and procedures to manage and

mitigate money laundering and terrorist financing risks and affiliating and integrating Financial Institution's money laundering and terrorist financing risk management with the overall risk management relating to the Financial Institution.

20.1. The Requirements for CCTV Systems

As part of the constant commitment to enhance operational risk management and safeguard banking operations against risks of being abused for money laundering and financing of terrorism, bank should be installed in place a robust CCTV system installed fully operational both within and outside of the premises. The business premises refer to the head office, branches, areas of Automated Teller Machines, Cash Recycling Machines and Cash deposit Machines (ATMICRM/CDM), cash centers, outlets, and any other place or places where Customer Due Diligence (hereinafter referred to as CDD) is conducted.

20.2. Placement of CCTV cameras

In order to enhance the effective usage of the CCTV system, bank need to ensure that CCTV cameras are installed at appropriate locations, in a manner that the camera is able to clearly capture, monitor and record the relevant areas where business operations take place. These capture, Click or tap here to enter text. monitor and record the relevant areas where business operations take place. locations are required to include the counters, customer interaction areas where CDD takes place, areas where safe deposit boxes are located, safe or vault and other cash handling areas, ATMs/CDMs, vehicle parking areas, the entrance and exit of the branch premises, any other suitable areas, both inside and outside the building as determined by the bank.

20.3. Functions of CCTV system

Bank should ensure all images captured and recorded by the CCTV cameras are visible, recognizable and clear. The visual images or videos rendered through the CCTV cameras need to have the capability of identifying the features of the individuals, if any, that transact and should be clearly discernible from one image from another. In addition, adequate lighting must be maintained in order to capture clear CCTV footage.

Higher quality digital equipment should be used in CCTV systems to capture a clear frontal image of individuals. The CCTV systems should permit easy viewing, recording and retrieval of high-quality images (e.g., adequate number of pixels for improved zoom capabilities) of all

information contained in CCTV system. Necessary technical specifications (e.g., resolution, frame rate) need to be maintained at a standard level to achieve an effective CCTV surveil lance.

The CCTV systems of ATMs/CRMs/CDMs should remain operational throughout the 24-hours of a day - every day of the year, including during times when the Fl is closed for business.

20.4. Real time monitoring

Bank should ensure real-time monitoring at the head office and/or branches or at a central monitoring unit, as far as practicable. LEAs) to mitigate immediate risks that may arise to the F1's premises or to

Bank is advised to obtain assistance of its security services personnel or law enforcement agencies equipment, to its customers or to potential customers, or to any person at the vicinity of the CCTV camera, if such risk is detected based on CCTV footage obtained on real-time basis.

20.5. Maintenance of records

Bank should maintain all information captured in the CCTV system for a minimum period of 90 days according FIU requirement and ability of the bank by end of year 2022.

Bank may retain the CCTV recordings relevant to observed suspicious activities for a longer period.

Further, bank should be retained the CCTV recordings relevant to a Suspicious Transactions Report furnished to FIU or any other related CCTV footage of a possible offending until the relevant investigations are concluded by the LEAs or other relevant competent authorities as per instruction given by FIU, LEAs or any other competent authority from time to time.

The bank should ensure that its CCTV system(s) are capable of transferring the information to data storage devices, to allow retrieving and viewing of the CCTV records on electronic apparatus, such as computers

To confirm the credibility of the CCTV records, bank should ensure the timing of CCTV recording is properly set, synchronized and is consistent with the time and date of the operations that takes place at the business premises.

20.6. System administration and maintenance

Bank is expected to allocate adequate resources for CCTV monitoring systems, and sufficiently train the authorized personnel and staff to operate the CCTV system.

In order to ascertain effective surveillance and monitoring of business operations, FIs should ensure that the CCTV system(s) deployed is/are properly maintained and operational and remain under good working condition at all times.

The CCTV system should be equipped with the relevant features and functions to enable to implement control measures that will prevent such system from being manipulated or misused by any unauthorized parties.

Bank need to ensure that all information and records of the CCTV systems maintained safely and securely without unauthorized access and adequate controls are in place to prevent unauthorized alterations of records and access by unauthorized parties, by designating and appointing officers with appropriate responsibility and authorization levels, limiting system access only to relevant personnel to ensure proper accountability for the assigned functions.

Bank is expected to have procedures and mechanisms to ensure that regulators, LEAs and the FIU are able to obtain information and records in relation to money laundering investigations and prosecution upon request without delay.

Bank is required to issue internal operational guidelines on placement, functionality, monitoring, record keeping, system maintenance and administration, and include it as a part of AML/CFT policy as well with the approval of BOD.

Procedures should be in place for periodical review and audit of the CCTV system(s) for number of existing cameras in the premises at branch level and where standalone ATM/CDM are located. Audits and reviews should ensure the adequacy of the number of cameras, functionality, accuracy, operability, record keeping and other salient requirements. A report of such review/ audit on the adequacy of CCTV coverage should be submitted to the Board of Directors (BOD) and to the senior management

Based on the report submitted to the BOD, if the quality and coverage of CCTV systems are inadequate or more quality and coverage is desired, the senior management and the BOD are advised to take appropriate steps to rectify such deficiency or increase the coverage as appropriate. Further, immediate steps should be taken to replace or upgrade the equipment soon after any malfunction is detected.

Bank should ensure activities relating to the maintenance and recalibration of the CCTV system including system upgrading, reformatting and removal of records are clearly recorded in the system's maintenance log and reported to the senior management, as appropriate.

21. Record Keeping

The Bank shall maintain all records of specific / reported or /unusually large transactions for a minimum period of 6 years from completion of such transaction.

As well as, bank shall maintain Board Minutes relating to ML/TF Risk Assessment of the Bank.

The records shall be protected and maintained according to specific transactions which belong to ongoing inspections/ investigations/ and legal cases identified by the Bank / FIU or the legal entity.

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

May collect information on individuals / corporate clients who are counted under suspicious transactions and within the list of freezing or sanctioned.

Bank may maintain 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, Board minutes regarding the AML/CFT issues of the bank shall be maintained for a minimum period of six years commencing from the date on which the business relationship was fulfilled or the occasional transaction was effected. 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.

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

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.

22. Miscellaneous

The bank shall verify whether any prospective customer or beneficiary appears on any list of designated person or entities issued under any regulation made in terms of the united Nations Act, No.45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism and 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.

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.

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.

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.

When 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 always held by the clients during the continuation of the account with them.

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”.

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.

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.

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.

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

All staff members are required to comply with the FIU directives on Know Your Customer (KYC)& Customer Due Diligence (CDD), Political Exposed Persons (PEPs) and Identification of Beneficial Ownership at all times. This has been communicated through the Internal Operations Circular No.2020/04 dated 23rd January 2020 & Addendum of Operations Circular No.2020/04 - I dated on 23rd June 2020, Internal Operations Circular No.2020/05 dated 24th June 2020 and Internal Operations Circular No.2020/06 dated 25th June 2020.

KYC of the active customers should be reviewed and updated according with their risk categorization as per mentioned below.

- High Risk- Frequently and at the granting loan.
- Medium Risk- Once a two year or at the granting loan
- Low Risk- Once a three year or at the granting loan

It is the responsibility of the Regional General Managers, District Managers, Branch Managers and Heads of Department to educate employees coming under their purview of the importance of AML/CFT policy, KYC and CDD rules and the requirements on Customer Identification. Special emphasis must be made to train the Account Opening Officers in this regard.

Management will contribute and support at combatting process on ML/FT as a key responsibility of their duties.

Bank may establish a process and will take measures to mitigate all levels of risks on ML& FT through maximum controls for the secure of the bank and customers as well.

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 half yearly basis.

23. Governance

It became the responsibility and all are committed to the fight against Money Laundering and Terrorists Financing within the bank. The potential of the bank with 272 branch networks together with a huge customer processing thousands of transactions a day. For the safeguard of the customer base, bank has to draw fullest attention on implementation AML procedures.

We believe that high attention on KYC create the maximum customer relationship which is worth compromising our commitment to combating money laundering and terrorist financing. To fulfill this commitment, bank may have established Department headed by a Chief Compliance Officer who is functioning as an independent officer competent enough to negotiate and reporting directly to the Integrated Risk Management Committee (IRMC) and the Board of Directors as well. Also, he may responsible act on;

- Chief Compliance Officer functions as the Anti-Money Laundering Compliance Officer.
- Lead negotiable and train employees in Money Laundering and terrorist Financing Prevention practices and controls.
- Develop system to capture suspicious transactions.

24. Reviewing of the Policy.

The approved Anti Money Laundering policy can be reviewed as when it seems necessary. However, the Policy may have reviewed once in two years.

Reviewed – December, 2025