PEOPLE'S BANK

COMPLIANCE MANUAL

2023

INTRODUCTION

Purpose and Scope of the Manual

People's Bank was set up in 1961 to mobilize rural savings and channel it towards the process of development. It was established to provide banking services to population groups that had previously been excluded from the financial services industry with special emphasis to develop the Co-operative movement in Sri Lanka. It is governed by the People's Bank Act No. 29 of 1961 as amended and the Banking Act No. 33 of 1988 as amended.

The Bank is committed to follow Best practices and market standards in areas of accountability, transparency and business ethics in order to promote sustainability. Good governance and Corporate Social Responsibility (CSR) form an integral part of market standards. At the core of these efforts are integrity issues and the reputation risk the Bank faces in its activities.

To manage these issues the Bank has established an independent Compliance function. This manual is intended to define the roles and responsibilities regarding management of Compliance risk of the Bank. For this end the Compliance Policy has been compiled based on the rules and regulations prevailing in the Banking Industry, the International Principles and best practices in Compliance and Directives issued by the Central Bank of Sri Lanka.

The Compliance Policy of the Bank has been approved by the Board of Directors. This Manual describes the Policy established and details the procedure adopted in its Implementation. This Policy should be read with

- Policy and Procedure on Anti Money Laundering and Combating of Financing of Terrorism
- Code of Best Practices in Corporate Governance
- Code of Conduct
- Disciplinary Code
- Customer Charter
- Whistle Blowing Policy set up in the Bank
- Compliance Manual and
- Right to Information Act No. 12 of 2016.

Responsibility of the Manual

Compliance Risk is the risk of legal and regulatory sanctions, material financial loss or loss to the reputation, a Bank may suffer as a result of its failure to comply with laws, rules and regulations.

The Bank's Compliance function can be defined as "An independent function that identifies, assesses, advises on, monitors and reports on the Bank's compliance risk".

The Compliance function sets appropriate mechanisms for coordination to ensure compliance risk is managed effectively. The manner in which the Compliance function discharges its responsibilities is reflective of the level and impact of the Compliance risk facing the bank, giving greater focus to areas where Compliance risk is assessed to be high while preserving appropriate coverage of all such risks identified.

Compliance is the responsibility of all officers within the Bank. All business lines and functions within the bank must carry out their responsibilities to ensure the effective management of Compliance risk.

(a) Business lines, through appropriate managerial and supervisory controls, are primary responsible for managing compliance risk inherent in the day-to-day activities, processes and systems to which they are accountable.
(b) The compliance function is responsible for ensuring that controls to manage compliance risk are adequate and operating as intended as well as assessing and monitoring of Compliance risk faced by the Bank.
(c) The internal audit function is responsible for providing independent assurance to the Board of Directors on the quality and effectiveness of the Bank's overall internal controls, risk management and governance systems and processes, including those instituted by the Compliance function.

INTERNATIONAL PRINCIPLES ON COMPLIANCE FUNCTION – BASLE COMMITTEE

1. Responsibilities of the Board of Directors for Compliance

The Board of Directors have ultimate responsibility for the level of risk assumed by the Bank. Accordingly, the board should approve the Bank's business strategies and significant policies, those related to managing and taking risks.

Even though the Board has delegated the day-to-day compliance management responsibility to Bank officers and staff they should take steps to develop an understanding of the risks the bank faces. The Board should provide clear guidance regarding the level of risk acceptable to the Bank and should ensure that senior management implements the procedures and controls necessary to comply with the policies that have been adopted. The Board should also take steps to develop an appropriate understanding of the risks the Bank faces specially through briefings from Internal and external auditors. Using this knowledge and information, the Board of Directors should provide clear guidance regarding the level of risk acceptable to the Bank and should ensure that senior management implements the procedures and controls necessary to comply with the policies that have been adopted.

2. Responsibilities of Senior Management for Compliance

The Senior Management is responsible for implementing a program to manage the compliance risk associated with the Bank's business model, including ensuring compliance with laws and regulations both on a long-term and a day-to-day basis. Management should be fully involved in the Bank's activities and possess sufficient knowledge of all areas to ensure that appropriate risk controls are in place and that accountability and lines of authority are clearly delineated. Senior Management is also responsible for establishing and communicating a strong awareness of and need for, effective risk controls and high ethical standards.

3. Compliance Function Principles

The Bank's Compliance function should be independent. The Chief Compliance Officer should report to the Board Integrated Risk Management Committee. The Chief Compliance Officer should have sufficient resources to carry out the responsibilities allocated to the Department. The compliance function will indulge in the Bank's method set out to identify the compliance risk and report the resultant trends from Compliance assessments and reviews undertaken and tighter monitoring of complex compliance activities across all business lines and activities.

4. Other Compliance Matters

The Bank must ensure that the scope of responsibilities of the Compliance function sufficiently covers all businesses and branches including those activities delegated to a third party on its behalf. This means that the Bank must also ensure compliance with all legal and regulatory requirements applicable locally.

The manner in which the compliance function discharges its responsibilities must be reflective of its assessment of the level and impact of the compliance risk faced by the Bank. Accordingly, the compliance function must give greater focus to areas where Compliance risk is assessed to be high, while preserving appropriate coverage of all compliance risks identified.

REGULATORY FRAMEWORK

The rules and regulations established and issued in the form of Directives and Guidelines pertaining to Licensed Commercial Banks by the Central Bank of Sri Lanka are applicable to People's Bank. With regard to the Compliance Function the following rules and guidelines have made the establishment of an independent Compliance function imperative.

1. Central Bank Circular No. PS/21/98 dated 14.9.1998 on Appointment of Chief Compliance Officers
    - The Bank should establish an independent compliance function to ensure compliance in respect of banking and other statutory requirements.
    - The person appointed should be with a sufficient seniority to carry out the task.

2. Banking Act Direction No. 11 of 2007 Corporate Governance for Licenced Commercial Banks in Sri Lanka
    - The Board Integrated Risk Management Committee should establish a Compliance function to assess the Bank's compliance with laws, regulatory guidelines, internal controls, and approved policies on all areas of business operations.
    - A dedicated person selected from Key Management Personnel should carry out the compliance function and report to the Board Integrated Risk Management Committee periodically.

3. Financial Transaction Reporting Act No. 6 of 2006
    - Every institution is required to appoint a Chief Compliance Officer who shall be responsible for ensuring the Institution's compliance with the requirements of the Act.

4. In order to ensure that the Banks acts in compliance with the prevailing rules, regulation and Laws established in the country, the Compliance function among other things mainly considers following rules and regulations.
    - Convention on the Suppression of Terrorist Financing Act
    - Prevention of Money Laundering Act
    - Inland Revenue Act
    - Debt Recovery Act
    - Mortgage Act
    - Foreign Exchange Act
    - Labour laws
    - Stock Exchange Rules
    - Sri Lanka Accounting Standards
    - Securities and Exchange Commission Act No.

- Finance Act
- Withholding Tax Act
- Banking Act
- People's Bank Act

FINANCIAL CRIME AND ANTI MONEY LAUNDERING

The Bank adopted AML/ CFT Policy and Compliance Policy stating its commitment to comply with AML/CFT obligations under the law and regulatory directives and to actively prevent any transaction that otherwise facilitates criminal activity or terrorism.

The Bank has formulated and implemented internal controls and other procedures that will deter criminals from using its facilities for money laundering and terrorist financing and to ensure that its obligations are always met.

The Chief Compliance Officer has been designated with the relevant competence, authority and independence to implement the Compliance program approved by the Board of Directors/ Board Integrated Risk Management Committee. The Chief Compliance Officer will comply promptly with all the requests made pursuant with the law and provide information to the Financial Intelligence Unit (FIU) of Central Bank of Sri Lanka (CBSL).

The Compliance Policy of People's Bank covers following areas. (**Annexure 1**)

I. Overview of the Compliance Function
II. International Principles on Compliance Function
III. Compliance Function at People's Bank
IV. The Duties and Responsibilities of Chief Compliance Officer
V. Mandatory Compliance Functions
VI. Ancillary Compliance Functions
VII. Role of Compliance at People's Bank
VIII. Coverage
IX. Role of the Employees

As stated in the Compliance Policy, the Bank has put in place a Policy and Procedure on Anti Money Laundering and Combating of Financing of Terrorism for the Bank covering following areas (**Annexure 2**).

<u>Procedure</u>

The procedure for responding to authorized requests for information on money laundering and terrorist financing by the Financial Intelligence Unit (FIU) of the CBS should comply with the following:

(i) Searching immediately the Bank's records to determine whether it maintains or has maintained any account for or has engaged in any transaction with each individual, entity or organization named in the request;
(ii) Reporting promptly to the FIU the outcome of the search
(iii) Protecting the security and confidentiality of such requests
(iv) Gathering the information/ documents requested by FIU to carry out investigations on money laundering or terrorist financing.

(v) Handing over the documents and giving statements to law enforcement agencies such as CID, FCID, Bribery Commission etc. on the instructions of FIU.

(vi) Monitoring customer transactions and if suspicious forwarding a Suspicious Transaction Report (STR) to the Compliance Department.

COMPLIANCE MONITORING POLICY AND PROCEDURE

Compliance with Internal Policies

1. Code of Conduct

It is the Policy of the Bank to conduct its business in full compliance with the laws and regulations applicable to its business activities. To this end, all employees of the Bank are expected and directed to comply with the legislative /regulatory requirements and directions and to manage the business of the Bank with honesty, integrity and respect one another and the Bank as a whole.

To achieve this end the Code of Conduct of People's Bank provides an outline of the standards or professional and ethical conduct that all employees are expected to conform to, and to ensure that the employees are aware of the standards of personal integrity that are required when conducting the business of the Bank. (**Annexure 3**)

The Chief Compliance Officer is responsible for the effective administration and monitoring of the Code of Conduct which covers following areas:

I. Conduct
II. Responsibilities
III. Confidentiality
IV. Conflict of Interest
V. Insider Dealing/ Insider Trading
VI. Outside Employment
VII. Competition and Fair Dealing
VIII. Bribery and Corruption
IX. Customer Service and Handling Customer Complaints
X. Cleanliness, Hygiene and Safety
XI. Compliance with Laws, Regulations and Bank's Internal Circulars
XII. Protection and use of Bank Assets
XIII. Use of our Information System

2. Disciplinary Code

The Disciplinary Code of the Bank has been put in place for the disciplinary control of the employees of the Bank. Any employee found guilty of committing an act of misconduct by way of omission or commission are subject to disciplinary action under this Code. It also sets out the ways of responding to detected offences and penalties for non- compliance. (**Annexure 4**)

3 Customer Charter

The Customer Charter of the Bank has been compiled on the guidelines issued by the Banking Act Direction No. 8 of 2011 on "Customer Charter of Licensed Banks". Through the successful

implementation of this Charter the Bank aims to strive and improve the service provided by the Bank to its customers. (**Annexure 5**)

The Charter covers the areas such as

1. Information
2. Protection from Agents of the Bank
3. Handling Complaints
4. Special attention and care
5. Customer Obligations towards the Bank

COMPLIANCE RISK MANAGEMENT

The Compliance function shall discharge its responsibilities in a manner which is reflective of its assessment of the level and impact of the Compliance risk faced by the Bank. Accordingly, the Compliance function must give greater focus to areas where Compliance risk is assessed to be high, while preserving appropriate coverage of all Compliance risks identified.

Compliance Risk is the risk of legal and regulatory sanctions, material financial loss or loss to the reputation, a Bank may suffer as a result of its failure to comply with compliance laws, rules and regulations. This risk arises in following areas.

Institutional Compliance includes issues of governance, internal structure and decision-making process, principles of procurement, principles of Community Social Responsibility (CSR), disclosure policies, sustainability reporting and adherence to internal instructions.

Operational Compliance includes the assessment of integrity risk and reputation risk in the Bank's transactions, in particular certain principles, such as Anti-Money Laundering (AML), Counter Terrorist Financing (CTF) and Know Your Customer (KYC) as well as compliance issues in relation to the development of new products or business practices.

Conduct Compliance includes risk in terms of conflict of interest, insider trading and other issues related to professional conduct of members of the Board of Directors, Corporate and Executive management and all other Bank employees.

<u>Identification, assessment and monitoring of Compliance Risk</u>

The Compliance function shall identify and assess the Compliance risk associated with the Bank's activities. They shall have adequate knowledge and exposure to key business processes of the Bank Viz: Development of new products, the strategic planning process including entry into new lines of business, establishment of customer relationships and any material changes in the nature of such relationships and keep up with material changes in the Bank's business.

The risk assessment considers the effectiveness of the following elements:

a) Board and Senior Management oversight
b) Policies, Procedures and Limits
c) Risk monitoring and management information systems
d) Internal controls

Further, the Bank shall use a range of indicators to identify, assess and systematically monitor the level of Compliance risk. These indicators may be qualitative or quantitative in nature and may include, but are not limited to trends in customer complaints, irregular trading or payments activity and assessments by regulatory authorities.

The Bank shall establish principles to be followed by all officers and explain the main processes by which Compliance risk is identified and managed. As stated in the Compliance Policy, the primary responsibility to manage Compliance risk lies with the business lines and it is the responsibility of business lines to develop and update systems, policies, processes and procedures to manage Compliance risk inherent in business activities.

The Compliance function shall also perform appropriate tests to evaluate the adequacy of internal controls put in place to manage Compliance risk and promptly follow up on any identified deficiencies and plans to address such deficiencies.

KNOW YOUR CUSTOMER AND DUE DILIGENCE

Know your customer (KYC)

The Bank shall always establish any new business relationship only after all relevant parties to the relationship have been identified and the nature of the business they intend to conduct has been ascertained. Once a business relationship is established, any inconsistent activity shall be examined to ensure whether any element of suspicion is present.

The bank shall obtain information on Purpose of opening the account and usage, Expected source and nature of credits into the account, Anticipated volumes, Source of wealth and maintain the certified copies of the documents obtained to verify name, date of birth, nationality, address etc. as and when necessary.

The process is put in place to open accounts Non face to face using the electronic interface provided by the Department of Registration of Persons to identify and verify the authenticity of the customer.

Customer Due Diligence (CDD)

The Bank shall undertake customer due diligence measures when:

a) Business relationships are established;
b) Carrying out occasional transactions above the applicable designated threshold as may be determined by Financial Intelligence Unit (FIU) CBSL from time to time, including where the transaction is carried out in a single operation or several operations that appear to be linked;
c) Carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between banks;
d) There is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds;
e) There are doubts about the veracity or adequacy of previously obtained customer identification data.

Measures for CDD

a) The Bank shall identify its customers whether permanent or occasional; natural or legal persons and verify the customer's identity using reliable independently sourced documents, data or information.
b) It shall carry out on going due diligence on the business relationships to ensure that the transactions being conducted are consistent with the Bank's knowledge of the customer, it's business and risk profiles, and the source of funds.
c) It shall ensure that documents, data or information collected under the CDD process are kept up-to-date, particularly the records in respect of higher-risk business relationships or customer categories.
d) The Bank shall ensure that it does not keep anonymous accounts or accounts in fictitious names.

Risk Categorization

The Bank categorizes the customer based on risk at the opening of the account/ business relationship and shall perform enhanced due diligence for higher risk categories of customers, business relationships or transactions.

Steps shall be taken to review the risk rating initially given based on the risk status of the customer;

Low Risk- As and when necessary
Medium Risk- Once in every two years
High Risk- Annually
Also, where there are low risks, the Bank may apply reduced or simplified measures.

Politically Exposed Persons (PEPs)

Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions both in Sri Lanka and in foreign countries but are not limited to:

- Heads of State or Government
- Politicians
- Senior government officials
- Judicial or Military officials
- Senior executives of state-owned Corporations/ Government or Autonomous Bodies
- Family members and close associates of PEPs

Acting in accordance with the Guidelines on Identification of Politically Exposed Persons issued by the Financial Intelligence Unit, the Bank has established a Policy on Politically Exposed Persons and under the Policy PEPs have been divided to two categories as

- Internal PEPs (all Key Management Persons and above) &
- External PEPs (all categories described in the Policy and others decided by the Bank as per the risk).

The approval requirements vary for the said categories. As per the Policy,

- External PEPs

- Approval of the Corporate Management before entering into a relationship- The business lines have been instructed to forward the account opening requests of External PEPs and obtain the approval from Deputy General Manager (Channel Management).
- Approval of the Board of Directors has to be obtained to grant accommodation/ facilities of external PEPs except for Government salaried professional employees.

Internal PEPs

- approval is not needed to start a relationship.
- approval of the Chief Executive Officer/ General Manager to grant accommodation/ facilities.

Suspicious Transactions

Systems are put in place at the Bank to monitor suspicious transactions.

- Anti Money laundering monitoring system put in place shall send alerts to the Compliance Department and a team appointed to monitor alerts take necessary steps and forward to Chief Compliance Officer to file a Suspicious transaction report with FIU.
- If any feedback or more details/ information are required for a generated alert, the Compliance Department shall forward the alert to the relevant Business unit and the business unit shall give the necessary information within three working days.
- A follow-up mechanism shall be conducted by the Regional Head Office to ensure that the branches send the required information on time.
- The established system also facilitates the business units to forward details of a suspicious transaction to the Chief Compliance Officer.

ASSESSMENTS AND REVIEWS

1. Branch Assessments

   The Bank has appointed 24 Regional Compliance Officers to look after the compliance aspects of 24 regions of the Bank. In this context the appointed Regional Compliance Officers shall ensure that the branches coming under their purview

   - Act in compliance with rules and regulations issued by the Central Bank of Sri Lanka and other regulatory authorities.
   - Follow the instructions and guidelines issued by the Bank through Circulars.

   In order to ensure the above, among other things they shall

   - Conduct assessments of branches on a regular basis, using the approved check list, deciding the time frame of the re-visit according to the risk status of the Branch.
     - High Risk Branches/ Service Centres- Monthly
     - Medium Risk Branches/ Service Centres- Once in every two months
     - Low Risk Branches- Once in every three months
     - Low Risk Service Centres- Once in every six months
     - The branch shall be assessed through a marking scheme prepared for this purpose **(Annexure 6)** and forward to the Compliance Department.

- Marks will be allotted out of a total of 200 and the risk ratings given to the branches are as follows:
    - Up to 110- Low Risk
    - 111-190- Medium Risk
    - 191 and above- High Risk
- Compliance Department shall evaluate and maintain a soft copy of the reports and forward the report to the Regional Manager with instructions to rectify the errors.
- The Regional Managers shall forward the reports to relevant branches and inform Compliance Department on the steps taken within 14 days of sending the report.

- Carry on the error correction process pertaining to transactions of Rs. 1,000,000/- and above that has to be submitted to FIU.
    - The relevant report with errors marked shall be forwarded to the Channel Management Department with instructions to be circulated among Branch Network for data correction.
    - The Branch Network with the assistance of the Assistant Regional Managers and Regional Compliance Officers will update the Core Banking System with correct information.
    - The Assistant Regional Managers and Regional Compliance Officers shall ensure that the errors are rectified, and Core Banking System updated within the given time and send the confirmation to the Channel Management Department who will confirm same to Compliance Department.

2. Department Assessments

   The Core Departments/ Units which carry out activities under the guidelines of Central Bank of Sri Lanka shall be assessed by the Compliance Department. The assessments shall not be carried out at Finance and Management Accounting Department, as Compliance Department checks the accuracy of web returns prepared by Finance and Management Accounting Department.

   Compliance Risk status of the Core Departments/ Units shall be measured through the following marking scheme.

   a. Direct Responses
      Yes- 01 mark
      No- 00 mark

   b. Detailed Responses
      Not complied with- 01 mark
      Complied up to 50%- 02 marks
      Complied up to 75%- 03 marks
      Fully complied- 04 marks

The Department/ Unit shall be risk rated based on the total marks obtained as follows:

- 00-29 – Poor

- 30-59 – Average
- 60-89 – Good
- 90-100- Excellent

Continuous assessments shall be carried out by Compliance Department on a risk-based approach as follows:

- Poor- Re-visit within six months
- Average- Re-visit within one year
- Good- Re-visit within 18 months
- Excellent- Re-visit within 2 years

3. Reviews

- The Compliance Department shall carry out reviews of the branch assessments conducted by Regional Compliance Officers on a sample basis.
- Four branches per month shall be reviewed by the Compliance Department.
- The branches where the reviews should be carried out shall be decided based on the risk status of the branch at the end of every year. This list shall be included in the Annual Compliance Program and forwarded to the Board of Directors for their approval.
- The approved check list used by the Regional Compliance Officers shall be used to carry out the reviews as well.
- A report on the review findings shall be forwarded to the Channel Management Department instructing to rectify the errors and provide with an updated report within 14 days.

Regional Compliance Officers at their branch assessments shall decide the sample of accounts as follows:

- If number of Accounts opened at the branch in previous year is less than 3,000- 150 mandates
- If number of Accounts opened at the branch in previous year is between 3,000 & 6,000 - 200 mandates
- If number of Accounts opened at the branch in previous year is 6,000 or above- 250 mandates

Compliance Department at their branch reviews, shall decide the sample of accounts as follows:

- If number of Accounts opened at the branch in previous year is less than 3,000- 100 mandates
- If number of Accounts opened at the branch in previous year is between 3,000 & 6,000 - 150 mandates
- If number of Accounts opened at the branch in previous year is 6,000 or above- 200 mandates

4. Assessment of Subsidiary

Assessing the Compliance status of People's Leasing and Finance PLC shall be carried out through a questionnaire **(Annexure 7)** prepared on a quarterly basis. In addition, an on site review shall be conducted at People's Leasing and Finance PLC once in every two years. If any non-compliances are identified those shall be reported to the Board Integrated Risk Management Committee.

TRAINING

In house training shall be conducted by the Compliance Department covering all business units on following topics

- AML/KYC
- CDD Measures
- Risk Categorization
- Reporting Suspicious Transactions
- Right to Information Act
- AML System
- Other compliance related areas such as PEPs, Correspondence Banking, Abandoned property etc.

Training shall be conducted on an annually prepared training plan approved by the Board of Directors.

REPORTING REQUIREMENT OF FIU

As required by the provisions of the Financial Transaction Reporting Act, the Bank shall report transactions over Rs. 1,000,000/- to the Financial Intelligence Unit. The reports generated by the system will be forwarded to the Branch Network through Channel Management Department for error correction and system updation and once the corrections are done the report shall be submitted to FIU by the Chief Compliance Officer.

FOREIGN EXCHANGE COMPLIANCE

The Bank shall conduct its activities in compliance with Foreign Exchange regulations issued from time to time. The Directions, Circulars and instructions issued by the Department of Foreign Exchange shall be communicated by the relevant business unit to all employees of the Bank giving clear instructions on steps that should be adopted to be in compliance with the instructions issued by the Department of Foreign Exchange.

The Bank shall appoint a Compliance Officer to act as the Compliance Officer for Foreign Exchange matters and issues that has to be clarified shall be forwarded to the Department of Foreign Exchange through the appointed Compliance Officer.

The Bank shall forward all reports required under the Directions or Circulars issued, in the manner the Department of Foreign Exchange has prescribed on a timely basis.

BANK SUPERVISION DEPARTMENT

The Bank shall conduct its activities in compliance with Directions, Rules, Regulations, Instructions and Circulars issued by the Bank Supervision Department from time to time. All instructions issued by the Bank Supervision Department shall be communicated by the relevant business unit to all employees

of the Bank giving clear instructions on steps that should be adopted to be in compliance with the instructions issued.

The Bank shall forward all reports required under the Directions or Circulars issued, in the manner the Bank Supervision Department has prescribed on a timely basis. Also, the Compliance function shall ensure that all information requests forwarded by the Bank Supervision department are responded on a timely manner and all returns that should be submitted to the Bank Supervision Department through web are submitted on time.

The compliance function shall on a sample basis verify the accuracy of the web returns submitted to the Bank Supervision Department and ensure that accuracy of all returns will be checked within a period of three years following a risk-based approach.

The Compliance Department shall forward Affidavits and Declarations to the Bank Supervision Department on every new appointment/ change made to the Executive or Corporate Management of the Bank on a timely manner.

ANNUAL DECLARATION

The Annual Declaration (**Annexure 8**) that has to be made by all employees of the Bank at the beginning of every year shall be prepared and circulated by the Compliance Department under the signature of Chief Executive Officer/General Manager.

SUBMISSION OF AFFIDAVITS ON THE APPOINTMENT OF CHIEF EXECUTIVE OFFICER AND CORPORATE AND EXECUTIVE MANAGEMENT

As instructed by Bank Supervision Department of Central Bank of Sri Lanka, Affidavit introduced by Banking Act Determination No. 01 of 2019 on Assessment of Fitness and Propriety of Chief Executive Officer and Officers performing Executive Functions in Licensed Banks **(Annexure 9)** shall be completed by Compliance Department and forwarded to Bank Supervision Department for approval, under the signature of Chief Executive Officer/General Manager.

SUBMITTING PAPERS TO BOARD OF DIRECTORS AND BOARD INTEGRATED RISK MANAGEMENT COMMITTEE

The Compliance function shall update the Board of Directors on a monthly basis through a Board Paper submitted on the compliance status of the Bank. The Board Paper shall be prepared on the responses received from the Department Heads, Unit Heads and Regional Managers and the compliance status verified by the Compliance Department through their assessments and reviews.

Reports shall be submitted to the Board Integrated Risk Management Committee on a quarterly basis as and when a need arises.

RISK SCORE CARD

The Compliance Department shall prepare a risk score card at the end of each year calculating the compliance risk status of the Bank and forward same to the Board of Directors for their information and decision making.

CREDIT INFORMATION BUREAU

The Bank shall liaise with the Credit Information Bureau (CRIB) so that the customer credit information is accurately maintained on the CRIB system. Access to the site by the Bank Officers are through passwords authenticated by the CRIB Compliance Officer of the Bank. All resetting and issuing of new passwords for the branch users shall be handled by the Compliance function in collaboration with the Credit Information Bureau.

The Compliance function shall communicate with the Credit Information Bureau and the business units to address the issues in customer identification documents and system updations.

Trainings for the Bank officers who handle granting of credit facilities shall be organized by the Compliance Department with the participation of the Credit Information Bureau as and when required.

OFFICIAL LANGUAGE COMMISSION

The Compliance Department acts as the main correspondent unit of the Bank when transacting with the Official Language Commission.

It is the duty of the Bank to take steps to ensure that the Bank operates in compliance with the Directions and Instructions issued by the Official Language Commission. The Bank must take every step to have all documents and information in all three languages and must ensure that all communications with customers are made in all three languages as instructed by the Official Language Commission.

It is the duty of the Compliance function to ensure that these instructions are followed by the Bank and if any non-compliance exists take necessary steps to ensure compliance with the issued instructions.

RIGHT TO INFORMATION ACT

The Right to Information Act No. 12 of 2016 has been issued by the Government of Sri Lanka and as required by Section 23 of the Act the Bank has taken steps to establish a committee to act as Information Officers and another committee to act as Designated Officers.

The Committee of the Information Officers which consists of three members, including Chief Compliance Officer shall be responsible for dealing with requests for information made to the Bank and to render all necessary assistance to any citizen making such request to obtain information.

As directed by the Act, the Committee, on receipt of the request, takes immediate steps to inform the requestor that the response will be sent within 14 days and ensures that the reply is sent within the given time period.

The branch network has been instructed to forward every request they receive to the Chief Compliance Officer, and necessary steps are taken by the Chief Compliance Officer to ensure that the Bank acts in compliance with the provisions of the Right to Information Act.

Annexures:

1. Compliance Policy
2. Policy and Procedure on Anti Money Laundering and Combating of Financing of Terrorism
3. Code of Conduct and Amendments
4. Disciplinary Code
5. Customer Charter
6. Compliance Assessment check list
7. People's Leasing and Finance Questionnaire
8. Annual Declaration
9. Affidavit to assess Fitness and Propriety of Chief Executive Officer and Officers performing Executive Functions

COMPLIANCE POLICY

PEOPLE'S BANK

INTRODUCTION

People's Bank was established by the Government of Sri Lanka with a mandate to develop the Co-operative movement in Sri Lanka, rural Banking and agricultural sector credit by providing credit to co-operative societies, cultivation committees and other persons and is governed by the People's Bank Act No 29 of 1961 as amended and the Banking Act of Sri Lanka No. 33 of 1988 as amended.

Additionally, Bank is also required to comply with a large number of regulatory disclosures and prudential requirements. The Bank is also subjected to taxation and is bound to comply with various laws and regulations applicable to the Banking Industry.

In today's fast tracking global economy where there is a constant change in Laws and Regulations, it is possible to overlook and lost sight of laws and regulations that apply to our duties, thus creating violations which brings about sanctions. In this complexed environment each of us is challenged in the rapidly evolving business and it also impairs the good name and reputation of the Bank.

The Bank has to conduct its business with high standards of ethics and integrity in order to enhance the reputation with customers, stakeholders and regulators. Therefore, it is the policy of the Bank to conduct the business in full compliance with the laws and regulations applicable to the business. As such all employees of the Bank are expected and directed to comply with the legislative/ regulatory requirements and directions.

The Bank takes such steps as are necessary to ensure that in the performance of their responsibilities, staff, management, and the bank officials act in compliance with the highest standards of integrity in accordance with Laws and regulations to avoid or minimize the risks arising out of the Bank's activities.

To manage these issues the Bank has established a compliance function and has put in place a Compliance Policy of the Bank. This Policy which has been approved by the Board of Directors intends to present how People's Bank defines compliance and the role and responsibilities of the compliance function in the Bank.

Prepared based on the rules and regulations prevailing in the Banking industry, the International Principles and best practices on Compliance Function and directives issued by the Central Bank of Sri Lanka, this Policy is not a standalone document and must be read with the other Policies, Manuals, operating circulars of the Bank and Directions issued by the Central Bank of Sri Lanka in general. But in particular this Policy should be read with

- ✓ AML and CFT Policy
- ✓ Code of Best Practices in Corporate Governance
- ✓ Code of Conduct
- ✓ Disciplinary Code
- ✓ Customer Charter
- ✓ Whistle Blowing Policy
- ✓ Compliance Manual
- ✓ Right to Information Act No. 12 of 2016

The Compliance Policy will be subjected to review annually to ensure that it reflects developments in the market and best practices taking into account the changing environment of the Banking industry.

March 2023

COMPLIANCE FUNCTION

1.1 Overview

Compliance Risk is the risk of legal and regulatory sanctions, material financial loss or loss to the reputation, a Bank may suffer as a result of its failure to comply with compliance laws, rules and regulations.

Compliance starts at the top. It will be most effective in a corporate culture that emphasises standards of honesty and integrity and in which the Board of Directors and Senior Management lead by example. It concerns everyone within the Bank and should be viewed as an integral part of the Bank's business activities. A Bank should hold itself to high standards when carrying on business, and at all times strive to observe the spirit as well as the letter of the law. Failure to consider the impact of its actions on its shareholders, customers, employees and the markets may result in significant adverse publicity and reputational damage, even if no law has been broken[1]

A Bank's compliance function can be defined as

" An independent function that identifies, assesses, advises on, monitors and reports on the bank's compliance risk, that is, the risk of legal or regulatory sanctions, financial loss or loss to reputation a bank may suffer as a result of its failure to comply with all applicable laws, regulations code of conduct and standards of good practice".

The compliance function aims to prevent, and where necessary, identify and respond to any non-compliance with the Bank's obligations under the laws, regulations, codes and its own organizational standards. An important priority of the compliance function is to encourage a culture of valuing compliance with obligations, consistent with the profile of a good corporate citizen.

The International Principles on the Compliance Function laid down by the BASLE Committee on Banking Supervision are as follows:

1.2 International Principles on Compliance Function- BASLE Committee

1.2.1 Responsibilities of the Board of Directors for Compliance

Principle 1

The Bank's Board of Directors has the responsibility for overseeing the management of the Bank's compliance risk. The Board should approve the Bank's Compliance Policy, including a Charter or other formal document establishing a permanent compliance function. At least once a year, the Board or a Committee of the Board should review the Bank's Compliance Policy and its ongoing implementation to assess the extent to which the Bank is managing its compliance risk effectively.

1.2.2 Responsibilities of Senior Management for Compliance

Principle 2

The Bank's Senior Management is responsible for the effective management of the Bank's compliance risk.

Principle 3

The Bank's Senior Management is responsible for establishing and communicating a Compliance Policy, for ensuring that it is observed and for reporting to the Board of Directors on the management of the Bank's compliance risk.

Principle 4

The Bank's Senior Management is responsible for establishing a permanent and effective compliance function within the Bank as part of the Bank's Compliance Policy.

1.2.3 Compliance Function Principles

Principle 5

The Bank's compliance function should be independent.

Principle 6

The Bank's compliance function should have the resources to carry out its responsibilities effectively.

Principle 7

The responsibilities of the Bank's compliance function should be to assist Senior Management in managing effectively the compliance risk faced by the Bank. If any of the responsibilities of the compliance function are carried out by staff in different departments, the allocation of responsibilities to each department should be clear.

[1] Basel Committee on Banking Supervision

Principle 8
The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function.

1.2.4 Other Matters

Principle 9
Banks should comply with laws and regulations in all jurisdictions in which they conduct business, and the organization structure of the compliance function and its responsibilities should be consistent with local legal and regulatory requirements.

Principle 10
Compliance should be regarded as a core risk management activity within the Bank. Specific tasks of the compliance function may be outsourced, but they must remain subject to appropriate oversight by the Head of Compliance.

The Compliance Policy of the Bank is prepared based on the above rules together with the other international best practices followed in compliance and the rules and regulations introduced by the Central Bank of Sri Lanka.

COMPLIANCE FUNCTION AT PEOPLE'S BANK

2.1 Introduction
Violation of Laws and Regulations would bring about sanctions. It also impairs the good name and reputation of the Bank. Thus, an effective Compliance function is required to ensure that the Bank is insulated from such consequences.

Compliance with laws, rules and standards helps to maintain the Bank's reputation with, and thus meet the expectations of, its customers, the markets and the society as a whole. Although compliance with laws, rules and standards has always been important, compliance risk management has become formalized within the past few years and has emerged as a distinct risk management discipline.

Compliance should be a part of the culture of the Bank and it must just not be the responsibility of the compliance staff. However, the Bank can manage its compliance risk more effectively when the Bank has a separate compliance function in place, whose functions would include the following:

a) Ensure that the Banks Business activities are conducted in accordance with the laws and regulations pertaining to the industry.

b) Ensure that all employees of the Bank, follow accepted ethical standards in discharging their duties

c) Interpret the Laws and Regulations constructively so as to facilitate business but not to breach the spirit of such regulations or to endanger the reputation of the Bank.

d) Protect the Banks tangible and intangible assets, the financial security of the business and most importantly the good reputation of the Bank.

e) Provide regular updates to staff when there have been changes in legislations/regulations pertaining to the Banking business, so as to ensure compliance awareness at all times.

f) Ensure that there is an effective Corporate Governance culture across all levels of the Bank.

g) Align the Bank's corporate activities and behaviour to ensure that it operates in a safe and sound manner maintaining the trust and confidence of the public.

2.2 Regulatory Requirement

Establishment of an independent Compliance Function has been made mandatory for the Financial Institutions under following rules and guidelines:

2.2.1 Central Bank Circular No. PS/21/98 dated 14.9.1998 – Appointment of Compliance Officers

- The Banks should establish an independent compliance function to ensure compliance in respect of banking and other statutory requirements.
- Appoint a Compliance Officer with sufficient seniority.

2.2.2 Banking Act Direction No. 11 of 2007 – Corporate Governance for Licensed Commercial Banks in Sri Lanka

- The Committee shall establish a compliance function to assess the bank's compliance with laws, regulations, regulatory guidelines, internal controls and approved policies on all areas of business operations. A dedicated Chief Compliance Officer selected from Key Management Personnel shall carry out the compliance function and report to the Board Integrated Risk Management committee periodically.

2.2.3 Financial Transaction Reporting Act No. 6 of 2006

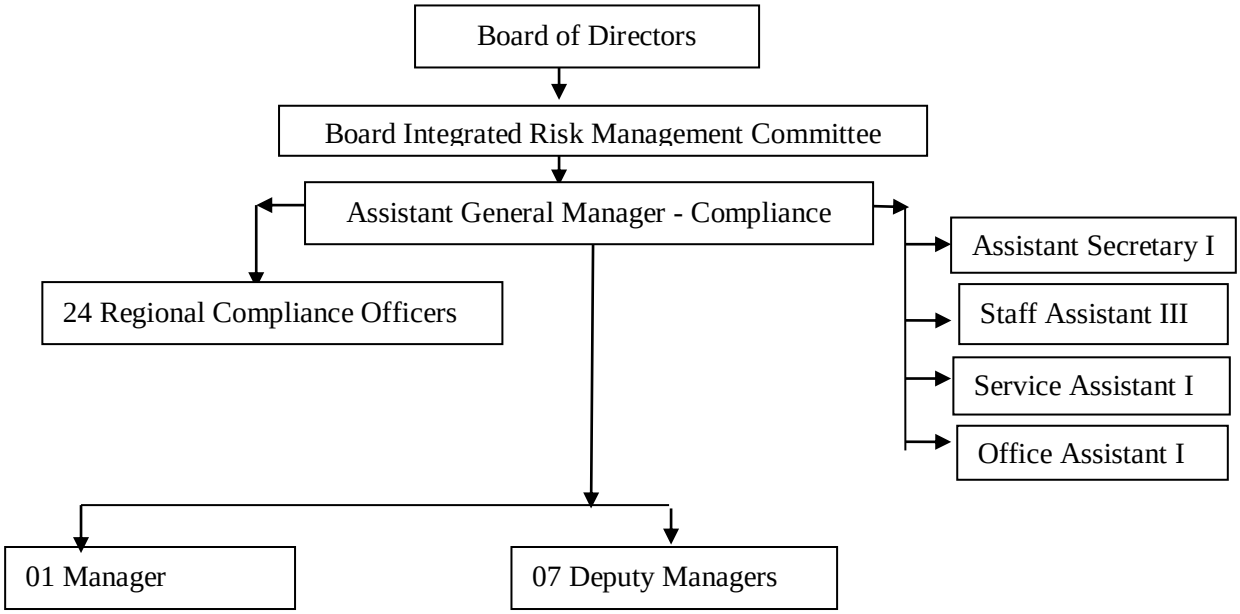
- Every institution shall be required to appoint a Compliance Officer who shall be responsible for ensuring the Institution's compliance with the requirements of the Act

2.3. The Duties and Responsibilities of the Chief Compliance Officer

Acting in compliance with the prevailing rules, at People's Bank the Chief Compliance Officer will be appointed from the Senior Management who will be a Key Management Person. The duties of the Chief Compliance Officer can be seen in two folds. The Chief Compliance Officer is mainly responsible in performing the mandatory

functions entrusted to him/her by the prevailing rules and regulations in the industry while carrying out the duties that can be considered as Ancillary Functions.

2.3.1 Organization Chart



In the Bank, the compliance function is managed by a dedicated Chief Compliance Officer. It is established as an independent unit and is not engaged in any other business of the Bank. The compliance function is responsible for coordinating the Bank's management of compliance risk. The compliance function is given access to all information and Departments, Branches, Units or Teams for the purpose of discharging its responsibilities in an independent manner and also has the right to conduct investigations of possible breaches of the Compliance Policy. Compliance function is also empowered to request assistance from specialists within the Bank and/or appoint outside experts to perform this task. It is further, free to report to the Board Integrated Risk Management Committee, Board Audit Committee and also to the Board of Directors of any breaches or non compliance of any policy, rule or regulation.

Also, the Compliance Function of the Bank is responsible for ensuring the Bank's compliance under the statutes which are put in place to prevent Money Laundering and Terrorist Financing. Namely,

- ✓ Convention on the Suppression of Terrorist Financing Act No. 25 of 2005
- ✓ Prevention of Money Laundering Act No. 5 of 2006
- ✓ Financial Transactions Reporting Act No. 6 of 2006

Additionally, it is also responsible for the implementation of

- ✓ Central Bank Guidelines on Know Your Customer (KYC) and Customer Due Diligence (CDD)
- ✓ Guidelines on Identification of Beneficial Ownership for Financial Institutions
- ✓ Guidelines on Politically Exposed Persons

Thus, the duties and responsibilities of the compliance function are defined below:

2.4 Mandatory Compliance Functions

- Develop compliance policies and procedures designed to eliminate or minimize the risk of non-compliances with regulatory requirements and damage to the Bank's reputation and to ensure these policies and procedure are adhered to in the spirit as well as in the letter.

- Develop a Code of Conduct/Ethics for staff setting out the best practices and to monitor and ensure compliance with it at all levels.

- Develop an Anti Money Laundering and Combating of Financing of Terrorism Policy together with the Know Your Customer (KYC) regulations to be issued and adhered to across all branches, units and departments of the Bank.

- Maintain regular contact and a good working relationship with regulators based upon clear and timely communication and a mutual understanding of the regulator's objectives.

- Promote, across the Bank network, and wherever it is considered appropriate, best practices developed in the areas of Compliance.

- Understand and apply, all new legal and regulatory developments relevant to the business of the Bank.

- Provide timely reports to management with information on regulatory developments, changes in the law and any other developments insofar as they give rise to compliance issues relevant to the Bank's business.

- Highlight serious, or present, compliance problems and where appropriate work with Management to ensure that they are rectified within an acceptable time frame.

- Ensure that the relevant business units submit accurately completed Daily/Weekly/ Fortnightly/Monthly/Quarterly/Annually Compliance reports to the Central Bank of Sri Lanka on the Banks compliance with Central Bank Directives and Guidelines as and when required by Law.

- To prepare and submit a Risk Assessment Report of the Bank annually to Board Integrated Risk Management Committee.

- To prepare and submit Quarterly Compliance reports to the Board Integrated Risk Management Committee and the Board Audit Committee as and when necessary and monthly reports to the Board of the Bank on the Bank's Compliance with Statutory regulations applicable to the banking business.

- Put in place a Customer Charter for the Bank prepared based on the Directions issued by the Central Bank of Sri Lanka in this regard.

- Prepare a Code of Best Practice in Corporate Governance for the Bank based on the Central Bank Directive on Corporate Governance for LSB's and be responsible for implementation and monitoring compliance with the same.

- Function as the Anti Money Laundering Compliance Officer, responsible to have in place systems and controls for monitoring transactions and reporting of suspicious transaction to the Financial Intelligence Unit. Also responsible to train staff on compliance matters including AML and developing of an e-learning module to ensure that the training needs of entire branch network is fulfilled.

- Prepare all other Policies and implement Procedures to minimize Compliance Risk and Reputation Risk for the Bank.

- Act as the CRIB Compliance Officer and liaise with Credit Information Bureau in order to maintain updated credit details of the customers.

- Act as the Information Officer appointed under the Right to Information Act and take measures to ensure that timely actions are being taken by the Bank to be in compliance with the Right to Information Act.

2.5 Ancillary Compliance Functions

- Provide an advisory service to Management and Staff in relation to regulatory, reputational and ethical matters.

- Promote throughout the business the belief that compliance is not a negative process but a positive contribution to the success of the Bank, so that the principles and importance of compliance are clearly understood by all.

- Secure early involvement in the design and structuring of new products and systems to ensure that they conform to local regulatory requirements and internal compliance and ethical standards.

- Ensure that compliance aspects of all Statutory Web Returns submitted to Central Bank of Sri Lanka will be checked within a time period of Three Years following a risk based approach.

- Ensure that assessments and reviews are undertaken at appropriate frequencies to assess compliance with regulatory rules and internal compliance standards as follows.

- ✓ The Regional Compliance Officers to visit the branches coming under their purview as stated below and assess the compliance status of the branches using the check list approved by the Board Integrated Risk Management Committee:

  Branches
  - Low Risk- Once in every three months
  - Medium Risk- Once in every two months
  - High Risk- Monthly

  Service Centers
  - Low Risk- Once in every six months
  - Medium Risk- Once in every two months
  - High Risk- Monthly

- ✓ Compliance Department to review the compliance status of four branches per month selecting the branches on a risk based approach and the risk rating to be calculated based on the scores given by the Regional Compliance Officer.

- ✓ Compliance Department to carry out compliance assessments of Head Office Departments which are subject to the rules and regulations issued by the Central Bank of Sri Lanka and risk rate the Departments. Thereafter, subsequent reviews to be conducted following risk based approach.

- ✓ Compliance Department to carry out compliance assessments of its Subsidiaries which are governed by the rules and regulations of Central Bank of Sri Lanka as follows
  - Quarterly- Through a Questionnaire
  - Once in every two years- Conducting on site examination

- Represent the compliance function on relevant internal and external committees.

- Ensure that compliance policies and procedures are clearly communicated to Management and Members of Staff.

- Liaise with the Bank's audit function, both internal and external, to ensure that auditors are familiar with local regulatory and ethical requirements so that they are able to ensure that compliance issues are properly addressed.

- Those compliance weaknesses identified as a result of audits are followed up.

The Compliance Function though established as an independent unit within the Bank, acts hand in hand with all other Departments, specially, Risk Management, Internal Audit, Channel Management and Process Management Departments in order to ensure that the Bank acts in compliance with all rules and regulations within the business while providing a fully compliant banking service to the customers.

Thus the Compliance Function of the Bank, is not merely a policing function but rather one that is designed to assist all employees and the Bank in complying with the laws pertaining to the industry.

ROLE OF COMPLIANCE AT PEOPLE'S BANK-LEGAL & REGULATORY BACKGROUND AND APPLICABILITY

The Compliance Function at People's Bank is aimed at establishing a fully complied compliance environment at Head Office and across its branch network. Keeping this in mind, the Bank has set up the compliance function as a part of the culture of the Bank. As stated above, though the compliance function acts hand in hand with other functions of the Bank it is established separately and independently. While confirming the status of compliance of the Bank it also assists all employees and the Bank to act in compliance with the laws and regulations prevailing in the industry.

In order to achieve same, the Bank applies all Laws, rules and standards of the industry, such as laws on Money Laundering and Terrorist Financing, rules imposed in relation to carrying out Foreign Exchange Transactions, conduct of other businesses, privacy, data protection, etc., which are relevant to the business activities taking place throughout the Bank.

The applicable laws, rules and standards are likely to have various sources, including primary legislation, rules and standards issued by supervisors, market conventions, codes of practice promoted by industry associations and

internal codes of conduct applicable to the staff members of the Bank. They are likely to go beyond what is legally binding and embrace broader norms of integrity and fair dealing.

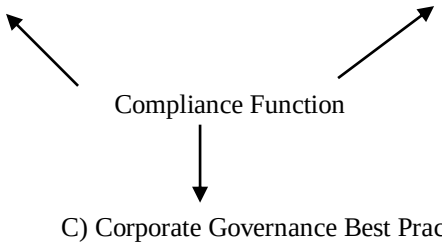
3.2 Decisions of the Bank

- ✓ Establish a Compliance Department under the guidance of the Chief Compliance Officer who is dedicated to the task of overseeing People's Bank Policies, Procedures and Practices.
- ✓ Establish a culture that values and rewards the implementation of appropriate controls and compliance procedures.
- ✓ Use independent audit, risk management and compliance functions to help evaluate the Bank's compliance with applicable laws, rules and regulations.
- ✓ To rely on those closest to the customers- local branch manager to provide guidance and understand fully with whom we are doing business with and to ensure that the business we conduct on behalf of our customer is proper.
- ✓ Continue to update our policies and procedures that meet or exceed applicable norms in the banking industry.
- ✓ Develop internal procedures and technology that assist us in monitoring transactions for the purpose of identifying possible suspicious and/or illegal activities.
- ✓ Report to the Board of Directors and its sub committees any material compliance failures in the Bank.
- ✓ Ensure through the Board and its sub committees that compliance issues are resolved effectively and expeditiously by Senior Management with the assistance of the compliance function.
- ✓ Assess the status of performance of the branch network through Regional Compliance Officers.
- ✓ Audit, assess and review the status of performance of the branch network, Subsidiaries which are governed by the rules and regulations of Central Bank of Sri Lanka as well as other Departments through Audit, Risk and Compliance.
- ✓ Train the existing staff as well as the new recruits on compliance issues.
- ✓ Liaise with Credit Information Bureau in order to maintain updated credit details of the customer.
- ✓ Act as a member of the Committee appointed as Information Officers under Right to Information Act to ensure that the Bank take steps to act in full compliance with the Act.

3.3. Coverage

A) External Regulations

B) Internal Regulations



C) Corporate Governance Best Practices

3.3.1 Compliance with External Regulations

i. Presently following Statutes/ Regulations are mainly applicable to the operations of the Bank.

- Banking Act
- People's Bank Act
- CRIB Act

- Withholding Tax Act
- Finance Act of Sri Lanka
- Companies Act
- Securities and Exchange Commission Act
- Accounting Standards of Sri Lanka
- Rules of the Stock Exchange
- Labour Laws
- Foreign Exchange Act
- Mortgage Act
- Debt Recovery Act
- Inland Revenue Act
- Prevention of Money Laundering Act
- Financial Transaction Reporting Act
- International Convention on the Suppression of Terrorist Financing Act
- Right to Information Act

ii. Pursuant to the Banking Act, the **Central Bank** issues Directives/Regulations from time to time, which Banks are required to comply with.

3.3.2 Compliance with Internal Policies

✓ **Code of Conduct**

It is the Policy of the Bank to conduct its business in full compliance with the laws and regulations applicable to its business activities. To this end, all employees of the Bank are expected and directed to comply with the legislative/ regulatory requirements and Directions and to manage the business of the Bank with honesty, integrity and respect to one another and the Bank as a whole.

As such, the Code of Conduct of People's Bank provides a general outline of the standards of professional and ethical conduct that all employees are expected to conform to, and to ensure that the employees are aware of the standards of personal integrity that are required when conducting the business of the Bank.

The Chief Compliance Officer is responsible for ensuring the effective administration and monitoring of the Code of Conduct which covers following areas:

i. General Conduct
ii. Responsibilities
iii. Confidentiality
iv. Conflict of Interest
v. Insider Dealings
vi. Outside Employment
vii. Competition and Fair Dealing of People
viii. Bribery and Corruption
ix. Customer Service and Customer Complaints
x. Cleanliness, Hygiene and Safety
xi. Compliance with Laws, Regulations and Bank Circulars
xii. Protection and the use of the Bank Assets
xiii. Use of the Computer System

✓ **Policy on Anti Money Laundering and Combating Financing of Terrorism**

The Chief Compliance Officer is responsible for ensuring that the Bank has systems and procedures in place for prevention of Money Laundering and Terrorist Financing and as such is responsible for co-ordinating and monitoring compliance of the Anti Money Laundering Policy. People's Bank Anti Money Laundering Policy covers the areas such as

1. Know Your Customer Policy
2. Suspicious Transaction Reporting
3. Record keeping requirements for Banks
4. Training
5. Anti Money Laundering Monitoring Controls and Penalties
6. Combating of Terrorist Financing
7. Financial Action Task Force (FATF) Recommendations

8. Basel Policies on Know Your Customer and Customer Due Diligence for Banks and Financial Institutions

Legislation

1. Prevention of Money Laundering Act No. 5 of 2006
2. Financial Transactions Reporting Act No. 6 of 2006
3. Convention on the Suppression of Terrorist Financing Act No. 25 of 2005

✓ **Disciplinary Code**

Disciplinary Code of People's Bank has been put in place for the disciplinary control of the employees of the Bank. Any employee found guilty of committing an act of misconduct, by way of omission or commission are subject to disciplinary actions under this Code. Disciplinary Code also sets out the ways of responding to detected offences and penalties for non compliance.

✓ **Customer Charter**

The Customer Charter of People's Bank is put in place in compliance with the guidelines issued by Banking Act Direction No. 8 of 2011 on "Customer Charter of Licensed Banks". Through the successful implementation of this Charter the Bank aims to strive and improve the service provided by the Bank to its customers. The Charter covers the areas such as

1. Information
2. Protection from Agents of the Bank
3. Handling complaints
4. Special attention and care
5. Customer obligations towards the Bank.

✓ **Compliance Manual**

The Compliance Manual is intended to define the roles and responsibilities regarding management of Compliance risk of the Bank. This manual describes the Policy established and details the procedure adopted in its implementation. The Manual covers the areas of;

- International Principles on Compliance Function
- Regulatory Framework
- Financial Crime and Anti Money laundering
- Compliance Monitoring Policy and Procedure
- Know Your Customer and Due Diligence
- Assessments and Reviews
- Training
- Reporting Requirement of FIU
- Exchange Control Compliance
- Bank Supervision Department
- Annual Declaration
- Submitting Papers to Board of Directors and Board Integrated Risk Management Committee
- Risk Score Card
- Credit Information Bureau
- Official Language Commission
- Right to Information Act

3.3.3 Code of Best Practice in Corporate Governance

Code of Best practice in Corporate Governance provides the structure through which the objectives and performance of the Bank is determined. The Code of Best Practice in Corporate Governance has been put in place complying with the Corporate Governance rules of the Code of Best Practice of Corporate Governance laid down as per Central Bank Direction No. 11 of 2007 as amended. The areas covered under this Code are

1. Principles of good Corporate Governance
2. Authority and Duties of the owner
3. The Board of Directors
4. The Chief Executive Officer and the Corporate Management
5. Performance viability and sustainability
6. Reporting and Accountability
7. Sub Committees of the Board
8. Subsidiary Companies

9. Regulatory Environment
10. Meeting of the General Body

3.4 Role of the Employees

In accordance with the rules and regulations, the Bank has established the Compliance Department as a separate unit headed by the Chief Compliance officer. However, acting in compliance with the prevailing laws, rules and regulations in the industry it is not just the responsibility of the compliance department. The employers of the Bank also have a duty to act in accordance with the prevailing laws, rules and regulations. To be effectively established compliance must start from the top and flow down to the employees.

3.4.1. Duties

a) Assist the Board in their tasks by conducting the day to day operations correctly, promptly and transparently.

b) Being professional in the role you play and being ethical, honest and just in all decisions made.

c) Assisting the Board and the Sub Committees in setting goals and targets for the institution and working together in achieving same.

d) Ensuring that there are no conflicts of interest.

e) Adhering to the Banks Code of Conduct and Disciplinary code and thereby ensuring the highest standards of Compliance & Governance.

3.4.2. Communication

It is the duty of each and every employee to speak up about their genuine concerns in relation to activities which they feel are wrong or illegal or otherwise harmful to the interests of the Bank. These will include but not limited to

- ✓ Disclosure of confidential information
- ✓ Allegations of any fraudulent activity including misusing the Bank records, misuse of Bank assets or misuse of the computer system of the Bank.
- ✓ Any non compliance with any of the policies of the Bank, Central Bank guidelines or any rule or regulation issued by any other authority.
- ✓ Any suspicion on money laundering or terrorist financing
- ✓ Insider Trading/ Insider Dealing

It is the policy of the Bank that any employee raising a concern in the genuine belief that a wrong doing has occurred or is about to occur will not be penalized in any way, even if after the investigation it is found that the concern was a mistake.

The Bank has introduced a Whistle Blowing Policy in the Bank under which any form of reprisal against anyone, who in good faith has raised a concern, is forbidden and shall be regarded as a serious offence and shall be dealt with as recommended by the Board Audit Committee. This Policy addresses the areas such as

1. Types of concerns that can be raised
2. Procedure
3. Maintenance of records
4. Protection
5. Roles, Rights and Responsibilities of the Whistle Blower

3.4.3. Procedure

The Whistle Blowing Policy states the procedure to say that employees shall report allegations or concerns first to the immediate senior officer. However, if the employee feels uncomfortable or reluctant to discuss the matter with the immediate senior officer or foresees a conflict of interest the employee can address the matter to the Board Audit Committee directly.

Thus, the overall responsibility of the compliance function is to assist the Bank in identifying, assessing, monitoring and reporting on compliance risk in matters relating to the institution, its operations and to personal conduct. By this the compliance function contributes in an independent manner to the overall risk management of

the Bank in protecting the integrity and reputation of the Bank and the staff and to strengthening the Bank's accountability and transparency.

PEOPLE'S BANK

POLICY & PROCEDURES

ON

ANTI MONEY LAUNDERING (AML)

AND

COMBATING OF FINANCING OF TERRORISM (CFT)

JANUARY 2023

(VERSION 1.8)

CONTENTS

		Page Nos.
1	People's Bank Policy on Anti Money Laundering and Combating of Financing of Terrorism	05-07
2	Legal Framework for Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) in Sri Lanka	08-10
3	Financial Intelligence Unit Rule No. 01 of 2016- Financial Institutions (Customer Due Diligence) Rules	11-29
4	Applicability of FIU Rule No. 01 of 2016	30-32
5	Suspicious Transaction/ Business	33-38
6	Anti Money Laundering (AML)/ Combating of Financing of Terrorism (CFT) – Monitoring and Controls	39-40
7	Risk Categorization Methodology	41-42
8	Risk Management	43-45
9	Identification of Beneficial Owners	46-47
10	Politically Exposed Persons	48-51
11	Glossary	52-54
12	Attachments: i. Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 1 of 2018 ii. Guidelines for Financial Institutions on Suspicious Transactions Reporting No. 6 of 2018 iii. Guidelines on CCTV operations iv. Guidelines on Identification of beneficial Ownership for Financial Institutions, No. 4 of 2018 v. A list of categories of customers that can be considered as PEPs vi. A list of Red Flags and Indicators for suspicion vii. Guidelines for Non Face to Face Customer Identification and Verification No 3 of 2020	

►*Introduction*

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

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

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

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

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

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

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

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

1. PEOPLE'S BANK POLICY ON ANTI MONEY LAUNDERING AND COMBATTING OF FINANCING OF TERRORISM

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

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

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

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

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

- Establishment of a Compliance Department under the Chief Compliance Officer who is dedicated to the task of overseeing People's Bank's policies, practices and procedures with regard to ML & TF.
- Establishment of a culture that values and rewards the implementation of appropriate controls and compliance procedures.
- Use of independent compliance, audit and risk management functions to help evaluate the Banks compliance with applicable ML & TF laws, rules and regulations.
- The Bank relies on those closest to its customers - the local Branch Manager to provide guidance and understand fully with whom we are doing business with – "**Know Your Customer" (KYC)** and to ensure that the business we conduct on behalf of our customers is proper.
- Development of internal procedures and technology that assists the Bank in monitoring transactions for the purpose of identifying possible suspicious activities.
- The Bank will continue to update its policies and procedures that meet or exceed applicable norms in the Banking Industry both locally and globally.
- Submitting reports on AML/ CFT risk on a quarterly basis to the Board of Directors to enable the Board to take necessary steps to mitigate the risk.
- The Bank recognizes and is aware that preventing ML & TF and adhering to KYC principles is an on going process that involves constant diligence and the difficulties faced when the Bank tries to keep pace with the ever more sophisticated schemes employed by criminals.

In line with the directives received, a policy document with following sections covering various functional aspects of KYC norms and Anti Money Laundering and Combating of Financing of Terrorism (AML & CFT) measures are set out herein.

a) What is Money Laundering and Terrorist Financing
b) The Sri Lankan Legislation
c) Know Your Customer (KYC) and Customer Due Diligence (CDD), based on the Financial Institutions (Customer Due Diligence) Rule No. 1 of 2016 issued by the Central Bank of Sri Lanka.
d) Applicability of the Directive at People's Bank
e) Identifying and reporting Suspicious Transactions
f) Risk Management and Monitoring Controls
g) Beneficial Owners
h) Politically Exposed Persons

A. What is Money Laundering

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

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

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

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

a) The real source of criminal money must be concealed and will not be done with public knowledge.

b) The form in which money is held must be changed in order to hide identity.

c) The trail of transaction must be obscured to defeat any attempted follow-up by law enforcement agencies.

d) The launderer must maintain constant control on the monies as he cannot legally declare any theft of such money.

C. Stages of Money Laundering

Money Laundering occurs in three stages -

Stage 1- Placement
Placement means the consolidation and placement of different proceeds of criminal money in the financial system through different sources, or smuggling them out of the country. The objective of the launderer is to remove the proceeds of the illegal transaction to another location without detection and to transform them into transferable assets.

Stage 2 - Layering

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

Stage 3 - Integration

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

D. What is Terrorist Financing?

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

Article 2

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

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

    b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict or otherwise and the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an International Organization to do or to abstain from doing any act; or

    c) any terrorist act.

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

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

A) PREVENTION OF MONEY LAUNDERING ACT (PMLA)

- The offence of Money Laundering is defined as receiving, possessing, concealing, investing, depositing or bringing into Sri Lanka, transferring out of Sri Lanka or engaging in any other manner in any transaction, in relation to any property derived or realized directly or indirectly from "Unlawful Activity" or proceeds of "Unlawful Activity".

- Any movable or immovable property acquired by a person which cannot be part of the known income or receipts of a person or money/ property to which his known income and receipts have been converted, is deemed to have been derived directly or indirectly from unlawful activity, in terms of the PMLA.

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

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

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

  b. Persons who receive possess or come into control of property derived directly or indirectly from the commission of predicate offences, knowing or having reason to believe the true nature of such

property (to this group belong persons employed at Financial Institutions/ Banks) which are used by criminals to launder ill gotten money.

- Following are considered as Predicate Offences

  Offences under-
  - The Poisons, Opium and dangerous Drugs Ordinance
  - Laws or Regulations relating to prevention and suppression of terrorism
  - The Bribery Act
  - Firearms Ordinance, Explosives Ordinance, Offensive Weapons Act etc.
  - Laws relating to cyber crimes
  - Laws relating to offences against children
  - Laws relating to offences against trafficking of persons
  - Any law punishable with death or imprisonment of seven years or more, whether committed within or outside Sri Lanka.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Introduction

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

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

As required by the above rules the Bank shall

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

- Documenting the risk assessments and findings
- Considering all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied
- Keeping the assessment up to date through a periodic review and
- Having appropriate mechanisms to provide risk assessment information to the supervisory authority.

✓ Have proper risk control and mitigation measures including

- Internal policies, controls and procedures to manage and mitigate money laundering and terrorist financing risks that have been identified.
- Management Information systems that provide reliable data on the quantity and nature of Money Laundering/ Terrorist Financing risks and effectiveness with which risks are being mitigated.
- Monitor the implementation of those policies, controls, procedures and enhance them if necessary and
- Take appropriate measures to manage and mitigate the risks, based on the risk based approach.

✓ Conduct risk profiling on the customers considering

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

- Products, services, transactions or delivery channels of the customer (cash based, face to face or non face to face, cross- border) and
- Any other information regarding the customer.

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

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

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

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

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

- Results of monitoring activities carried out for combating money laundering or terrorist financing risks.
- Details of recent significant risks involved in either internally or externally and its potential impact to the Bank
- Recent developments in written laws on money laundering and suppression of terrorist financing and its implications for the Bank.

CDD for All Customers

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

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

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

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

a. Entering into business relationships;

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

- 1. The Bank shall-
  a. Identify its customers prior to entering into business relationships;
  b. Obtain the information specified in Rule No. 1 of 2016, verify such information, as applicable and record same for the purpose of identifying and initial risk profiling of customers, at the minimum;
  c. Obtain following information for the purpose of conducting CDD, at minimum:
     i. Purpose of the account;
     ii. Sources of earning;
     iii. Expected monthly turnover;
     iv. Expected mode of transactions;
     v. Expected type of counterparties (if applicable).

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

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

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

- If there is a beneficial owner, the Bank shall obtain information to identify and take reasonable measures to verify the identity of the beneficial owner of the customer using relevant information or data obtained from a reliable source, adequate for the Bank to satisfy itself that the Bank knows who the beneficial owner is.

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

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

- In any case where the delayed verification is allowed following conditions shall be satisfied:
  a. Verification shall be completed as soon as it is reasonably practicable but not later than 14 working days from the date of opening the account;

b. The delay shall be essential so as not to interrupt the normal conduct of business of the Bank; and
c. No suspicion of money laundering or terrorist financing risk shall be involved.

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

- The Bank shall take the measures to manage the risk of delayed verification which may include limiting the number, type and amount of transactions that can be performed, as stated in chapter 4 of this Policy.

- If the Bank is unable to act in compliance with the above, it shall
  a. In relation to a new customer, not open the account or enter into the business relationship or perform the transaction; or
  b. In relation to an existing customer, terminate the business relationship, with such customer and consider filing a suspicious transaction report in relation to the customer.

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

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

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

  ii. The background and purpose of such transactions shall be inquired into and findings shall be kept in record with a view to making such information available to the relevant competent authority when required and to make suspicious transaction reports.

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

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

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

- The frequency of the ongoing CDD or enhanced ongoing CDD shall commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profiles and nature of transactions.

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

- The Bank shall perform such CDD measures as may be appropriate to the existing customers based on its own assessment of materiality and risk but without compromise on the identity and

verification requirements. In assessing the materiality and risk of an existing customer, the Bank may consider the following-

a. The nature and circumstances surrounding the transaction including the significance of transaction;
b. Any material change in the way the account or business relationship is operated; or
c. The insufficiency of information held on the customer or change in the information of the customer.

- The Bank shall conduct CDD on existing customer relationships at appropriate times, taking into account whether and when CDD measures have previously been conducted and the adequacy of data obtained.

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

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

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

- The Bank shall

a. With regard to transactions or series of linked transactions exceeding Rs.200,000/- or its equivalent in any foreign currency conducted by occasional customers, one off customers or walk in customers conduct CDD measures and obtain copies of identification documents;
b. With regard to occasional customers, one off customers or walk in customers who wish to purchase remittance instruments such as pay orders, drafts exceeding Rs.200,000/- or its equivalent in any foreign currency conduct CDD measures and obtain copies of identification documents;
c. With regard to all cash deposits exceeding Rs.200,000/- or its equivalent in any foreign currency made into an account separately or in aggregate by a third party customer, have on record the name, address, identification number of a valid identification document, purpose and the signature of the third party customer.

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

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

CDD for Legal Persons and Legal Arrangements

- The Bank shall in the case of a customer that is a legal person or legal arrangement,

a. Understand the nature of the business of the customer, its ownership and control structure;
b. Identify and verify the customer in terms of the requirements set out below.

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

    a. Identity of all Directors and Shareholders with equity interest of more than 10% with the requirement imposed on the legal person to inform of any change in such Directors and Shareholders;
    b. If there is a doubt as to whether the person with the controlling ownership, interest is the beneficial owner or where no natural person exerts control through ownership interest, the identity of the natural person, if any, exercising control of the legal person or arrangement through independent sources;
    c. Authorization given for any person to represent the legal person or legal arrangement either by means of Board Resolution or otherwise;
    d. Where no natural person is identified under the preceding provisions, the identity of the relevant natural persons who hold the positions of senior management;
    e. When a legal person's controlling interest is vested with another legal person, the Bank shall identify the natural person who controls the legal person.

- In order to identify the beneficial owners of a legal arrangement, the Bank shall obtain and take reasonable measures to verify the following-

    a. For Trusts, the identities of the author of the Trust, the trustees, the beneficiary or class of beneficiaries and any other natural person exercising ultimate effective control over the Trust (including those who control through the chain of control or ownership); or
    b. For other types of legal arrangements, the identities of persons in equivalent or similar positions.

Non Governmental Organizations, Not for Profit Organizations or Charities

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

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

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

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

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

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

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

Customers and Financial Institutions from High Risk Countries

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

  2. The Secretary to the Ministry of the Minister to whom the subject of Foreign Affairs has been assigned or the subject of Defence has been assigned, as the case may be, shall specify the high risk countries referred above-

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

  ii. independently taking into account, the existence of strategic deficiencies in anti money laundering and combating of financing of terrorism policies and not making sufficient progress in addressing those deficiencies in those countries.

  iii. Upon specifying the high risk countries as specified in (ii) above the Bank shall publish the list of high risk countries in its official website.

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

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

  a. Limiting business relationships or financial transactions with identified countries or persons located in the country concerned;
  b. Review and amend or, if necessary terminate, correspondent banking relationships with Financial Institutions in the country concerned;
  c. Conduct enhanced external audit, by increasing the intensity and frequency, for branches and subsidiaries of the Financial Institution or financial group, located in the country concerned; and
  d. Conduct any other measures as may be specified by the Financial Intelligence Unit.

Politically Exposed Persons (PEPs)

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

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

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

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

Correspondence Banks

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

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

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

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

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

(iii) core business activities;

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

(v) Money laundering prevention and detection measures;

(vi) The purpose of the account or service;

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

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

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

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

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

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

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

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

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

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

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

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

Wire Transfers

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

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

- The Bank shall ensure that all cross-border wire transfers to be always accompanied with the following :-

(a) Originator information :-

(i) name of the originator;

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

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

(b) beneficiary information : -

(i) name of the beneficiary; and

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

- Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country and shall include the originator's account number or unique transaction reference number.

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

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

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

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

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

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

Intermediary Financial Institution

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

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

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

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

  (a) when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and

  (b) what is the appropriate follow up action.

Beneficiary Financial Institution

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

- For cross-border wire transfers, the Bank shall verify the identity of the beneficiary, and maintain the information in accordance with the Act if the identity has not been previously verified.

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

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

  (b) what is the appropriate follow up action

Money or Value Transfer Service Providers

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

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

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

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

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

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

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

- 1. The Bank shall follow special precautionary measures to make a distinction between formal money transmission services and other alternative money or value transfer systems (ex: hundi, hawala etc.) through which funds or value are moved from one geographic location to another, through informal and unsupervised networks or mechanisms.

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

B. Account Opening Guidance

I. Face to Face

1. Individual Customer

(a) The following information shall be obtained:

(a1) In the case of all customers

- Full name as appearing in the identification document;
- Official personal identification or any other identification document that bears a photograph and the NIC Number of the customer (ex: National Identity Card for citizens of Sri Lanka and valid Passport for foreigners)
- Permanent address as appearing on the identification document. If residential address differs from the permanent address residential address shall be supported by a utility bill not over three months old or any other reliable proof of residence. Utility bills are to be specified as electricity bill, water bill and fixed line telephone operator's bill. No post box number shall be accepted except for state owned enterprises. In the case of "C/O", property owner's consent and other relevant address verification documents are required to be obtained.
- Telephone number, fax number, and e-mail address;
- Date of birth;
- Nationality;
- Occupation, business , public position held and the name of employer and geographical areas involved;
- Purpose of which the account is opened;
- Expected turnover/ volume of business;
- Expected mode of transactions;
- Satisfactory reference as applicable; and

(a2) In the case of non- resident customers

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

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

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

2. Proprietorship/ Partnership Accounts

(a) The following information shall be obtained

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

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

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

3. Corporation/ Limited Liability Company

(a) The following information shall be obtained

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

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

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

- Copy of the Certificate of Incorporation;
- Copy of Form 40 (Registration of an existing company) or Form 1 (Registration of a company) under the Companies Act and Articles of Association;
- Board Resolution authorizing the opening of the account;
- Copy of form 20 (change of Directors/ Secretary and particulars of Directors/ Secretary) under the Companies Act;
- Copy of form 44 (full address of the registered or principal office of a company incorporated outside Sri Lanka and its principal place of business established in Sri Lanka) under the Companies Act;
- Copy of Form 45 List and particulars of directors of a company incorporated outside Sri Lanka with a place of business established in Sri Lanka) under the Companies Act;
- Copy of the Board of Investment Agreement, if a Board of Investment approved company;

- Copy of the export Development Board (EDB) approved letter, if EDB approved company;
- Copy of the certificate to commence business, if a public quoted company;
- Name of the person or persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board resolution as the case may be;
- Latest audited accounts if available.

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

4. Clubs, Societies, Charities, Associations and Non Governmental Organization

(a) The following information shall be obtained

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

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

- Copy of the registration document/ Constitution/ Charter etc.;
- Board Resolution authorizing the account opening;
- Names of the persons authorized to give instructions for transactions with a copy of the Power of Attorney or Board/ Committee Resolution.

➢ Bank accounts for charitable and aid organizations and Non Government Organizations (NGO)s should be opened only with the registration of the regulatory authority empowered to regulate charitable and aid organizations, non-governmental organizations and non-profit organizations for the time being and with other appropriate credentials. Due regard should be paid to specific directions governing their operations i.e. issued by the Department of Bank Supervision and Department of Supervision of Non Bank Financial Institutions of the Central Bank and the Director- Department of Foreign Exchange.

5. Trusts Nominees and Fiduciary Accounts

(a) The following information shall be obtained

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

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

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

6. Stocks and Securities Sector specific requirements

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

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

(b) Certification requirement-

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

(A) For non-resident applicant-

- By the Company Registrar or similar authority;
- By a Sri Lankan Diplomatic Officer or Sri Lankan Consular Officer in the country where the documents were originally issued;
- By a Solicitor, an Attorney-at-Law, a Notary Public practicing in the country where the applicant resides;
- By the Custodian Bank;
- By the Global Custodian (the Custodian Bank shall certify the authenticity of the signature of the Global Guardian) or
- By a Broker.

(B) For resident applicants-

- By the Registrar of Companies or the Company Secretary (applicable in respect of corporate bodies);
- By an Attorney-at- Law or a Notary Public;
- By a Broker; or
- By the Custodian Bank.

The person certifying shall place the signature, full name, address, contact telephone number and the official seal (Not applicable for Brokers, Custodian Banks and Global Custodians)

Where the application is titled in the name of the 'Registered Holder/ Global Custodian/ Beneficiary' and forwarded through a Custodian Bank, a copy of the SWIFT message or similar document issued by the Global Custodian instructing the local Custodian bank to open the account on behalf of the Beneficiary company shall be submitted together with a Declaration from the Global Custodian that a custody arrangement or agreement exist between the Global Custodian and Beneficiary.

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

The Bank should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview.

II. 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.

1. 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.
2. 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.
3. Also steps shall be taken to obtain the quality images of passport
4. The electronic interface provided by Department of Registration of Persons shall be used by the Bank to independently verify the identity of the customer.
5. The Bank shall be responsible with ensuring AML/CFT compliance of all parties involved with online payment platforms introduced by the Bank and shall take steps to act in compliance with the provisions of Financial Transaction Reporting Act, Financial Institutions (Customer Due Diligence) Rules and all other Rules, Regulations and Guidelines issued thereunder in relation to followings for all parties involved in online payment platforms.
    - Identification and verification of customers
    - Conduct ongoing due diligence on customers and scrutiny of transactions
    - Identification and reporting of suspicious transactions
    - Wire transfer requirements
    - Targeted financial sanctions screening
    - Record keeping
    - All other reporting requirements

C. General Provisions

1. The Bank is required to appoint a Key Management Person who is from Senior Management level of the Bank as the Chief Compliance Officer, who shall be responsible for ensuring the institution's compliance with the requirements of the Act and the above said Rules.

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

3. Develop and implement a comprehensive employee due diligence and screening procedure to be carried out at the time of appointing or hiring of all employees whether permanent, contractual or outsourced.

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

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

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

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

8. The Bank shall
   - ✓ Undertake the risk assessments prior to the launch or use of new products and technologies;
   - ✓ Take appropriate measures to manage and mitigate the risks which may arise in relation to the development of new products and new business practices and
   - ✓ Monitor pre-loading of credit cards, as that may amount, inter-alia, to the abuse of credit cards, for money laundering or terrorist financing purposes, file a Suspicious Transaction Report if suspicious transactions are detected.

D. <u>Record Keeping</u>

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

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

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

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

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

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

For the purpose of this rule relevant domestic authority means-

a. Any public authority (including a supervisory authority established as independent non-governmental authority with statutory powers) with designated responsibilities for prevention of money laundering and suppression of terrorist financing;
b. Any authority that performs the function of investigating and prosecuting money laundering and terrorist financing associated offences and seizing or freezing and confiscating assets relating to such offences; and
c. Any authority receiving reports on cross border transportation of currency.

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

E. Miscellaneous

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

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

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

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

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

21. When Foreign Currency Accounts and temporary rupee accounts are opened for non-nationals/foreign passport holders who are resident in Sri Lanka, a local address shall be obtained as their permanent address during their stay in the Island. A copy of the passport, visa with validity period, foreign address and the purpose for which the account is opened shall be made available in the file. On the expiry of the visa, the account shall cease to operate unless and otherwise appropriate instructions are received. On leaving the Island the account shall either be closed or be converted into a non-resident account. The Bank shall ensure that a valid visa is held at all times by the clients during the continuation of the account with them.

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

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

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

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

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

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

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

4. APPLICABILITY OF FIU RULE NO. 01 OF 2016

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

It is the Policy of the Bank to prevent the use of its facilities for the laundering of money derived from criminal activities. All Employees must be alert to the possibility of the Bank being unwittingly involved in the activities of third parties, who may seek to use bank facilities to hide the source of criminal funds.

As such,

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

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

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

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

The following are the broad guidelines in this regard:

1. Individual/Joint Accounts

a) The individual Account opening/Mandates and information profile of the customers (KYC Form) which is prepared incorporating the basic requirements should be duly completed by the Customer/s and also signed by them as being correct. An authorized officer must put his signature in this document to certify that the information was

provided in his/her presence and the Manager, after perusing all account opening documents must sign the mandate certifying the accuracy of the documents obtained.

b) The Operations Manager/ Branch Manager should also fill out the Risk Categorization form as a means of assessing the risk of Money Laundering/Terrorist Financing, before the end of each working day for accounts opened on a particular date. This is the responsibility of the Operations Manager/ Branch Manager.

The branch network is also required to monitor the transactions of

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

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

- A photocopy of the identification document
- A copy of the Address Verification Document, in the event, the current address of the customer differs from that of the Identification Document
- Any other additional document specified in Chapter 3.

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

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

b) Additionally, for

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

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

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

iv) NGOs/ Charities/ Clubs/ Societies/ Other
02 office bearers who are the authorized signatories of the entity to complete individual profile of the customer (KYC) form

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

d) The Operations Manager/ Branch Manager should also fill out the Risk Categorization form as a means of assessing the risk of Money Laundering/ Terrorist Financing, before the end of each working day for accounts opened on a particular date.

General Guidelines

1. All staff members are required to comply with the FIU Directives on Know Your Customer (KYC) and Customer Due Diligence (CDD) at all times. This has been communicated through the Chief Compliance Officer's Circular Letter No.6552/2007 dated 4th September 2007 and Compliance Officer Circular Letter Nos. 6552/2007(1) dated 24.8.2012 and 6552/2007(2) dated 15.3.2016.

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

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

4. The following important provisions are further highlighted:

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

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

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

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

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

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

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

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

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

5. SUSPICIOUS TRANSACTION/BUSINESS

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

"Where an Institution –

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

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

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

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

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

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

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

Suspicious Cash Transactions

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

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

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

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

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

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

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

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

Suspicious Transactions using Customers' Accounts

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

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

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

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

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

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

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

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

Suspicious Investment Related Transactions:

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

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

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

Suspicious Transactions using Electronic Banking Services

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

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

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

Suspicious International Banking and Financial Transactions

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

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

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

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

Suspicious use of Letters of Credit (LC)

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

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

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

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

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

Suspicious Loan Transactions:

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

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

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

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

Informal Value Transfer Systems (IMVTS)

1. Receipt of foreign remittances to accounts initially and its gradual decrease/cessation followed by the receipt of Sri Lankan Rupees.

2. Receipt of frequent third-party deposits and transfer of those funds to multiple third party accounts.

3. Minimal / no ATM withdrawals but substantial number of online debit fund transfers from accounts with names of receivers as narrations.

4. Receipt of frequent third-party deposits and withdrawal of such funds from abroad.

5. Accounts having an insignificant daily balance but an unusually high credit and debit turnover.

6. It inquiries are made by the Bank, accountholders themselves declaring to be engaged in IMVTS operations.

Scams

1. A local person establishes a banking relationship on behalf of a third party, maybe a foreigner.
2. The accounts are operated by a third party or a foreigner(s).
3. Often customers' use of forged / stolen NICs to establish business relationships.
4. The customer's company name is very similar to a very well-known, global company name, but not quite the same (e.g., P&G Printing, GE Electricians, Amazing Books)
5. The customer's company name or email address is not available in the internet.
6. The individual who operates the account(s) hardly visits a bank branch.
7. Majority of ATM transactions are carried out from locations which are not in the vicinity of the customer's residential address or the employment address.
8. The withdrawals are carried out using ATM machines and often they use the ATMs of the other banks.
9. Often uses ATMs situated in under-lit areas.
10. Avoids the CCTV cameras at or in the vicinity of ATMs.
11. The account holder cannot be contacted: the correspondence sent to the customer repeatedly returned as undeliverable despite having an active account with ongoing transactions.
12. Deposits are made stating the purpose as "custom fees", "clearance fees", etc.
13. Frequent third-party deposits but depositors identify themselves in the deposit slip or in the remarks in an online transfer using their names and NICs.
14. An inquiry or a complaint from a third party regarding the account stating that the account holder is collecting funds.

Recognizing & Reporting Of Suspicious Transactions

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

Reporting
In the first event of your suspicion:

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

How to report a Suspicious Transaction

To reiterate, the law requires employees to report any reasonable suspicion that they may have about a customer or his/her transactions.

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

Reporting procedures

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

- the suspected customer or any other related person is not alerted
- the matter is dealt with quickly and professionally
- the external authorities are notified and provided with the necessary records, if appropriate

The Bank has put in place procedures to report suspicions with supporting information,

i. Through the format issued to the branch network.
ii. Through the AML system put in place to monitor suspicious activities.

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

Role of the Chief Compliance Officer on receiving the Report

At the Bank,

- when the Chief Compliance Officer receives the Suspicious Transaction Report, (STR) the Chief Compliance Officer shall decide whether the report gives rise to knowledge or suspicion that a customer is involved in money laundering.
- If further information is needed the Chief Compliance Officer shall collect the required information from the relevant branch/ unit.
- If the Chief Compliance Officer believes that the suspicions may be justified and require further investigation, must report to the Financial Intelligence Unit (FIU)

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

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

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

The importance of timing

The Bank is aware that,

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

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

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

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

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

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

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

CHIEF COMPLIANCE OFFICER

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

Responsibilities of the Chief Compliance Officer

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

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

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

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

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

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

  a) Provide feedback to staff on compliance queries.

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

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

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

Independent Compliance Testing

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

Record Keeping Obligations

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

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

It is also required that :

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

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

All records maintained should be available to authorized persons promptly on request without undue delays.

7. RISK CATEGORIZATION METHODOLOGY

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

- evidence of an individual's permanent address sought through independent verification by field visits;
- personal reference (i.e. by an existing customer of the same institution);
- prior bank reference regarding the customer and the customer contact with the Bank;
- The customer's source of wealth;
- Verification of details relating to employment, public position held (previous/present), if any, supplied by the customer.
- Obtaining & verifying additional information on the customer such as details of occupation, volume of assets, information available in public data- bases, internet search, etc.)
- Regular updation of identification data of customer and Beneficiary owner
- Obtaining additional information on nature of business
- Obtaining information on reasons for transactions performed
- Obtaining information on source of funds/ wealth of the customer
- Obtaining the approval of Senior Management.

A. Low Risk

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

Example:

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

B. Medium Risk

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

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

Example:

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

C. High Risk

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

Examples:

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

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

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

a. Low Risk Customers – Once in every three years

b. Medium Risk Customers – Once in every two years
c. High Risk Customers – Annually

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

8. RISK MANAGEMENT

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

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

- The front office functionaries (Counter Staff) at the operational points are vested with greater responsibility of effectively administering KYC procedures to protect bank against financial frauds and Money Laundering & Terrorist Financing. The bank resolves that the KYC requirements shall be realised without inconveniencing the customer and rather it shall be through convincing them that it is well intended in their long term interest and in the interest of the Banking Community and the Regulator.

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

  The operational staff shall continue to be trained on an on-going basis on the basic requirement of proper,
  - Customer identification or KYC
  - Maintenance of records of transactions and identification

- Listing and submission of details of large value currency transactions reports which will certainly help banks to check/reduce operational risks and also vulnerability to frauds.

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

- The bank shall continue to ensure that compliance to KYC guidelines is evaluated periodically in the background of the conditions obtained in respect of the bank's Policies, system and Procedures, Legal and Regulatory requirements. Compliance Report on the implementation of KYC guidelines shall continue to be placed at the Board of Directors monthly.

- The Bank shall ensure that the Internal Audit Department regularly/periodically and the Compliance Department randomly observe audit requirements of KYC guidelines and verification of its implementation at branches and other operational units of the Bank.

CCTV Operations

- In order to enhance operational risk management and safeguard the Bank being abused for money laundering and financing of terrorism, the Bank shall have in place a fully operational robust CCTV system installed both within and outside of the premises of the Bank such as Head Office, Branches, areas of Automated Teller Machines, Cash Deposit Machines etc.

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

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

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

- The CCTV systems of ATMs and CDMs shall remain operational throughout 24 hours of a day, every day of the year including the times when the Bank is closed for business.

- Real time monitoring shall be conducted by the Bank and the services of the security services personnel or Law enforcement agencies shall be obtained to mitigate the immediate risk, if such risks are detected.

- The Bank shall maintain information captured in the CCTV system for a minimum period of 90 days but shall retain for a longer period if suspicious activities are observed. Furthermore if instructions are received from Law Enforcement Authorities or any other Competent Authority the Bank shall retain CCTV recordings relevant to a suspicious Transactions Report furnished to FIU until the relevant investigations are concluded.

- The Bank shall ensure that CCTV system is capable of transferring the information to data storage devices.

- The Bank shall,

- Allocate adequate resources with sufficient training
- Ensure that CCTV systems are properly maintained and equipped with relevant features and functions to enable implementing control measures
- Ensure that all information and records are maintained safely and securely without unauthorized access
- Have procedures and mechanisms to ensure that Regulator, Law Enforcement Authorities and FIU are able to obtain information and records
- Put in place periodical review and audit of CCTV systems and submit the report on the same to the Board of Directors and Senior Management
- Ensure that based on the report submitted the Board of Directors and Senior Management shall take appropriate steps to rectify deficiencies identified, increase the coverage, replace or upgrade the equipment
- Ensure activities relating to maintenance and recalibration of CCTV system are clearly recorded in the system's maintenance log and reported to the Senior Management.

Instructions issued by Financial Intelligence Unit are attached.

Training to Staff members (KYC/ AML/ CFT)

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

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

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

Customer Education

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

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

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

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

9. IDENTIFICATION OF BENEFICIAL OWNERS

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

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

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

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

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

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

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

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

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

8. Furthermore, the Bank shall take steps to identify the beneficial owners through following means;
    - Share Register
    - Annual Returns
    - Trust Deed
    - Partnership Agreement
    - Constitution and/ or Certificate of Incorporation
    - Constitution of a registered co-operative society
    - Minutes of the board meetings
    - Information that can be obtained by open source search or commercially available databases.
    - Verification through mother company or branches, Correspondence Bank, other agents of the Bank, Corporate Registries etc. (for foreign legal persons & arrangements)
    - Relevant identification information available from reliable sources such as public registers (for Companies listed in Stock Exchange)

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

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

11. 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

12. A delayed verification is permitted to be carried out to verify the identity of beneficial owners when;
    - risk level of the customer is low & verification is not possible at the point of entering into the business relationship
    - there is no suspicion of money laundering or terrorist financing risk involved
    - delay will not interrupt the normal conduct of business

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

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

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

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

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

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

10. POLITICALLY EXPOSED PERSONS

Regulatory Framework

The Regulatory framework consist of two regulations issued by the Financial Intelligence Unit (FIU) of Central Bank of Sri Lanka and Financial Action task Force (FATF) recommendations titled International Standards on combating Money laundering and the Finance of Terrorism and Proliferation. Two related regulations issued by FIU are

- Customer Due Diligence Rules No. 01 of 2016
- Guidelines on identification of Politically Exposed persons No. 03 of 2019

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.

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 step-children and adopted children) and their spouses
- Parents (including step-parents)
- 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 (specially those who are acting in a financial fiduciary capacity) of PEPs.

Procedure adopted at the Bank

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

i. Local PEPs
- 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 Sabas 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.

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

- 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.

- 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.

ii. 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.

iii. Duration of Treating a Person as a PEP

- Members of Parliament/ Provincial Councils/ Pradeshiya Sabas/ Municipal Councils immediate family members and close associates- as PEPs for life time

- 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.

iv. Identification of PEPs

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.

v. 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 (Deputy General Manager- Channel Management) 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 shall be granted with the prior approval of the Board of Directors.

vi. General Provisions

a. 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.

b. 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.

c. 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.

d. 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

e. 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 o the findings of the assessment.

GLOSSARY

Beneficiary –

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

Beneficiary Financial Institution –

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

Beneficial Owner –

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

Board of Directors –

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

Customer –

In relation to a transaction or an account includes –

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

(e) Such other person as may be prescribed.

Correspondent Banking –

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

Close Associate Includes –

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

Controlling Interest –

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

Company Act –

The Companies Act No.7 of 2007.

Existing Customer –

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

Financial Action Task Force –

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

Financial Group –

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

Finance Company –

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

Immediate Family Member –

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

Intermediary Financial Institution –

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

Legal Person –

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

Legal Arrangement –

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

Licensed Bank –

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

Majority- owned subsidiary –

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

MVTS –

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

Money Laundering –

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

Ordering Financial Institution –

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

Person –

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

Politically Exposed Person –

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

Payable through Account –

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

Risk Based Approach –

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

Shell Bank –

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

Straight through Processing –

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

Terrorist Financing –

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

ශ්‍රී ලංකා මහ බැංකුව
fNa0 It›{B M6uf5I
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය නිතියිියල් උළවරිතල් පිරිවු **Financial IntelIIgence Unit**

Guideline No. 1/18

Ref: 037/05/002/0018/017

11" January 2018

To: CEO's of All Financial Institutions

Dear Sir/Madam,

Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. o6 of 2006 and the Financial Institutions (Customer Due Diligence) Rules, No. ol of 2016.

This guideline shall be treated as minimum instructions and indications to identify and assess the risk of Money Laundering & Terrorist Financing (ML & TF) in their businesses and take effective measures to mitigate the identified risk. It is important that all financial institutions will prepare their own risk assessment and mitigation report in line with this guidelines.

Yours Faithfully,

Director
Financial Intelligence Unit

Cc : Compliance Officer

14 වන මහල, අංක 30, ජනාධිපති මාවත, ¥4 @iâ iocq. g•c. ›o e +«@ud? +ocei@mg Qsc@fi›+j i Level ¥4 , Pa. 30, Jaiiadhipathl Maratha,
තැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව த. பெ. இல. 590, கொழும்பு 01, இலங்கை P. O. Box. 590, Colombo 01, Sri Lanka.

94 14 2477125/509 94 11 2477692 fiu@cbsLlh www.fiusrilanha.Nov.ik

Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018

Introduction

1. The Financial Intelligence Unit of Sri Lanka (FIU), acting within the powers vested with it under the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA), issued the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 by Gazette Extraordinary No. 1951/13, dated January 27, 2016; effective from the date of issue, applicable to institutions which engage in "finance business" as defined under Section 33 of the FTRA.

2. As applicable under Rule 3 of the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016, the rules introduce, inter alia, provisions requiring financial institutions identified under the rules to take measures specified therein for the purpose of identifying, assessing, and managing Money Laundering (ML) and Terrorist Financing (TF) risks posed by its customers and business activities.

Risk Management

3. Every Financial Institution should identify and analyze ML/TF risks present within the financial institution and design and effective implementation of policies and procedures that are commensurate with and that mitigate the identified risks to ensure sound ML/TF risk management.

4. In conducting a comprehensive risk assessment to evaluate ML/TF risks, every financial institution should consider all the relevant risk factors present in its customer base, products, delivery channels and services offered (including products under development or to be launched) and the jurisdictions within which it or its customers do business.

5. Risk assessments should be based on specific operational and transactional data and other internal information collected by the financial institution as well as external sources of

information such as national risk assessments conducted by Sri Lanka and by governmental agencies of foreign jurisdictions where the financial institution has business relationships, either through customers or branch/subsidiary networks, country reports from reliable international and regional organizations, such as reports and reviews prepared by the Financial Action Task Force (FATF), FATF-style regional bodies such as the Asia/Pacific Group on Money Laundering (APG), International Monetary Fund (IMF) and World Bank publications, and information from reliable commercial intelligence providers.

6. Financial Institutions are required to have a risk management framework to address ML/TF risks. Such a framework includes policies, controls and procedures that enable them to identify, measure, monitor, control and mitigate effectively the ML/TF risks that have been identified.

Risk Management Framework

Corporate Governance

7. The FIU expects financial institutions to establish a robust and effective corporate governance framework that ensures transparency, accountability and high ethical conduct in all aspects of their operations. Institutions should adopt a Code of Ethics that promotes consistently high standards of ethical conduct by all employees. A sound corporate governance framework includes the use of effective policies and procedures, monitoring and reporting mechanisms and internal controls. Measures that ensure appropriate separation of functions and the avoidance of conflicts of interests are essential hallmarks of an effective corporate governance regime. The Board of Directors (BoD) is ultimately responsible for establishing a corporate vision, strategy and business model and for overseeing an institution's corporate governance culture and is expected to develop mechanisms including board committees to achieve this objective. Senior management is responsible for ensuring the effective functioning of the corporate governance framework on a day-to day basis.

I. Board of Directors (BoD)

8. Members of the BoD should have a good understanding of the institution's business model and operations and the general business climate in which it operates. They should have the qualifications and experience necessary to understand the institution's business model and operations and how these relate to Sri Lanka's general economic and social environment. The BoD should ideally be comprised of both executive and non-executive directors to ensure a desirable level of independence from the institution's management function.

9. The BoD should establish the institution's overall risk appetite and should ensure that mechanisms are in place to effectively mitigate risk. The BoD must ensure that appropriate policies, procedures and controls are in place to manage such risks and should also ensure that arrangements are in place for the effective reporting on all issues related to the functioning of the risk management framework. The BoD is ultimately responsible for the institution's operations, its management of the risk to which it is exposed and its compliance with all laws, regulations and guidelines to which it is subject.

II. Senior Management

10. An institution's senior management is responsible for implementing the corporate vision, strategy and business model approved by the BoD. Senior management should demonstrate a firm understanding of all aspects of the institution's business model and is responsible for developing the components of the risk management framework. Senior management is responsible for ensuring that the institution has all the resources necessary to effectively manage risk. They are also responsible for ensuring that effective communication and reporting arrangements are in place to support good risk management practices. This includes ensuring that all staff members are aware of the requirements of the risk management framework and their specific roles and responsibilities. Senior management is responsible for ensuring that internal reporting mechanisms, including reports to be sent to the BoD, are developed to provide accurate and timely information relevant to the effective management of risks.

The Risk Management Function

11. The FIU expects institutions to develop an effective risk management function. The risk management function responsible for ensuring that the institution effectively identifies, measures, monitors, and controls and mitigates risks. From a day-to-day operational perspective risk management supports senior management and the BoD to achieve the ML/TF risk management objectives discussed in this guidance note. The risk management function should be commensurate with the, size, nature and complexity of the institution's business model and operations.

Policies and Procedures

12. The FIU expects the senior management to develop policies and procedures to effectively manage the ML/TF risks that arise from an institution's operations. Policies and procedures developed by senior management should be approved by the BoD. Policies and procedures should set out the day-to-day measures that should be employed to ensure that the institution effectively identifies, measures, monitors and controls ML/TF risks. They should therefore be developed to reflect the risks implicit in an institution's customers, products and services, delivery channels and geographic regions. Policies and procedures should be comprehensively documented and communicated to all staff. They should also be subject to periodic review to ensure they are appropriate in light of changes to the institution's ML/TF risk profile.

13. Policies and procedures should clearly set out lines of responsibility and accountability for the execution of the risk management function and should also establish effective reporting lines for all persons and business units involved in the management of ML/TF risks.

14. An effective risk management framework should establish limits in the context of the institution's stated appetite for ML/TF risk and the overall effective implementation of the risk management system. Policies and procedures should limit, for example, an

institution's exposure to the ML/TF risks arising from exposure to specific types of customers, products and services, delivery channels and geographic regions. An effective ML/TF risk management framework should include a mechanism to report incidents where established limits have been breached and the frequency of such events.

Internal Controls

15. An on-going system of internal controls is an essential component of a risk management framework. Institutions are expected to employ measures on an on-going basis to ensure adherence to establish policies and procedures as well as relevant laws, regulations and guidelines.

16. Arrangements should be in place to reinforce the "four eyes" principle and avoid conflicts of interest. Measures should be employed, for example, to ensure adequate separation between operational and control functions such as front office and back office activities.

17. Institutions are expected to develop effective internal audit arrangements. The internal audit function should be an independent function with a direct reporting line to the Board Audit Committee. The internal audit function should periodically assess the effectiveness of the institution's ML/FT risk management framework and practices paying specific attention to the institution's adherence to established policies procedures and limits and applicable laws, regulations and guidelines.

18. Institutions are also expected to ensure that their ML/TF risk management framework and practices are subject to external audit review.

The Compliance Function

19. The FIU expects institutions to develop an effective compliance function as a component of its ML/TF risk management framework. The compliance function should be commensurate with the, size, nature and complexity of the institution's business model and

operations. The compliance function is separate from the internal audit function as it is a component of an institutions day-to-day operational activity. The compliance function should on an-ongoing basis assess the extent to which the institution is complying with established policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines. The effectiveness of the compliance function rests heavily on the effectiveness with which the Mangement Information System (MIS) generates accurate and timely reports related to the management of ML/TF risks. Compliance officer should possess sufficient seniority and knowledge and be up to date with recent laws and regulations

Risk Monitoring and Reporting

20. To effectively control and mitigate risk, institutions may need to develop MIS systems that provide reliable data on the quantity and nature of ML/TF risks and the effectiveness with which risks are being mitigated. The MIS system used by an institution should be commensurate with the size, nature and complexity of its business model and operations. Such systems should constantly measure ML/TF risks, changes to the nature of such risks and should also report on adherence to the policies and procedures designed to mitigate risks. The system should, for example, not only identify instances in which policies and procedures have been breached but should maintain a record of all such incidents. The system should provide timely reports to all business units and senior management to allow them to make judgments on the measures necessary to manage risks. Reports should also be prepared and submitted to senior management and the BoD indicating how well the institution is managing risk and highlighting instances of breaches of risk management policies, procedures and limits and obligations arising from applicable laws, regulations and guidelines.

Training

21. The FIU expects institutions to have effective arrangements in place to train their staff on all issues related to their AML/CFT regime. It is important that staff understand the institution's inherent ML/TF risks and the nature of the measures that have been developed

to mitigate these risks. Training must be provided for all staff upon joining the institution and should be an-ongoing activity. Apart from general training provided to all staff, targeted training programs should be developed for specific categories of staff in light of the nature of their work in the context of ML/FT risks. AML/CFT awareness raising programs should be conducted for members of the BoD.

Assessing ML/TF Risk – Some Guidance

22. The following guidance sets out a methodology for the conduct of an assessment of ML/TF risks by a financial institution. It is not mandatory to follow this methodology, however, the FIU requires that each financial institution should undertake a comprehensive assessment of its ML/TF risks and develop appropriate risk management processes.

I. Identification of Vulnerabilities:

23. Financial Institutions are required to take appropriate steps to identify aspects of their business activities, including types of customers and transactions, which may be vulnerable to ML/TF and should in doing so, take into account the findings of the National Money Laundering and Terrorist Financing Risk Assessment of Sri Lanka[1]. Financial institutions should consider the following areas when identifying risk factors of their business that make them susceptible to ML/TF.

i. The nature, size and complexity of the business

The size and complexity of a financial institution plays an important role in how attractive or vulnerable it is for ML/TF. For example, a large financial institution is less likely to know its customers personally and this could offer a greater degree of anonymity to customers than a smaller financial institution.

[1] A copy of this report can be found at the FIU's website, http://www.fiusrilanka.gov.lk/docs/Other/Sri_Lanka_NRA_on_ML_2014_-_Sanitized_Report.pdf

Similarly, a financial institution that conducts complex transactions across international jurisdictions could offer greater opportunities for ML/TF than a purely domestic business.

ii. The products and services the business offers

Some products and services are more attractive for ML/TF. When considering whether the products and services the business offers could be susceptible or attractive for ML/TF, the following is a list of indicators (not exhaustive) that identifies ML/TF risk arising from products and services that are commonly offered by financial institutions.

- private banking services such as prioritized or privileged banking
- credit/ debit and other top-up cards
- non- face-to-face business relationship or transaction
- payment received from unknown or unrelated third parties
- any new product & service developed
- services to walk-in customers
- mobile banking
- single premium insurance policy

iii. The types of customers the financial institution deals with

Listed below are some indicators (not an exhaustive list) to identify ML/TF risk arising from customers.

Categories of customers pose a higher risk of ML/TF can include:

- new customers that wish to carry out a large transaction(s)
- non face-to-face customer on-boarding
- customers involved in occasional or one-off transactions above the threshold (either specified in the FTRA, the Customer Due Diligence (CDD) Rules or the financial institution's internal limits)
- customers who use complex business structures that offer no apparent financial benefits

- customer or a group of customers making numerous transactions to the same individual or group
- customers who are Politically Exposed Persons (PEPs)
- customer who has a business which involves large amounts of cash
- customer whose identification is difficult to check
- customer who bring in large amounts of used notes and/or small denomination notes.
- customers conducting their business relationship or transactions in unusual circumstances for example: significant and unexplained geographic distance between the financial institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, frequent and unexplained movement of funds between institutions in various geographic locations
- non- resident customers
- corporate customers whose ownership structure is unusual and excessively complex
- customers whose origin of wealth and/or source of funds cannot be easily verified or where the audit trail appears to be broken and/or unnecessarily layered
- customers that are non-profit organizations
- customers who conduct business through or are introduced by "gatekeepers" such as accountants, lawyers, or other professionals
- customers of a type that have been identified in National or Sector Risk Assessments as higher risk

iv. the countries that the financial institution deals with

Financial institutions should give consideration to the following factors as indicators of higher risk for ML/TF:

- any country subject to United Nations sanctions embargoes or similar measures
- any country identified by credible sources such as the FATF as lacking adequate AML and CFT system
- any country which is identified by credible sources as having significant level of corruption, tax evasion, and other criminal activity
- any country identified by credible sources as supporting TF

- any country that are identified by credible sources as tax havens

v. the business delivery methods or channels

The way the financial institution delivers its products and services affects its vulnerability to ML/TF.

The following are some indicators (not an exhaustive list) that may help to identify ML/TF risk involved with business delivery methods or channels

- non-face-to-face customers (via post, telephone, internet,) that pose challenges for verifying the identity of the account holder/customer.
- indirect relationships with customers (via intermediaries, gatekeepers, pooled accounts)

II. Risk Assessment

24. Having identified the threats involved, financial institutions need to assess and measure ML/TF risk in terms of the likelihood (chance of the risk event occurring) and the impact (the amount of loss or damage if the risk event occurs). The risk associated with an event is a combination of the likelihood that the event will occur and the seriousness of the damage it may do.

Likelihood scale

25. A likelihood scale refers to the potential of an ML/TF risk occurring in the business for the particular risk being assessed. Three levels of likelihood of ML/TF risk are shown below, but financial institutions can have as many scales as are necessary for their circumstances.

i. Very likely - Almost certain;
ii. Likely- High probability;
iii. Unlikely- Low probability, but not impossible.

Impact scale

26. An impact refers to the seriousness of the damage that is likely to be caused if the ML or TF occurs. In assessing the possible impact or consequences, the assessment should be made from a range of viewpoints relevant to the business. Those set out below are not exhaustive. The impact of ML/TF occurring could, depending on the individual financial institution and its business circumstances, be rated or looked at from the point of view of:
    i. how it may affect the business in terms of financial loss relating to market perceptions (for example loss of investor confidence) and reputation or through fines or other sanctions (such as loss or suspension of business licenses) imposed by a regulator
    ii. the risk that a particular transaction may be seen to contribute to the activities of a terrorist or terrorist organizations.
    iii. the risk that a particular transaction may result in funds being used for any unlawful activity as defined in Section 33 of the FTRA
    iv. how it may affect the reputation of the financial institution if it is found to have aided, investigated, prosecuted or otherwise implicated in an illegal act, which may lead to loss of important commercial relationships (such as correspondent accounts) or being shunned by the community of customers or shareholders/investors

27. Three levels of impact of an ML/TF risk to financial institutions are shown below as an example. However, the FIU encourages financial institutions to develop their own ML/TF risk processes and assessments for dealing with certain customers/undertaking transactions in the way that best suits their business model/activities.
    i. Major- significant consequences, that inflict substantial damage, possibly resulting in the closure of the financial institution, cessation of business activities, regulatory sanctions being imposed or financial/reputational damage being experienced by the financial institution which will have a significant impact on business activities.
    ii. Moderate- moderate impact, involving substantial damage to the business and its reputation.
    iii. Minor- minor or negligible consequences or effects upon the financial institution.

28. Based on the likelihood and impact scale, it is suggested that financial institutions should assess an overall risk score. The risk rating may be used to aid decision making and help in deciding what action to take in view of the overall risk. A suggested risk rating derivation can be seen in the risk matrix *(Annex 1)*. However, institutions are encouraged to adopt their own approach to assessing, identifying and quantifying ML/TF risk. Irrespective of the methodology adopted, the FIU requires institutions to develop a framework and implement practices to effectively identify, measure, monitor, control and mitigate ML/TF risks as required by the FTRA and CDD Rules.

i. Extreme - risk almost certain to happen and/or to have very serious consequences on the financial institution, including its financial standing and reputation.
   Response: Do not allow transaction to occur/or customer relationship to be established or reduce the risk to acceptable level through risk mitigation, such as enhanced due diligence.
ii. High - risk likely to happen and/or to have serious consequences.
   Response: Do not allow transaction/establishment of customer relationship until risk reduced through risk mitigation, such as enhanced due diligence.
iii. Medium - possible this could happen and/or have moderate consequences.
   Response: Mitigate risk; normal CDD and other requirements apply.
iv. Low - unlikely to happen and/or have minor or negligible consequences.
   Response: Mitigate risk: simplified CDD and other requirements apply.

III. Risk Mitigation

29. Once the financial institution assesses the ML/TF risk of individual customer, product/service, delivery channel and risks related to geographic region, it should develop strategies policies and procedures to manage and mitigate the risk.

Examples of a risk reduction or mitigation are:

i. Setting transaction limits for high-risk products or delivery channels

ii. Having a management approval process for higher risk customers, products, services, or deliver channels

iii. Risk rating customers and applying different requirements for high or low risk customers including applying different identification and verification methods and enhanced customer due diligence requirements

iv. Not accepting customers who wish to transact with a high-risk country or customers that are considered to be higher risk based on the institution's board-approved customer acceptance policy.

Risk Management Strategies

30. Financial institutions shall adopt the following components, among others, as part of their risk management strategy:

i. Develop and implement ML/TF risk management objectives at the board and senior management level of the financial institution and monitoring progress of implementation of objectives.

ii. Implement clearly defined management responsibilities and accountabilities regarding ML/TF risk management.

iii. Provide adequate staff resources to undertake functions associated with ML/TF risk management.

iv. Introduce staff reporting lines from the ML/TF risk management system level to the board or senior management level, with direct access to the board members or senior managers responsible for overseeing the system.

v. Implement procedural controls relevant to particular services and products, customers, and delivery channels that have been identified as being vulnerable to ML/TF.

vi. Documenting all ML/TF risk management policies and ensuring that these are kept up to date and reviewed regularly reflecting both the scope and nature of the institution's activities and the findings of risk assessments conducted by authorities. Such policies should also identify processes relating to non-compliance, including reporting of suspicious transactions to the FIU.

vii. Provide appropriate training programs for staff to develop expertise in the identification of ML/TF risks across the financial institution, including reporting of suspicious transactions.

viii. Develop an effective information management system which produce detailed and accurate financial, operational and compliance data relevant to ML/TF risk management.

Enhanced and Simplified Due Diligence Measures

31. There are circumstances where the risk of ML/TF is higher and enhanced CDD measures must be taken and, where the risks of ML/TF are lower, simplified CDD measures may be taken. These enhanced and simplified measures are outlined below:

Enhanced due diligence measures for high risk customers/transactions

32. Every financial institution should examine and document, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of ML/TF are higher, financial institutions should be required to conduct enhanced due diligence (EDD) measures for higher-risk business relationships which may include:

i. Obtaining and verifying additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet search, etc.)
ii. Updating more regularly the identification data of customer and beneficial owner
iii. Obtaining and verifying additional information on the intended nature of the business relationship
iv. Obtaining and verifying information on the source of funds or source of wealth of the customer
v. Obtaining and verifying information on the reasons for intended or performed transactions
vi. Obtaining and verifying the approval of senior management to commence or continue the business relationship
vii. Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
viii. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Simplified CDD measures for low risk customers/transactions

33. Where the risks of ML/TF are lower, the financial institutions are, subject to the regulations, allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring).

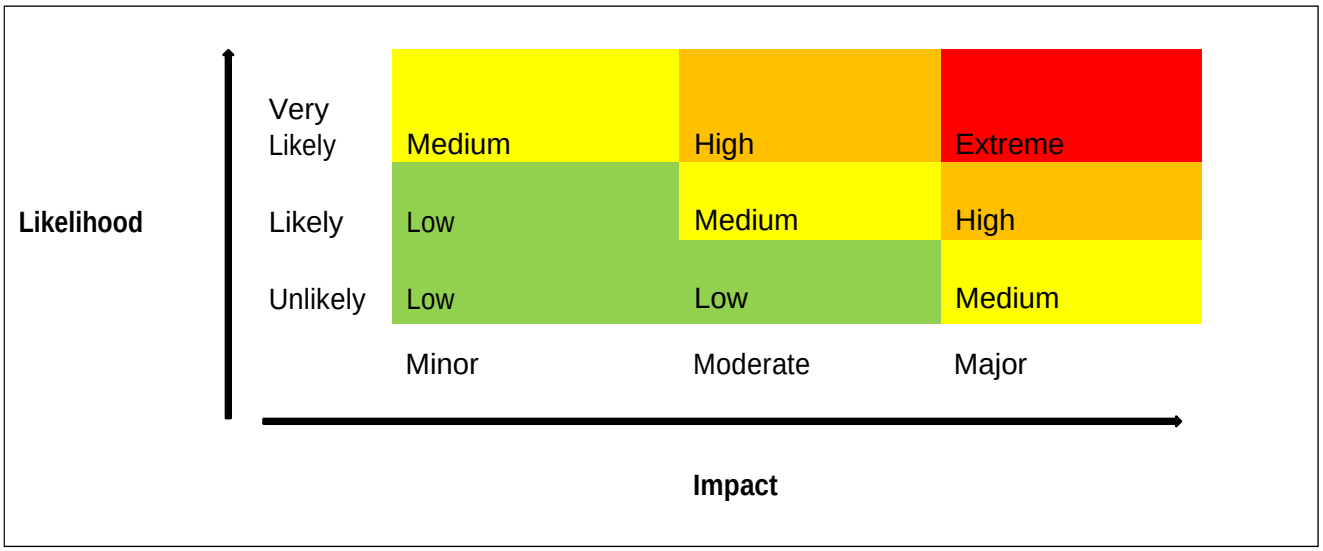
Examples of possible measures are:

i. Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (delayed verification)
ii. Reducing the frequency of customer identification updates
iii. Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
iv. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established

34. Simplified CDD measures are not acceptable whenever there is a suspicion of ML/TF, or where specific higher-risk scenarios apply.

Annex 1

Overall AML/CFT Risk



CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதல் பிரிவு **Financial Intelligence Unit**

Ref : 037/03/011/0001/018

Guidelines — 06/2018

August 06, 2018

To: CEOO of All Financial Institutions

Dear Sir / Madam,

Guidelines for Financial Institutions on Suspicious Transactions Reporting,
No. 06 of 2018

The above mentioned guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Suspicious Transactions (Format) Regulations of 2017.

Yours faithfully

D M Rupasinghe
Director
Financial Intelligence Unit

Cc : Compliance Officers

14 වන මහල, අංක 30, ජනාධිපති මාවත, තැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව
14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை கொழும்பு 1 த. பெ. இல. 590, கொழும்பு 01, இலங்கை
Level 14 , No. 30, Janadhipathi Mawatha, P . O. Box. 590, Colombo 01, Sri Lanka.
1 94 11 2a77125/509 t" 94 11 2477G92 @ fi«ecbsLik www.cbsl.gov.lk

Guidelines for Financial Institutions on Suspicious Transactions Reporting, No. 06 of 2018

Introduction

1. These Guidelines are issued pursuant to section 15(1)(j) of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) applicable to Financial Institutions that engaged in or carrying out "finance business" as defined in Section 33 of the FTRA.

2. Suspicious Transactions (Format) Regulations of 2017 was issued on dated April 21, 2017 by Gazette Extraordinary No. 2015/56 applicable to Institutions which include institutions that engaged in or carrying out "finance business" as defined in Section 33 of the FTRA. These Guidelines are provided as an aid to interpret and apply Suspicious Transactions (Format) Regulations of 2017. These Guidelines are not intended to be exhaustive and do not constitute legal advice from the Financial Intelligence Unit (FIU). Nothing in these Guidelines should be construed as relieving Financial Institutions from any of their obligations under the Suspicious Transactions (Format) Regulations of 2017 or the FTRA.

3. The quality of a Suspicious Transaction Report (STR) is important in increasing the effectiveness of the quality of analysis and investigations undertaken by FIU and law enforcement agencies relating to such STR which would assist in preventing abuse of the Sri Lankan financial system by criminals and terrorists. Quality, in this sense, means reports should be based on results from an AML/CFT programme that is effectively implemented and that the content in reports are complete, accurate and latest. This guideline aims at assisting Financial Institutions in improving the quality of STRs submitted.

Legal Obligation

4. Section 7 of the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) requires:

   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. 5 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 therefrom, report the transaction or attempted transaction or the information to the Financial Intelligence Unit.

Such reports are herein referred to as Suspicious Transaction Reports (STR).

5. As stated above as per the section 7 of the FTRA all "Institutions", should report suspicious transactions to the FIU. Institution means, any person or body of persons engaged in or carrying out any finance business or designated non-finance business as defined in the Section 33 of the FTRA.

6. As per Section 14 (1) (b) (iv) of the FTRA every institution is required to establish and maintain procedures and systems to implement the reporting requirement under Section 7 of the FTRA. Further, Section 14 (1) (d) requires every Institution to train its officers, employees and agents to recognize suspicious transactions.

7. As per Rule 15 of the Financial Institutions Customer Due Diligence Rule, No 1 of 2016, the internal AML/CFT Policy approved by the Board of Directors should include policies, procedures on the detection and internal reporting procedure of unusual and suspicious transactions and the obligation to report suspicious transactions to the Financial Intelligence Unit.

Prerequisites for Development of Suspicion

8. Reporting of suspicious transactions is a major functionality in the operation of an effective institutional AML/CFT programme. For the AML/CFT function to be meaningful, they must result from a Financial Institution's effective implementation of the FTRA, including all rules and instructions issued in relation to the FTRA. Financial Institutions without such effective implementation either tend to submit STRs that are inaccurate, incomplete or inappropriate or they may fail to report suspicious transactions entirely. Such failures expose the financial institution to regulatory, reputational, operational, and legal risks. In some cases, such failures may also expose both natural and legal persons to criminal liability.

9. For all but the very smallest institutions with the most intimate customer relationships, information about customers and transactions should be captured in a systematic manner and incorporated into their compliance and risk management processes. For larger Financial Institutions, this almost always means an electronic information

system. Such systems typically operate based on rules, scenarios and profiles that seek to measure and assess deviance of observed patterns from expected patterns, or seek to measure and assess conformity of observed patterns to known patterns of abuse of the financial system. Such systems need to be carefully configured to reflect the specific assessed risks of the Financial Institution. Such systems need to be continually evaluated and adjusted to maximize effectiveness, need to be continually updated with new operational and third-party information and need to be fully integrated into the Financial Institution's risk management process. When such systems generate alerts, it is important that the alerts are reviewed by the Financial Institution's Compliance Officer. While such system-generated alerts may be the cause for an STR, such alerts are not by themselves likely to form a complete STR in accordance with these guidelines and are not an acceptable substitute for such an STR.

Systems that operate in isolation are not effective. A system can only operate based on the information that is available to it. Systems are not generally capable of intuition or inference or human levels of perception. As such systems operate based on rules, scenarios and profiles that are designed by humans. For these reasons, Financial Institutions should not rely exclusively on systems to the exclusion of human involvement.

10. Whatever the source of customer and transaction knowledge, and whatever the technical sophistication of the AML/CFT system there must be an institutional will to make the system work. That is, there must be a will to detect suspicious transactions, to recognize in good faith such suspicious transactions for what they are when detected, and fully and accurately report such transactions, when recognized. Such institutional will is most effectively created by a commitment from those at the Senior Management including the Board of Directors of the Financial Institution and propagated through concrete actions and demonstrations (e.g. development of effective internal policies, processes and training programmes, compliance audits, investment in systems, consistent, fearless and disciplined exercise of judgment) to the rest of the staff of the Financial Institution.

Suspicion

11. Financial Institution must develop its own operating definition for suspicion. A Financial Institution's operating definition of suspicion should incorporate elements of unresolved and unsubstantiated but persistent feelings of doubt about an objective set of facts and circumstances relating to a behaviour, to a single transaction, to a series of transactions, attempted transaction or to any combination thereof. It can be a feeling that something is not as it was expected to be, or as it was explained to be, given the totality of knowledge of the circumstances in which that something exits. The feeling of doubt cannot be relieved by proof, one way or another, since no proof is available. The definition should allow formation of a belief that is not firmly grounded or perfectly

clear. At the same time, the definition should not allow these beliefs to be fanciful or fleeting. Certainly, the definition should count as suspicious behaviours and activities that are unusual for the circumstances and not adequately or believably explained.

The operating definition for suspicion must pass a test of reasonableness. If the definition is too narrow or rigid, it may exclude generation of reports that concern unknown or unanticipated unlawful circumstances (i.e. “false negatives”) and may also result in avoidance behaviour by criminals. On the other hand, a definition that is too broad or flexible might result in large number reports that are insufficiently analyzed and that do not reflect unlawful circumstances (i.e. “false positives” or “over compliance”). For Financial Institutions where electronic information systems are integrated into their processes, operating definitions are partially implemented by the triggers, profiles, scenarios and rules defined by the Financial Institution. Suspicious indicators and typologies may also be elements of such definition. The concept of “unusual” patterns of behaviour and transactions should also reflect in these definitions.

A non-exhaustive and unofficial list of suspicious indicators for transactions and behaviours is provided in Appendix I. The Financial Institution should complement this list with the Financial Institution’s own indicators. When using indicators, it should be remembered that these indicators are not formulae and they do not necessarily indicate the presence of criminality. Conversely, the lack of known indicators does not necessarily mean the absence of criminality, in part because criminals may adjust behaviour to avoid such indicators. Instead, indicators, and especially combinations of indicators, should cause increased scrutiny that may lead to the formation of suspicion.

12. Financial Institutions being over compliance or malicious compliance will not generate expected quality of the STR. Overcompliance and malicious compliance are strongly discouraged.

    Over compliance results when Financial Institutions submit a large volume of reports that are inadequately analyzed or that fail to meet a reasonable standard of suspicion. Over compliance can be viewed as an attempt to transfer risk management from the Financial Institution to the FIU.

    Malicious compliance is when an Financial Institution submits reports that, although they may contain some superficial elements of suspicion, are known by the Financial Institution to not actually of suspicious nature.

13. If after consideration of facts and circumstances available to the Financial Institution in good faith and within the context of the Financial Institution’s own understanding of suspicion and risks for the Financial Institution, and after gaining a thorough understanding of the FTRA and its implementing rules, regulations, circulars and guidelines, the Financial Institution has doubts about whether a behaviour or activity should be reported as suspicious, the best course of action is to report.

Reporting of STRs

14. **When Financial Institutions are provided with access to the LankaFIN system:** All reports must be submitted via LankaFIN online system or a successor system designated by the FIU followed by the signed hard copy of the STR submitted to the FIU by delivery or post.

15. **When Financial Institutions are not provided with access to the LankaFIN system:** Signed hard copy of the STR should be submitted to the FIU by delivery or post.

16. The Financial Institutions may submit STRs through other forms such as by way of email, fax or telephone in urgent situations to be followed by submission though LankaFIN and/or signed hard copy as appropriate within twenty-four hours.

Timing of Reporting

17. The FTRA requires suspicious reports to be submitted to the FIU as soon as practicably possible but no later than two working days of formation of suspicion. This means that, regardless of the Financial Institution's processes, procedures and steps after the initial formation of suspicion, the suspicion itself must be reported even if the Financial Institution's process has not completed. The Financial Institution's process for dealing with suspicion may proceed concurrently with the reporting of suspicion.

    For example, if the Financial Institution has a customer that receives a wire transfer in circumstances that the Financial Institution immediately considers to be suspicious, the Financial Institution must report the suspicious circumstances of that transaction as soon as practicable but within two working days even while the Financial Institution may continue with the internal processes that to verify the authenticity and details of the wire transfer.

18. If, after sending the report, the Financial Institution discovers additional facts and circumstances to either support or refute the Financial Institution's initial suspicion, then the Financial Institution should inform the FIU appropriately.

Content of Reporting

19. **Completeness:** A single STR must stand alone and contain complete information about the suspicion. A STR should provide a full picture of the suspicion itself as well as the objective facts and circumstances that gave rise to and support that suspicion. Where multiple transactions and/or behaviours are connected with a suspicion, a single report should be filed capturing all of these.

20. **Form Narrative:** The narrative portion of the report is most important. This is particularly true with respect to LankaFIN since other form fields capture only a limited amount of information. This is the Financial Institution's chance to fully describe the suspicion and the objective facts and circumstances that gave rise to and support the Financial Institution's suspicion. In any case the Financial Institution is unable to provide the full detailed narrative through LankaFIN, the Financial Institution may provide the narrative in a separate document and submit to the FIU along with the signed hard copy of the STR. In such cases, the Financial Institution should mention a brief summary of the narrative in the LankaFIN system and explicitly mention that a full narrative will be sent with the hard copy. The narrative should attempt to answer to the extent possible the basic descriptive questions of **what, who, when, where, why and how**.

    Financial Institutions should refrain from providing vague details of suspicions such as 'several high value third party deposits from several branches around the country'. Instead, Financial Institutions should provide clear quantitative and qualitative data such as '10 number of third party deposits having values between LKR 75,000 – 90,000 from Jaffna, Trincomalee, Kandy, Matara, Galle, Kataragama and Badulla branches during September, 2017' and provide relevant supporting documents (e.g. account statement for September 2017 including the details of third party depositors / deposits).

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

    - What is the nature of the suspicion?
    - What offenses may have been committed?
    - What transactions, attempted transactions, behaviours, facts, belief and circumstances are involved and relevant to the suspicion?
    - Who are the natural and legal persons involved?
    - Who are the beneficial owners?
    - What are their identifiers such as names, ID numbers, registration numbers, etc.?
    - What are their addresses?
    - What are their occupations or lines/types of business?
    - Who are their employers?
    - What political exposure do they have, if any?
    - How are they connected with each other and with the transactions?
    - What were their roles in the transactions?
    - What property is involved?
    - What is the nature and disposition and estimated value of involved property?
    - When and where did the transactions or attempted transactions or behaviours occur?

- How, if at all, do the timing or location of the transactions contribute to the Financial Institution's suspicion?
- Why do these facts and circumstances support the suspicion?
- How was the suspicion formed?
- What triggers or indicators are present?
- What actions have been taken by the reporting Financial Institution?
- What related STRs have the Financial Institution already submitted?
- What red flags are present?
- What deviations from expected activities have taken place?

Financial Institutions are required to provide reasonable grounds for the suspicion and are requested to refrain from citing unjustifiable reasons such as 'relationship between customers cannot be derived with the surnames', 'funds from African countries', etc.

The narrative should be structured in a logical manner so that information can be conveyed to the FIU analyst as efficiently, completely and accurately as possible. Essay formats could be used for STR narratives i.e. having an introduction, a body, and a conclusion. Paragraph breaks can be used to divide the narrative into logical units and enhance readability. Within the body, information could be presented in a chronological manner when attempting to demonstrate possible causal links along a timeline. It is advised to minimize the use of Financial Institution's internal jargon and acronyms brandings, product names by using generic descriptors instead. For example, use "six-month term deposit account" rather than "Mega-Six Platinum Elite Plus Super Saver Account." Use punctuation and sentence case. Narrative should not be so brief as to compromise the goals of the narrative. It is advised to avoid words that do not contribute to the meaning of a sentence and to refrain from using too generic narratives such as 'the transaction pattern does not match with the customer profile'.

21. **Accuracy:** It is imperative that factual information provided in the report is accurate. This is particularly true for identifiers such as names, ID numbers, registration numbers, etc. All spellings and transcriptions of identifiers should be double checked. A single inaccurate digit in a passport number or an NIC, or a misplaced or transposed character in a name, can make the difference between a successful and an unsuccessful analysis. Identifiers for legal entities (e.g. company / business registration number, registered name of company) should be exactly identical in every respect to those found on the official registration documents.

Submission of Supporting Documents

22. Financial Institutions are required to submit relevant supporting documents along with the STR. If the Financial Institution is unable to submit the supporting documents via LankaFIN, the Financial Institution should submit the relevant supporting documents

through email and/or along with the signed hard copy of the STR. In such cases, Financial Institutions should mention in LankaFIN that additional supporting documents are submitted via email or through post.

23. Supporting documents should support rather than replace the STR contents, including the narrative. It is not acceptable to only refer to a supporting document in the narrative when information from the supporting document can be directly included in the narrative. For example, if the suspicion involves a letter of credit, all the details from the letter of credit that are related to the suspicion should be included in the narrative. A copy of letter itself can then be provided as a supporting document.

24. An indicative and non-exhaustive list of supporting documents along with corresponding scenarios are given below for reference.

Scenario	**Indicative list of Supporting documents**
Third party deposits	Bank Statements List of third party deposits Details of third party depositors
Foreign inward remittance	Bank statement Copy of SWIFT message
Suspicion regarding forged / altered identity (NIC/ Passport / Driving license)	Copy of the document
Suspicion related to a company	Registration documents Director details

Miscellaneous

Confidentiality

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

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

Breach of Confidentiality

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

Protection for Persons Reporting STRs

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

Failure to Report STRs

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

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

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

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

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

Further Information Requests

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

Appendix I—Suspicious Indicators

This appendix contains a list of indicators related to customer behaviours and activities. This list is necessarily non-exhaustive and incomplete and should be modified and supplemented as necessary by each Financial Institution. Indicators are not formulae and they do not always indicate the presence of criminality. Conversely, the lack of indicators does not mean the absence of criminality. **However, the presence of an indicator, and especially the presence of multiple indicators, should cause increased scrutiny by the Financial Institution and such scrutiny may lead to the formation of suspicion.**

General Indicators

- Any behaviour unusual for the circumstances.
- Any activity unusual for the customer.
- Any activity unusual in itself.
- Any knowledge that leads the Institution to believe that unlawful activity may be involved.
- Any unresolved and persistent feelings of doubt related to customers and their transactions and attempted transactions.

General Behavioural/Customer Indicators

- Customer talks about or hints about involvement in criminal activities, even if in a humorous way.
- Customer does not want correspondence sent to home address.
- Customer appears to have accounts with several financial institutions for no apparent reason.
- Customer repeatedly uses an address but frequently changes the names involved.
- Customer uses addresses in close proximity of each other.
- Customer is accompanied and watched when visiting the Financial Institution.
- Customer shows unusual curiosity about internal systems, controls and policies.
- Customer has only vague knowledge of the amount of a deposit.
- Customer presents confusing or inconsistent details about the transaction.
- Customer over justifies or explains the transaction.
- Customer tries to convince Financial Institution staff to alter or omit reporting data.
- Customer is secretive and reluctant to meet in person.
- Customer is nervous, not in keeping with the transaction.
- Customer insists that a transaction be done quickly.
- Customer attempts to develop a close rapport with staff.
- Customer offers money, oversized commissions, gratuities or unusual favours for the provision of services.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer jokes about needing or not needing to launder funds.
- Customer has no apparent ties to the community.
- Customer has irregular work/travel patterns.

Account Opening/Identity Indicators

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only possesses copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details.
- Customer unnecessarily delays presenting corporate documents.
- All identification presented is foreign or otherwise unreasonably difficult to verify.
- All identification documents presented appear new or have recent issue dates.
- Customer is unemployed, or is an independent consultant, or switches jobs frequently.
- Customer conspicuously displays large amount of cash.

Indicators for a Businesses

- Lack of regular business hours.
- Unusually profitable business.
- Profitable business in a failing industry.
- Business receipts and incomes above industry norms.
- Cash intensive business.
- Use of high cost or inconvenient methods when lower cost or more convenient methods are available.
- Apparent lack of in-depth knowledge of his own business or industry.

General Transaction Indicators

- Transaction is unusual for the customer.
- Transaction is unusual for the country.
- Transaction is unusual for the industry.
- Transaction is unusual for any other reason.
- Transaction seems to be inconsistent with the customer's apparent financial standing or usual pattern of activities.
- Sudden unexplained increase in wealth.
- Transaction appears to be out of the ordinary course for industry practice or does not appear to be economically advantageous for the customer.
- Transaction uses account(s) that have been dormant.
- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

Cash Transaction Indicators

- Customer suddenly starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past.
- Customer frequently exchanges small bills for large ones.
- Customer uses notes in denominations that are unusual for the customer, when the norm in that business is much smaller or much larger denominations.
- Customer presents notes that are packed or wrapped in a way that is uncommon for the customer.
- Customer deposits musty or extremely dirty bills.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Customer consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Customer presents uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which could trigger reporting requirements.
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer frequently purchases traveler's checks, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the customer.
- Customer asks the Financial Institution to hold or transmit large sums of money or other assets when this type of activity is unusual for the customer.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (for example, student, unemployed, self-employed, etc.).
- Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area) .
- Customer consistently claims that source of funds is gambling winnings with no evidence of corresponding losses.

Indicators Involving Loans

- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.

- Loans that lack a legitimate business purpose; provide the bank with significant fees for assuming little or no risk; or tend to obscure the movement of funds (*e.g.*, loans made to a borrower and immediately sold to an entity related to the borrower).
- Customer claims true ownership of assets used for collateral, even though assets held in a different name.

Trade Financing Indicators

- Items shipped are inconsistent with the nature of the customer's business (*e.g.*, a steel company that starts dealing in paper products, or an information technology company that starts dealing in pharmaceuticals).
- Customers ship items through high-risk jurisdictions, including transit through countries recognized as non-compliant with AML/CFT requirements.
- Customers involved in potentially high-risk activities, including activities that may be subject to export/import restrictions.
- Obvious over- or under-pricing of goods and services.
- Obvious misrepresentation of quantity or type of goods imported or exported.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Customer requests payment of proceeds to an unrelated third party.
- Shipment locations or description of goods not consistent with letter of credit.
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Transactions with Overseas or Offshore Jurisdictions

- Accumulation of large balances, inconsistent with the known turnover of the customer's business, and subsequent transfers to overseas or offshore account(s).
- Frequent requests for travelers checks, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-value deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transferred by customer to/from offshore jurisdictions on an in-and-out (pass through) basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the customer's business or with national trade patterns.
- Use of a credit card issued by an offshore bank.

Suspicious Patterns involving Multiple Transactions

- Round trip transactions where funds are transferred to one destination, and then return in roughly the same amount from a different origin.
- Structured transactions that break transactions into smaller amounts to avoid reporting.
- Distributer/collector transactions where multiple accounts funnel into one, or one funnels into multiple without adequate explanation. This is an especially strong indicator when accounts may be controlled by single beneficial owner.

Transactions Involving Proxies

- Transactions where a person who is matched by two attributes (e.g. name and address, or name and birthday, or birthday and address) appears to maintain multiple accounts with variations in one of these parameters.
- Transactions with multiple accounts at the same address.
- Transactions where the address does not exist in public records.
- Transactions where the name does not exist in public records.
- Transactions where the account holder is a PEP.
- Transactions where the account holder is a relative or close associate of a PEP.
- Transactions where the account holder shares an address with a PEP.
- Large transactions by people with low-income jobs, especially when employed by or related to high wealth individuals.
- Transactions in the name of very young people.
- Transactions in the name of dead people.
- Transactions in the name of people living in areas where such wealth would be abnormal.

Red Flag Indicators for Specific Sectors

Securities Sectors

- Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the client or their financial ability.
- Any dealing with a third party when the identity of the beneficiary or counter-party is undisclosed.
- Client attempts to purchase investments with cash.
- Client wishes to purchase a number of investments with money orders, traveller's cheques, cashier's cheques, bank drafts or other bank instruments, especially in amounts that are slightly less than the reporting threshold, where the transaction is inconsistent with the normal investment practice of the client or their financial ability.
- Client uses securities or futures brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the client or their financial ability.

- Client wishes monies received through the sale of shares to be deposited into a bank account rather than a trading or brokerage account which is inconsistent with the normal practice of the client.
- Client frequently makes large investments in stocks, bonds, investment trusts or other securities in cash or by cheque within a short time period, inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- The entry of matching buying and selling of particular securities or futures contracts (called match trading), creating the illusion of trading.
- Transfers of funds or securities between accounts not known to be related to the client.
- Several clients open accounts within a short period of time to trade the same stock.
- Client is an institutional trader that trades large blocks of junior or penny stock on behalf of an unidentified party.
- Unrelated clients redirect funds toward the same account.
- Trades conducted by entities that you know have been named or sanctioned by regulators in the past for irregular or inappropriate trading activity.
- Transaction of very large value.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.
- All principals of client are located outside of Sri Lanka.
- Client attempts to purchase investments with instruments in the name of a third party.
- Payments made by way of third party cheques are payable to, or endorsed over to, the client.
- Transactions made by your employees, or that you know are made by a relative of your employee, to benefit unknown parties.
- Third-party purchases of shares in other names (i.e., nominee accounts).
- Transactions in which clients make settlements with cheques drawn by or remittances from, third parties.
- Unusually large amounts of securities or stock certificates in the names of individuals other than the client.
- Client maintains bank accounts and custodian or brokerage accounts at offshore banking centres with no explanation by client as to the purpose for such relationships.
- Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti-money-laundering system.

Money/ Currency Changers

- Customer requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Customer exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Customer is reluctant to divulge the source of currency
- Customer is unable to produce relevant documents to support transaction
- Customer requests that a large amount of foreign currency be exchanged to another foreign currency.
- Customer instructs that funds are to be picked up by a third party on behalf of the payee.

Mobile Money Service Providers

- Customer used multiple names/identities, in conjunction with providing multiple addresses, making it difficult to ascertain the true identity of the customer.
- The frequency of the customer's visits was excessive, and also involved the use a wide range of agent locations.
- The purpose of the transactions, and the relationship between the beneficiary and the ordering customer, does not appear to make business sense.
- Multiple senders transferring funds to a single individual
- Currency notes used are in “used notes” and/or small denominations (“used notes” may imply that notes are worn, dirty, stained, give off unusual smell, etc.)
- Customer attempts to send money to a person on a sanctions list
- Customer fails to provide verifiable identity information or refuses to provide verifiable identity information either for the customer and/or for the beneficiary
- Customer attempts to use or uses unusual or suspect identification documents.
- The customer wishes to engage in transactions that are inconsistent with the customer’s stated purposes when the account was initially set-up.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

@@23 @t.;,cJ C,ts)ts)a)
!BLDIJUJLWW L6TT6II!J3I◆!i:J ulrfl6lJ
FINANCIAL INTELLIGENCE UNIT

◆ (got») ®◆ @◆o◆E>
◆6\)f6161Dffi ID◆„IIJ 6lJ1'61ffil
CENTRALBANKOFSRILANKA

◆oC"> 30, des>IEJaffi ®le)o), ee>l◆® OJ, @ @otl'llE)
®}6U. 30, 661ffildi)udi) L006l◆ 6il>◆, G&rr@tb4 - 01, ◆6Uffil6l>&
No. 30, Janadhlpathl Mawatha, Colombo 01, Sri Lanka

Circular No. 01/2022

Ref: 037/06/008/0006/020

January 10, 2022

To: CEOs / General Managers / Managing Directors of All Financial Institutions

Dear Sir/Madam,

Amendment to the Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021

Further to the Guidelines issued dated July 20, 2021, on the above.

Clause 15 of the above guidelines is amended as below.

15. Fis should maintain all infonnation captured in the CCTV system for a minimum period of 90 days.

Yours faithfully,

D R Karunaratne
Director/ Financial Intelligence Unit

Cc;

1. Director, Bank Supervision Department of the Central Bank of Sri Lanka
2. Director, Department of Supervision of Non - Bank Financial Institutions of the Central Bank of Sri Lanka
3. Director General, Securities and Exchange Commission of Sri Lanka
4. Compliance Officers, all Financial Institutions

ir 011-2477125
011-2477509
011-2477692
011-2477708
◆ flu@cbsl.lk
dflu@cbsl.lk
◆ www.flusrllanka.gov.lk

@@ot})J ®m @r;o<c>
CENTRALBANKOFSRILANKA
@@i:s §w c,Ci)
[61wlw6i) L6TT6l.l'6J ulrft61J
FINANCIAL INTELLIGENCE UNIT
l'.l'oCl 30, des>)WGffi ®)E)Cl), ®l® 01, @ @oQ)JE)
.@)GU. 30, U6Ul!T€LI LDIT6U6il), GffirT@IDLI - 01, .@j6'1)6il)ffi
No. 30, Janadhlpathl Mawatha, Colombo 01, Sri Lanka

Guidelines No.02/2021

Ref: 03 7/06/008/0006/020

July 20, 2021

To: CEOs / General Managers/ Managing Directors of All Financial Institutions

Dear Madam/Sir,

Guidelines for Financial Institutions on CCTV Operations for AML/CFT Purposes, No. 2 of 2021

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 06 of2006 and the Financial Institutions (Customer Due Diligence) Rules, No. OJ of 2016.

YOURS faithfully,

E H Mohotty
Director/ Financial Intelligence Unit

Cc;

1. **Director, Bank Supervision Department of the Central Bank of Sri Lanka**
2. **Director, Department of Supervision of Non - Bank Financial Institutions of the Central Bank of Sri Lanka**
3. **Director General, Securities and Exchange Commission of Sri Lanka**
4. **Compliance Officers, all Financial Institutions**

011-241112s
011-2477509
011-2477692
011-2477708

flu@cbsl.lk dflu@cbsl.lk

www.tlusrllanka.gov.lk

Guidelines for FinancialInstitutions on CCTV operations for AML/CFT purposes, No. 2 of 2021

PARTI

Introduction

1. These Guidelines are issued pursuant to section 15(1)U) of the tfinancial Transactions Reporting Act, No. 06 of 2006 (hereinafter refe1Ted to as tfTRA).

2. These Guidelines are applicable to tfinancial Institutions (hereinafter referred to as tfis) that are engaged in or carrying out "finance business" as defined in Section 33 of the FTRA where closed-circuit television (hereinafter refe1Ted to as CCTV) systems are being used where relevant.

3. These Guidelines should be read along with the tfinancial Institutions (Customer Due Diligence) Rules, No. 0 I of 2016, issued by Gazette Extraordinary No. 1951/13, dated January 27, 2016 (hereinafter referred to as COD Rules). More specifically, these Guidelines should be referred together with Rules 7 and 11 of the COD 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 tel'orist financing risks and affiliating and integrating tfinancial Institution's money laundering and te1rnrist financing risk management with the overall risk management relating to the tfinancial Institution.

4. These Guidelines are issued in addition to the operational directives or circulars that are issued by the respective sector regulators with regard to CCTV systems.

5. These Guidelines are not intended to be exhaustive and do not constitute legal advice from the Financial Intelligence Unit. Nothing in these Guidelines should be construed as relieving tfis from any of their obligations under the tfTRA and regulations and rules issued thereunder.

Part II

The Requirements for CCTV Systems

6. As pat1 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, every FI is advised to have 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 (ATM/CRM/CDM), cash centers, outlets, and any other place or places where Customer Due Diligence (hereinafter referred to as CDD) is conducted.

7. In ensuring the CCTV system installed is effective to enable proper surveillance and monitoring of the business operations, all Fis should consider setting up a system of necessary standard with proper processes and controls, which could, at a minimum, cover the requirements set in in these Guidelines.

Placement ofCCTV cameras

8. In order to enhance the effective usage of the CCTV system, FIs 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 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 business premises, any other suitable areas, both inside and outside the building as detennined by the FI.

9. The CCTV surveillance systems must be aligned in a suitable manner and at an angle as to obtain a complete and unimpeded view of the area. Further, CCTVs need to be positioned in a manner where the capturing and processing inf01mation of the CCTV system is not interfered or impeded by internal or external lighting, glare, or any object.

Functions of CCTV system

I 0. Fis 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 f'om another. In addition, adequate lighting must be maintained in order to capture clear CCTV footage.

11. Higher quality digital equipment should be used in CCTV systems to capture a clear frontal images of individuals. The CCTV systems should pennit 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 surveillance.

12. 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 FI is cJosed for business.

Real time monitoring

13. Fis should ensure real-time monitoring at the head office and/or branches or at a central monitoring unit, as far as practicable.

14. Fis are advised to obtain assistance of its security services personnel or law enforcement agencies (LEAs) to mitigate immediate risks that may arise to the FI's premises or to 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.

Maintenance of records

15. Fis should maintain all infom1ation captured in the CCTV system for a minimum period of 180 days.

16. Fis, at their discretion, may retain the CCTV recordings relevant to observed suspicious activities for a longer period.

17. The FIU, LEAs or any other competent authority would, fom time to time, instruct the Fls to retain 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.

18. The Fis should ensure that its CCTV system(s) are capable of transfen-ing the info1mation to data storage devices, to allow retrieving and viewing of the CCTV records on electronic apparatus, such as computers.

19. To confirm the credibility of the CCTV records, Fis 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.

System administration and maintenance

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

21. In order to asce11ain 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.

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

23. Fis need to ensure that all inf01mation 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.

24. Fis are 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.

25. FIs are required to issue internal operational guidelines on placement, functionality, monitoring, record keeping, system maintenance and administration, and include it as a pa11 of AML/CFT policy as well with the approval of BOD.

26. 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.

27. Based on the repo1t 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. Fmther, immediate steps should be taken to replace or upgrade the equipment soon after any malfunction is detected.

28. Fis should ensure activities relating to the maintenance and recalibration of the CCTV system including system upgrading, refo1111atting and removal of records are clearly recorded in the system's maintenance log and reported to the senior management, as appropriate.

ශ්‍රී ලංකා මහ බැංකුව

CENTRAL BANK OF SRILANKA

මූල්‍ය බුද්ධි ඒකකය நிதியியல் உளவறிதற் பிரிவு **FInanclal Intelligence Unit**

Ref: 037/07/006/0004/018

GuideWnes-04/2018

19 April 2018

To: CEO's of All Financial Institutions

Dear Sir / Madam

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

The above Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 and the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016.

Yours faithfully

D M **Rupasinghe**
Director
Financial Intelligence Unit

Cc : Compliance Officer

14 වන මහල, අංක 30, ජනාධිපති මාවත,
තැ. පෙ. 590, කොළඹ 01, ශ්‍රී ලංකාව

14 ஆம் மாடி, இல. 30 சனாதிபதி மாவத்தை
த. பெ. இல. 590, கொழும்பு 01, இலங்கை

tenet ia , He. 30, Jana0tip&1 Moatha,
P. 0. Bar. 590, Colombo 01. Sri Wka.

94 11 2477125 / 509 94 11 2477692 fiu@cbsl.lk **www.fiusrilanka.gov.lk**

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

I. Introduction

1. This Guideline is issued pursuant to section 15(1)(j) of the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA).

2. The Financial Intelligence Unit of Sri Lanka (FIU), acting within the powers vested with it under the FTRA, issued the Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (CDD Rules) by Gazette Extraordinary No. 1951/13, dated January 27, 2016, effective from the date of issue, applicable to institutions that engage in "finance business" as defined under Section 33 of the FTRA.

3. Rules 28-31, 48-50 of the CDD Rules established, inter alia, provisions requiring Financial Institutions (FIs) identified under the Rules to take appropriate measures to identify and verify the natural person(s) who are the ultimate "beneficial owners" of a customer that is a legal person or legal arrangement, as defined in Rule 99 of the CDD Rules.

4. This Guideline is provided as an aid to interpret and apply CDD Rules. The Guideline is not intended to be exhaustive and it does not impose legally binding practices on any FIs, and it does not constitute legal advice from the FIU. Nothing in this Guideline should be construed as releasing FIs from any of their obligations under the CDD Rules or the FTRA.

II. Background/Context

Who is a beneficial owner?

5. As per the Rule 99 of the CDD Rules, the "beneficial owner" of the legal person or legal arrangement is a natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted including the person who

exercises ultimate effective control over a person or a legal arrangement. According to Rule 49, controlling ownership interest means an interest acquired by providing more than ten percent (10%) of the capital of a legal person.

6. It is an FI's obligation to determine the natural person(s) who is/are the ultimate beneficial owner(s). The ultimate beneficial owner must be a natural person and cannot be a company, an organization or a legal arrangement. There may be more than one beneficial owner associated with a customer.

7. If the customer is a natural person, the person can be treated as the beneficial owner unless there are reasonable grounds to show that he is acting on behalf of another or if another person is the beneficial owner of the property of the customer.

Why is it important to identify the beneficial owner?

8. Corporate entities such as companies, trusts, foundations, partnerships, and other types of legal persons and arrangements conduct a wide variety of commercial and entrepreneurial activities. However, despite the essential and legitimate role that corporate entities play in the economy, under certain conditions, they have been misused for illicit purposes, including money laundering (ML), bribery and corruption, insider dealings, tax fraud, terrorist financing (TF), and other unlawful activities. This is because, for criminals trying to circumvent anti-money laundering (AML) and countering the financing of terrorism (CFT) measures, corporate entities provide an attractive avenue to disguise the ownership and hide the illicit origin.

9. Various studies conducted by Financial Action Task Force (FATF), World Bank, United Nations Office on Drugs and Crime (UNODC) have explored the misuse of corporate entities for illicit purposes, including for ML/TF. In general, the lack of adequate, accurate and timely beneficial ownership information facilitates ML/TF by disguising:
   a) the identity of known or suspected criminals,
   b) the true purpose of an account or property held by a corporate entities, and/or

c) the source or use of funds or property associated with a corporate entities.

Ways in which beneficial ownership information can be hidden/obscured

10. Beneficial ownership information can be obscured through various ways, including but not limited to;
    a) use of shell companies [1] (which can be established with various forms of ownership structure), especially in cases where there is foreign ownership, which is spread across jurisdictions,
    b) complex ownership and control structures involving many layers of ownership, sometimes in the name of other legal persons and sometimes using a chain of ownership that is spread across several jurisdictions,
    c) bearer shares and bearer share warrants,
    d) use of legal persons as directors,
    e) formal nominee shareholders and directors where the identity of the nominator is undisclosed,
    f) informal nominee shareholders and directors, such as close associates and family,
    g) trust and other legal arrangements, which enable a separation of legal ownership and beneficial ownership of assets,
    h) use of intermediaries in forming legal persons, including professional intermediaries such as accountants, lawyers, notaries, trust and company service providers,

III. Establishing the Beneficial Owner

A) Beneficial owner of Legal Persons

11. As per Rule 99 of the CDD Rules, "legal person" means any entity other than a natural person that is able to establish a permanent customer relationship with a financial institution or otherwise owns property and includes a company, a body corporate, a foundation, a partnership or an association.

[1] Shell companies are companies that are incorporated with no significant operations or related assets, including an absence of physical presence

12. In the process of identifying beneficial owner(s) of a legal person, FIs have to consider three main elements:

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

13. The beneficial owner(s) of a customer (legal person) may satisfy one or more of the three elements identified above. Accordingly, it would not be sufficient to simply apply only the ownership element in determining beneficial ownership.

Ownership

14. As per Rules 28 and 48, FIs are required to understand the ownership and control structure of their customers when the customer is not a natural person. According to Rule 49, the prescribed threshold for controlling interest is interpreted as owning more than ten percent (10%) of the customer. The ownership could be direct as well as indirect through aggregated ownership as illustrated below.

Figure 1: Simple Indirect Shareholding

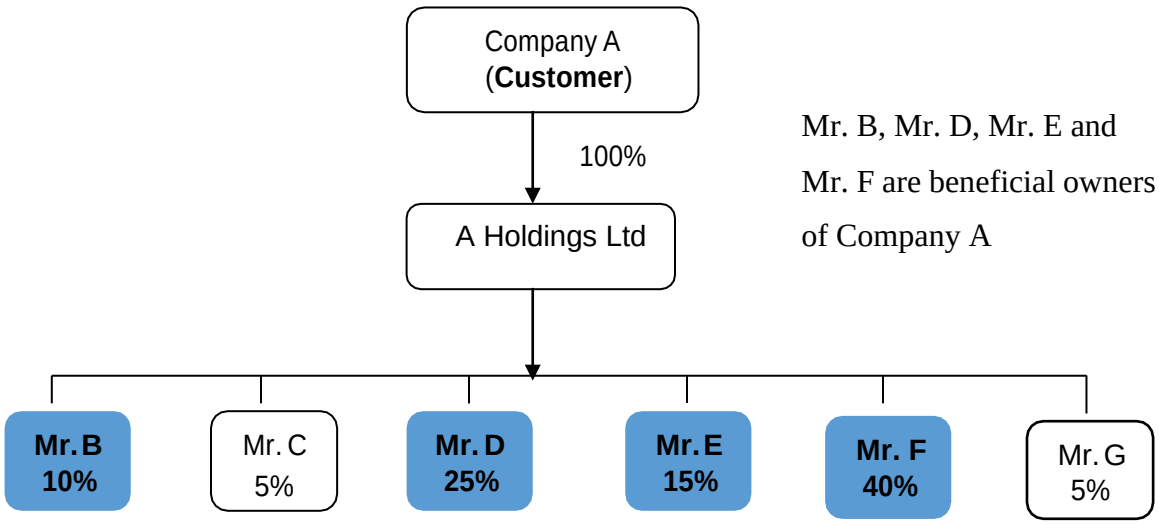
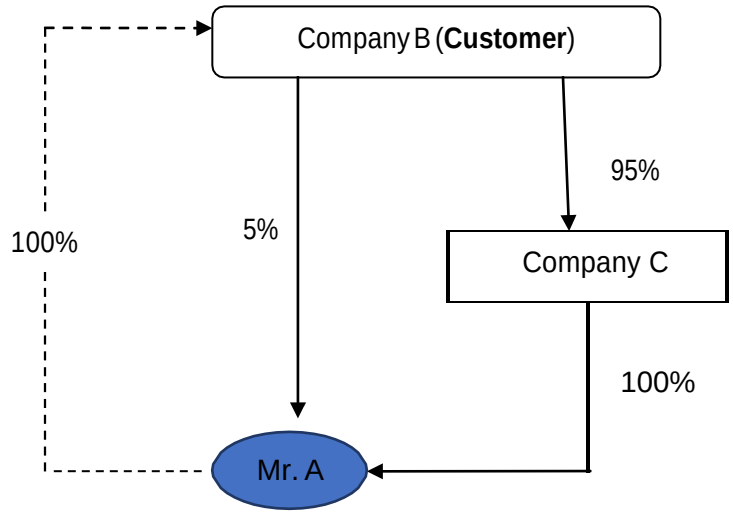
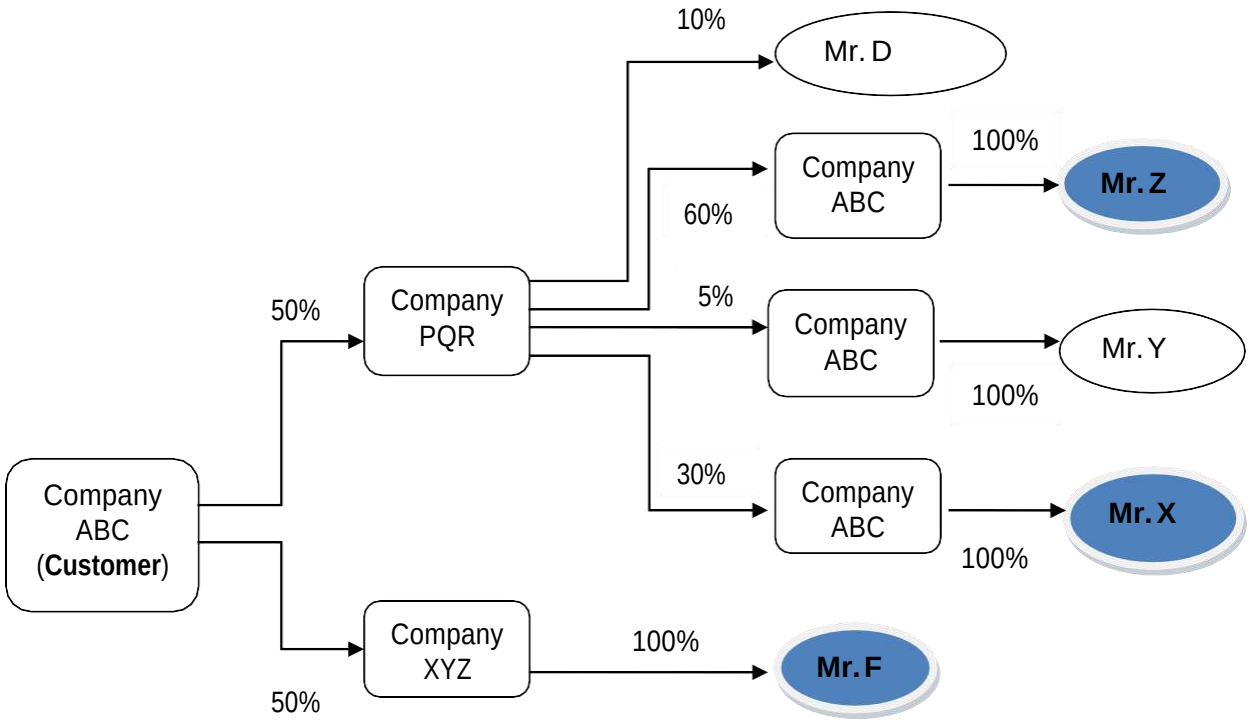


Figure 2: Direct and Indirect Share Holdings



Mr. A is the sole beneficial owner of Company B (Direct 5% + Indirect 95%)

Figure 3: Multi-level indirect shareholdings



Mr. F, Mr. X and Mr. Z are beneficial owners of Company ABC through indirect shareholding

15. A natural person that exercises control over a controlling portion of equity interest, either directly, via nominees or via family members or close associates (whether disclosed or undisclosed) who nominally own or control the shares, can be considered as a beneficial owner. A majority shareholder or a majority formed by some combination of shareholders that are nominees for a natural person is also a beneficial owner.

16. For some customers, ownership may be spread over a large number of individuals with all individual owning less than ten percent (10%). In such instance, because no individual(s) owns more than ten percent (10%), the effective control element outlined below would be more appropriate to determine the beneficial owner(s)/controller(s).

Effective Control

17. Effective control of a legal person is an important component that determines the beneficial ownership. Such control can be direct or indirect, formal or informal. At a direct and formal level, it is essential to understand the customer's governance structure as an aid in identifying those natural persons that exercise effective control over the customer. In deciding the effective controller(s) in relation to a customer, FIs should consider,
    a) a natural person who can hire or terminate a member of senior level management;
    b) a natural person who can appoint or dismiss Directors;
    c) Senior managers who have control over daily/regular operations of the legal person/arrangement (e.g. a CEO, CFO or a Managing Director).

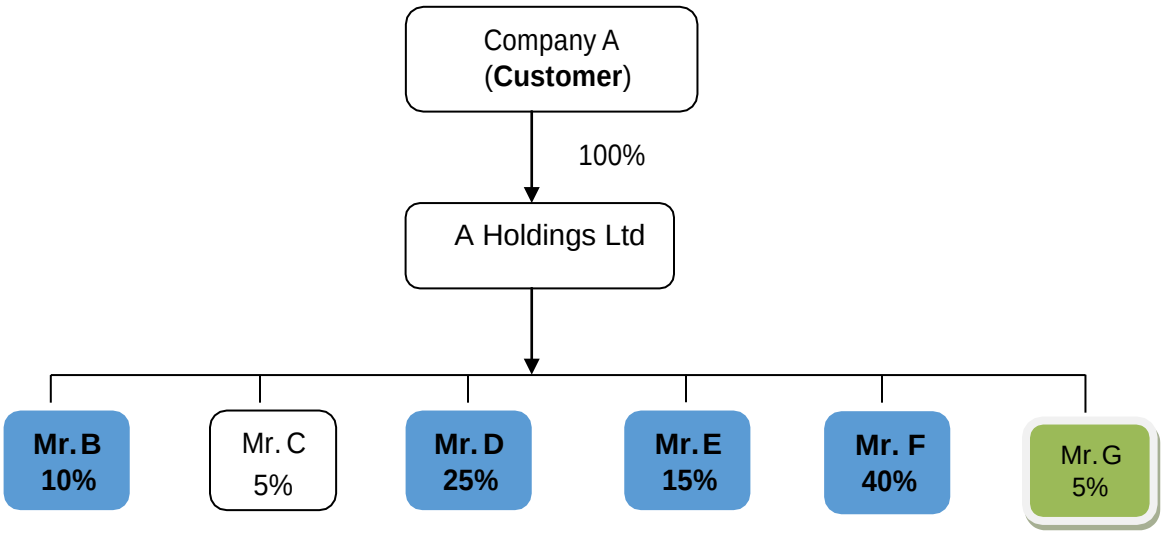
18. Natural persons may also control the legal person through other means such as:
    a) Personal connections to persons in positions such as Executive Directors/ CEOs/ Managing Director or that possess ownership;

b) Significant authority over a legal person's financial relationships (including with financial institutions that hold accounts on behalf of a legal person) and the ongoing financial affairs of the legal person;

c) Control without ownership by participating in the financing of the enterprise, or because of close family relationships, historical or contractual associations, or if a company defaults on certain payments;

d) Use, enjoyment or benefiting from the assets owned by the legal person even if control is never exercised.

Figure 4: Effective Control



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

Person on whose behalf a transaction is being conducted

19. Another aspect of the definition of beneficial ownership is a person on whose behalf a transaction is conducted. This may be the individual who is an underlying client of the customer. An example is, if a FI knows that person 'A' is conducting an

occasional transaction on behalf of person ‘B’, and then person ‘A’ and person ‘B’ should be identified and verified along with any other beneficial owners that may be a party to transaction.

20. Acting on behalf of the customer is when a person is authorized to carry out transactions or other activities on behalf of the customer. However, ‘Authority to act’ should not be confused with effective control.

21. There are instances where persons are acting on behalf of a customer may not necessarily be the beneficial owners of that customer.

22. As per Rule 29, the FI has to identify the natural persons that 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 also should be verified through documentary evidence including specimen signatures of the persons so authorized.

B) Beneficial owner of legal arrangements

23. As defined under Rule 99, legal arrangement includes an express trust, a fiduciary account or a nominee.

24. All trusts have the common characteristic of causing a separation between legal ownership and beneficial ownership. Legal ownership always rests with the trustee. Beneficial ownership can rest with the author of trust, trustees or beneficiaries, jointly or individually.

25. As per Rule 50, FIs should identify and take reasonable measures to verify information about a trust, including, 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).

26. FIs are required to obtain trust documents (e.g. deed of trust, instrument of trust, trust declaration, etc.) and the provisions of the trust document must be fully understood within the context of the laws of the governing jurisdiction. The FIs should take reasonable measures to verify trust document through independent means (e.g. Registry of Trust, Notary)

Example:

Person 'A' is the author of a trust for the benefit of his child. The trustee seeks to establish a relationship with a financial institution to help manage the assets of the trust. Even though the trustee is the controller of the assets of the trust he may not be the ultimate beneficial owner and the main focus of CDD should include person 'A'" as well.

IV. Identification and Verification of beneficial ownership information

27. As per Rule 30, FIs should obtain information to identify and take reasonable measures to verify the identity of the beneficial owner(s) of the customer using relevant information or data obtained from a reliable source, adequate for the FIs to satisfy itself that it knows who the beneficial owner(s) is.

28. Accordingly, the identification of beneficial owner is mandatory. Once the FI establishes who the beneficial owner(s) of a customer is/are, the FI must collect at least the following information in relation to each individual beneficial owner:

    a) full name;

    b) official personal identification or any other identification number;

    c) permanent/ residential address.

29. As per Rule 31, FI is required to 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.

30. Accordingly, once the identity is established, the FIs have to take reasonable measures to verify the identity of the beneficial owner(s). The reasonable measures for verification should be determined subject to the risk and complexities of the ownership and control structure of the legal person or arrangement.

31. Simplified verification procedures can be applied for verification of beneficial ownership of legal persons that are already subject to rules regarding corporate governance and transparency such as those that apply to firms with shares that publicly trade on a well-regulated exchange, or with simple and locally-familiar ownership structures or legal persons who are expected to conduct low risk transactions.

32. For the verification of beneficial ownership, some of the documentation that FIs can rely on may include (but not limited to) the following:
    a) Share register,
    b) Annual Returns,
    c) Trust deed,
    d) Partnership agreement,
    e) The constitution and/or certificate of incorporation for an incorporated association,
    f) The constitution of a registered co-operative society,
    g) Minutes of the board of directors meetings,
    h) Information available through open-source search or commercially available databases.

33. In case of foreign legal persons and arrangements FIs may also has to take additional measures such as verification through mother company or branches, correspondence bank, other agents of the bank, corporate registries etc.

34. As per Schedule I of the CDD Rules, 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, FIs can use relevant identification information available from reliable sources (e.g. a public register) to identify the Directors and major Shareholders.

35. As per Rule 49 (d), FIs have to identify the natural persons holding senior management positions as beneficial owners when FIs are unable to determine the beneficial owner as there is no person owning more than ten percent (10%) of the customer's equity or no individual exercising control over the customer.

Periodic Review of Information

36. As per Rule 40, FIs should periodically review the adequacy of information obtained in respect of beneficial owners to ensure that the information is up to date. The review period and procedures thereof should be decided by each FI in its internal AML/CFT Policy according to the risk-based approach.

37. Any material/significant change in customer circumstances may necessitate a review of beneficial ownership. Some examples of material/significant changes include:
    a. a public company is taken private;
    b. a shareholder or group of shareholders takes effective control of voting shares;
    c. a new partner is added, or an existing partner is removed;
    d. change in management positions;
    e. new trustees are appointed;
    f. a trust is dissolved;
    g. a new account is opened for the same customer;
    h. transactions are attempted that are inconsistent with the customer's profile.

Delayed Verification

38. As per Rules 31 and 32, FIs are allowed to delay the verification of identity of beneficial owners when,

a. risk level of the customer is low and 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.

39. As per Rule 33, when delayed verification is allowed, FIs should adopt risk management procedures relating to the conditions under which the customer may utilize the business relationship prior to verification. These procedures should include a set of measures, such as a limitation of the number, types and/or amounts of transactions that can be performed and the monitoring of large or complex transactions being carried outside the expected types of transactions for that relationship.

40. As per Rule 36, FIs should not establish a business relationship or conduct any transaction with a customer who poses a high money laundering and terrorist financing risk, prior to verifying the identity of the beneficial owner.

41. As per Rule 35, when an FI is unable to comply with CDD measures as required in CDD Rule including identification and verification of beneficial ownership information, the FI should not enter into the business relationship or perform the transaction with new customers and terminate the business relationship with existing customers and consider making a suspicious transaction report in relation to the customer.

V. Other Requirements

Declaration of beneficial ownership by the customer

42. FIs may obtain beneficial ownership information either by obtaining the required information on a standard certification form (Certification Form (Appendix A) or by any other means, up to the satisfaction of the FIs with regard to the identification of the beneficial owner(s).

43. Use of the form is optional and FI may substitute this form with a version that is suitable, whether paper or electronic, so long as the required information is collected, protected, preserved and made available to competent authorities upon demand and records are maintained in accordance with the CDD Rules and FTRA.

44. FIs are required to document the procedure to be followed in the identification and verification of beneficial ownership requirements relating to legal persons and arrangements in the AML/CFT Policy approved by the Board of Directors.

Record Keeping Obligations

45. The FIs are required to maintain records of identification and verification information relating to beneficial ownership as prescribed under Part V of the CDD Rules and FTRA.

Beneficial owners who are Politically Exposed Persons (PEPs)

46. As per Rule 59, FIs are required to implement appropriate internal policies, procedures and controls to determine if the beneficial owner is a politically exposed person. Through such process if the FI identifies any beneficial owner as a PEP, the relationship should be considered as high risk and subject to enhanced due diligence as required in the CDD Rules.

Sanctions

47. Failure to comply with the beneficial ownership requirements as required under the CDD Rule will be a violation of the Section 2 (3) of the FTRA and will be punishable under Section 19 of FTRA.

VI. Examples

Example 1: Record for ownership and control structure of a legal person

ABC Company Ltd. is a private limited liability company registered under the Companies Act, No. 7 of 2007. Mr. A owns 25% of the shares and BC Company Ltd. owns the balance 75% of shares of ABC. Mr. S is Managing Director of ABC

Company and; the Board of Directors consists with his wife, Mrs. S, ABC's Chief Financial Officer; and their three children.

In this example, FIs required to record:

- the ownership of the Company - shared by Mr. A (25% of the shares) and BC Company Ltd. (75% of the shares);
- the ownership structure of the entity - ABC Company Ltd. is a privately traded.
- the identification of all members the Board of Directors (Mr. S's Family) as they are having effective control;
- Identification of Mr. A as he is having more than 10% of ownership
- identification of all of the individuals who own or control, directly or indirectly, 10% or more of the shares of BC Company Ltd since it owns 75% of the shares, it also exercises control. However, in a case like this, FI must research further to determine whether any individual owns enough shares of BC Company Ltd. that would constitute 10% of ABC Company Ltd., or until FI determine that there is no such individual;
- the manner in which FI obtained this information; and
- the measures taken to verify accuracy of information.

Example 2
Record for ownership and control structure of partnership

Rainbow Property Developers is a partnership engaged in buying and selling of real estate in Western Province owned by two partners (Mr. T and Mr. J). Mr. T and Mr. J have signed a partnership agreement stating that Mr. T will invest Rs. 5,000,000 in the partnership to rent space for the Rainbow Property Developers and other administrative expenses, and Mr. J will be solely responsible for operations of the business. All decisions related to the partnership must be unanimous; in case of a disagreement, either partner can decide to end the partnership. Mr. T & Mr. J will split the profits from the business 50/50. If they decide to end the partnership, Mr. T

will get 55% of the proceeds of the sale of the business assets, while Mr. J will get 45%.

In this example FI, is required to record:

- the ownership structure of the entity, including the details of the partnership between Mr. T & Mr. J;
- identification of Mr. T and Mr. J as both control the partnership;
- the manner in which, the FI obtained this information; and
- the measures taken to confirm accuracy of information.

Note: The business structure is important in this example as the ownership and control of the partnership is shared between Mr. T & Mr. J. The FI needs to retain a copy of the partnership agreement to meet record keeping requirements as well as confirm the accuracy of the beneficial ownership information obtained. In the absence of such agreement it should be recorded that the partnership exists between Mr. T and Mr. J without having a written agreement.

Issued on April 19, 2018

APPENDIX I—Beneficial Ownership Form

Declaration of Beneficial Ownership	
This form has been issued under the Customer Due Diligence Rue No 1 of 2016 issued in terms of the Section 2(3) of the Financial Transactions Reporting Act of 2006. This form, or an approved equivalent, is required to be completed by all customers of financial institutions designated under the Acts to the best of their knowledge. The original completed and signed and witnessed version of this form must be retained by the financial institution and available to the competent authorities upon request.	
Customer Identification:	
Name and Designation of Natural Person Opening Account	
Name, Reg. No. and Address of Legal person for Which the Account is Being Opened	
Name, Deed No., Trustee and Address of Legal arrangement for Which the Account is Being Opened	
I declare that I:	
☐	am the beneficial owner[2] of the customer for this account.
☐	am not the beneficial owner* of the customer of this account. Complete identifying information for all beneficial owners that own or control 10% or more of the customer's equity, beneficial owners on whose behalf the account is being operated, and at least one person who exercises effective control of the legal entity regardless of whether such person is already listed.

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

	Name	NIC or Passport # /Country of Issue/Country of Citizenship	DOB	Current Address	Source of Beneficial Ownership (1=Equity (indicate %), 2=Effective Control, 3=Person on Whose Behalf Account is Operated)	Check if Politically Exposed Person (PEP) [3]
						☐
						☐
						☐
						☐

Details of the Customer Authorized to Act on Behalf of Entity
Name :
NIC/Passport :
Date of Birth :
Signature : (By signing you attest to the veracity of all information contained herein and you acknowledge and understand the above warning)

Verification of Beneficial Ownership

Authorized Financial Institution Official
Name :
Title :
Date :
Signature and Seal: (by signing, you attest that you have identified the Customer whose signature is on this form and have witnessed said signature)

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

A LIST CATEGORIES OF CUSTOMERS THAT CAN BE CONSIDERED AS PEPS

DOMESTIC PEPS

A.

1 The President
2 The Prime Minister
3 The Speaker and the Deputy Speaker of the Parliament
4 Cabinet Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers
5 Members of Parliament
6 Leaders of Political Parties

B.

7 Governors of Provinces
8 Chief Ministers of Provinces
9 Mayor, Chairman of Municipal Councils
10 Chairman of Provincial Councils
11 Members of Municipal Councils/ Provincial Councils / Local Government Bodies
12 Commissioners/ Secretaries to Municipal Councils/ Provincial Councils / Local Government Bodies

C.

13 Chief Justice
14 Attorney General
15 Judges of Supreme Court
16 Judges of the Court of Appeal
17 Solicitor General of the Attorney General's Department
18 Judges of High Courts/Provincial High Courts
19 Judges of District Courts
20 Judges of Magistrate Courts
21 Registrar of Supreme Court
22 Registrar of the Court of Appeal
23 Registrars of Judges of High Courts/Provincial High Courts
24 Registrars of District Courts
25 Registrars of Magistrate Courts

D.

26 Ambassadors /High Commissioners
27 Consul-General/ Deputy Head of Mission/Charge d'affaires/Honorary Consul
28 Ministers plenipotentiary and Envoys Extraordinary
29 Representatives of UN agencies and Heads of other international organizations

E.

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

32 Secretary /Senior Additional Secretaries/ Additional Secretaries to the Cabinet of Ministers, Non-Cabinet Ministers, State Ministers, Deputy Ministers
33 Deputy Secretary to the Treasury
34 Secretary/ Senior Additional Secretaries /Additional Secretaries/ Deputy Secretaries to Ministries
35 Members of the Monetary Board
36 Governor / Deputy Governors / Assistant Governors and Heads and Additional Heads of Department of the Central Bank of Sri Lanka
37 Advisors to the President/ Prime Minister / Ministers/ Ministries
38 Chief of staff of presidential secretariat
39 Auditor General
40 Secretary General of Parliament
41 District Secretaries/ Government Agent and Secretaries
42 Heads and Senior Officials of Government Departments
43 Chairmen and Senior Officials of State Enterprises
44 Chairmen and Senior Officials of State Corporations / Statutory Boards/ Authorities/ Public Corporations

F.

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

G.

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

H.

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

FOREIGN PEPS

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

A LIST OF RED FLAGS AND INDICATORS FOR SUSPICION

A. PEPs attempting to shield their identity:

1. Use of corporate vehicles (legal entities and legal arrangements) to obscure
    i) ownership,
    ii) involved industries or
    iii) countries.
2. Use of corporate vehicles without valid business reason.
3. Use of intermediaries when this does not match with normal business practices or when this seems to be used to shield identity of PEP.
4. Use of family members or close associates as legal owner.

B. Red flags and indicators relating to the PEP and his behavior

1. The PEP makes inquiries about the institution's AML policy or PEP policy.
2. The PEP seems generally uncomfortable to provide information about source of wealth or source of funds.
3. The information that is provided by the PEP is inconsistent with other (publicly available) information, such as asset declarations and published official salaries.
4. The PEP is unable or reluctant to explain the reason for doing business in the country of the FIs/DNFBs.
5. The PEP provides inaccurate or incomplete information.
6. The PEPs seeks to make use of the services of a FIs/ DNFBs that would normally not cater to foreign or high value clients.
7. Funds are repeatedly moved to and from countries to which the PEPs does not seem to have ties with.
8. The PEP is or has been denied entry to the country (visa denial).
9. The PEP is from a country that prohibits or restricts its/certain citizens to hold accounts or own
   certain property in a foreign country.

C. PEP's position or involvement in businesses:

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

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

1. Arms trade and Defence industry.
2. Banking and finance.
3. Businesses active in government procurement, *i.e.*, those whose business is selling to government or state agencies.
4. Construction and (large) infrastructure.
5. Development and other types of assistance.
6. Human health activities.
7. Privatization.
8. Provision of public goods, utilities.

RED FLAGS ON INFORMAL VALUE TRANSFER SYSTEMS

Money or Value Transfer Services perform an important role in the economy and the financial sector of a country. Money or Value Transfer Services can be classified into two types as Formal and Informal Money or Value Transfer Services based on the functional formality and characteristics. Formal Money or Value Transfer Services are expected to capture all economic transactions that add value to the national output of the country. However, Informal Money or Value Transfer Services (IMVTS) pose a significant threat to a nation's economy since the value created through IMVTS is not considered when assessing the national output. Furthermore, IMVTS could be abused for Money Laundering/Terrorist Financing (ML/TF) and related unlawful activities.

IMVTS mainly involve four parties and two geographical locations, i.e., sender, receiver and two IMVTS operators. In IMVTS, money is given by the sender in the first geographical location to an IMVTS operator of that location, to transfer the money to the receiver in the second geographical location, with the support of an IMVTS operator in the second location, preferably to settle payables. Above transactions are carried out with the use of the two currencies of the respective locations and it should be noted that no inward/outward remittances occur between the said locations.

Accordingly, the Financial Intelligence Unit (FIU) wishes to share the following list, that includes several red flag indicators observed by the FIU when carrying out analysis on Suspicious Transactions Reports received pertaining to IMVTS.

1. Receipt of foreign remittances to accounts initially and its gradual decrease/cessation followed by the receipt of Sri Lankan Rupees
   (This could be an indication that the accountholder(s) has shifted from formal money transfers systems to IMVTS)
2. Receipt of frequent third-party deposits and transfer of those funds to multiple third-party accounts
   (This could be an indication that the accountholder(s) is involved in IMVTS)

3. Minimal / no ATM withdrawals but substantial number of online debit fund transfers from accounts with names of receivers as narrations
   (This could be an indication that funds received to the country through IMVTS are distributed to the beneficiaries)
4. Receipt of frequent third-party deposits and withdrawal of such funds from abroad
   (This could be an instance where IMVTS intersect formal value transfer systems)
5. Accounts having an insignificant daily balance but an unusually high credit and debit turnover
   (This could be an indication that accounts are solely used for the purpose of distributing funds received through IMVTS)
6. Upon inquiries made by the reporting entity, accountholders themselves declaring to be engaged in IMVTS operations

The financial institutions are hereby required to take cognizance of the above red flags/ risk indicators and take appropriate actions to reduce the possible ML/TF risk, if any, arising from these transactions, including considering escalating the indicators to the level of raising STRs with the FIU.

Red Flag Indicators - 04/2021

Trend in Foreign Currency Outflows via ATMs: Cash withdrawals in the United Arab Emirates (UAE)

The Financial Intelligence Unit (FIU) has observed significant number of transactions where foreign currency withdrawals from the UAE are reported using locally issued ATM cards.

It was noticed that some individuals collect deposits to the individual accounts from several areas of Sri Lanka and the accumulated funds in these accounts have been withdrawn almost immediately, via ATMs in the UAE**.**

FIU observed the following common characteristics when analyzing the patterns of the transactions:

1. Often, the majority of the accounts have been opened recently (in 2021).
2. Rupee value of most of the cash withdrawals from ATMs in the UAE is around Rs.100,000 to 200,000 per withdrawal. Occasionally, several such withdrawals had been taken place on the same day.
3. A significant number of suspected accounts have been opened at bank branches located in areas such as Kandy, Kalmunai, Wellampitiya, Kanthale and Colombo.
4. The ATM withdrawals were made from the UAE within 2 – 3 days after the opening of those reported accounts.
5. Cash has been withdrawn using several ATM cards at the same location at the same time, suggesting a single user having multiple cards or a group of persons acting in concert.

These activities suggest that the transactions may be linked to:

a. money laundering or terrorist financing activities
b. trade related activities, where ATM cards issued by banks are being misused for bulk withdrawals in foreign jurisdictions; or
c. activities linked to transfer funds without declaration at the border – suspicion is linked to tax evasion, or informal money, or value transmitters' (hawala or hundi) outflows.

The financial institutions are required to take appropriate actions to reduce the possible ML/TF risk, if any, arising from these transactions. Particular attention has to be drawn to:

I. Possible foreign exchange violations
II. The account holders allowing third parties to use their debit cards for cash withdrawals in foreign countries
III. Ongoing monitoring of customers after establishing the business relationship should be strengthened
IV. Necessary actions should be initiated, if the account holders are not reachable through the given contact numbers
V. If there is any suspicion, it has to be reported to the FIU under section 7 of the FTRA

l@ot»l ®m @t;o c>
8)60r616Ulffi lD��lU6lJr:ilffil
CENTRALBANKOFSRILANKA

i@?S���Q)Q
[6l�wlUJoo �61l6l.J�l'f>!D t.'.irft&lf
FINANCIAL INTELLIGENCE UNIT

t,ot»30,�ijeo,®lt>a>,�J�®01,@@otme>
�6\). 30, cf60TIT,U{bl l.OfT6l.J$l)6l»�, G6>fT@LD4 - 01, �6\)ffiJ6IDffi
No. 30, Janadhlpathl Mawatha, Colombo 01, Sri Lanka

Guidelines-03/2020

Ref: 037/05/006/0009/020

October 22, 2020

To: CEOs / General Managers and Managing Directors of All Financial Institutions

Dear Sir/ Madam,

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

The above mentioned Guidelines will come into force with immediate effect and shall be read together with the Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) and Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (CDD Rules) as amended from time to time.

Yours faithfully,

Director
Financial Intelligence Unit

Cc;

1. Director, Bank Supervision Department of Central Bank of Sri Lanka
2. Director, Department of Supervision of Non-Bank Financial Institutions of Central Bank of Sri Lanka
3. Director, Payments and Settlements Department of Central Bank of Sri Lanka
4. Director General, Securities and Exchange Commission of Sri Lanka
5. Director General, Insurance Regulatory Commission of Sri Lanka
6. Commissioner General, Department for Registration of Persons
7. Compliance Officers, all Financial Institutions

tr 011-2477125 alt 011-2477692 flu@cbsl.lk www.flusrllank.gov.lk
011-2477509 011-2477708 dflu@cbsl.lk

E H Mohotty

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

Part I - Introduction

1. These Guidelines are issued pursuant to section 15(1) (j) of the Financial Transactions Reporting Act, No. 06 of 2006 (FTRA).

2. These Guidelines are issued to Financial Institutions (FIs) to facilitate verification of identity (verification against the original document) when onboarding non face-to-face[1] individual customers (natural persons) using electronic interface provided by the Department for Registration of Persons (hereinafter referred to as DRP).

3. These Guidelines will come into force with immediate effect and shall be read together with the FTRA and Financial Institutions (Customer Due Diligence) Rules, No. 01 of 2016 (CDD Rules) as amended from time to time.

4. These Guidelines may be modified from time to time or withdrawn in the event of any unforeseen risks arising in the future or when more effective and reliable methods for establishing and verifying customer identity in non face-to-face onboarding come into force.

Part II - Scope

5. These Guidelines provide alternate methods to meet the requirement of "verification against original document" for individual customers who are natural persons as detailed in the following:

    a) Schedule to the CDD Rules under Rule 27 – Item (1) (b)(i)—verification of identity document
    b) Schedule to the CDD Rules under Rule 27 – Item (1) (b)(ii)—verification ofaddress

6. All other requirements imposed under CDD Rules will be applicable to customers onboarded using the above method without any exception.

Part III - Methods of Application

7. Verification of individual customer identity document

    a. Claimed Identity. FIs must continue to identify their customers in full accordance with CDD Rule 27(1)(a) and obtain all information described in Rule 27(1)(b) from the customer.

        Claimed identity information may be obtained by the FI in any manner that safeguards its integrity during the process of transmission. Potential modes of obtaining identity

[1] **Non-face-to-face** interactions are considered to occur remotely, meaning the parties are not in the same physical location and conduct activities by digital or other non-physically-present.

information include but are not limited to electronic forms, mobile app, video conferencing, secure email, kiosks/ ATMs/ CDMs, registered post, etc.

Use of agents, third-party service providers acting as agents or reliance on third-party FIs or designated non-finance businesses to collect information on claimed identity is not permitted for this alternate method.

b. Existence of Claimed Identity. FIs may use electronic interface published by the DRP to obtain information to independently validate the customer's claimed identity, provided:

   i. The interface is accessed with the unique credentials assigned to the FI by the DRP;
   ii. The interface is accessed strictly in accordance with its terms of use;
   iii. The interface returns to the FI a record that uniquely matches the claimed identity information provided by the customer in a form suitable for verification of customer identity claims and that includes an image of the person to which the identity has been assigned that is suitable for the purpose of associating the record with the claimed identity of the customer;
   iv. The FI has no reason to believe that the interface, or the effectiveness thereof, has been maliciously compromised in any way.

c. Associating Claimed Identity with Customer. The following steps must be performed in order to associate the claimed identity with the customer:

   i. Obtaining Customer Imagery and other documents from the Customer:
   High-quality still images[2] of the customer, ID documents and address verification documents must be obtained. For customers not physically present in Sri Lanka, passport images must also be obtained containing customer biographical data, a current visa and an entry stamp or any other entry permitting official document for the country where they are located. The imagery should be of sufficient quality to read details and to inspect security features of the identity document, to identify unique facial features of the customer, and to detect any potential alterations to the document. Ideally, the imagery should be obtained from a device known to be associated with the customer (e.g. a mobile phone) or from a dedicated device operated by, or on behalf of, the FI (e.g. kiosk devices).

   ii. Obtaining Customer Real-Time Video from the Customer
   A staff member of the FI must engage in a high-quality real-time video[3] conference with the customer and verify the possession of his identity documents and address verification documents during this real-time video conference. For customers not physically located in Sri Lanka, passport and visa data from (i) must also be verified. The customer should respond via real-time video conference to FI inquiries in order to establish the authenticity of the imagery and the accuracy of other customer provided information.

[2] High-quality still images refer to resolution equivalent to 300 PPI/ DPI (Pixels Per Inch / Dots Per Inch) or higher.
[3] High-quality real-time video refers to consistent resolution equivalent to 360p (pixels) or higher with minimal frame droppage.

iii. Obtaining Customer Imagery from DRP

FIs must use electronic interface published by DRP in order to obtain information to authenticate the validated identity information against the customer claimed identity, in accordance with the provisions detailed in paragraph 7(b). As a practical matter, the only currently available information for this purpose is a photographic image associated with a National Identity Card (NIC).

iv. Authenticating Claimed Identity to Customer

The following modes shall be used to authenticate the claimed Identity to the Customer:

1. Algorithmically: FIs that intend to authenticate a claimed identity algorithmically using data and images obtained from both the customer and DRP must obtain prior approval from the FIU in the form of an "enforcement forbearance" by submitting an application to the CBSL "Regulatory Sandbox" and completing the FIU's addendum to the application. Without such a forbearance and FI agreement with the FIU to abide by the terms of the forbearance, FIs are not permitted to authenticate claimed identities using this mode.

   The Sandbox Framework documents along with the Sandbox application form can be downloaded at https://www.cbsl.gov.lk/en/public-notices. For any inquiries or clarification contact Payments and Settlements Department of Central Bank of Sri Lanka on 2477542, 2477642 or e-mail to sandbox@cbsl.lk.

2. Manually: Manual comparison by employees of the FI should be made in all cases when an algorithmic comparison has not been approved by the FIU through guidelines or specific letters of forbearance [e.g. obtained through the CBSL Regulatory Sandbox]. The standard for successful non face-to-face authentication should be at least as rigorous as for the FI's face-to-face mode.

3. A combination of algorithmic and manual modes may also be used. However, if the algorithmic mode employed has not been approved by the FIU through guidelines or specific letters of forbearances then the manual mode must stand-alone as being determinative.

When the claimed identity cannot be verified or authenticated the FI must not enter into a business relationship with the customer or process transactions on behalf of the customer using this alternative verification method.

8. Verification of Individual Customer Address

Individual Customer addresses may be verified using data matching the customer's claimed identity obtained by the FI through a DRP electronic interface. If the address provided by the customer differs from the address obtained through a DRP electronic interface, the FI must instead verify the customer's address using independent data or services provided electronically to the FI directly from one or more sources specified in Schedule to the CDD Rules under Rule 27- Item (1)(a)(a1)(iii).

9. Instances where FIs should refrain from opening accounts or establishing business relationships non face-to-face.

    a. When non face-to-face customer uses any other identification document other than national identity card such as passport or driver's license to identify himself.

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

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

    d. When identity documents presented by the customer appear damaged or degraded to the point that they are no longer fit for the purpose of identification.

    e. When identity documents presented by the customer appear altered or when document security features cannot be validated or when the integrity of the document for any other reason is suspected.

    f. When the customer refuses or unable to comply with any aspect of the FI's established non face-to-face onboarding procedures. The customer cannot be onboarded using non face-to-face mode if customer fails to cooperate with full completion of the FI's established non face-to-face onboarding procedure. Such non-compliance can take many different forms including but not limited to a refusal or inability to adjust ambient lighting, a refusal or inability to remove anything that obscures a clear view of the customer's face, customer refusal or inability to remain still or to still the image capturing device, a refusal or inability to answer questions posed by the onboarding officer(s).

    g. When a failure of FI systems prevents the FI from fully executing their established non face-to-face onboarding procedures to include, for example, recording and secure storage of onboarding video and image captures of identity documents.

    h. When the claimed identity cannot be shown to exist using the DRP electronic interface.

    i. When details of the customer's claimed identity are not consistent with details obtained for the claimed identity through the DRP electronic interface.

    j. When a non face-to-face customer presents a NIC with a photo image which the onboarding officer matches with data and imagery from the DRP but which the officer cannot positively match with the current appearance of the customer claiming the identity.

    k. When a non face-to-face customer appears to have intentionally modified his appearance in a manner intended to compromise ability of the FI to accurately identify and verify the customer and to fully complete its established non face-to-face onboarding procedure.

l. When a claimed identity cannot be authenticated to the customer due to an inability to match with a high degree of confidence the images obtained of the customer and of customer identity documents with corresponding images obtained from DRP.

m. When the FI has reason to doubt the veracity of any customer claims, whether related to identity or otherwise.

n. When customer behavior causes the FI to doubt the legal intents or purposes of the customer in establishing business relations.

o. When the FI is unable to identify the current location (eg. using GPS or any other suitable mechanism to identify the location and to determine whether customer is a resident or a non-resident) of the customer by the FI.

p. Where the FI has a reasonable suspicion on the document authenticity in any manner.

10. Policies, Training, Record Keeping and Audit

    a. The FI must establish clear policies and procedures for non face-to-face customer identification and onboarding prior to applying the alternate methods described herein.
    b. The FI must conduct at least an entry level training programme and carry out ongoing training for relevant onboarding staff prior to applying the alternate methods described herein.
    c. FI records that are unique to the alternate methods of customer identification and onboarding contained herein are fully subject to CDD rules regarding record keeping and must be retained in a form sufficient for an internal or external auditor to independently reconstruct the full identification process for any specific customer. Retention of video images is recommended. In the case when a suspicion related to customer identity is formed, the retention of video is mandatory.
    d. FI customer identification programmes using the alternate methods described herein must be included in the FI's internal audit scope under Anti Money Laundering and Combating the Finance of Terrorism (AML/CFT) aspects in order to determine efficacy of the programme and to detect operational deviations from policy.

Part IV - Risk Management

11. The non face-to-face methods of identity verification described herein must be considered in the context of the FI's "risk-based approach" prior to use. If necessary, the FI's risk assessment must be updated to reflect the impact of the non face-to-face methods.

12. Customer risk profiles must reflect any non face-to-face methods of identification used for the purpose of their identification.

13. Customers identified using non face-to-face methods described herein should be monitored and managed as higher risk and subject to enhanced CDD until such time as they are able to present an original identification and the FI is able to verify and make a copy thereof.

14. In addition to the above requirements of treating non face-to-face onboarded customers as of high risk, customers located outside of Sri Lanka must be risk managed in accordance with the known risks of the jurisdiction where the customer is located.

Part V – STR Reporting

15. The entirety of the circumstances, most especially those related specifically to non face-to-face customer identification, must be considered in order to determine whether filing a suspicious transaction report with the FIU is warranted in relation to non face-to-face customer onboarding.

16. Such circumstances may include but not limited to impersonation, any doubt on document authenticity, forged ID and address verification documents, altered ID or address verification documents, altered images, spoofing, reluctance to cooperate or provide additional information for verification, suspicious behavior, discrepancies in information provided.

Part VI - Enforcement

17. The FIU will forbear on enforcement of Schedule to the CDD Rules under Rule 27- Items (1) (b)(i) and Schedule to the CDD Rules under Rule 27- Item (1) (b)(ii) when:
    a. the non face-to-face methods of customer identification contained herein are applied to a particular individual customer, and;
    b. this Guidance is strictly followed in its entirety by the FI; and
    c. this Guidance remains in force.

October 22, 2020

CODE OF CONDUCT

CONTENTS

	Page
1. Introduction to the Code	3
2. Vision	4
3. Mission	5
4. Our Business Values	6
5. Our Pledge	7
6. People's Bank Song	8
7. History of People's Bank	9
8. Conduct	11
9. Responsibilities	12
10. Confidentiality	16
11. Conflicts of Interest	17
12. Insider Dealing/ Insider Trading	19
13. Outside Employment	20
14. Competition and Fair Dealing	21
15. Bribery and Corruption	22
16. Customer Service and Customer Complaints	23
17. Cleanliness, Hygiene and Safety	26
18. Compliance with Laws, Regulations and Bank's Internal Circulars	28
19. Protection and use of Bank Assets	29
20. Use of Our Computer System	30
21. Compliance with the Code	32
22. Acknowledgement	33

01. Introduction to the Code

The People's Bank's reputation is a priceless asset that each and every one of us must maintain. Our reputation not only affects whether or not someone will choose to be our customer, it also determines whether that person is proud to be associated with the organization. Our business is strongly based on a tradition of trust. Our most valued asset is our Human Resource – i.e. our employees and the principles which we have upheld and stood for over the years.

In addition to government sponsorship, our success is due in large measure to the dedicated professionalism and talents of our people.

We value our customers, our stakeholders and the reputation what we have built as a leading financial conglomerate in Sri Lanka. As we continue to grow and expand in a new environment which is competitive, the People's Bank standard for integrity and personal respect must be maintained and protected at all times.

It is the policy of the Bank to conduct our business in full compliance with the laws and regulations applicable to our business activities. To this end, all employees of the Bank are expected and directed to comply with the legislative/ regulatory requirements and directions and to manage the business of the Bank with honesty, integrity and respect to each other and the Bank as a whole. Our reputation was built by the stakeholders and our employees and it must be continuously maintained by the employees themselves.
As an employee, one is faced with a number of decisions and problems each day. Therefore, it is one's personal responsibility to uphold the high standards of business conduct laid down herein.

In our rapidly evolving business, each of us is challenged by a complex environment. Therefore, it is not possible to predict and find solutions for every possible situation we may encounter. Employees are therefore encouraged to seek the advice of their superior or the Compliance Officer whenever they are in doubt.

Therefore, the principal objective of this Code is to provide a general outline of the standards of professional and ethical conduct that all employees are expected to conform to, and to ensure that you are aware of the standards of personal integrity that are required when conducting both the People's Bank's business and your own.

02. OUR VISION

TO BE THE BANK OF THE

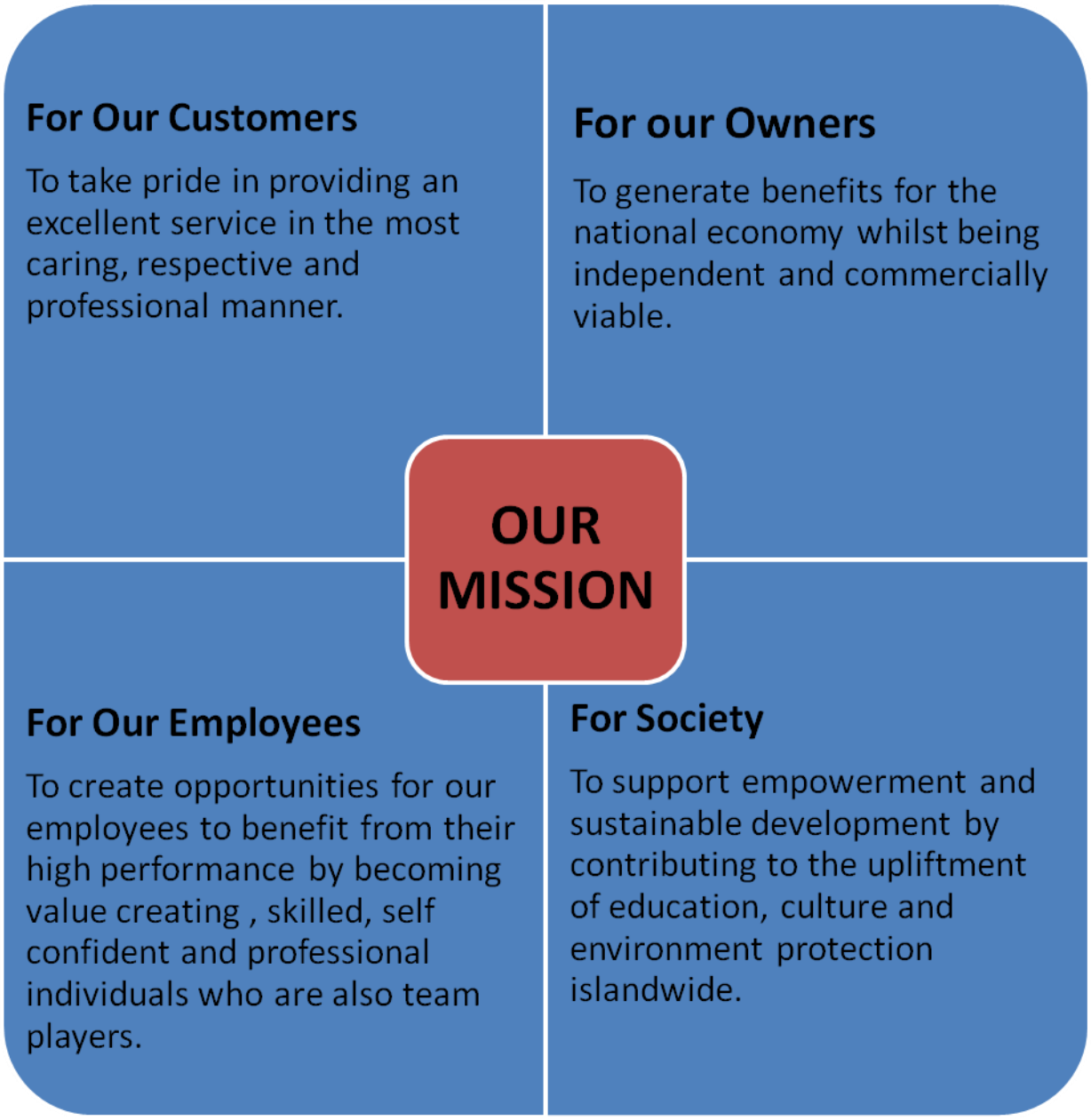
ASPIRING PEOPLE OF SRI LANKA

EMPOWERING PEOPLE TO BECOME VALUE CREATING,

COMPETITIVE AND SELF RELIANT

IN THE FACE OF COMPETITION

03. OUR MISSION



04. OUR BUSINESS VALUES

- We recognize that the primary reason for our existence is to create value for all the people of the Nation by becoming a major source of high quality capital formation.

- In all our activities we will exercise our duty of utmost care in the interests of our depositors.

- We will promote long-term ethical relations with our customers through truth and fair dealing.

- We will put our customers at the centre of everything we do by minimizing bureaucracy, demanding hands-on management, fast decisions and implementation.

- We will demand the highest standards of personal integrity at all levels, putting the Bank's interest ahead of individuals.

- We will create an environment of mutual respect and trust where employees demonstrate their performance and achieve their full potential.

- We will develop our business by encouraging high performing teams that recognize and support every employee's skill, commitment and link to the community.

- We are committed to complying with the spirit and letter of all laws and regulations, adhering to the highest standards of Corporate Governance, transparency, disclosure and ethical conduct.

- We will conduct ourselves as good corporate citizens promoting the environment and sustainable development.

05. OUR PLEDGE

(Given by Employees of People's Bank)

- I am a proud employee of the State – owned People's Bank. I am committed to providing the customers with a service of excellence.

- I pledge myself to accord a maximum contribution to steer my Bank towards prosperity and to make the lives of fraternal citizens comfortable.

- I will follow an eight- pronged approach with the objective of accomplishing this pledge;

    1. I will do whatever should be done today, today itself. It will not be postponed for the next day.

    2. I will accord a cordial welcome to the public and endeavour to meet their requirements and expectations.

    3. I pledge to act in compliance with the norms and regulations of People's Bank. However I consider that the results expected of my service are more important than the mere following of regulations.

    4. I will refrain from making use of the position I hold in People's Bank and the assets of People's Bank improperly or for personal advantage, directly or indirectly. I consider it my bounden duty to protect public properties and assets of People's Bank and to use them with due care.

    5. I will act conscientiously and do only what is correct, in keeping with the principles of People's Bank.

    6. I will perform my duties impartially irrespective of People's social status and standing.

    7. I will speak, act and behave in a manner that will uphold the dignity and honor of People's Bank, both in and out of the office.

    8. I will act with a sense of team spirit and unity with my colleagues for the efficient performance of the service expected of me.

06. PEOPLE'S BANK SONG

Sirasata Dina Dina Sevana Salaswana
Ipaduna Upadina Siri Lanka Dana
Diva Mathurak vana
Desa Resa Nangwuwa Mahajana Bankuwa //

Niwasin Niwasata Gamingamata (Sithumina Palanda)//
Ge-dora Watupiti Kamhal Dasa Dahasin Pubuda
Samupakaraya Mau ekaye nalavuna Bilinda
Mahajana Bankuwa Mathu – Mathuwath Janatha Dinida

Sirasata Dina Dina Sevana Salaswana
Ipaduna Upadina Siri Lanka Dana
Diva Mathurak vana
Desa Resa Nangwuwa Mahajana Bankuwa

Guru- gedarata Yana Daru Parapurakata (Sarana Deva)//
Dheevara Kamkaru Gove Nivase Duk Andura Niva
Raja Situ Kulayada Palatath Dee Naya Sahana Pawa
Mahajana Bankuwa Babale Yugayen Yugaya Geva

07.HISTORY OF PEOPLE'S BANK

People's Bank was incorporated under the People's Bank Act No 29 of 1961 as amended to bridge the gap in the financial services industry. One of the main goals was to take banking to the "unbanked", catering to the banking requirements of the rural sector. More specifically, the main objectives of the Bank were the development of the Co-operative movement, promoting rural banking and granting agricultural credit, leading to a resurgence of the rural sector. The Bank was also authorized to carry out normal commercial banking functions, as a backup for its specialized operations. In keeping with the basic objectives of establishing the Bank the ownership of the Bank was divided between the Government and the Co-operative sector. While the Government assumed a state Bank in the by holding 50% of its shares, the balance 50% was made available for subscription by the Co-operative societies. Thus the Government and the Co-operative Societies were the lawful subscribers to the share capital of the Bank. Later, due to diverse reasons, this percentage of ownership changed to give the Government the greater portion of share capital. The Bank functions under the general direction of a Board of Directors, while the executive functions are carried out by the Chief Executive Officer/ General Manager of the Bank.

Since its inception, the Bank has progressed rapidly, achieving significant growth within a relatively short period of its establishment and becoming on of the premier banking institutions in the country by 2000. The phenomenal growth recorded by People's Bank is almost unparallel to that of any other institution in Sri Lanka's banking industry. The rapid growth of our organization has been observed in many respects such as deposit mobilization, granting of advances, the growing employee base and the countrywide branch expansion drive. Today People's Bank has the widest branch network totaling 737 branches, 468 ATMs and over 15.1 Million loyal deposit account holders. The Bank's total deposits have shown a significant growth from a mere Rs 25 Million in 1961 to a record Rs.769 Billion in 2014 and continue to grow.

In 2013 People's Bank was awarded an AA+ (Sri) investment grade long-term debt rating by Fitch Ratings, reflecting the systematic importance of the Bank to the nation, the substantial reforms, undertaken since 2000, the recent profit recorded, and commitment to further restructuring, leading to recapitalization.

Over the years, one of the most notable project completions was the commencement and implementation of the core banking project. The new core banking system replaces the five archaic IT systems and will increase efficiency and productivity heralding a completely new culture within our operations. The Core Banking Solution roll out will improve the functionality and services available to customers and management, establishing effective and efficient controls together with strategic policies and disciplines.

Nowadays the Bank is strengthened with **"Internet Banking and "Mobile Banking"** facilities also. The Bank joined the pilot phase of the common ATM Switch "Lanka Pay" which is scheduled to be extended in future. Adding value to the People's International Visa Card, the Bank issued a specially designed pre generated card named "People's Debit Card".

People's Bank is currently in the process of implementing the second phase of its development plan, which sets out goals for the next 5 years from 2014 to 2018. The phase 2 business strategies will ensure further progress and development of the Bank in the years to come.

08. Conduct

All employees should conduct themselves with **professionalism, honesty** and **integrity.** Always be **courteous, polite** and **respectful** to each other and all, you would come into contact within the course of your duties at the Bank. It is also an overriding obligation to conduct business with utmost good faith.

Employees are also requested to avoid using slang and colloquial terms when addressing one another and customers.

It is one's duty to exert the correct influence over the conduct of your colleagues and to ensure that all your subordinates conduct themselves properly.

Employees should be mindful of their obligation to maintain the high standards of competence, morality and dignity expected by People's Bank.

True ethical conduct is more than merely abiding by the letter of the law, it requires an unswerving commitment to honorable behavior even at the sacrifice of personal advantage.

9. Responsibilities

Responsibility

As an employee of People's Bank, it is your responsibility to uphold the values of a true corporate citizen.

Employees should be responsible when giving advice to customers. Only give advice on those matters in which one is competent to deal with, and seek or recommend specialist advice where needed, as mis-selling a product or service to a customer without regard to the customer's interest, exposes us to reputational damage and legal action. Therefore it is the responsibility of employees to know about products of the Bank and not sell products or services to customers that do not meet the requirements of the customer.

As a Bank we are subject to various laws and regulations, and where reports, publications and returns are submitted by employees of the Bank, they should take responsibility for the accuracy, completeness and timeliness of the same as any inaccurate, incomplete or untimely report will severely damage the reputation of the Bank and may be cause for legal action.

Appearance

High standards of professionalism and decency are expected from all employees at all times.

Every employee has a responsibility to maintain the quality of their work environment. Employees are expected to dress in a modes, unassuming manner that will not give offence to customers. The dress code for male employees would be trousers, long/short sleeved shirt with collar and a tie. Usually the dress code for female employees would be a sari.

Employees are prohibited from reporting to work in jeans, T-shirts and other attire unsuited to a professional place of business.

All employees will behave as professionals when appearing before the management, customers and members of the general public. Employees must

take pride in their personal appearance and always project an image complimentary to the public's perception of the Bank.

One's clothes and appearance should be neat and clean while one's attitude is polished and poised, so as to gain acceptance within the business community. With regard to events sponsored by the Bank, employees will dress in a manner suitable to the event they are attending. All formal attire should project an image of corporate professionalism.

The above section of code may be subject to revisions at the discretion of the Bank as will be issued and communicated to staff by circulars periodically.

Attendance and Punctuality

As an employee, it is your duty to report to work in a consistent, timely manner. Absenting yourself without prior approval will be regarded as a direct violation of the Bank's rules and adversely affect your career and progress within the Bank. As such,

1. Employees are requested to be punctual and present themselves at their office, work station, meeting, seminar or other official event on time.
2. Employee attendance will be recorded through the signing of an attendance book/access control system cards or by any other means decided and approved by the management of the Bank.
3. Employees are prohibited from leaving the work place during banking hours without the prior approval of their Superior Officer.

Bank Identity Card

A People's Bank Identity Card is issued to all employees. This is issued in the best interests of all staff, with security being a key factor. As such you are required to wear the ID Card at all times while on official duty.

The following instructions should be further adhered to in this respect:

1. Bank ID Cards are not transferable.
2. The information displayed on the card cannot be altered without permission from the management.

3. Each ID Card should be handed over to the Bank when terminating one's employment with the Bank (retirement/resignation/any other reason).
4. The ID Card is the property of People's Bank and its loss should immediately be reported to the HR Division. Failure to do so would result in disciplinary action being taken against the said employee. Replacement of Bank ID Cards can be obtained through the payment of a "replacement fee" as will be decided by the Bank at its discretion from time to time.

Telephone Usage

Telephone lines are to be kept free for official business telephone calls. the lines must be easily accessible to our customers who will require various services. Personal calls could be taken only if it is absolutely necessary. The Bank expects you to keep such calls as short as possible. Employees are not expected to make personal long distance/trunk calls through the operator.

Similarly employees should not use their personal mobile phones while at work except in cases of emergency. In case of mobile phones provided officially, such phones should be used for official purposes only.

All such mobile phones should be kept on silent mode during office hours, especially when employees are dealing with customers or attending meeting.

Undue Influence

Employees are forbidden to endeavor or attempt to unduly influence the Chairman, the Board of Directors or the Senior Management of the Bank to gain a special favoured consideration with regard to their promotions, transfers or other personal matters.

Such deeds will be considered as acts committed to the detriment of the progress, development and advancement of the Bank

Maintenance of Account

Employees are expected to maintain all personal accounts with the Bank, in an appropriate, correct and exemplary manner. Issuing cheques that exceed one's account balance is a serious offence that would result in disciplinary action being taken against the employee.

Concern on Costs

All employees should be aware of and avoid unnecessary and excessive expenditure. Every employee should take personal responsibility to switch off lights, air conditioners and other electronic equipment when leaving the office and not to leave such tasks to others.

Stationery and other Bank assets should be used with proper care and minimum wastage.

The proper management of expenses is one crucial factor to the future success of the Bank.

Meetings

As Bank employees functioning with responsibility, it is prohibited for them to engage themselves in the following activities in any premises owned by the Bank, such as the People's Bank Head Office, Branches and Service Centres, etc. without the prior approval of the Chief Executive Officer/General Manager.

a) Leading or conducting of meetings without permission (other than Departmental meetings or meetings conducted on official matters).
b) Demonstrations, displays or distribution of notices and leaflets.
c) Any other gathering detrimental to the image and reputation of the Bank.

10. Confidentiality

Prior to the assumption of duties all employees shall be required to sign a Declaration of Secrecy whereby they pledge strict secrecy in respect of all data, information and other matters, such employee becomes aware of in the course of performing his or her duties at People's Bank.

Employees are privy and have access to information while being employed at People's Bank. All these information which includes information pertaining to customers, technical information, information relating to fellow employees or any information which persons come into contact with while being employed at People's Bank will be considered "Material Confidential Information". Such "Material confidential Information" should not be disclosed to a fellow employee, nor any other person except in the following circumstances.

- With another employee of People's Bank who has a need and has been requested to, by the CEO/General Manager.
- If required by Law or by a Court of Law.

An employee's obligation to protect confidential information continues even after he or she leaves People's Bank.
Customers and employees are entitled to have information they provide to People's Bank kept confidential.

Employees should avoid keeping confidential documents in office areas or public areas where they may be read by unauthorized persons. When not in use such documents should be stored in locked cabinets or other secured locations.
Confidential databases and other confidential information accessible by computer should be maintained in computer files that are password protected or otherwise secured against intrusions by unauthorized persons.

Even if an employment, relationship is terminated, all rights to intellectual property, customer information, proprietary information, service designs, computer codes and all information generated or obtained as part of the employment remain the exclusive property of People's Bank.

11. Conflict of Interest

A conflict of interest occurs when an employee's private interest interferes with the interest of People's Bank as a whole. All employees should actively avoid any private interest that influences their ability to act in the interests of People's Bank or where it makes difficult to perform their work objectively and effectively.
Conflict of interest can be of two broad types –

a) **Personal Conflict of interest**

This is where the employee's personal interest can be put ahead of the interest of People's Bank or of one of its customers. For example, working with any customer, competitor or a supplier while being in employment at People's Bank.

b) **Business Conflict of Interest**

- Where People's Bank can have a conflict of interest with the customer or
- Where in acting for two or more customers who have a conflict of interest over the subject matter of a deal/engagement or
- Where confidential information about a current customer can be used for another customer.

In such instances of (a) and (b), employees shall disclose them to his/her immediate superior for further decision making on the issue.

The employee and the immediate superior who have doubts about the propriety of any course of action should always seek the advice of the Compliance Officer.

Employees shall not approve, process or be directly involved in Banking transactions involving.

- Themselves
- Any of their immediate family members (parents, spouse, children, brothers or sisters)
- Any Firm/Company in which they or their family members (as set out above) have significant interest.

Further employees should not access their own personal bank accounts or accounts of their immediate family members, maintained at People's Bank, taking advantage of the passwords provided to them and the IT system of the Bank.

Employees shall also not misuse or abuse their positions at People's Bank in obtaining favoured benefits from customers/suppliers of the Bank.
When one is faced with a conflict of interest situation, one should always ask oneself the following.

- Is it legal?
- Is it fair?
- Is it in the best interests of People's Bank?
- Is there an alternative course of action to follow and then decide judgmentally which course of action to follow?

Once the above mentioned have been assessed and considered fairly and astutely, only then should the employee decide on what action one should take.

c) **Conflict Due to Presence of Relatives within the Bank**

To ensure that there is no conflict to the Bank's interests and there is no real or perceived favoritism when closely related employees work in close proximity, at the same location or within the same unit, department or branch, the following good governance guidelines need to be adhered.

- Employment of a close relative of an employee is not encouraged.
- The onus of disclosure of existing and/or possible future relationship that an employee may have with another employee lies with them both.
- Employee should disclose any relationship that exists or is formed with another employee, for example, through marriage, to the Head of the Department or Branch Manager and to the HR Department.

- As means of good governance related employees will not be assigned to work in the same department/unit or branch of the Bank.

- Employees are precluded from handling, supervising, approving any account of one's spouse or close relative in a branch or location where one's spouse or close relatives have dealings with.

- Employees are not allowed to access or view the accounts of any close relative.

(With regard to this chapter, close relatives mean and include one's spouse, children, brothers or sisters and parents).

12. Insider Dealing/ Insider Trading

Insider Trading is dealing with investments such as shares and bonds whilst in possession of non public price sensitive information (insider information). It also includes giving "tips" or vital information to others - friends, relatives or third parties based on this insider information.

Insider Dealing/Insider Trading is considered an offence in Sri Lanka. Therefore employees shall not buy or sell in "listed securities" like shares/bonds/debentures, etc., whilst in possession of insider information which they have as received as a result of being employed at People's Bank, until such time as the information becomes publicly available or ceases to be relevant information of a material non public nature.

To be amongst the best corporate citizens of our country, we must act with integrity and honesty, and must avoid making gains through dealings when in possession of insider information.

13. Out side Employment

No employee of People's Bank shall engage either directly or indirectly as a principal, agent, director, employee, partner or joint venture in any trade, business or any outside employment, without the prior specific sanction in writing of the Chief Executive Officer/General Manager.

Employees may volunteer their participation in non- profit, charitable, religious or educational activities on a personal basis and conducted on their own time outside one's working hours at the Bank, and should not be represented as an expression of endorsement of People's Bank. Similarly, resources of the Bank should not be utilized for such personal activities. The use of People's Bank stationery and computer systems for such outside activities is also prohibited.

14. Competition and Fair Dealing

Employees may engage in vigorous yet fair competition and shall not make inaccurate or unfair criticism of any competitor.

It is further a policy of People's Bank that service standards be consistent for all our customers regardless of race, religion, colour, age or any other basis which can be deemed discriminatory.

Employees must treat fellow employees fairly without any discriminatory behaviour, manipulation or harassment.

15. Bribery and Corruption

Employee must not give or accept bribes or engage in any form of corruption.
Bribery and corruption damages our business values and reputation.
Employees shall not at any time,

1) Offer or make any kind of unofficial payment to any person who has decision-making powers.
2) Offer payment to a customer, potential customer or a supplier to obtain business dealings.

Similarly employees shall not accept any kind of unofficial payment in order for such employee to assist in obtaining a benefit for the customer or supplier.
If an employee suspects an approach from anyone is aimed at, seeking or offering a bribe from or to oneself or a fellow employee, the employee should report same to the immediate superior for necessary action.

16. Customer Service & Handling Customer Complaints.

As a State Bank, People's Bank is determined to set an example to the banking world by adopting the standards of fair banking practices that are expected by customers when they undertake transactions with us. The Bank adopting the guidelines issued by the Central Bank of Sri Lanka has put in place a "Customer Charter", which aims at improving our service with the support and cooperation of the customers.

This Charter mainly covers following areas:

- Helping the customers to understand the financial products/ services offered by the Bank, such as;
  - providing adequate information of the products/services,
  - explaining their financial implications, and
  - helping the customers to choose the appropriate banking products/ services.

- Providing Key Facts Document in the form of brochures/ leaflets written in simple language. They should be available in languages preferred by the customers (i.e. Sinhala/ Tamil/ English) disclosing the following basic information;
  - Description of the products/ services,
  - Financial and other benefits,
  - Fees/ Charges/ Commission/ Interest etc,
  - Procedures to be followed,
  - A common complaint procedure.

- Preparing advertisements which contain factual information on products/ services and avoid publishing misleading information;

- Displaying following information in the Head Office, all branches and other banking outlets;
  - Current interest rates,
  - Bank Licence,
  - Buying and selling rates of foreign currencies,
  - Fees and commissions,
  - Credit rating of the Bank,
  - The contact details of the Financial Ombudsman and Credit Counseling Centre,
  - Banking hours and Holiday notices,

- Sending periodic statements to customers regarding transactions and balances in their deposits or loans,

- Organizing specific financial literacy programs to improve customer awareness.

- Disclosing "Terms and Conditions" relevant to each and every product or service.

- Refraining from
  - Harassing customers,
  - Using abusive debt collection practices,
  - Disclosing customer information to others,
  - Giving false or misleading information about our products/ services,
  - Unduly influencing customers or the general public to buy or get involved in the Bank's products/ services.

- Resolving customer complaints with transparency and effectively by
  - Implementing a quick and effective resolution mechanism on disputes between customers and the Bank,
  - Having a written procedure for receiving complaints,
  - Acknowledging the receipt of any complaint in writing within a reasonable period,
  - Facilitating the complaints received verbally or in writing,
  - Establishing a Management Information System regarding complaints,
  - Assigning an officer to handle complaints,

- Providing special attention to the customers such as elderly, disabled or customers with low financial literacy in order to facilitate them to have a fair access to banking services.

  The manner in which we handle complaints by customers is a major factor in the retention of customers. Customers who have had their complaints dealt with and resolved in an efficient manner will often continue to be loyal customers over many years.

  Complaints, if they are dealt with quickly and professionally, will serve as a means of improving our standards of customer service.

  When a Customer Complaint is made –

  - it must be dealt with in a courteous manner.
  - it must be recorded and be informed to the immediate superior.

- a response should be sent out without delay.
- all efforts should be taken to settle/rectify the complaint quickly if the complaint is justified.

When addressing customers, wherever possible it is best to address them with the appropriate title attached to their names and to avoid colloquial language. One must always be courteous even under trying circumstances with difficult customers.

All correspondence of customers must be responded without delay. It is essential that employees are prompt in handling customers' queries and requests.

Employees are also encouraged to meet customers by prior appointment. In the event an appointment cannot be kept by the employee, the customer should be informed at the earliest possible time and a new date should be arranged with the customer's convenience in mind.

Employees should answer the telephone as soon as it rings. In the event a nearby telephone rings more than three times, an attempt should be made to pick up the phone of that employee.

One should always be courteous on the phone and wherever possible, should identify oneself with one's name and department. When an employee answers the phone of, another it should always be the practice to note down the caller's name, the number and if required, write down the message and hand/e-mail it to your fellow employee.

17. Cleanliness, Hygiene and Safety

Safety

People's Bank is committed to providing a safe and healthy working environment for all its employees.

Employees are expected to be aware of the Bank's security procedures and evacuation plans in cases of fire and other emergencies.

It is the responsibility of every employee to execute duties in a manner that would ensure the safety of themselves and their colleagues, as well as the customers of the Bank.

In the event an employee comes across unsafe working conditions or any breaches of security, it should be brought to the notice of the relevant Head of Department for necessary action.

Where, any electrical connections appear to be loose or electrical equipment is not in working condition, bring it to the attention of the maintenance staff responsible for repair. Do not attempt to repair or attend to these, yourself.

Cleanliness

The cleanliness and the hygienic condition of People's Bank have to be the responsibility of every employee.

A well-maintained, clean premise helps to enhance the image of the Bank in the minds of the customer. It is the duty of every employee to ensure that the highest standards of cleanliness are maintained.

Some broad guidelines in this regard are set out below.

- Dispose of unwanted litter in the wastepaper baskets provided.
- Do not clutter your desks and walkways with files and documents. Keep documents and files tidily. Unwanted documents should be shredded or disposed of accordingly as per the Bank's regulations.
- All documents/papers must be collated stapled/filed in a neat manner, rather than having loose untidy leaves scattered all over.

- Use the toilets properly. Flush them each time you use them. Keep the floors dry and clean.
- All meals should be consumed in the lunch rooms or cafeteria.
- Lunch parcels brought from home and other personal belongings such as helmets, shopping bags should be kept out of the vision of outsiders.
- The Bank's ATM (PET) machines must be well taken care of and maintained by the employees of the Bank. It is important that the machines are in good working condition and in a clean environment for customers. If an employee learns of customers disgruntled due to the ATM failures, etc. they must inform the relevant senior management as soon as possible.

18. Compliance with Laws, Regulations and Bank's Internal Circulars.

It is the People's Bank policy to comply with all applicable laws, rules and regulations. It is the personal responsibility of each employee to adhere to the standards and restrictions imposed by those laws, rules and regulations.

Employees must comply not just with the letter, but also with the spirit of all relevant legal and regulatory requirements.

Employees are also individually responsible for compliance with the Bank's internal procedures and guidelines. Breaches are not acceptable and will be taken seriously by the management. The practice of competitors or others does not necessarily make such activities acceptable.

If an employee discovers that they are unintentionally breaching a law or regulation, it must be reported immediately to one's immediate superior who should report same to the Compliance Officer for necessary advice to rectify such a situation.

Violation of a law or regulation always brings about sanctions which will impair the name and reputation of People's Bank. Therefore, we must all endeavour to comply with applicable laws and regulations at all times.

People's Bank is committed to exemplary governance and ethics. Employees must be able to demonstrate this to all our stakeholders and regulators.

We must be open and honest when dealing with our regulators, if we discover a non-compliance issue, it should never be covered up. The assistance of the Compliance Officer should be sought to inform the regulator and remedy the situation.

19. Protection and Use of Bank Assets.

All employees are entrusted with protecting the property of People's Bank. Therefore employees have an obligation to look after the Bank's assets and ensure their efficient use for legitimate business purposes only.

Proprietary and customer information, computer generated or otherwise is the property of People's Bank, and is only to be used for legitimate business purposes.

To ensure the protection and proper use of People's Bank assets, each employee should-

- exercise reasonable care to prevent theft, damage and misuse of property.
- property reports the actual or suspected theft, damage or misuse of property to one's immediate superior.

Acts of dishonesty against the Bank or its customers involving theft, destruction or misappropriation of the Bank's property is strictly forbidden.

20. Use of Our Information System

The following rules of conduct are laid down to all users of the computer system of People's Bank (This is issued as a mere guideline and will not override any of the provisions of the IT Security Manual issued by the IT Department of the Bank).

- All information and files residing on Bank-owned PCs and network are the property of the People's Bank.
- Personally-owned PCs and peripheral hardware may not be attached to the Bank's network without the approval of the Head of IT and CEO/General Manager.
- Personally-owned software may not be installed on the Bank's equipment, unless approved by the Head of IT.
- Copying, selling or distributing software directly or indirectly in violation of license agreements, copyright law and the use of pirated software in People's Bank's computer network is strictly prohibited.
- The Banks' PCs or networks should not be used to access pornographic or other inappropriate websites.
- All information and the computer programmes are the property of People's Bank, and these facilities shall only be used for the performance of the employee's specific job and not otherwise.
- An employee shall not, disclose one's authentication password or user ID to another employee, unless authorized to do so by the immediate supervisor.
- All employees shall refrain from insecure conveyance/ storage of passwords.
- All employees would be held responsible and accountable for protection of information one uses or distributes, regardless of he medium on which it is transmitted and/or stored (i. e. paper, diskette, CD, tape, etc.).

- Entry is not allowed for unauthorized employees to areas such as server rooms, printer rooms etc.

- Smoking and consumption of food in server rooms/ printer rooms etc is prohibited for all employees.

- Employees shall take proper care in handling of Diskettes, Tapes, CDs etc (eg; Avoiding magnetic materials near such storage media/ ensuring proper atmospheric conditions for their storage etc).

- All employees shall avoid;
  a) Unauthorized use of another person's e-mail,
  b) Sending viruses through e-mail attachments,
  c) Transmitting confidential or sensitive Bank information in an unencrypted form, and
  d) Inappropriate auto forwarding of e-mail.

- All employees shall not use e-mail in manner that;
  a) Interferes with normal business activities or hampers employee productivity,
  b) Embarrasses People's Bank,
  c) Consumes more resources,
  d) Involves solicitation,
  e) Is associated with any for-profit outside business.

- Employees shall refrain from sending profane, obscene or derogatory e-mails.

21.Compliance with the Code

People's Bank intends to enforce the provisions of this Code in a consistent manner regardless of the status/grade of the employee.

The Compliance Officer shall be responsible for the effective implementation and monitoring of the Code.

The Compliance Officer shall periodically carry out checks/audits in such form and manner as may be determined by the Compliance Officer in order to determine effective compliance with the provisions of the Code.

Where an employee has not complied with any of the provisions of this Code he/she shall immediately bring it to the notification of one's superior who shall notify the Compliance Officer of such failure to comply. Depending on the gravity of the violation/breach, the Compliance Officer shall together with the Head of Department, decide and take action against the employee concerned. The investigation and disciplinary procedure will be as per the guidelines laid down in People's Bank Disciplinary Code and other Circulars in this regard.

In the event the Compliance Officer becomes aware of any alleged violation such employee will be called upon to offer an explanation within a stipulated time. Thereafter appropriate action as set out above will be carried out against the defaulter.

All employees will receive a copy of this Code of Conduct and shall sign an acknowledgement (as per format set out in the Annexure) certifying that the employee has received, read and understood this Code of Conduct.

The Code of Conduct contains the general guidelines for conduct by employee. We expect and require all employees, regardless of their grades or locations to adhere to these standards.

People's Bank reserves the right to amend, supplement or discontinue provisions contained herein without prior notice at any time.

Annexure

23. Acknowledgement of the Code of Conduct

I ……

(Name)

of ……

(Address)

being an employee of the People's Bank does hereby acknowledge receipt of a copy of the Code. I further agree that I have understood the provisions contained herein and agree to abide by this Code at all times.

Declared this …….. day of …….

2015 at …….. (Place)

…… ……..

(Signature of Declarant) (Service No.)

- Original to be retained in the personal file of the employee with the copy to be retained in the Branch/Department.

DISCIPLINARY CODE OF THE

PEOPLE'S BANK

OF

SRI LANKA

INDEX

Section Number		Page Number
01	Preamble	01
02	Definitions and Explanations	01
03	Employees to whom this Code is Applicable	04
04	Obligations of Employees	04
05	General Conduct of Employee	06
06	Disciplinary Action	05
07	Disciplinary Authority and Powers	06
08	Obligations of Officers Exercising Disciplinary Powers	07
09	Staff Committees	07
10	Authorized Officers	09
11	Tagging and Removal of Tag from Personal Files	09

12	Preliminary Investigations	10
13	Disciplinary Action When Civil/Criminal Proceedings are Pending	13
14	When a Disciplinary Inquiry Reveals a Criminal Offence	14
15	Employees Convicted in a Court of Law	14
16	Remanding of Employees	15
17	Compulsory Leave, Pending Preliminary Investigation or Inquiry	15
18	Interdiction Pending Disciplinary Proceedings	16
19	Salary during the Period of Interdiction	16
20	Permission to Leave the Island or Resignation During Pendency of Disciplinary Proceedings	17
21	Disciplinary Proceedings	17
22	The Charge Sheet and Answer to the Charge Sheet	18
23	Summary Inquiry	20

24	Formal Inquiry	20
25	Appearance and Information to the Accused Employee before Inquiry	22
26	Documents	22
27	Representation at the Disciplinary Inquiry	23

PROCEEDINGS TO BE ADOPTED AT A DISCIPLINARY INQUIRY

28	Reading Out Charges	24
29	Recording of Proceedings	25
30	The Defence	26
31	Conclusion of Inquiry and Submissions	26
32	Findings of the Inquiry Officer	27
33	Order of the Disciplinary Authority on the Findings of the Inquiry Officer	27
34	Communication of Order of Punishment	28
35	Right of Appeal and Procedure to be followed on Receipt of an Appeal	28
36	Appeals – Powers of the Disciplinary Authority	29
37	Punishments	29
38	Custody of the Record/s of the Disciplinary Matters/ Proceedings	31

39	Circular Instructions			32
40	Amendments to the Code			32
41	General			32
	Acts of Minor Misconduct	-	Schedule I	33
	Acts of Grave Misconduct	-	Schedule II	34
	Charge Sheet	-	Schedule III	37
	Notice of Formal Inquiry	-	Schedule IV	38
	Appeal	-	Schedule V	39

DISCIPLINARY CODE OF THE PEOPLE'S BANK OF SRI LANKA

1. Preamble

1.1 These rules and regulations are enacted for the disciplinary control of employees of the People's Bank of Sri Lanka, under and by virtue of the provisions of the People's Bank Act No. 29 of 1961. These rules and regulations are termed the Disciplinary Code of the People's Bank of Sri Lanka and hereinafter shall be known and referred to as the Code.

1.2 Where the General Manager, with the consent and concurrence of the Board of Directors has delegated any powers or functions pertaining to the disciplinary control of an employee, to any Officer or Officers of the Bank, (whether temporarily or permanently) every act or acts carried out legally in accordance with such delegation, shall be deemed to have been the act and deed of the said General Manager or Board of Directors.

1.3 All investigations, inquiries, interrogations and other matters commenced and pending under the previous procedures shall be deemed to have commenced and, continued as under the present code, with the coming into operation of this code. This code has been approved and adopted by the Board of Directors of the People's Bank of Sri Lanka.

2. Definitions and Explanations

2.1 The **"Bank"** shall mean the People's Bank of Sri Lanka, as constituted by Act. No. 29 of 1961.

2.2 The **"Chairman"** shall mean the Chairman of the Board of Directors of the People's Bank of Sri Lanka.

2.3 The **"Board"** shall mean the Board of Directors of the Bank or any body of persons or officers appointed by the Board to act on their behalf.

2.4 The **"General Manager"** shall mean the General Manager of the Bank.

2.5 **"Act of Misconduct"** means acts of minor misconduct and acts of grave misconduct, as specified in schedules I & II of this Code.

Any employee found guilty of committing and act of misconduct, by way of omission or commission (which are set out in schedules I & II hereof) shall be subject to disciplinary action. Such acts of misconduct set out in the above schedules are not comprehensive and others may be added from time to time, whether before or after the commission of an act, or omission to commit an act.

2.6 **"Authorized Officer"** means and refers to an Officer authorized by the Disciplinary Authority or any Officer as referred to under section 10 below, to initiate and conduct preliminary investigations in respect of any act of misconduct, whether of omission or commission.

2.7 **"Appropriate Authority"** means the Regional Manager, Head of the Department or Chief Manager (I & I), Chief Manager (HRM) or any person or persons appointed to perform a specific duty under the provisions of this Code.

2.8 **"Appellate Committee"** means a committee constituted and appointed as per section 9.2 & 9.3 of this code to consider appeals by employees on whom punishments have been meted out, and to make such recommendations as are appropriate in the circumstances of the case.

2.9 **"Bank Document"** means and refers to any document paper or writing maintained by the Bank in the course of day to day transactions and within the control and custody of the Bank, and includes all ledgers, registers, negotiable instruments etc., as contemplated by section 90 of the Evidence Ordinance and Evidence (Special Provisions) Act No. 14 of 1955.

2.10 **"Compulsory Leave"** means suspension from duty with full remuneration in instances where the employee is suspected of having committed an act of grave misconduct and his continuing presence in the Bank is detrimental to the conduct of the preliminary investigation or that it is not desirable to allow the suspect employee to continue to exercise his functions as detailed under sections 17.1 & 18.1 below.

2.11 **"Disciplinary Authority"** means the Chairman and the Board of Directors, or the General Manager or the Executive Operations Committee appointed by the Chairman and the Board of Directors and authorized by the Board to act on their behalf on all disciplinary matters, or any other such person or persons appointed by the Chairman and the Board of Directors or the General Manager and authorized to act on their behalf.

2.12 **"Employee"** means a permanent employee on a contract of continuous employment.

2.13 **"Formal Inquiry"** means an inquiry held by an Inquiry Officer in accordance with the provisions of section 24 of this code in respect of the commission or alleged commission of an act of misconduct.

2.14 The pronoun **"He"** and its derivatives shall mean and refer to any person whether male or female.

2.15 **"Inquiry Officer"** means an Officer appointed to conduct a summary or a Formal Inquiry, in accordance with the provisions of section 21.1. Such Officer is selected from the panel of Inquiry Officers.

2.16 **"Interdiction from the Service"** means suspension from duties of an employee against who prima facie evidence had been disclosed during the course of a preliminary investigation in respect of an alleged commission of an act of grave misconduct which is established may result in a severe form of punishment such as dismissal being meted out to him.

2.17 **"Month"** means a calendar month i. e.: the period of time from a day in one month to the corresponding date in the following month, less by one day.

2.18 **"Negligence"** means and refers to lack of proper care and caution or due diligence by an employee in the performance of a duty entrusted to him, by way of omission or commission. Negligence includes lack of supervision, and wilful neglect or duty, and exposing Bank funds and property to avoidable risks, which may result in wanton loss and damage to the Bank.

2.19 **"Preliminary Investigation"** means and refers to an investigation of an exploratory nature, held by an Authorized Officer in respect of an act of misconduct, and conducted in accordance with the provisions of section 12 hereof.

2.20 **"Resignation"** means voluntary relinquishment of duties by an employee from the service of the Bank.

2.21 **"Representative"** means and refers to a person appointed at the request of a suspect to defend him at an inquiry. Such person shall be an Officer of the Bank, and be on a grade equal to that of the suspect, or of a higher grade. Permission to retain a representative should be requested for in writing from the Regional Manager/Head of the Department or the Chief Manager (I & I).

2.22 **"Staff Committee"** means a committee appointed to assess and evaluate the contents of a Preliminary Investigation Report, submitted by an Authorized Officer, in order to determine as to what further steps and/or disciplinary recommendations should be taken against an employee, in respect of whom the Preliminary Investigation Report has been submitted.

2.23 **"Summary Inquiry"** means an inquiry held by an Inquiry Officer in accordance with the provisions of section 23 of this code in respect of the commission or alleged commission of an act of misconduct.

2.24 **"Termination of Employment"** (Termination of Services) means the discontinuance of the services of a permanent employee by the Bank.

2.25 Words importing the singular number include the plural number, and vice versa.

3. Obligations to Whom this Code is Applicable

3.1 All employees in the permanent service of the Bank including.

3.1.1 Employees who have reached the age of retirement but are on an extension of service.

3.1.2 Employees who have been interdicted and/or sent on compulsory leave prior to retirement.

4. **Obligations of Employees**

Every employee of the Bank is under a duty to,

4.1 Be regular and punctual in his attendance.

4.2 Discharge his duties efficiently, diligently and with integrity.

4.3 Carry out all lawful orders and instructions given to him by a Superior Officer. (However when it is apparent, that such orders and instructions are contrary to established Banking practices and procedure, the subordinate employee shall refuse to carry out such orders and the matter must be forthwith brought to the notice of a higher authority).

4.4 Safeguard the property, interests and reputation of the Bank.

4.5 Conduct himself in a fit and proper manner both inside and outside the Bank maintaining cordial relationships with customers as well as the public at large, in order to uphold the reputation of the Bank, in a manner that the image of the Bank is not sullied.

4.6 Keep the Bank informed of his place of abode and or residence, and any changes thereafter. Such information as appearing in the registers of the Bank shall be conclusive proof as to his residence or place of abode, for all purposes.

4.7 Not engage in any type of business undertaking.

5. **General Conduct of Employee**

Every employee of the Bank should,

5.1 Refrain from any form of activity which might result in pecuniary embarrassment to him which will in turn will affect his duties of the Bank.

5.2 Avoid his private interests clashing with his duties at the Bank.

5.3 Abstain from utilizing property of the Bank for private work including vehicles, unless with the written sanction of the Authorized Officer.

5.4 Not accept any inducement, consideration, or remuneration from any party in respect of contracts or transactions with the Bank.

5.5 Not enter into any agreement or any contract with any other employee of the Bank, a customer or a person out side the Bank, which would conflict with his duties in the Bank.

5.6 Maintain strict confidentiality in respect of all transactions entered into within the premises of the Bank, and refrain from releasing any information to the media, likely to cause embarrassment to the Bank.

5.7 Inform his Superior Officer of any criminal charge that has been preferred against him in a Court of Law.

5.8 Refrain from exhibiting displaying, or circulating any notices pamphlets, posters or other publication and conduct of meetings in the place of work within the premises of the Bank without prior permission having been obtained from the Head of the Department or the General Manager.

5.9 Familiarize himself with the provisions of this code as well as all circulars, orders or instructions that may be issued from time to time pertaining to this duties, obligations and responsibilities.

6. **Disciplinary Action**

6.1 Disciplinary action will be instituted against an employee consequent to the following matters that come under the purview of this code. Acts of minor misconduct such as acts or wrongful omissions which are not of a grave nature are described under schedule I of this code.

6.2 Acts of grave misconduct such as acts or wrongful omissions which are of a serious nature and which are punishable with severe punishments are described under schedule II of this code.

6.3 Misconduct outside the work place or out of working hours is punishable under this code if it impairs the discipline of the Bank, such as an assault or abuse or threat by one employee to another as a result of any matter incidental to the work place or, an assault, abuse, threat or intimidation of a Superior Officer on account of some grievance connected with the employee's work.

7. Disciplinary Authority and Powers

Under this code the Chairman and the Board of Directors, or the General Manager shall be the Disciplinary Authority and be vested with the following powers and functions, to deal with an accused officer, as enumerated below.

7.1 Chairman and the Board of Directors

7.1.1 Interdiction/sending on compulsory leave and re-instatement, demotion or termination of any employee of the Bank.

7.1.2 Any other punishment for an act of misconduct (Minor or Grave) committed by any employee.

7.1.3 Consider appeals made by employees on punishments meted out under 7.1.1 and 7.1.2 above.

7.2 General Manager

7.2.1 Interdiction and sending on compulsory leave and re-instatement of any employee in Grade I, or below.

7.2.2 Deal with any act of misconduct committed by any employee in Grade I or below.

7.2.3 Consider appeals made by employees on punishments meted out under section 7.2.1 and 7.2.2 above.

8. Obligations of Officers Exercising Disciplinary Powers

8.1 Any act of misconduct or any lapse by an employee which calls for punishment should be dealt with under this code as early as possible. In the event this code is silent on any matter, it should be reported to the Disciplinary Authority through the normal channels, and directions obtained.

8.2 No punishment shall be meted out to an employee unless he has been informed of the nature of his misconduct, offence committed, or lapse on his part and has been provided with an opportunity to explain or defend himself as provided for under this code.

8.3 Every employee against whom disciplinary Action is to be taken shall be informed of it in writing without delay, and no disciplinary action shall be considered as having been taken unless he has been so informed. Punishment may be meted out to him only in respect of the offence or offences he has been found guilty of. Such punishment, or any strictures passed on him shall be entered in his personal file.

8.4 Summary or Formal inquiries should be conducted by a person appointed from the Panel of Inquiring Officers, under section 21.1.

9. Staff Committees

Staff committees shall function in the Bank at various levels at the Regional Head Offices, Corporate Division and Head Office to consider the findings of a Preliminary Investigation Report. The staff committee thereafter will make its observations and recommendations to the Disciplinary Authority for necessary action.

9.1 The staff committees set up to handle disciplinary matters at various levels are as follows: -

9.1.1 **Staff Committee – Regional Head Office**

Shall comprise of the Regional Manager and at least two Assistant Regional Managers of the Region. The Asst. Law Officer and/or Superintendent of Security attached to the Region may be called in to advise the committee as and when necessary.

9.1.2 **Staff Committee – Zonal Office**

Shall comprise of the zonal Asst. General Manager and Regional Managers of the Zone. The Asst. Law Officer and/or Superintendent of Security attached to the relevant Region, may be called into advise the committee as and when necessary.

9.1.3 **Staff Committee – Corporate Division**

Shall comprise of an Asst. General Manager and two Grade I Officers of the Corporate Division. The Asst. Law Officer or Superintendent of Security attached to Corporate Division, may be called into advise the committee as and when necessary.

Note :

1. The above committees shall not include Authorized Officers who conducted the Preliminary Investigation in respect of the misconduct of the employee in question.

2. Observations and recommendations of the staff committees referred to under 9.1.1 to 9.1.3 above along with the Preliminary Investigation Report should be sent to the C.M. (I & I)/A. G. M. (I & I) who in turn shall submit same to the relevant Head Office AGMM or DGMM staff committee for further review and consideration.

9.1.4 **Head Office – Staff Committees**

Grade I Officers Staff Committee

Shall comprise of three Grade I Officers attached to Head Office, and/or attached to the Corporate Division.

9.1.5 **Assistant General Managers Staff Committee**

Shall comprise of three Asst. General Managers attached to Head Office and/or attached to the Corporate Division.

9.1.6 **Deputy General Managers Staff Committee**

Shall comprise of three Deputy General Managers of the Head Office and/or attached to the Corporate Division.

Note :

The Chief Legal Officer and/or Security Superintendent may be called into advise the committees mentioned under 9.1.4 to 9.1.6 above as and when necessary.

9.2 All appeals against punishments imposed by an initial disciplinary committee shall be considered by the Head Office AGMM or DGMM staff committee, provided however, that, no member who has sat in the initial staff committee shall be eligible to participate in the subsequent appeal therefrom.

9.3 Head Office staff committees as mentioned in sections 9.1.5 and 9.1.6 above, may function as special staff committees and/or as appeal committees, appointed for the purpose, by the Disciplinary Authority, when necessary.

10. **Authorized Officers**

10.1 The following Officers are authorized to initiate and conduct a preliminary investigation into alleged acts of misconduct of an employee of the Bank. The Authorized Officer conducting the preliminary investigation should always be an Officer in the same grade or of a higher grade than the suspect employee.

10.2 Any Officer in the Special Grade such as Deputy General Manager, Assistant General Manager, is competent to conduct such preliminary investigation.

10.3 Regional Manager or any Grade I Officer.

10.4 Asst. Regional Manager and/or any Grade II Officer nominated for such purpose.

10.5 Any Officer in the Grade of Asst. Security Superintendent or above.

10.6 Any other Officer nominated by the Disciplinary Authority.

11. **Tagging and Removal of Tag from Personal Files**

11.1 In the case of employees in Grade II and below, if a prima facie case could be established in respect of act of misconduct, tagging of the personal file will be done by the Assistant General Manager (I & I) in consultation with the Deputy General Manager In Charge of Administration.

11.2 If the act of misconduct is in respect of an employee in Grade I and above the tagging of personal file will be done by the Deputy General Manager In Charge of Administration in consultation with the General Manager or the Chairman.

11.3 Tagging of the personal file shall be notified to the employee concerned, and the Regional Manager or Head of the Department, by the Chief Manager (Human Resource Management) on receipt of the decisions referred to under section 11.1 and/or 11.2 above.

11.4 Removal of tags will be done on imposition of a punishment or exoneration of the employee, on receipt of the decision of the Disciplinary Authority by the Chief Manager (Human Resource Management) and such removal shall be inform to the employee concerned and to the Regional Manager or the Head of the Department by the Chief Manager (HRM).

12. **Preliminary Investigaitons**

12.1 Where any act of misconduct by an employee of the Bank is reported, it shall be in the responsibility of the Zonal Assistant General Manager, or the Regional Manager, or in case of Head Office Departments and Corporate Division, the respective Asst. General Manager or the Deputy General Manager or nominate an Authorized Officer in accordance with section 10, above, to conduct a preliminary investigation.

12.2 It is the duty of an Authorized Officer to carry out a preliminary investigation into the misconduct alleged to have been committed by an employee in order to ascertain, whether a prima facie case can be made out against the employee.

12.3 At the commencement of such investigation the Authorized Officer shall keep in mind that there is no accused, but only a suspect. Such investigation is of an exploratory nature and should be conducted impartially and expeditiously. On being appointed to carry out such investigation he shall conclude same within 30 days of such appointment, and submit his report along with the Draft Charge Sheet if applicable (see Section 22.1 below) within 14 days of the conclusion of the investigation to the Appropriate Authority who in turn will submit same to the relevant Staff Committee. Any undue delay in this regard will be viewed seriously by the Disciplinary Authority.

12.4 The procedure to be followed in respect of a preliminary investigations is as follows: -

12.4.1 The Authorized Officer shall have the right to summon any employee to record the statements in the conduct of the investigations, and shall have access to Bank records and documents relevant to the investigation.

12.4.2 The Authorized Officer investigating shall follow the normal channels of official communication in contacting witnesses, examining

documents and records etc. – through the Branch Manager, Regional Manager or the Heads of Depts. an exceptional circumstances, where such procedure would entail delay and/or result in the loss of valuable evidence, he may conduct the investigation directly.

12.4.3 All relevant documents pertaining to the alleged misconduct should be impounded immediately and kept under the custody of Regional Manager/Head of the Department or International Division or assistant General Manager (I & I) to be utilized if necessary at a summary or formal inquiry. Such documents should be sealed, if possible in the presence of the suspect, and his initials placed thereto.

12.4.4 The Authorized Officer investigating is not bound to give prior notice to any witness of the time, date or place at which the Preliminary Investigation will be conducted, but he may do so where he considers it necessary and provided, he is reasonably satisfied that no evidence is likely to be tampered with as a result of such prior notification. No person is entitled to represent the witness at a preliminary investigation when his statement is being recorded.

The examination of witnesses can be done in any order and at any place or time, at the discretion of the Authorized Officer.

12.4.5 The Authorized Officer investigating shall in the first instance, question employees and witnesses in order to ascertain whether the evidence of such witnesses is relevant to the matter under investigation. If he is satisfied that the information given is relevant, he should proceed to obtain written statements of such witness preferably, in the language most familiar to the witness.

12.4.6 It is not incumbent on the Authorized Officer that he should record statements on the same day or in a particular order.

12.4.7 Where the suspect informs the Authorized Officer that he desires to make an unqualified admission of guilt, the Authorized Officer shall proceed to record same forthwith in the presence of two witnesses. At the conclusion, of the statement, the suspect shall declare in his own hand writing that such admission was made of his own free will and accord, and is free from any threat, coercion, duress, promise of reward or under compulsion, and shall place his signature thereto

that such statement has been read over and explained to him by the Authorized Officer.

12.4.8 Every employee is under a duty to provide, when called upon to do so by the authorized Officer, orally or in writing any pertinent information relating to any act of misconduct committed or alleged to have been committed by him or any other employee of the Bank or relating to an incident which has caused or is likely to cause loss or damage to the Bank. He shall also be under a duty to sign such statement when called upon to do so by the Authorized Officer. These requests may be made orally or in writing.

12.4.9 The duty referred to in the preceding paragraph shall include the duty to give evidence at a Formal Inquiry or in a Court of Law on behalf of the Bank.

12.4.10 If a written or oral statement has been obtained under duress by the Authorized Officer, the employee who has been subjected to such duress shall immediately, and in any case within three days of making such statement, excluding Sundays and Public holidays inform the Chief Manager (HRM) in writing of the fact and nature of the duress and indicate the parts of the statement which he wishes to retract. On receiving such information the Chief Manager (HRM) shall take appropriate action.

12.4.11 The Authorized Officer should record the statements of the suspect or suspects at the earliest available opportunity. All statements should be prepared in duplicate.

12.4.12 The name, grade, service number and the place of work of the witness and the date, time and place of recording statements, should be clearly entered before the statement of a witness is recorded. When a statement has been recorded it should be read over and explained to the witness, and any alternations or interpolations made thereafter, signed by the employee or witness.

12.4.13 The Authorized Officer, shall, at the end of each page of the statement of the witness obtained the witnesses signature or thumb impression as the case may be, if it is in a language understood by him. I it is in some other language he should be required to write out in his own hand-writing that the statement has been read out and explained to him and to place his signature or thumb impression thereafter.

12.4.14 Where the person questioned is not an employee of the Bank, the statement should be obtained by way of an affidavit and such affidavits in the absence of the witness shall be admissible as evidence at a domestic inquiry.

13. Disciplinary Action When Civil/Criminal Proceedings are Pending

13.1 The pendancy of criminal proceedings against an employee in respect of an act of misconduct within the meaning of this code shall not by itself be a reason for abstaining from or suspension of disciplinary proceedings under the code, provided however, that disciplinary proceedings by the Bank may be suspended or postponed pending conclusion of criminal proceedings by the Police, if the employee concerned establishes to the satisfaction of the Bank that the holding of the Domestic Inquiry will prejudice his interests in the criminal case or if the Bank is of the view that the prior conclusion of the criminal proceedings is necessary for the proper conduct of the Domestic Inquiry.

13.2 Where civil criminal proceedings are pending against an employee affecting his employment, after consideration of the nature of the offence and the degree of involvement, steps may be taken through the respective staff committees, with recommendation to the Disciplinary Authority, either to interdict or to take other appropriate action.

13.3 Where a civil/criminal action is pending against an employee and such action is not in relation to his employment, but effects the reputation of the Bank and/or the intergrity of the employee of the Bank the Assistant General Manager (Investigation & Inquiries) shall call upon the employee to furnish him with a written statement of the facts of such action and on his failure to do so within 14 days, the Asst. General Manager (I & I) shall take steps through the relevant staff committees, for suitable disciplinary action to be taken against such employee.

13.4 If for any reason whatsoever, the Bank has to await the decision of Court before taking disciplinary action against an employee, such employee should be informed that disciplinary action against him has been laid by pending a decision of Court on the matter.

14. When a Disciplinary Inquiry Reveals a Criminal Offence

14.1 During the course of a disciplinary inquiry, or investigation if a criminal offence is disclosed, the Officer conducting such inquiry or Investigation shall communicate the fact of such offence to the Regional Manager, Head of the Dept. who in consultation with the AGM (I & I) shall take steps to report such matter to the Police or take appropriate legal action.

14.2 Either during the pendancy of, or at the conclusion of a disciplinary inquiry, no employee can by reason of the fact that he had been acquitted or discharged by a Court of Law or that no punishment has been imposed on him by Court, claim.

14.2.1 That the disciplinary inquiry should not proceed against him further or that it should be abandoned. Or

14.2.2 That only a nominal punishment should be inflicted on him. Or

14.2.3 That such punishment as may already have been imposed on him at the disciplinary inquiry be set aside altogether, or be reduced.

15. Employees Convicted in a Court of Law

15.1 If an employee is convicted for a criminal offence in a Court of Law, that affects the reputation of the Bank or the intergrity of the employee concerned he shall report the findings of guilt or conviction immediately to the Branch Manager, Regional Manager or the Head of the Department.

15.2 Where it has been brought to the notice of the Bank, whether by the employee himself or other source that he has been convicted by a Court of Law or found guilty of an offence as contemplated by 15.1 the Branch Manager, the Regional Manager or the Head of the Department shall report same to the AGM (I & I). The AGM (I & I) shall forward a report with his

observations to the disciplinary authority, and thereafter the Bank may call upon the employee to show cause why he should not be dealt with, under this code.

15.3 Where an employee has been convicted in a Court of Law for a criminal offence, the Bank reserves the right to decide on the course of action to be taken against or punishments to be given to the employee in respect of the offence.

15.4 The fact that an employee has been acquitted or discharged by a Court of Law for a criminal offence committed in the course of his employment, shall not preclude the Bank from taking disciplinary action against the employee on the identical facts and charges.

16. Remanding of Employees

16.1 If an employee is remanded by a Court of Law in connection with any act of misconduct related to his employment in the Bank he should be interdicted forthwith. When he is released from remand the question as to whether or not he should be interdicted or sent on compulsory leave would be determined by the Disciplinary Authority.

16.2 When an employee is remanded by Court of Law in connection with an offence committed outside the scope of his employment in the Bank, such employee may at any time at the discretion of the Disciplinary Authority, be interdicted or sent on compulsory leave. When he is released from remand, the question as to whether the order of interdiction or order of compulsory leave be withdrawn, is left to the discretion of the Disciplinary Authority.

17. Compulsory Leave, Pending Preliminary Investigation or Inquiry

17.1 The Regional Manager or the Head of the Department may transfer or recommend transfer of an employee to another Branch or Department or Region if he considers such action necessary until the preliminary investigation or inquiry is concluded. If the Authorized Officer is of the view that the presence of the employee who is suspected of having committed an act of grave misconduct is detrimental either to the interest of the Bank or the conduct of the Preliminary Investigation, the Authorized Officer may recommend to the relevant authority to place the employee on compulsory

leave. When an employee is sent on compulsory leave, the Chief Manager (HRM) and Chief Manager (I & I) should be notified forthwith.

17.2 When an employee is on compulsory leave he shall not be entitled to receive his salary increments as and when they fall due, or receive any bonus paid to other Bank employees. Any request for loan facilities during the period of compulsory leave should be referred to AGM (I & I) for clearance.

17.3 An employee who is sent on compulsory leave is entitled to his salary with all his allowances and amounts due to him under the Bank's Medical Scheme.

17.4 Where an employee sent on compulsory leave is exonerated after an inquiry, the period he has been on compulsory leave shall be treated as having been in active service in the Bank, and be entitled to all salary increments and bonuses as may accrue to such employee.

18. **Interdiction Pending Disciplinary Proceedings**

18.1 Where an employee is sent on compulsory leave and in the course of the preliminary investigation on offence is disclosed, which if established would result in such employee being subject to a severe punishment such as dismissal, such employee should be immediately interdicted.

18.2 At any stage of an investigation if it transpires that there is prima facie evidence to establish, that the employee has committed, or has aided and abetted in the commission of an act of grave misconduct which might result in such employee being subject to a severe punishment such as a dismissal the disciplinary authority may interdict the employee concerned.

18.3 An employee interdicted from service should surrender the identity card issued by the Bank and any other property of the Bank in his custody or possession to the Regional Manager/Branch Manager or Head of the Department. He should be warned that if he desires to enter the Bank's premises he shall obtain with the prior written permission of the Chief Manager (Human Resources) or the respective Regional Manager.

19. **Salary During the Period of Interdiction**

19.1 Where an employee is interdicted he will not be entitled to receive from the Bank any salary or any part thereof during the period of interdiction provided, however, where the period of such interdiction exceeds 06 months, the General Manager may, at this discretion, authorize the payment of half the salary, at the written request of the employee under interdiction taking into consideration the nature of the charges and any other extenuating circumstances.

19.2 Where an employee is interdicted, subject to the provisions of section 18.1 & 18.2 above, such employee shall not be entitled to receive from the Bank any privileges or benefits, by way of bonus, increment, any loan of whatsoever type, and any payment under Bank's Medical Scheme.

19.3 If an employee after Inquiry, either Summary or formal, is found guilty of all or part of the charges preferred against him, the disciplinary authority may order that the employee be recalled for service but should not be paid either the whole or part of the salary, withheld during the period he was under interdiction, in addition to any other punishments imposed.

19.4 Where an employee is convicted but not subject to imprisonment for any criminal offence committed outside the scope of his employment in the Bank and is under interdiction, the Bank at its discretion may recall him for service. The payment of any arrears of salary would also be at the discretion of the Bank.

19.5 If an employee after the conclusion of a summary or formal inquiry is found not guilty, or exonerated from all the charges preferred against him, he is entitled to receive his salary inclusive of increments that were withheld, and all benefits such as bonuses and other emoluments due under the Bank's medical scheme, during the period under interdiction and such period of interdiction shall be considered a period of leave granted with full pay.

20. **Permission to Leave the Island or Resignation During Pendancy of Disciplinary Proceedings.**

20.1 If an employee leaves the Island without the approval of the General Manager, he shall be deemed to have committed a grave offence and may be liable for dismissal from the service of the Bank.

20.2 If an employee tenders his resignation before disciplinary inquiries have commenced or during the pendancy of disciplinary inquiries or before finalization of the proceedings, the disciplinary authority may at its discretion, reject or accept such resignation subject to certain terms and conditions, or decide to proceed with the inquiry.

21. **Disciplinary Proceedings**

21.1 **Penal of Inquiry Officers**

The disciplinary authority shall appoint a panel of Inquiry Officers and such panel consist of the following Officers.

21.1.1 Persons approved by the Board of Directors from Officers who have retired from Public Service or from the service of any public corporation, or the Judicial Service.

21.1.2 The disciplinary authority with the recommendation of the Assistant General Manager (I & I) shall appoint an Inquiry Officer from the above approved panel of Inquiry Officers to conduct any inquiry, formal or summary.

21.2 **Prosecuting Officers**

The Prosecuting Officers shall be appointed by the Assistant General Manager (I & I) on the recommendation of the Regional Manager or the Head of the Department to prosecute at a Disciplinary Inquiry from one of the Officers mentioned below.

21.2.1 The Officers appointed as Prosecuting Officers shall not be junior in grade to the employee charged with the act of misconduct, or have had any direct involvement in the subject matter, or the inquiry. Such Officer, preferably, may be the Authorized Officer who conducted the Preliminary Investigation.

21.2.2 The Disciplinary Authority shall at any time remove a Prosecuting Officer, at its discretion.

22. <u>The Charge Sheet and answer to the Charge Sheet</u>

22.1 If a Preliminary Investigation Report discloses a prima-facie case against an employee necessitating a formal inquiry, then the Authorized Officer shall prepare a Draft Charge Sheet as per Section 12.3 above and forward same alone with the copies of documents supporting the charges to the Appropriate Authority. The Appropriate Authority will submit same to the relevant staff committee which will in turn be submitted to the Chief Manager (I & I) with its recommendations. If this staff committee happens to be a committee other than the Head Office staff committee, these recommendations will be reviewed by an Appropriate Head Office staff committee.

22.2 If the Head Office staff committee recommends that a Charge Sheet be issued to an employee, then the Chief Manager (I & I) should consult the Chief Law Officer with regard to the finalization of the Charge sheet.

22.3 Once the charge sheet has been finalized and received from Chief Manager (I & I) the appropriate authority shall within 14 days issue the charge sheet to the employee, calling for his written explanation within 14 days of the receipt of same and,

22.3.1 To show cause why he should not be disciplinary dealt with under the provisions of the Disciplinary Code of the Bank.

22.3.2 The state in writing the grounds under which he depends to exculpate himself.

Provided that an employee served with a charge sheet may, on valid grounds adduced by him be granted such extension of time not

exceeding a further 14 days as the appropriate authority may consider reasonable for the purpose of enabling such employee to answer the charge sheet.

22.4 The charge sheet shall contain, inter-alia, particulars of the date place and time of the commission of the Act of Misconduct, and the person against whom, and/or the thing in respect of which, the same was committed. The charge sheet should preferably be in the form appearing in Schedule III and contain a list of documents that may be produced at the inquiry.

22.5 In the case of an employee under interdiction the charge sheet shall be posted under registered cover to his last known place of residence or abode, as set out in section 4.6 above and the Receipt of Registration of posting shall be conclusive proof that the charge sheet has been duly delivered to him.

22.6 The accused employee called upon to answer the charge sheet shall furnish a full statement of the facts he will be relying upon for his defence.

22.7 On receipt of the reply to the charge sheet by the suspect, the appropriate authority shall within 07 working days of the receipt thereof, forward same to the Chief Manager (I & I)/Assistant General Manager (I & I), who shall submit same to the relevant Head Office staff committee for its recommendation.

22.8 In the event of the employee failing to respond to the charge sheet within the stipulated period or had not requested for further time for reply to same he shall be considered guilty of all the charges enumerated in the charge sheet.

22.9 On a receipt of the explanation offered by the employee in response to the charge sheet, the Disciplinary Authority after considering the recommendations of the relevant Head Office Staff committee may exonerate, punish or institute a formal or summary inquiry against the employee.

22.10 If the employee admits or pleads guilty to only some of the Charges, a formal inquiry may be necessary.

23 **Summary Inquiry**

23.1 Where the employee admits to all the charges, at a preliminary investigation a Summary Inquiry will be held by an Inquiry Officer appointed by the Disciplinary Authority.

23.2 The Inquiry Officer may hold a Summary Inquiry in such a manner as he may think fist and proper, provided that the employees shall be informed of the case against him and offer an opportunity to make a plea to mitigate and minimise the punishment. No witnesses are summoned at such an inquiry and the defence shall consist of an explanation by the employee. The employee will also not have a right to be represented.

23.3 If the Inquiring Officer is satisfied that the charges against the accused have been established, he should forward his findings to the Asst. General Manager (I & I) immediately.

23.4 If an accused employee who has earlier admitted the offence, pleads not guilty, the Inquiry Officer should examine the documents etc. placed before him and come to a conclusion as to whether despite the accused's plea of not guilty, the inquiry Officer holds the accused guilty. In such an event he shall give his reasons for arriving at such a conclusion. If the Inquiry Officer feels at the conclusion of the summary inquiry that a formal inquiry should be held he should forward the record to the Asst. General Manager (I & 1) setting out his reasons for doing so.

24. **Formal Inquiry**

24.1 If the Disciplinary Authority is not satisfied with the reply to the charge sheet he may cause a formal inquiry to be held.

24.2 A formal inquiry shall be conducted by an Inquiring Officer appointed by the Disciplinary Authority.

24.3 Where more than one employee is to be charged in respect of acts of misconduct, committed in the execution of the same transaction or event the matter shall be reported to the Assistant General Manager (I & I) and a ruling obtained as to whether there should be separate inquiries.

24.4 The Charge Sheet may be amended before the suspect has pleaded to the charges and under no circumstance should it be amended thereafter, except under the following instance.

24.4.1 Where there is a numerical or grammatical error apparent on the face of the record, or in order to clarify or rectify any ambiguity or contradiction, but subject to the condition that a charge of one kind should not be converted into another, under the guise of this section.

24.5 The decision of the Inquiry Officer on any matter of procedure shall be final. Such decision and any objection thereto should be entered of record.

24.6 If on the date appointed for the holding of the formal inquiry the employee fails to attend or inform the Inquiry Officer of his inability to attend the inquiry the Inquiry Officer may postpone the same for another date not less than seven working days from the date of the inquiry and inform the employee in writing that if he fails to attend the inquiry on such subsequent date or does not give satisfactory reasons for his inability to be present, the inquiry would be held ex-parte.

24.7 On the date fixed for the ex-parte inquiry the Prosecuting Officer shall lead the evidence of such witnesses and produce such documents, as shall be necessary to establish the charges preferred against the accused employee.

24.8 Where possible the proceedings at a disciplinary inquiry should be held in the language familiar to the employee and the evidence of a witness should be taken in the language familiar to him. If, however, the language in which the proceedings are held and the evidence of witnesses is not understood by the employee and /or his representative the evidence given by the witness should be translated and explained to him.

24.9 The format of a letter fixing a formal inquiry is at schedule IV of the code.

25. **Appearance and Information to the Accused Employee before Inquiry**

25.1 On receipt of the notice as referred above in section 24.9 the employee or his representative shall file, a list setting our particulars of the documents, on which the employee will be relying for his defence.

25.2 At the commencement of the formal inquiry, the date, time and place at which it is held, the names of the Inquiry Officer employee and his Representative, and Officer leading evidence for the Bank should be entered of record. Similarly when a Formal Inquiry is resumed after a postponement or adjournment, the foregoing particulars should be entered of record at the commencement of proceedings each day. At the end of each day of a sitting, the time of conclusion of such sitting should be entered.

25.3 At the formal inquiry the only persons permitted to be present will be the Inquiry Officer, the prosecuting Officer, any Officer assisting him the accused employee and his Representative, the witness giving evidence, and the employee recording evidence.

25.4 The Bank shall afford every opportunity to the accused employee and his Representative in the conduct of the defence. Such assistance shall include the release of the Representative and witnesses if any, on the dates of Inquiry. They will however not be entitled to any remuneration by the Bank by way of subsistence, travelling/transport etc. on such days.

26. **Documents**

26.1 On a written request of the accused or his representative to the Prosecuting Officer to examine any listed documents, intended to be produced at the inquiry, permission should be granted to inspect same or take down notes of same at least 7 days prior to the commencement of the inquiry, subject to security precautions, and with prior notice to the Prosecuting Officer.

26.2 The documents mentioned under section 26.1 above, shall not include minutes of the Board of Directors, minutes of the meetings of any staff committee of the Bank, documents in the personal file, statements obtained at a Preliminary Investigation, Preliminary Investigation Report and Report of findings at a Formal Inquiry.

26.3 The original of an official document (a document in the custody of an officer of the Bank) may be produced at an inquiry. If the original documents are not available due to official reasons a certified copy or a Photostat Copy of that document would suffice.

26.4 In the case of a document which is not an official document, the original document must be produced at the inquiry. Where such document does not form part of the record, a certified copy produced must be verified by examining the original before the Inquiry Officer makes a decision.

26.5 The Officer leading evidence in support of the charges at a Formal Inquiry shall have access to documents which will be used in evidence by the Defence.

27. **Representation at the Disciplinary Inquiry**

27.1 An employee who is called upon to answer to charges at a formal inquiry shall be entitled to appoint a person to represent him and defend him at such inquiry. For this purpose he should inform the Bank on or before the dates specified in the notice of the formal inquiry as per schedule 1V. Only the following categories or persons shall be eligible for appointment as a representative.

27.1.1 Any employee of the Bank other than one who holds a post lower in grade than that of the suspect employee or one who exercises direct supervisory control over such employee at the time of the commission of the offence.

27.1.2 Any employee subjected to a formal inquiry shall not be entitled to appoint as his “representative”, an employee already an accused in another formal inquiry or under interdiction or on compulsory leave.

27.1.3 Any employee who has the knowledge or who had been involved in the act of commission or omission of the suspect employee shall not be nominated as a “representative” of such suspect employee at a formal inquiry.

27.2 The appointment of a representative shall be binding on the employee until revoked in writing by him, before the Inquiry Officer, and notice thereof given to the Disciplinary Authority or until such representative becomes for some reason unable to act in that capacity, or refuses to act or to continue to act in such capacity, or the representative dies or becomes incapable of acting in such capacity. In such an event the accused employee may appoint another representative, to continue the inquiry.

27.3 All acts of commission or omission by the representative or statements made by him in the course of disciplinary proceedings, shall be deemed to be the acts of commission or omission or statements of the employee himself, and for all purposes be fully effectual as if such acts were done or omitted to be done or statements made by the employee.

27.4 It is an offence for a representative so appointed to charge fees for appearing for an accused employee.

27.5 No witness intended to be called for by the prosecution or the defence could be appointed as the representative at a formal inquiry.

PROCEEDINGS TO BE ADOPTED AT A DISCIPLINARY INQUIRY

28. **Reading Out Charges**

28.1 The Inquiry Officer, at the commencement of the Inquiry, shall read out the charges to the employee and ascertain from him whether he is guilty or not. The inquiry Officer shall thereafter, enter of record the plea given by the employee.

28.2 If the employee pleads guilty to the charges, the Inquiry Officer should warn the employee that his plea may result in his dismissal from the Bank or that he may be otherwise dealt with. The inquiry Officer shall enter of record of his having so warned the employee. The Inquiry Officer shall thereafter, question the employee whether in spite of such warning he still pleads guilty, and if the employee answers in the affirmative his plea should be entered of record and the signature of the employee and of his Representative obtained. The employee and/or his Representative may then be allowed to plead in mitigation.

28.3 If the employee pleads not guilty to the charges, the Inquiry Officer shall call upon the Prosecuting Officer to lead the evidence of the witnesses for the Bank. The Prosecuting Officer may produce documentary evidence in support, if any. Provided that, in the event of fresh documents being introduced in the course of the inquiry, every opportunity should be afforded to the adverse party of examining same.

29. **Recording of Proceedings**

29.1 All proceedings should be recorded clearly and legibly.

29.2 At any stage of the inquiry, where the Inquiry Officer considers it necessary, or where a request is made by any party, evidence may be recorded in question and answer form.

29.3 The prosecuting officer may lead the evidence of his witnesses in any order he prefers.

29.4 The examination of a witness by the party who calls him is known as the Examination-in-chief. No leading questions shall be permitted in the Examination in Chief. When the Examination-in-Chief of a witness is over, the opposite side has the option of questioning him. This is called Cross Examination.

29.5 When a witness is cross examined, questions may be asked from him in order to test his veracity, accuracy or credibility even though his answers to such questions may directly or indirectly implicate him. However such questions must be relevant and should not be asked for the purpose of insulting, annoying or browbeating the witness.

29.6 Subsequent to the cross examination, the party calling a witness has the right of re-examination of such witness. The purpose of re-examination is to clarify matters arising out of the cross-examination. If however new material is disclosed in re-examination, the other party has the right to cross-examine such witness on such new material, with the permission of the Inquiry Officer.

29.7 No witness shall contradict the statements made by him in the course of a Preliminary Investigation. If the employee or any witness contradicts the statements made by him in the course of a preliminary investigation, the Prosecuting Officer shall request the employee or witness to explain such contradiction. Their reply, if any, shall be recorded. If they remain silent such fact should also be recorded.

29.8 On refusal by a witness or the employee to answer a question the Inquiry Officer shall record such refusal and the reasons therefore.

29.9 Doing or saying anything in disrespect of the authority of a Prosecuting Officer or Inquiry Officer, within or outside the premises of the Bank, by a Bank employee would constitute an offence under Schedule 11.

29.10 Both parties shall be entitled to receive a copy each of the proceedings at the end of each day.

30. **The Defence**

30.1 If after recording the evidence of all witnesses for the Prosecution, the Inquiry Officer is satisfied that the charges have not been proved, he may not call the defence to lead their evidence. He may conclude the inquiry at this stage and submit his report to the Chief Manager (I & I).

30.2 If the defence does not call any witnesses and/or the accused employee declines to give evidence on his own behalf, that fact must be entered of record. The evidence of witnesses called by the defence should be recorded subject to cross examination and re-examination, as per Section 29.4, 29.5 and 29.6 above.

31. **Conclusion of Inquiry and Submission**

31.1 After the evidence of all witnesses have been recorded the Prosecution and the Defence will both be permitted to make their submissions orally or in writing if they so desire on the day itself, or on an appointed date pertaining to:

31.1.1 The evidence led at the inquiry.

31.1.2 The charges preferred against the employee.

31.1.3 The innocence or guilt of the employee in respect of the charges preferred against him.

31.1.4 Mitigating circumstances, if any.

31.2 At the conclusion of the inquiry, the Inquiry Officer shall find out from the accused employee and his Representative whether they are satisfied with the manner in which the inquiry was conducted. The reply given should be entered of record (with the signature of the employee and the Representative) entered therein as follows :-

"We are satisfied with the conduct of the Inquiry".

OR

"We are not satisfied with the conduct of the Inquiry for the following reason/reasons."

31.3 The written submissions of both parties together with documents, if any, shall be forwarded to the Inquiry Officer on a date to be fixed by him, within one month of the conclusion of the inquiry.

32. **Finding of the Inquiry Officer**

32.1 After the conclusion of the Inquiry, the Inquiry Officer shall forward his report in triplicate together with the record of the proceedings and all documents produced to the Chief Manager (I & I) within 30 days from the receipt of the submissions.

32.2 The said report should be based on facts and inferences drawn from such facts and shall also state whether he finds the accused guilty or not in respect of each charge preferred against him, together with reasons therefore.

32.3 The Inquiry Officer may comment on the demeanor of witness and their credibility or otherwise and his reasons therefore.

32.4 The Inquiry Officer shall not make any recommendations regarding punishment. However he may draw the attention of the Disciplinary Authority to mitigating circumstances, if any, or any other matter of a special nature requiring the attention of the Disciplinary Authority.

33. **Order of the Disciplinary Authority on the Finding of the Inquiry Officer**

33.1 The Chief Manager (I & I) on receipt of the report of the Inquiry Officer shall submit it to the relevant Staff Committee in consultation with the Assistant General Manager (I & I). If the suspect employee is found not guilty of all the charges, the staff committee after considering all the circumstances shall exonerate the employee of the charges preferred against him, and the staff committee shall recommend to the disciplinary authority that the employee should be exonerated, and re-instated in the service of the bank, in case of an interdiction.

33.2 If after a consideration of the findings, the staff committee is of the view that the accused employee is guilty of one or more or all the charges, the Staff committee shall recommend to the Disciplinary Authority, an appropriate form of punishment taking into consideration the accused employee's record of work, conduct and length of work etc. If the Disciplinary Authority is satisfied with the findings and recommendations of the Staff Committee, then it shall make an appropriate order compatible with such findings.

34. Communication of Order of Punishment

34.1 When a punishment is imposed on an employee in respect of any offence (major or minor) it shall be communicated by the Chief Manager, (Human Resources Management) within 14 days of the receipt of the order from the Chief Manager (I & I) to the employee. Such order pertaining to punishment shall state the offences (Charges) in respect of which the employee has been found guilty of. It shall be entered in the personal file of the employee. A copy of such communication should be sent to the relevant Head of the Department or the Regional Manager and Branch Manager.

34.2 In the event of such employee being transferred from one Region to another Region or to a Department, the Regional Manager of the new Region or the Head of the new Department shall be similarly informed by the Chief Manager (Human Resource Management) of the punishment imposed, provided the effective period of such punishment has not expired.

35. Right of Appeal and Procedure to be followed on Receipt of an Appeal

35.1 An Employee dissatisfied with any punishment imposed by the Disciplinary Authority may himself tender a written appeal regarding same within thirty (30) days of order of punishment being communicated to him.

35.2 The appeal shall be substantially in the form given in Schedule V and shall set out fully the grounds on which the appeal is made. It should be submitted to the Chief Manager (HRM) through the respective Head of Department/Regional Manager/Branch Manager.

35.3 On receipt of an appeal, the Chief Manager (HRM) shall refer it to the Chief Manager (I & I) immediately.

35.4 Thereafter the Chief Manager (I & I) shall submit same within 14 days to the appropriate Staff Committee with his observations. The Staff Committee to which an appeal is referred shall consider the grounds on which the appeal is based and make its recommendations to the Disciplinary Authority.

36. **Appeals – Powers of the Disciplinary Authority**

36.1 Based on the recommendation of the appropriate Staff Committee the Disciplinary Authority shall either dismiss the appeal or quash or vary the punishment imposed.

36.2 The order made by the Disciplinary Authority on an appeal shall be final and conclusive. Such order shall be communicated to the employee by the Chief Manager (HRM) immediately.

36.3 Pursuant to an Appeal, if the punishment earlier imposed has been varied or quashed this fact should also be conveyed to the Regional Manager and Branch Manager or Head of the Department to which the employee is attached.

37. **Punishments**

37.1 Punishments such as dismissal and discontinuance from service are imposed for grave offences, when the nature of the offence itself tends to erode the trust and confidence vested in a Bank employee. Punishments can be deterrent, preventive or of a reformatory nature. The imposition of a particular form of punishment is dependent on the nature and gravity of the offence and the degree of guilt of an employee as well as the attendant circumstances.

37.2 Any one or more of the forms of punishments listed below may be imposed.

37.2.1 Letter of Advice

37.2.2 Caution

37.2.3 Reprimand (effective period is 2 years)

37.2.4 Severe reprimand (effective period is 3 years)

37.2.5 Surcharge

37.2.6 Token Recovery

37.2.7 Transfer on Disciplinary grounds

37.2.8 Suspension from duty

37.2.9 Suspension of increment/s

37.2.10 Stoppage of increment/s

37.2.11 Deferment of increment/s

37.2.12 Deferment of a promotion to higher post/higher Grade for a specific period

37.2.13 Reduction in grade, or rank by reversion to the next lower class or grade of the Bank's service

37.2.14 Retirement as a merciful alternative to dismissal. (In the event of an employee above 55 years of age).

37.2.15 Calling upon to resign.

37.2.16 Dismissal

37.3 **Stoppage of Increment**

37.3.1 Stoppage of Increment means the withholding of an increment for a specific period. At the end of the specified period the increment will be granted in addition to any increment/s that may have fallen due in the meantime. No arrears of increment are payable.

37.4 **Deferment of Increment**

Deferment of Increment means the non-granting of a specific number of increments for a specific period.

37.5 **Suspension of Increment**

37.5.1 Suspension of Increment means the withholding of the increment for a specific period of time. If an employee whose increment has been suspended fails to show any improvement in his work within the period of suspension, the suspended increment may be converted to one of stoppage

37.5.2 Suspension of Increment may not be imposed for a period exceeding one year after which the suspended increment may be restored with arrears of suspended increment or the increments be stopped altogether as per Section 37.3 above.

37.6 **Suspension from Duty**

Suspension from duty may not be imposed for a period exceeding 30 days. During the period of suspension the employee will not be entitled to his salary and other benefits e.g. medical etc. Suspension will also result in the period of suspension being reduced from the period of service of the employee.

38. Custody of the Records/of the Disciplinary Matters/Proceedings

38.1 Originals of all records/documents relating to all disciplinary matters shall be kept under the custody of the Regional Manager/Head of the Department who should forward same to the Chief Manager (I & I) as and when requested. These records/documentation shall be kept in safe custody till the punishments are imposed and any appeals decided. The release of these records/documents to the places of origin shall be done only after clearance from the Chief Manager (I & I).

38.2 The Records of Disciplinary Proceedings shall be kept by the Chief Manager (I & I) in his custody at Head Office for a period of six years.

38.3 Records of Disciplinary Proceedings shall not be destroyed if there is any matter pending before a Court of Law or a Labour Tribunal.

38.4 Records which has been retained for more than six years may be destroyed subject to section 38.3 above after duly entering the necessary details in a separate Register and duly authorised by the Chief Manager (I & I).

39. Circular Instructions

39.1 If any circular or circulars that have been issued or will be issued by the Bank from time to time on the instructions of the Disciplinary Authority in respect of any misconduct and if such circular or circulars issued or to be issued by the Bank prescribe any special procedure or procedures to be followed in dealing with an accused employee alleged to have committed an act of such misconduct, then in such instance the special procedure or procedures laid down in such circular/s shall be followed in dealing with the employee notwithstanding anything to the contrary hereinbefore contained. However, if such circular or circulars does/do not prescribe any special procedure or procedures, then the procedure set out in this code shall be applicable.

40. **Amendments to the Code**

40.1 The Disciplinary Authority shall have the power to make any amendments and/or alterations from time to time to the rules contained in this code.

41. **General**

41.1 No error, omissions, or irregularity in the conduct of an investigation or inquiry under the code shall entitle an employee to have the proceedings quashed, or punishment imposed, reversed, altered or set aside for that reason alone, unless it can be shown that such error, omission or irregularity has resulted in a miscarriage of justice, or violated the principles of natural justice or infringed on the rule of law.

Schedule I

Acts of Minor Misconduct

1. Absence from work without excuse

2. Habitual late attendance at work without excuse.

3. Negligence at work

4. Slackness or Malingering

5. Distribution or exhibition of hand bills, pamphlets, posters etc. within the premises of the Bank, without the sanction of the authorities

6. Violation of instructions given in respect of the maintenance of premises, machinery, equipment and furniture etc.

7. Smoking in any part of the premises where smoking is prohibited

8. Overstaying leave without due notice

9. Failure to attend Instructions/Training classes

10. Idling whilst on duty or failure to perform the allotted quantum of work, for the day.

11. Misuse of Bank's stationery and equipment

12. Failure to wear uniforms according to instructions, while on duty.

13. Failure to wear the Bank's identity card within the premises

14. Permitting unauthorized persons to enter the premises of the Bank, or transport of goods or persons in the vehicles of the Bank, without permission

15. Exceeding the stipulated period for meals and rest pauses.

16. Incivility or causing inconvenience to any member of the public who attends the Bank for transaction of business.

17. Any other act or omission which in the opinion of the Disciplinary Authority will be regarded an act of Minor Misconduct.

18. Failure to provide funds in their accounts to repay loans on due dates by an employee of the Bank where such employee had made arrangements with the Bank to repay any such loan from their accounts.

Schedule II

Acts of Grave Misconduct

01. Breach of Regulations and circular instructions of the Bank

02. Theft, Extortion, robbery, Misappropriation, Breach of Trust, cheating, mischief, in respect of any property within or outside the Bank.

03. Conspiracy or abatement in respect of misconduct under item No. 02 above.

04. Divulging of information obtained in the course of employment of the Bank, transmitting documents or contents of the documents which are in the custody of the Bank, maliciously and without authority and thereby causing loss to the Bank and damage to the image of the Bank.

05. Breach of Oath of Secrecy imposed on the employees of the Bank by Statute as well as by Circulars.

06. Using, any type of communication equipment or voice, media, e-mail, etc., initiating or propagating rumors, and creating false allegations, gossip and other related type of misbehavior.

07. Borrowing money from outside sources of guaranteeing or becoming surety for loans of third parties without prior written permission of the Bank.

08. Trespass within the premises of the Bank and in areas within the premises, where employees are forbidden from entering or any unauthorized entry to any Departments or to any Bank Branch without prior approval of the relevant authority.

09. Forgery of falsification of documents or Accounts or tampering with documents.

10. Abuse, intimidation, assault, altercation, insult or causing annoyance to any employee or customer of the Bank within or outside the premises of the Bank.

11. Conviction in a Court of Law of an offence under the Penal Code or other Penal Law.

12. Giving or acceptance of bribes or being associated therewith in any manner as will constitute an offence under the Bribery Act.

13. Insolence or disrespect to any person within the premises of the Bank.

14. Sabotage.

15. Any type of computer forgery using passwords of others hacking and electronically entering into other areas and accessing classified information breaking firewalls and using e-mail address of others to conduct forgery and crime using computers.

16. Wanton damage or loss to property belonging to or in the custody of the Bank.

17. Gross negligence resulting in a loss to the Bank.

18. Sleeping whilst on duty.

19. Persistent unauthorized absence from duty.

20. Drunkenness or smelling of liquor or being under the influence of liquor Narcotic drugs within the Bank's premises whilst on duty.

21. Disorderly behavior or gambling within the premises of the Bank.

22. Wilful failure on the part of an employee to comply with any lawful orders given to him by a Superior Officer, in relation to his duties including defying transfer orders issued by the management from time to time.

23. Improper conduct of personal Bank Account/s.

24. Refusal to give evidence or giving false evidence at a disciplinary inquiry of investigation

25. Leaving the place of work during working hours without permission

26. Making false allegations against Superior Officers or other employees of the Bank.

27. Casting offensive remarks at a superior officer or a member of the Board, or an investigating or inquiring officer.

28. Hindering a superior officer or other employee of the Bank from performing his duties.

29. Reckless or negligent handling of equipment or driving a vehicle belonging to the Bank in a reckless or negligent manner and/or under the influence of liquor.

30. Unauthorized use of a vehicle of the Bank or diverting from the usually accepted route without reasonable cause.

31. Failure on the part of an employee, being aware of the commission of any act of misconduct by another employee to inform authorized officers of the commission of such act of misconduct.

32. Engage in any business activity or undertaking.

33. Making contradictory or substantially different statement at a formal or summary inquiry from the statements made at a preliminary investigation.

34. Obtaining Credit Cards from other Banks or financial Institutions without the permission of the General Manager.

35. Failure by the driver or the user of a Bank vehicle to report an accident involving a vehicle belonging to the Bank within 24 hours to the relevant authority.

36. Any repetition of an act of minor misconduct which in the opinion of the Disciplinary Authority is regarded as grave misconduct.

37. Seeking third party assistance intervention and influence of politicians and other prominent members of Public with a view to gain undue advantages in securing transfers or their cancellations, promotions, individual benefits and other assistance.

38. Obstructing, neglecting, not attending to Bank work by engaging in meetings or other activities within/outside the Bank premises during working hours for which prior permission of the management has not been obtained.

39. Any other act or omission which in the opinion of the Disciplinary Authority will be regarded as an act of grave misconduct.

40. Any type of action or omission which would cause or be liable to bring the good name of People's Bank into disrepute or otherwise damage People's Bank's image.

Schedule III

Registered Post

Mr. .....

.....

.....

Charge Sheet

1. You are hereby required to show cause in writing why you should not be Disciplinarily dealt with under the provisions of the Disciplinary Code of the Bank in that you did.

   (a) (Set out here the specific Charges giving details as required under Section 22.4 of the Disciplinary Code)

   (b)

2. Your, explanation (if any) stating the grounds upon which you depend to exculpate yourself should reach the undersigned within * days of this letter. In respect of each of the charges mentioned above, you must state separately whether or not you are guilty of the same.

3. If no explanation is received from you within the time mentioned above, it will be presumed that you have no explanation to offer and that you are guilty of the said charges.

Appropriate Authority

(Section 2.7)

Date:

* The number of days **which should not be less that 14** in terms of Rule 22.3 of the Disciplinary code may be decided according to the circumstances of each case.

Schedule IV

Registered Post

Mr. .....

.....

.....

Notice of Formal Inquiry

1. Further to the Charge Sheet dated ..... requesting you to show cause why you should not be punished for the commission of the Act (s) of Misconduct therein described and your explanation thereto dated ..... I have been directed by the Disciplinary Authority to inform you that he is not satisfied with your explanation and that a Formal Inquiry should be held against you. You are accordingly hereby requested to attend the Formal Inquiry under Section 24 of the Code which will be held on ..... at ..... a.m. / p.m. at ..... with your "Representative", witnesses and documents (If any)

2. At the Formal, Inquiry, you will have the right to be represented by a "Representative" who should have the necessary qualifications in terms of the Section 27.1 of the Disciplinary Code of the Bank. Please state in writing the name and address of your "Representative" on or before ..... failing which it will be presumed that you do not wish to be represented.

3. The following documents will be produced against you at the Formal Inquiry should you or your "Representative" wish to examine the same, please let me know at least seven working days prior to the date of the Formal Inquiry so that arrangements may be made for the purpose. If you fail to do so, it will be presumed that you do not wish to examine such documents.

(a)

(b)

(c)

(d)

If you do not present yourself at the Formal Inquiry, the determinations shall be made ex-parte.

Appropriate Authority

(Section 2.7)

Date :

Schedule V

Section 40

Date: .....

Appeal

Chief Manager (HRM)

People's Bank, Head Office

P.O. Box 728,

Colombo 02

Appeal Against the Order of Punishment Imposed Upon Mr. .....

1. At the time of the incident for which I was punished I functioned as the ..... in the .....

   (position) (Branch/Dept/RHO)

2. Consequent to the disciplinary proceedings I have been found guilty of the following charges/offences, according to the intimation of the Chief Manager (HRM) by his letter dated .....

3. Being aggrieved with the punishments imposed on me by the disciplinary authority in respect of the above offences/ charges, as well as the gravity of the punishment imposed upon me. I hereby tender an appeal, on the following grounds.

01.
02.

03.

04.

(List the grounds on which appeal is made in detail)

I request, that my appeal be considered, in light of the above details given by me and quash/ reduce the punishments imposed on me.

.....

Employee's Signature

& Service Number

CUSTOMER CHARTER

PEOPLE'S BANK

Introduction

Good customer relations is the heart of banking. Every individual sees their bank as one of their most important service providers, mainly as the relationship involves the management of their hard-earned money. Therefore people will be specially critical when deciding upon a bank or deciding to remain with one. Accordingly, in banking, customer retention is more of a challenge than it is in other industries.

In the present scenario of competitive banking, banks are required to become more and more customer-centric. Excellence in customer service has become the most important tool for sustained business growth as it focuses on building healthy relations between the bank and customers. Along with efficient service, providing customers with accurate and consistent information on the products and services of the bank, apt handling of complaints and providing special attention and care for those with physical and financial limitations will safeguard the interests of the customers and improve the confidence of the customers in the bank.

As a State Bank, People's Bank is determined to set an example to the banking world by adopting the standards of fair banking practices that are expected by customers when they undertake transactions with us. This Customer Charter is a product of the endeavor of People's Bank in adopting the guidelines issued by the Monetary Board, by its Banking Act Direction No. 8 of 2011 dated 5th October 2011, on "Customer Charter of Licensed Banks". The successful implementation of the standards set by this Charter along with a joint effort to strive to improve our service and to solicit the support and cooperation of customers will go a long way to reaching the goals of the Bank.

1. Information

People's Bank offers an extensive range of banking products and services to a wide range of business and individual customers. All customers of our Bank have their own unique needs and expectations when they visit our Bank. The employees, specially the front office staff, should assist the customers to understand the products and services offered by the Bank by providing them with adequate information and assist them in choosing the appropriate product that matches their requirement.

Many individuals will make the decision on whether to do banking with a particular institution based on the personalities and expertise of the front office staff as they are often the first point of contact for customers. Therefore all employees should have adequate knowledge about the services and the variety of banking products offered by the Bank. The employees should always be courteous and friendly when providing the required information to customers.

Customers may also seek information via telephone. Employees should answer the phone as soon as it rings and should not let a telephone ring more than three times, before it is answered. Employees should always be courteous on the phone and whenever possible should identify themselves with their name and department. The essential information that the customer requires should be provided along with directions on how to obtain further information should the need arise. If the employee is unable to provide the information the caller requires instantly, the caller's contact numbers should be obtained and the required information should be provided within a day. A register should be maintained for this purpose and reviewed at the end of the day to ensure that all customer queries have been answered.

In situations where the customer seeks information via e-mail, care should be taken to respond to the e-mails within a reasonable time period. Relevant links to obtaining further information such as the link to the People's Bank website and/ or the names and contact details of relevant bank officials in the branch/ department should also be provided.

1.1 Brochures/ leaflets

At People's Bank, brochures and leaflets are used to provide information about the bank's products and services and any other special business promotions that are being carried out. Brochures/ leaflets should be available on all products offered by the bank in Sinhala, Tamil and English and displayed in an easily accessible location to customers seeking such information. The following information should be included in the brochure/leaflet;

- Description of the product/ service

- Financial & other benefits to customers including any incentive and promotion.
- Fees/ charges, commission, interest etc charged from customers
- Procedure to be followed to obtain the product/ service.
- Major terms and conditions
- A Complaint procedure for customers

1.2 Advertising

Advertising is another marketing tool used by the Bank for the promotion of its business activities. The Bank uses mainly television, radio and print media for advertising. When advertising using media or other promotional material, only factual information should be included. This information should be provided in a simple and easy to understand manner. Any information that may mislead the public should not be provided when advertising. All advertisements should include contact details of relevant bank officials and also state that People's Bank is a licensed bank supervised by the Central Bank of Sri Lanka. All relevant staff members should be aware of the information provided via an advertisement and be able to assist the customers should any clarifications be required.

1.3 Display of information

Displaying the basic information the customer requires when they visit our bank can save time and energy of both the customer and the staff. The following information should be displayed conspicuously in the Head Office, all Branches and Service Centers, the Corporate Banking Division (CBD), Overseas Customer Services (OCS), Card Center and Off- shore Banking Unit of the Bank.

i) Current interest rates on all deposits and loan products

ii) Service Charges, Fees and Commissions

iii) Buying & selling rates of foreign currencies

iv) Credit rating of the Bank with underlying specifications

v) The contact details of the Financial Ombudsman and Credit Counseling centre (Annexures 7 & 8).

vi) Banking hours and holiday notices

vii) Any other relevant information (pawning rates…. etc)

viii) License of the bank

ix) Name of the branch/ department

x) Name board of the respective Department/ counter within the branch

The information should be updated on a regular basis or when any changes occur, and a responsible employee should be assigned for this purpose. It is the responsibility of the Branch Manager/ Department Head to ensure that the information displayed is accurate and complies with the stipulated format. The formats to display interest rates, exchange rates, service charges, fees and commissions have been issued with the Deputy General Manager (Operations) Circular Letter No. 7051/2011 dated 18.7.2011 and is also attached herewith marked Annexures 1 to 3.

1.4 Statements

Periodic statements either in printed form or electronic form as opted by the customer should be sent for all accounts other than for savings and dormant accounts. The statements should generally be produced on a monthly basis and mailed directly to the customer's mailing address. All statements should be mailed within one week of generation. In circumstances where the customer has given specific instructions to obtain daily statements or for personal pick-up, these requirements should be entertained. Statements should not be handed over to a third party unless specific authority of the account holder has been obtained. Care should be taken to maintain the confidentiality of the account information. Extra safety measures of disposal such as shredding should be used for undelivered statements.

E-statement facility is also obtainable through the internet banking facility via People's Net. Customers should be encouraged to obtain this facility as it provides safe and efficient access to the customer.

Statements for Credit Cards should include details on;

- The minimum payment required and due date
- Total interest charged if only the minimum payment is made

- Late payment fee if the minimum payment is not made on due date

1.5 Awareness programs

Customers and general public should be made aware of the financial products and services and any risks associated with them, by conducting awareness and financial literacy programs. The Branches/ Departments should conduct community programs aimed at improving the financial literacy of the community, particularly the disadvantaged groups.

1.6 Terms & Conditions

All customers of the Bank have the right to access and gain complete understanding of the terms and conditions relevant to each and every product or service they obtain from the Bank. It is the responsibility of the Bank employees to ensure that the customers have access to this information. The customer has the right to specifically know the following information for any product or service they obtain.

I. Details of the Bank's general charges such as interest rates, fees and commissions required to be paid by the customer including the method of computing interest charges.

II. The Bank's procedure for receiving complaints and the resolution mechanism.

III. The course of recovery actions the Bank may follow in the event of any default by the customer on his/her obligations and Bank's expenses that will be claimed from the customer.

IV. Any compensation required to be paid by a customer in case of pre-mature withdrawal/termination of participation in a product/service by the customer.

V. Any restrictions on opening of accounts, closing of accounts, maintenance of accounts (e.g., minimum balance), transfer of funds by customers and policies and procedures on dormant accounts and abandoned property.

VI. The disclosure of customer information to a party legally authorized to obtain such information.

VII. The rules regarding

(i) reporting of suspicious transactions and above-the-threshold transactions to the Financial Intelligence Unit

(ii) the reporting procedures that the customer should follow in the case of stolen cards /financial instruments and

(iii) liability of the Bank and the customer.

VIII. The procedures to be employed by the Bank to foreclose on the property held as collateral for a loan and the consequences thereof to the customer and options available to him/her.

The terms and conditions associated with each product offered by People's Bank should be available to the customers in their preferred language (Sinhala, Tamil or English). A copy of the relevant terms and conditions should be offered to the prospective customer seeking the use of a specific product/ service. Employees should ensure that the prospective customer understands the terms and conditions associated with the product/ service being obtained. Information on alternative products/ services should also be provided and thoroughly explained to the customer and reasonable time should be given for the customer to evaluate and make a decision. Any changes in the terms and conditions should be promptly updated in the documents and the customers should be informed in writing or through paper notice or any other appropriate way.

A Written confirmation should be obtained from the customer that they fully understand and accept the terms and conditions relating to the product or service they obtain. These should be filed with the other documents relating to the customer. The employees should ensure that the documents obtained are fully completed and signed by the customer. Obtaining customer signature on blank or incomplete documents should not be done under any circumstance. It is the duty of the relevant officer in charge to ensure that the customer has completed the documents and signed them with due knowledge of the terms and conditions.

1.7 Compensation for withdrawal/ cancellation of products/ services

In the event the Bank seeks to withdraw/terminate a product or service already on contract, especially deposit products, customers have the right to receive a reasonable time with an exit compensation scheme disclosed in advance.

2. <u>Protection from Agents of the Bank</u>

Presently at People's Bank the services of external agents have been obtained to conduct business activities related to following main business purposes.

- Issuance of Credit cards – Marketing, Promoting, Campaigning, new applications processing
- Merchant Acquiring for Credit cards – Acquiring merchants & Point of Sale (POS) installations, breakdown services, resolving merchant inquiries
- Recovery of credit card dues– past due/overdue customer visits, Collecting debts, granting settlements, following-up of the settlements granted

The agents should abide by the procedures set out by the 'Code of Conduct for Third Party Agents' attached herewith as annexure 4. Within it, the following special provisions for the protection of customers have been included;

- Agents should not use any intimidation or violence – verbally or physically against any individual.
- Shall not discuss, promote, print or publish by any means whatsoever any information pertaining to any customer.
- Shall not give false or misleading information about products/services.
- Shall not unduly influence customers or the general public to buy or get involved in the Bank's products/services.
- Shall not engage in getting any security documents signed outside the Bank.
- Third party details provided by the bank to trace a cardholder should be used for the said purpose only.
- The Agents should not take action against any third party individuals by making pestering phone calls during inconvenient hours, pestering their family members or any other individual related to the customers.

In addition, the agents have been advised to adhere to the Credit Card Guidelines No 01/2010 issued by the Central Bank of Sri Lanka, provided in annexure 5 below and any other guidelines issued by the Central Bank of Sri Lanka.

The customers of the Bank have the right to know the particulars of the agents appointed for customer services by the Bank and the precautions taken by the Bank to protect the customers from any malpractice of the agents.

3. Handling Complaints

Customer complaints are part of the business life of any corporate entity. This is more so for banks because banks are service organizations. As a service organization, customer service and customer satisfaction should be the prime concern of any bank. Proper handling of customer complaints is of paramount importance, since it safeguards the legitimate interests of the customer and as a consequence, the bank's good reputation is protected and the bank can avoid possible civil actions by customers. Having a complaint handling procedure aims at minimizing instances of customer complaints and grievances, and provides an opportunity for the bank to improve its service and strengthen its relationship with the customer.

3.1 Complaints handling procedure

Customers, who believe that the services offered to them are not of sufficient quality or if they are not satisfied with the service offered, may bring the issue to the attention of the relevant Bank staff. Complaints can be made verbally, in writing or over the telephone. The employees shall not insist that the complaint should be in writing. All branches/departments should have a complaints book and/or a complaints box available to the customers to record their complaints.

When a complaint is received, the employee;

- who receives the complaint should acknowledge the complaint promptly and thank the customer for bringing it to our notice
- Should apologize for the mistake if a mistake has been made or for any inconvenience caused , bearing in mind that it is our duty to treat the customer as if he or she is always right
- It must be dealt with in a courteous manner, avoiding arguments. Should assure and ensure that his or her needs and wants are attended to promptly.
- If the complaint cannot be attended to promptly, details should be obtained and realistic time frame needed should be communicated to the customer.
- The complaint must be recorded and be informed to the responsible officer

- A response should be given/ sent without delay, without waiting for reminders
- All efforts must be taken to settle/ rectify the complaint quickly and efficiently if the complaint is justified.

The Staff is encouraged to deal with a verbal complaint as soon as a customer mentions his dissatisfaction, and must try to resolve the complaint immediately.

In cases when the complaint is received by a letter or via e-mail, an acknowledgement should be sent to the complainant not later than the next working day mentioning the date on which the complaint has been received, the actions being taken, the time needed by the Bank to provide the customer with a solution as well as the name and the contact details of the Bank Employee with whom the customer can liaise with regarding any enquiries about the complaint.

When a complaint is received via telephone the identity of the customer must be verified along with the relevant contact details.

Anonymous complaints must be viewed with discretion but must be investigated regardless of the fact. If the complaint is justified the proper complaints handling procedure must be followed.

Each Branch/Department should record all complaints addressed to them in a Complaint Record Book, which should include;

- Date when the complaint has been received,
- Name/account number of the complainant,
- Substance of the complaint,
- Name and service number of the officer responsible for the complaint handling,
- The Bank's response- How the complaint was resolved, any reimbursement offered by the Bank, how it has been calculated and the response of the complainant to this offer,

- Date of the Bank's response.
- Lessons learned and procedures changed to avoid such tribulations in the future.

The format of the Complaint Record Book is given in Annexure 6.

All Branches/ Departments should assign an **officer** who is responsible for handling complaints and providing relevant information to the management regarding complaints. Customer complaints must be investigated thoroughly and promptly by the officer, as they might indicate service/procedural deficiencies or ineffectiveness which might lead to serious irregularities or fraud.

An employee must never handle a complaint made against him/her. Any complaint against the Branch Manager should be directed to the Assistant Regional Manager and if a complaint is made against the officer who is handling complaints, it should be handled by the Branch Manager or Operations Manager. Strict confidentiality must be maintained in situations where a serious complaint is made against an officer or staff member. Where litigation is threatened or instigated, the Chief Law Officer should be informed as early as possible and advice sought.

The officer responsible for complaints handling must:

- make a record of the complaint in the record book,
- try to resolve the complaint by directing it to the relevant officer/ department and arrange the response to the customer as soon as possible,
- Make all efforts to resolve the complaint within 10 working days from the date of the receipt.
- Periodically update customers on the status of the complaint.

Customer Complaints Record Book must be reviewed by the Assistant Regional Manager on a monthly basis, on a quarterly basis by the Internal Audit and on a random basis by the Compliance Officer to ensure that all customer complaints have been resolved and/or outstanding complaints are being dealt with.

The Branch Manager is ultimately responsible for the resolution of complaints in respect of customer service by the branch. He/she would be responsible for ensuring closure to all complaints received at the branch. It is his/ her duty to ensure that complaints are dealt in a prompt manner with transparency, impartially and in confidence. It is the Mangers' foremost duty to see that the complaints are resolved completely to the satisfaction of the customer and if the customer is not satisfied, then he or she should be provided with alternate avenues to express the issue. If the Branch Manager feels that it is not possible at his/her level to resolve the problem the matter should be directed to an appropriate higher authority. The customer should be provided with the details of the relevant officials at the Regional Head Office and the Head office. If the customer's complaint is not resolved within a reasonable time or if he is not satisfied with the solution provided by the Bank, the customer has the right to approach the Financial Ombudsman. The contact details of the Financial Ombudsman are given in Annexure 7 and should also be provided to the complainant.

4. <u>Special attention and care</u>

People's Bank being the 'Pulse of the People' has always been renowned for the humanity it shows to the people with special needs. The employees at all times should ensure that the elderly, disabled and customers with low financial literacy receive special attention to ensure that they have fair and equal access to the services offered by the Bank. In doing so the employees should ensure that they have easy access to the premises and to other banking facilities such as ATM Facilities. Treating people who need special care courteously and kindly and explaining until they understand the information required relating to the product or service that they obtain can go a long way in winning the hearts and consequently the loyalty of the customers.

All customers of People's Bank should be treated fairly and equally irrespective of their race, nationality, social status, occupation, age and gender. The bank is striving for zero gender discrimination and zero racial discrimination in all areas of banking. The employees should always maintain the principles of integrity and transparency and ensure that the products and services offered comply with the relevant laws and regulations.

5. <u>Customer obligations towards the Bank</u>

Customers should foster the relationship with the Bank fulfilling their obligations. In this regard:

a) Customers should not borrow beyond their affordable repayment capacity limit.

b) Customers should not allow the repayments or installments to go into arrears as prompt repayments will create a healthy relationship with the Bank.

c) If a customer wants to settle his/her loan before the end of the loan period, he/she has to pay a certain amount of money over the loan amount as agreed at the time of accepting the offer.

d) If the customer is unable to repay his/her loan outstanding as agreed, the Bank will have the right to recover the amount owing to the Bank including the Bank's expenses specified in the 'Terms & Conditions'.

e) If a customer finds himself/herself in financial difficulties, he/she should let the Bank know as early as possible. The sooner the Bank discusses the customer's problems, the easier it will be for both the customer and the bank to find a solution.

f) When a customer account goes into default, the first step the Bank takes is to contact the customer. In this regard, it is imperative that the customer should inform the Bank at all times of any changes to his/her address and contact details.

g) Customers should have the full knowledge and understanding of the product/service offered before entering into the contract.

h) Customers should duly fill and submit the required application forms and supporting documents on time.

i) Customers should exercise due care in all transactions with the Bank. The customer should take special care to read and understand before signing any document with the Bank. Placing their signature on blank/ incomplete documents should be avoided.

j) Customers should notify the Bank promptly of any fraudulent transaction/s or such attempts in their accounts with the bank whenever they become aware of such instances.

k) Customers should exercise utmost care in using and storing/handling Personal Identification Numbers (PIN) and security measures of other electronic cards issued by the Bank.

l) Customers should not treat any operational lapse of a bank on its obligations, other than any dispute on the amount payable to the Bank, as a reason for his/her non settlement or delay in settlement of a debt unless otherwise allowed by a Court of Law. All such incidents need to be resolved separately or individually.

m) Customers should make arrangements to apprise any adverse situations in the market related to their business activities.

Annexure 1

Interest rates

	Description	Mini. Rate as at ……	Max. rate as at ……
	Interest Rates on Deposits		
	Savings Deposits		
	Minor Savings Deposits		
	Call Deposits		
	Time Deposits - 1 Year		
	* Interest payable monthly		
	* Interest payable at maturity		
	NRFC Savings Deposits		
	* US Dollars		
	* Sterling Pound		
	* Euro		
	* Any other Currencies		
	Interest Rates on Advances		
	Export Bill Finance – Rupee Facilities		
	Import Bill Finance - Rupee Facilities		
	Lease Finance		
	Lending to Small & Medium Scale Industries		
	Residential Housing		
	Pawning		
	US Dollar Loans to Exporters		
	Overdrafts		
	* Permanent		
	* Temporary		
	Personal Loans		
	Vehicle Loans		
	Credit Cards		
	Agricultural Lending		
	Refinance Schemes		
	i. Agriculture & Animal Husbandry		
	* Tea Development Project (Revolving fund)		
	* Agro-Livestock Development Project		
	* Any other		
	ii. Small & Medium Enterprises Sector		
	* Sushana Loan Scheme		
	* Self- Employment Initiative Loan Scheme		
	* Any other		
	iii. Micro Finance Sector		
	* Poverty Alleviation Microfinance Project		
	* Small Farmers & Landless Credit Project * Any other		

Annexure 2

Foreign Exchange Rates

Exchange Rates	Rate : Rupees per unit of foreign currency as at						
	Currency notes		**Travellers Cheque/ draft**		**Telegraphic Transfers**		Import Bills
	Buying Rate	Selling Rate	Buying Rate	Selling Rate	Buying Rate	Selling Rate	
Australian Dollar							
Canadian Dollar							
Danish Kroner							
Euro							
Hong Kong Dollar							
Japanese Yen							
New Zealand Dollar							
Norwegian Kroner							
Pound Sterling							
Singapore Dollar							
Swedish Kroner							
Swiss Franc							
United States Dollar							

Annexure 3

Service Charges, Fees & Commissions

	Description	Rs. As at
	SERVICE CHARGES	
Savings Accounts		
	Charges for non-maintenance of minimum account balance as	
Current Accounts		
	Current Account monthly service charge	
	Charges for account statements	
	Cheque issuing cost	
	Stop payment order	
	Return cheques due to insufficient funds etc.	
Remittances		
	Inward credit to Sri Lanka rupee account	
	Inward remmittance to Foreign currency account	
	Issue of foreign currency demand draft, pay order etc.	
Travelers Cheques		
	Encashment of Traveller's cheques	
	Sale of Traveler’s Cheques etc.	
ATMs		
	Issuing Fee	
	ATM cash withdrawal - Own Bank	
	ATM cash withdrawal - Other Bank etc	
Credit Cards - Main cardholder		
	Annual Fee	
	Late Payment charges	
	Interest charges, etc.	
	FEES & COMMISSIONS	
	SLIPS Payment Charged	
	RTGS Payment Charges	
	Facility Arrangement Fees- Overdrafts	
	* Security Backed	
	* Clean Basis	
	Early Settlement Fees	
	* Residential Housing	
	* Vehicle Loans	
	Cheque Purchase Commissions	
	LC Commission	
	*LC Opening Fee & Commission	
	Shipping Guarantees	
	Bank Guarantees	
	Acceptance	

Annexure 4

Code of Conduct for Third Party Agents

1. Introduction

The main objective of recruiting an external institution to act as an Agent of the Bank is, to assist, strengthen and to carry out business processes in a profitable manner.

2. Objective

Objective of this documentation is to introduce a necessary Code of Conduct for the External Company and to its Agents to follow while exercising their assigned duties.

Initiating and following such conduct will result in obtaining a quality output while maintaining professionalism, integrity & goodwill.

3. Definitions

The Bank

People's Bank which was incorporated by the People's Bank Act No 29 of 1961 as amended (hereinafter referred as the "Bank") is the Institution which employs services of an External Agency to assist in carrying out an assigned duty of the Bank.

The Agency

A company duly registered under the Companies Act No 7 of 2007 of Sri Lanka or a partnership , sole proprietorship duly registered in the relevant authorities and approved for its services rendered by the bank, may carry out external activities.

Assigned Duties of Agent(s)

Any business activity stipulated under the agreement with approval granted to engage in business activities related to main business purposes.

4. Conduct and Disciplinary Controls of an External Agency/Agent

The Bank should be informed immediately about all arrangements that are made directly between the Client and the Agency or its representative(s), as well as all the events which are of importance for the proceedings.

As an Agent he/she should always be aware of the relevant rules, regulations and guidelines issued by the Central Bank of Sri Lanka or any other authority which are applicable and should not violate these conditions under any circumstances.

Should always demonstrate a higher degree of honesty, integrity and professionalism during his/her visits to bank clients.

Should have a broad and sound knowledge of the activities which are carried out individually.

Should be equipped with successful negotiation and convincing skills with an attractive personality.

As an Agent he/she should always use a formal dress code during all customer visits.

The Formal dress code should include the following.

- An employee identity card issued by the Agency indicating the Name and the designation.
- A visiting card with contact details of the Agent issued by the Agency.

An Agent should not introduce him/her self as an employee of the bank or any subsidiary company which belongs to the Bank without the written approval or amendment documentation given from the Bank.

If the Agent is appointed to recover monies due to the Bank from customers, an Agent should take the full responsibility while handling and **accepting money** and should always issue an official receipt endorsed by the Bank and also to take necessary precautions to safeguard the same.

An Agent must not take gifts, money, commission or any other benefits from customers of the Bank and/or any other individual.

Agents should always follow and act according to the law, and avoid taking any action prejudicial to the business, integrity, reputation or goodwill of the Bank. Agents should strictly abide to the following conditions/ requirements while carrying out their assigned duties.

- Agents should not make any intimidations or violence – verbally/physically against any individual.
- Third party details (referee details) provided by the Bank should be used for the stated purpose only.
- Agents should not take action against any third party individuals by making pestering phone calls during inconvenient hours, pestering their family members or any other individual related to the customers.
- Shall not give false or misleading information about products/services.
- Shall not unduly influence customers or the general public to buy or get involved in the Bank's products/services.
- Shall not engage in getting any security documents signed outside the Bank.

5. Secrecy of information

The agency is hereby bound and obliged to safeguard any information deemed sensitive in the process of issuing, acquiring merchants or at debt recovery to the best of the conduct and knowledge of the Agents deployed to attempt such duties.

In conjunction of the above an Agent shall abide by the following aspects pertaining to the process.

- Shall not discuss, promote, print or publish by any means what so ever any information pertaining to any customer details.

Any information not included in this documentation and any adherence to be complied with relation to the Code of Conduct should be simultaneously referred along with the initial Agreement signed and verified by the Agency with the Bank.

6. Rules, Regulations and Guidelines issued by the Central Bank of Sri Lanka and any other Authority

The company shall adhere to any other rule, regulation or guideline issued by the Central Bank of Sri Lanka or any other relevant authority from time to time.

Annexure 5

Credit Card Guidelines No: 01/2010

Credit Card Operational Guidelines

1. Introduction to the Guidelines

Over the past few years, the usage of Cards as a payment instrument for purchasing goods and services and/or cash withdrawals has increased significantly mainly due to the growing preference of the general public to use Credit Cards for their day to day transactions. The increase has been driven by customer convenience and transaction security. This is further evidenced by high increase in the volume of electronic Point Of Sales outlets (POS), and reward schemes and incentives offered by Credit Card issuers, to promote Credit Card usage. Central Bank of Sri Lanka (CBSL) through the Payment and Settlement Systems Act No. 28 of 2005 is entrusted with a legislative mandate to implement the national payment system policy and oversee the payment and settlement systems in the country to ensure safety, efficiency, competitiveness and stability. Having considered the timely requirement of improving the electronic payment mechanisms and at the same time ensuring customer protection, the CBSL took steps to execute the Service Providers of Payment Cards Regulations No. 1 of 2009 on 31 July, 2009. Following guidelines on operations of Credit Cards are issued by the CBSL, in order to ensure safe, secure and efficient operations when Credit Cards are used as a payment instrument. These operational guidelines for Credit Cards which are based on the above mentioned Regulations shall apply to all Service Providers engaged in Credit Card business and shall come into force with effect from **01 March, 2010**. In these guidelines words denoting or importing the singular number shall include the plural number and vice versa and words denoting or importing the masculine gender shall include the feminine.

2. Marketing of Credit Cards

Any institution (hereinafter referred to as "Card Issuer") enters into a contractual relationship with a Cardholder (hereinafter referred to as "the Customer") through the issue of a Credit Card shall ensure that marketing strategies of the Credit Card operations are designed and undertaken in accordance with the following guidelines.

2.1. Marketing staff shall disclose their official identity at promotional campaigns before or during the meeting with prospective and/or existing Customer.

2.2. Benefits, incentives, rewards or reduction of any charges / fees which are offered by the Card Issuers in any promotional campaign or any event with regard to Credit Card operations shall be clearly communicated to the Customers in legible writing (electronically or document form).

2.3. The terms and conditions relating to the Credit Card shall be clearly communicated to the Customers and the same shall be provided in writing in the preferred language of

communication, on request. The terms and conditions shall be displayed in the Card Issuers" web sites.

2.4. Card Issuers shall disclose their Code of Conduct/Institutional Policy on Credit Card operations to the Customers throughout the marketing process and the same shall be published in Card Issuers" official websites.

2.5. Marketing personnel of Card Issuers shall provide complete information on features, benefits and drawbacks to the Customers and shall not make false claims on any features / benefits which Card Issuers do not offer.

2.6. Misleading and unethical information/advertisements shall not be conveyed/ published by Card Issuers.

2.7. Card Issuers shall not engage in aggressive and hard selling marketing practices during working/office hours or inconvenient hours for the Customers, except with prior appointments.

2.8. Regular training and awareness sessions shall be conducted by Card Issuers for their marketing staff covering all aspects of Credit Card operations including charges to be paid by the Customers, safety measures, complaint/dispute resolution mechanisms etc.

3. Issue of Credit Cards

(a) Issue of Principal Credit Cards

3.1. Credit Card shall be issued only to an individual who has following eligibilities –

- a citizen or a resident of Sri Lanka who is above 18 years of age on the date of the application and has independent financial means;
- a non-resident provided that he has a Non Resident Foreign Currency Account/Resident Foreign Currency Account/Resident Non National Foreign Currency Account or Off Shore Banking Unit Account and all dues of the Credit Card are settled in foreign currency through such accounts.

3.2. Card Issuers shall be solely responsible for fulfillment of all "Know Your Customer" (KYC) requirements and such documents shall be maintained under safe custody.

3.3. Card Issuers shall not accept funds as deposits from the Customers at any time, in any way that contravene the provisions of the Banking Act and the Finance Companies Act.

3.4. Credit Card shall be issued by a Card Issuer on receipt of duly filled and signed application form from a prospective Customer, supported with necessary documents. Pre-approved cards shall be activated only after receiving of Customer′s signed acceptance. Unsolicited cards shall not be issued.

3.5. Card Issuer shall take utmost care in ascertaining credit worthiness of Customers. Credit risks shall be assessed independently, before issuing a Credit Card, taking all reasonable steps and using reliable modes to assess the creditworthiness of the Customer. Card Issuer shall obtain information available at the Credit Information Bureau (CRIB) to ascertain the creditworthiness of the Customer.

3.6. Card Issuer shall not issue a Credit Card to any Customer who has already obtained a Credit Card from same/any other Card Issuer by providing the same income particulars, without obtaining the aggregate credit outstanding liabilities of the Customer.

3.7. Card Issuer shall determine the credit limit for the Customer considering the cumulative limits enjoyed by the Customer from other Credit Cards on the basis of Customer"s self declaration and credit information obtained from the CRIB.

3.8. The prevailing credit limit may be increased temporarily subject to a maximum time limit of 6 months on the request of the Customer, based on the nature of the requirement. However, Card Issuer should be satisfied with the Customer′s ability to settle all the liabilities incurred on such extended facility.

3.9. Card Issuer shall not unilaterally upgrade or/and enhance Credit Card type/limit without informing the Customer in writing.

3.10. At the time of issuing a Credit Card to a Customer, applicable terms and conditions relating to the Credit Card shall be clearly communicated and same shall be provided in legible font size to the Customer in the preferred language of the Customer, even though such details have already been provided during the marketing campaign.

3.11. Any stipulation, caveat, clause or provision in terms and condition of the agreement/contract, which may result in an unreasonable curtailment of rights of the Customers, shall not be included.

3.12. Card Issuer shall notify the following details in simple language to Customers, in writing (electronically or in document form) and same shall be published in the web sites maintained by Card Issuer:

i. Benefits / services provided to the Customers;
ii. Terms and conditions as well as important information that the Customers shall be aware of in using the card and the consequences and risks;
iii. Rights, liabilities and obligations of the Principal Customers and Supplementary Customers;
iv. Joining fees, annual fees, administrative and handling fees or any other fees which the Customers are required to pay;
v. Cash advance limit and fee as appropriate;
vi. Interest free (grace) period;
vii. Calculation method of minimum payment;
viii. Calculation methods of overdue interest regarding both revolving credit (amount outstanding after paying the minimum payment) and cash advance, applicable annualized

interest rates and penalties/fees which have to be borne by the Customers. The calculation method of overdue interest shall be expressed clearly using examples;

ix. The late payment charges and the method of calculation of such charges with examples;

x. Method of computation of interest when partial payments exceeding the minimum payment due is paid by the Customer, with examples;

xi. The procedure for handling lost, stolen or destroyed Credit Cards and other complaints, and the time period required for dealing with such complaints;

xii. Contact numbers of dedicated telephone lines for handling complaints;

xiii. The rights and liabilities arising out of unauthorized third party use of a Credit Card ;

xiv. The procedure to be followed in the event of a discrepancy/dispute regarding a Credit Card transaction;

xv. Disadvantages for the Customers if they default i.e. Reporting procedures to CRIB etc.;

xvi. Procedure for cancellation of the Credit Card.

3.13. Card Issuers shall not encourage/ induce the Customers to use Credit Cards to acquire land or any other property, payment of monthly installments of any property acquired by the Customers or any third party, and/or any capital account transaction specified in the Exchange Control Act, Regulations, Directions or Guidelines issued by the relevant authorities.

3.14. Card Issuer shall state in the terms and conditions that Credit Cards are not to be used for any unlawful activity deemed as an offence under Sri Lankan Law. If any Customer is found to have used the Credit Card for such unlawful activity, Card Issuer shall immediately terminate the card facility and inform details of such transaction to the CBSL.

(b) Issue of Supplementary Credit Cards

3.15. Card Issuers shall give clear instructions to Principal/Supplementary/Add-on Customers on their responsibilities for liabilities incurred on the cards issued. The Principal Customer shall also be informed that they are ultimately liable for all the liabilities incurred by the Supplementary/Add on Customer.

3.16. Card Issuer shall not issue a supplementary, add-on or subsidiary card to any individual who is below eighteen (18) years of age except to students who are between 16 - 18 years of age and for educational purposes. Such exceptions shall be granted only for students who are direct dependents of the Principal Customer.

4. Interest Rates and Other Charges

4.1. Card Issuer shall quote interest rates and service charges separately on an annual basis, for purchase of goods or services and cash advance.

4.2. Card Issuer shall not charge any amount that was not explicitly indicated to the Customers at the time of issue of the Credit Card without prior notice to the Customer. However, this consideration will not apply for charges such as taxes, etc., levied by the government or any other statutory authority, time to time.

4.3. Prior notice shall be given to the Customers before offering any new charged service.

4.4. Any revisions in the schedule of charges/fees, interest rates, or terms and conditions and revision of any incentives, shall be communicated to all active Customers in legible writing/electronic means, at least ten (10) days before the effective date of the revision, if it was not communicated at the time of issue.

5. Billing Process

5.1. Card Issuer shall dispatch a billing statement on Credit Card transactions to each active Customer in writing or through electronic means at the end of each billing cycle (period). The billing statements shall fully disclose the following details:

i. Transaction date, merchant name, type of currency and amount billed;
ii. Date from which interest accrues;
iii. The calculation method regarding charges to be borne by the Customer;
iv. Amount of minimum payment to be made by the Customer;
v. Due date of minimum payment;
vi. Annualized percentage rate of interest for purchase of goods/ services and cash advances. (The said charges shall be included separately);
vii. Amount of penalty and interest charges for late payments;
viii. Acceptable modes of payment (i.e. through cash, direct debit, cheques, account transfer facility);
ix. Expected number of days a particular mode of payment may take for clearing and handling charges if any;
x. In the case of foreign currency transactions foreign currency amount and billed amount in LKR.

Format of the billing statement shall be published in the Card Issuers web site in all three languages.

5.2. Card Issuers are required to dispatch the billing statement at the end of each billing period to all active Customers at least fourteen (14) days before the payment due date.

5.3. If the Customer lodges a complaint regarding non-receipt of current billing statement of account, a copy of the statement shall be dispatched to the Customer free of charge, within ten (10) calendar days from the date of complaint.

5.4. Card Issuer shall make comprehensive and convenient arrangements in line with the business plan and requirements of the Customers for the collection of bill payments through designated branches, collection centers, cheque collecting boxes or other electronic channels provided by the Card Issuer.

5.5. Card Issuer shall inform the Customers about the status of the unrealized cheques within seven (7) working days from the date of receipt of unpaid cheques. Customer shall not be penalized for cheques submitted within the time prescribed by the Card Issuer but cleared after due date.

5.6. Card Issuer shall ensure that "due date" for payment does not fall on Saturday, Sunday or any other public/bank holiday(s) published/ gazetted by the CBSL/Government at the beginning of each year. However, if a Card Issuer is unable to adhere to this condition, the date payable has to be clearly mentioned in the statement, when the due date falls on a holiday.

6. Collection /Recovery Mechanism

6.1. Card Issuer shall ensure that collection of any dues against Credit Card transactions by Card Issuer are conducted prudently. Card Issuer shall not engage in any activity which is against the public interest in handling collections and shall exercise its rights using the principles of honesty and good faith.

6.2. Card Issuer shall ensure that recovery letters are issued to the last known address of the Customer and such letters should bear the designation, contact number(s) and office address of the concerned official.

6.3. Card Issuer shall ensure that the recovery process shall not resort to any verbal or physical harassment or threats to the Customers, their family members, referees or friends.

6.4. Card Issuer shall respond to the queries arising out of the recovery letters within a reasonable time period. The time period must be specifically defined in their Code of Conduct and shall be communicated properly to the Customers.

6.5. Procedure followed by the Card Issuer when recovering default payments shall be properly communicated to Customers, at the time of issuance of Credit Card. Card Issuers shall not divulge information regarding Credit Card defaults to third parties.

7. Confidentiality and Protection of Customer Rights

7.1. Card Issuer shall maintain the confidentiality of Customer information and shall be responsible for all such information used by marketing personnel, debt recovery agents or any other third party in the business process.

7.2. Card Issuer shall not reveal any information/contact details relating to Customers, obtained at the time of opening/issuing the Credit Card to any other person or organization without obtaining prior consent of the Customer. Card Issuer should satisfy themselves, based on specific legal advice, that the information being sought from third parties will not violate the provisions of the laws relating to secrecy in the transactions.

7.3. Unsolicited loans or other credit facilities shall not be offered to the Customers based on the Credit Card.

8. Dispute Resolution

8.1. Card Issuer shall have an appropriate dispute resolution mechanism and service procedures in place, commensurate with the volume of complaints and shall resolve the same within a minimum period.

8.2. Credit Card dispute resolution mechanism shall be disclosed on the official website of the Card Issuer. Card Issuer may also arrange online complaint registration procedure. Card Issuers shall develop a mechanism for tracing a complaint and same shall be communicated to the Customer.

8.3. Card Issuer shall resolve the disputed transactions of the Customer promptly and as per the franchise rules of VISA, MasterCard, AMEX or any other international card company/association, taking into account the nature of the transaction, distances, time zones, etc.

8.4. Card Issuer shall clearly communicate to the Customers, whether they would be allowed to use the Credit Card during the investigation period in the event of a dispute.

8.5. Card Issuer shall reverse interest and other charges on disputed transactions if the dispute is settled in favour of the Customer and accumulated interest shall be recovered only when the dispute is settled in favour of the Card Issuer.

8.6. Card Issuer shall provide related evidence regarding disputed transactions to the Customer without any charges, if complaint is settled in favor of the Customer.

9. Outsourcing of marketing/recovery functions and other operations

9.1 Card issuer may outsource marketing, recovery, and other operations such as card embossing, processing of applications and courier service to third party service providers.

9.2 Card Issuer shall clearly define the responsibilities and liabilities of the outsourced service providers.

9.3 Card issuer shall ensure the maintenance of confidentiality and secrecy of the customer information by outsourced service providers.

9.4 Card issuer shall ensure that the outsourced service providers adhere to the guidelines given in Section 2 and 6 above with regard to marketing and collection/recovery mechanisms respectively.

9.5. Card Issuer shall ensure that employees of outsourced service providers are properly educated and trained on their responsibilities such as soliciting customers, convenient hours for calling, conveying the correct terms and conditions applicable to Credit Card operations.

9.6 Card issuer shall have an exit mechanism for outsourced activities, if it is observed that an outsourced service provider is unable to continue the service.

10. Rights to impose non-compliance charges

Under the provisions of the Payment Card Service Providers Regulations No. 1 of 2009, CBSL reserves the right to impose non-compliance charges on Card Issuers on any violation of these guidelines.

11. Legal Provisions

11.1. Card Issuer shall have sound legal basis for Credit Card operations together with appropriate rules and procedures.

11.2. Appropriate processes shall be in place to ensure that rules and procedures as well as the contractual relationships with relevant parties (e.g. financial acquirers and card issuers, merchants and cardholders) shall be valid and enforceable. Where applicable, this shall be consisted of clear rules and procedures to regulate authorization and clearing and settlement of both domestic and cross-border transactions.

12. Business Continuity, Internal Control and Compliance

12.1 Card Issuer shall have sound and prudent management, administrative, accounting and control procedures to minimize financial and non-financial risks to which the Card Issuer may be exposed.

12.2 Card Issuer shall conduct risk analysis and feasibility study on new products/services. In addition, when there is a change of relevant circumstances, Card Issuer shall perform a review on the risk profile of existing products/services to assess risks relating to security and continuity of the product/service.

12.3 Card Issuer shall ensure to have an adequate number of properly trained and competent personnel to operate systems at an appropriate level.

12.4 Card Issuer shall provide Customers and relevant merchants with information the Card Issuer reasonably considers relevant to fraud awareness in the context of Credit Card operations and proper use or processing of cards to reduce the risk of fraud.

12.5 Card Issuer shall have comprehensive, rigorous and well-documented operational and technical procedures to address reasonable operational reliability, integrity of network and timeliness of transactions in case of malfunctions, system interruption and transmission failures or delays. Card Issuer shall also have in place a reasonable, effective, well-documented and regularly-tested business contingency plan to be used in the event of unforeseen interruption.

12.6 Card Issuer shall have a thorough due diligence and oversight process for managing outsourced relationships, if the Card Issuer considers that it may affect the operation of the Credit Card system.

12.7 Card Issuer shall design technical systems for Credit Card processing with sufficient capacity to continue ongoing operations, which shall be monitored periodically and upgraded when the Card Issuer considers reasonably necessary.

12.8 Card Issuer shall have sufficient clearing and settlement arrangements to enable efficient, reliable and secured operation of the Credit Card system.

12.9 Card Issuer shall review the security objectives, policies and operational services periodically.

12.10 Card Issuer shall ensure to perform an annual self-assessment of the Card Issuers compliance with the Regulations, Guidelines and Code of Conduct. Internal auditors, internal compliance officer or appointed independent assessor shall perform this self-assessment as part of their on-going functions.

12.11 Card Issuer shall have clearly defined and documented organizational arrangements, such as ownership and management structure and shall operate as the Card Issuer deems fit, with appropriate segregation of duties and internal control arrangements so as to reduce the likelihood of mismanagement and frauds.

12.12 Card Issuer shall have reasonably effective measures and controls to ensure compliance with these guidelines and their Code of Conduct.

13. General Conditions

13.1 The clearing of International Credit Cards issued and used in Sri Lanka shall be made in Sri Lankan rupees. The clearing of International Credit Cards issued in Sri Lanka and used in foreign countries or issued in foreign countries and used in Sri Lanka shall be made in the relevant foreign currency authorized by the respective principles.

Appendix: Most Important Terms (MITs)

a. "Cardholder" means any person authorized to use a Credit Card issued by a Card Issuer;

b. "Card Issuer" means an institution which issues a Credit Card and thereby enters into a contractual relationship with a Cardholder;

c. "Central Bank of Sri Lanka (CBSL)" means the Central Bank of Sri Lanka established under the Monetary Law Act. , No. 58 of 1949 (Chapter 422);

d. "Credit Card" means a payment card which indicates a line of credit granted by the Issuer to the Cardholder and where the Cardholder may settle the credit utilized in full or in part, before a specified date. Any amount of the credit utilized by the Card holder and not settled in full on or before the specified date, may be subject to interest, profit or other charges;

e. "Day" means a calendar day;

f. "Direct Dependent" is a child of a Principal Cardholder or a child whose guardian is the Principal Cardholder;

g. "Licensed Commercial Bank (LCB)" means a company or a body corporate licensed under the provisions of the Banking Act, No. 30 of 1988 to carry on banking business in Sri Lanka;

h. “Licensed Specialized Bank (LSB)” means any company or a body corporate which has been issued with license under the provisions of the Banking Act, No. 30 of 1988 to carry on the business of accepting deposit money and investing and lending such money;

i. “Principal” is a person, who is the sole owner of brand rights of the Credit Card;

j. “Unsolicited cards” means a Credit Card issued without obtaining signed acceptance from the Cardholder;

k. “Unsolicited Loans” means loans granted without obtaining signed acceptance from the Customer.

Annexure 6

Complaint Record Book

Date	Name/Account No of complainant	Substance of complaint	Responsible officer’s name and service number	The nature of bank’s response	Date of bank’s response	Lessons learned & procedures changed

Annexure 7

The Financial Ombudsman, Sri Lanka

The Financial Ombudsman has the power to inquire into and settle any complaints and disputes between individual customers and the financial institutions covered by the Ombudsman Scheme.

The present holder of this office is Dr. R. B Ranaraja.

The financial Ombudsman can be contacted via the following.

Address:	No 143A, Vajira Road, Colombo 5.	
	Telephone:	+94 11 259 5624
	Telefax:	+94 11 259 5625
	Email:	fosril@sltnet.lk
	Website:	www.financialombudsman.lk

Annexure 8

Credit Counseling Centre

The Credit Counseling Centre established by The Sri Lanka Banks' Association (SLBA) as a social initiative, is aimed at assisting individuals and companies to manage their debt.

Address:	UPADESHANA Credit Counseling Centre Center for Banking Studies, No 58, Sri Jayawardhanapura Mw, Rajagiriya
Telephone:	+94 11 2887 006-7
Fax:	+94 11 2873 247
Email:	upadeshana@gmail.com
Website:	www.slba.lk

ACKNOWLEDGEMENT OF THE CODE OF CONDUCT FOR CUSTOMER PROTECTION

I

……
……

(Name)

of

……
……

(Address)

being an employee of the People's Bank do hereby acknowledge receipt of a copy of the Code. I further agree that I have understood the provisions contained herein and agree to abide by this Code at all times.

Declared on this …….. day of …… …… 20…..

at …….

(Place)

……..
……

(Signature of Declarant) (Service No.)

*Original to be retained in the personal file of the employee with a copy to be retained in the Branch/ Department.

STRICTLY CONFIDENTIAL

Compliance Assessment Checklist for Branch

	Name of Branch & Code
Region & Region code:	
Date of Assessment:	
Period assessed:	
Arrival:	
Departure:	
Assessment Number:	

From Questions 1-10

Score	Rating
1	Yes
2	No

		Score	***Comments***
1	**Pawning**	**#**	**#**
*	Display of Opening and Closing time		
*	Bulk Pawning not conducted at the branch		
	Display of	**#**	**#**
*	Market value of sovereign gold		
*	Interest Rates		
*	Pound value of each carat		
	Maintenance of books	**#**	**#**
*	Stock book		
*	Sales book of pledges		
*	Issue of the pawning ticket with counterfoil and counterfoil should be signed by the pawner		
*	Proper maintaining of unclaimed balance records in the book (check with suspense account)		
*	Quarterly article verification		
*	Safes are under dual control		
*	Time lock book		
2	**Customer complaints (7606/2015)**	**#**	**#**
*	A book/ box maintained		
*	Compliant Management book maintained		
*	Action taken for recorded complaints		
3	**Display of rates of others (7051/2011)**	**#**	**#**
*	Interest rates		
*	Exchange rates		
*	Service charges, fees & commissions		
*	Credit rating		
	Update of rates & others	**#**	**#**
*	Interest rates		
*	Exchange rates		
*	Service charges, fees & commissions		

		Display of followings	**#**	**#**
	*	Bank license		
	*	Ombudsman Notice & Credit Counseling Center Notice		
	*	Profit & Loss Statement		
	*	Banking hours & holidays notices		
	*	Information on RTI committee (1246/2017)		
4		**Language proficiency**	**#**	**#**
	*	Branch has Tamil/Sinhala proficient staff members		
5		**Position of old KYC updating (7349/2013 & 7004/2011)**	**#**	**#**
	*	Book maintained for accounts opend without obtaining KYC		
	*	Stepes taken to update KYC		
	*	Stepes taken to review the existing KYC when required		
6		**Avabilabiity of Intranet access to all staff members**		
7		**Western Union Transactions (996/2013)**	**#**	**#**
	*	Book maintained for recording		
	*	Copies filed seperately (application & ID copy)		
	*	Form 2 Obtained		
8		**Attendance register maintained properly**		
9		**Beneficial owner details (1341/2019)**	**#**	**#**
	*	Details obtained in mandate		
	*	Details maintained in BTS		
10		**Unregistered society book maintained (CSA)**		

From Questions 11-28

Score	Rating
1	Excellent
2	Very Good
3	Good
4	Average
5	Poor

11		**Status of Mandates**	**#**	**#**
	*	Covered by checklist		
12		**Accuracy of KYC's**	**#**	**#**
	*	Covered by checklist		
13		**Risk Categorization**	**#**	**#**
	*	Incorrect		
	*	Not Done		
	*	Incomplete		
14		**Declaration for FATCA obtained & marked (1120/2014(2))**		
15		**Checked from AML system**		
16		**Checked from PEP list**		

17	**Knowledge on STR's (6795/2009(1))**		**#**	**#**
	*	Attended training and has knowledge of method of informing		
	*	Transaction have been monitored by the branch		
	*	Identified suspicious transactions duly and timely reported to compliance		
	*	Taken steps in compliance with the instructions issued on under-surveillance accounts		
18	**Staff dressed according to Code of couduct**			
19	**Staff wearing ID according to Code of Conduct**			
20	**Official Language commission regulations followed (All displays/ notices for customers should be in Sinhala & Tamil)**			
21	**Monitoring of over Rs. 200,000/- transactions**			
	*	Required information obtained for 3rd party deposits		
22	**Action taken for abandoned property**			
23	**Minor Accounts (938/2012)**		**#**	**#**
	*	Birth Certificate obtained for all accounts		
	*	ID copy of guardian obtained		
	*	KYC completed		
24	**CRIB**		**#**	**#**
	*	User ID's have been taken for 2 staff members who are currently present at the branch / staff member curently present at the service centers		
	*	All outstanding CRIB charges have been cleared		
25	**Over Rs. 1Mn report - Compliance with circular No. 1299/2018(1),1254/2017(1)**		**#**	**#**
	*	Daily report checked (P0105,P3004 & P3005)		
	*	Information completely updated in the system		
	*	Reports are submitted within the given time period		
26	**goAMl 3rd party clear**			
27	**AML system (8154/2018)**		**#**	**#**
	*	Active 2 passwords available at branches		
	*	Register maintained on password		
	*	Branch has cleared all alerts		
	*	If pending for more than 3 days, valid reasons are available		
28	**Compliance log book maintained & actions taken for the findings of the RCO**			
Total risk of the branch				**#**

Risk Rating

(%)	Rating	No of Errors	Topic
			Section 01 - **Mandate** *(11)*
			Section 02 - **KYC** *(12)*
			Section 03.1 - **Incorrect** *(13.1)*
			Section 03.2 - **Not Done** *(13.2)*
			Section 03.3 - **Incomplete** *(13.3)*
			Section 04 - **FATCA** *(14)*
			Section 05 - **Check AML** *(15)*
			Section 06 - **Check PEP list** *(16)*
			Total No of Citizen Fixed Deposits Mandates

(%)	Rating	No of Errors	goAML 3rd party clear *(26)*
			Total Transactions Completed
			Total Transactions

Name of Manager:	
Name of Operations Manager:	
Name of Assessor:	
Service Number:	
Signature of Assessor:	

-

Non Compliances are marked with "1"

NO	Section	01										02					03			04		05	06
	Account No	Mandate										KYC					Risk Categorization			FATCA		AML	PEP
		Manager not signed	Incomplete	Customer not signed	ID not obtained	Utility bill not taken	Address far	Address Incomplete	Employment	Customer Photograph	ID both sides available	Blank	Incomplete	Incorrect	PEP	FATCA Not Marked	Incorrect	Not Done	Incomplete	Declaration Not Obtained	Marked the Relevant Section	Check AML	Check PEP
1																							
2																							
3																							
4																							
5																							
6																							
7																							
8																							
9																							
10																							
11																							
12																							
13																							
14																							
15																							
16																							
17																							
18																							
19																							
20																							
21																							
22																							
23																							
24																							
25																							

-

Non Compliances are marked with "1"

NO	Section	01										02					03			04		05	06
	Account No	Mandate										KYC					Risk Categorization			FATCA		AML	PEP
		Manager not signed	Incomplete	Customer not signed	ID not obtained	Utility bill not taken	Address far	Address Incomplete	Employment	Customer Photograph	ID both sides available	Blank	Incomplete	Incorrect	PEP	FATCA Not Marked	Incorrect	Not Done	Incomplete	Declaration Not Obtained	Marked the Relevant Section	Check AML	Check PEP
26																							
27																							
28																							
29																							
30																							
31																							
32																							
33																							
34																							
35																							
36																							
37																							
38																							
39																							
40																							
41																							
42																							
43																							
44																							
45																							
46																							
47																							
48																							
49																							
50																							

-

Non Compliances are marked with "1"

NO	Section	01										02					03			04		05	06
	Account No	Mandate										KYC					Risk Categorization			FATCA		AML	PEP
		Manager not signed	Incomplete	Customer not signed	ID not obtained	Utility bill not taken	Address far	Address Incomplete	Employment	Customer Photograph	ID both sides available	Blank	Incomplete	Incorrect	PEP	FATCA Not Marked	Incorrect	Not Done	Incomplete	Declaration Not Obtained	Marked the Relevant Section	Check AML	Check PEP
51																							
52																							
53																							
54																							
55																							
56																							
57																							
58																							
59																							
60																							
61																							
62																							
63																							
64																							
65																							
66																							
67																							
68																							
69																							
70																							
71																							
72																							
73																							
74																							
75																							

-

Non Compliances are marked with "1"

NO	Section	01										02					03			04		05	06
	Account No	Mandate										KYC					Risk Categorization			FATCA		AML	PEP
		Manager not signed	Incomplete	Customer not signed	ID not obtained	Utility bill not taken	Address far	Address Incomplete	Employment	Customer Photograph	ID both sides available	Blank	Incomplete	Incorrect	PEP	FATCA Not Marked	Incorrect	Not Done	Incomplete	Declaration Not Obtained	Marked the Relevant Section	Check AML	Check PEP
76																							
77																							
78																							
79																							
80																							
81																							
82																							
83																							
84																							
85																							
86																							
87																							
88																							
89																							
90																							
91																							
92																							
93																							
94																							
95																							
96																							
97																							
98																							
99																							
100																							

People's Leasing and Finance PLC

	DIRECTIONS		Compliance Status	Comments	
	Licensing				
	Annual License Fee(1 of 2015)				
1	Has the Annual License Fee (based on total assets as per the following table) been paid to the Central Bank of Sri Lanka (on or before 31st December of the preceding calendar year)?				
	Total Assets	**Annual License Fee (Rs)**			
	Rs.5 billion or below	1,000,000/-			
	Above Rs.5 billion up to Rs.10 billion	1,500,000/-			
	Above Rs.10 billion up to Rs.20 billion	2,000,000/-			
	Over Rs. 20 billion	3,000,000/-			
	Capital				
	Capital Funds (1 of 2003)				
2	Does the company maintain capital funds of more than 10% of deposit liabilities at all times?				
3	Does the company maintain a reserve fund?				

4	Does the company Transfer funds to the reserve fund out of the net profits of each year, after due provision has been made for Taxation and Bad and Doubtful Debts, (based on capital funds to deposit liabilities ratios) based on the following?			
	Capital Funds	**Amount to be transferred**		
	More than 25% of total deposit liabilities	5%		
	10% to 25% of total deposit liabilities	20%		
	Less than 10% of the total deposit liabilities	50%		
	Capital adequacy ratio (No 3 of 2018)			
5	Has the Company maintained the minimum Capital Adequacy Ratio, at 8.00%, for Tier 1 Capital and at 12.00% for Total Capital since 01.07.2019.?			
6	Does the Company report to CBSL, through the web based system, using the format specified in the Act Directions No.03 of 2018 on or before 15th day of every month? [Position should be shown as at the last calendar day of each month.]			
	DIRECTIONS			
	Minimum core capital(2 of 2017)	**Compliance Status**	**Comments**	
7	Is the unimpaired core capital of the company not less than Rs. 1.5 billion by 01.01.2019.? (Rs. 2.00 billion by 01.01.2020 and Rs. 2.5 billion by 01.01.2021)			

	Credit			
	Classification and Measurement of credit facilities (No 01 of 2020)	**Compliance Status**	**Comments**	
8	Has the company made provisions for accommodations classified as non-performing?			
9	Is the company comply with minimum specific provisioning requirement as follows : Specific mention 5% Substandard 20% Doubtful 50% Loss 100%			
	Single Borrower limit (4 of 2006)			
10	Does the company adhere to the following single borrower limit requirements?			
	Maximum limit			
	Individual borrower 15% of the capital funds			
	Group of borrowers or subsidiary companies and/or associate companies 20% of the capital funds			
	Aggregate of single accommodations granted to individuals, groups, subsidiary companies and/or associate companies each of which exceed 10% of capital funds 50 % of the total outstanding accommodations			

	Maximum of a single unsecured accommodation or the aggregate of unsecured accommodations outstanding at any point of time from a single borrower 1 % of the core capital			
	Aggregate of unsecured accommodations outstanding at any point of time from all borrowers 5 % of the capital funds			
	DIRECTIONS	**Compliance Status**	**Comments**	
	Lending (1 of 2007)			
11	Has the company granted any accommodation; (i) to a director and/or a relative of a director of the finance company; (ii) to its holding company; (iii) on the security of its own shares or on the security of the shares of any of its subsidiary companies; (iv) to purchase its own shares; or (v) on the guarantee or indemnity of a director of the finance company, a relative of a director of the finance company or any employee of the finance company.			
12	Has the company granted any accommodation for the purchase of or subscription for fully paid shares in the finance company being a purchase or subscription by Trustees of or for shares to be held by or for the benefit of, employees of the company? If yes has prior approval of the director been obtained? Does the aggregate amount of accommodation exceed the equivalent of 10% of the total amount of the issued and paid up share capital of the finance company or 10% of the unimpaired adjusted capital funds of the finance company as per its last audited balance sheet, whichever is greater?			
13	Has the company recovered on any accommodation and /or charges of any description, other than interest, in excess of 5 % of the principal amount granted?			

	Investments			
	Investments (7 of 2006)			
14	Do the investments made in the ordinary shares of another company exceed 5 % of the capital funds of the finance company as shown in the last audited balance sheet?			
15	Does any such investment exceed 40% of the issued ordinary share capital of such investee company?			
16	Does the aggregate amount invested in the issued ordinary share capital of companies exceed 25 % of the capital funds of the finance company as shown in its last audited balance sheet?			
	Liquidity			
	Liquid assets (1 of 2009)4 of 2013/ 2 of 2020/ 7 of 2020			
17	Does the Company comply to the requirement that Daily Liquid assets should not be less than the total of; i) 6% of outstanding value of time deposits received by the finance company and the face value of certificates of deposit issued by the finance company; as appearing on the books of the finance company at the close of the business on the day AND ii) 10% of the outstanding value of savings deposits accepted by the company, at the close of the business on the day?			

	DIRECTIONS	Compliance Status	Comments	
18	Does the company maintain, in the form of Sri Lanka Government Treasury Bills, Sri Lanka Government Securities and Central Bank of Sri Lanka Securities, 5% of the average of its month end total deposit liabilities & borrowings of the twelve months of the preceding financial year?			
19	Are the above Sri Lanka Government Treasury Bills, Sri Lanka Government Securities and Central Bank of Sri Lanka Securities kept in the custody of one or more licensed commercial banks or one or more primary dealer companies?			
	Operational			
	Writing off of loans and advances (3 of 1991)			
20	Has the prior approval of the Monetary Board been obtained for writing off of the following types of loans or advances granted to any of the under noted persons or institutions? (a) any directors or any relative of such director; (b) any undertaking in which any director has an interest as a director, partner, manager, agent, investor, guarantor or a shareholder; (c) any subsidiary, associate or connected concerns or to companies corporate or unincorporated where the directors of a finance company hold directorships, shares or other investments; (d) any person who is a manager, officer or an employee of a company registered under the Finance Companies Act, No. 78 of 1988.			
	Register of written off loans (10 of 1991)			
21	Does the company maintain a register showing details of written off loans or advances from its books?			
22	Are they reported properly to the Director, Dept of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka?			

	Deposits (No. 1 of 2005)			
23	Does the company have any deposits except savings deposits repayable on demand or any time deposit repayable after a period of less than one month or more than sixty months from the date of receipt of such deposit? (1<deposits (months) <60)?			
24	Does the company issue a certificate to every depositor for each and every time deposit and a renewal notice in case of renewal?			
25	Are all such certificates or renewal notices signed by two officers who are authorized by the Board of Directors for the purpose of accepting/renewing deposits and issuing of such acknowledgment/renewal notice?			
	DIRECTIONS	**Compliance Status**	**Comments**	
26	Does the Renewal notice/ certificate contain the following? (a) registered name and address of the finance company; (b) date of deposit/renewal of deposit; (c) name of depositor, national identity card number or passport number and the address of the depositor; (d) amount of money received by the finance company by way of deposit or renewal of deposit in words and figures; (e) the annual rate of interest payable and the basis of payment (monthly or at maturity); (f) date on which the deposit is repayable; (g) names of officers who sign the acknowledgment/renewal notice; (h) serial number of the certificate; (I) account number of the deposit			

27	Are records maintained in respect of each time deposit containing the following? (a) Account number; (b) Name, address and national identity card number or passport number of each depositor; (c) Principal amount of such deposit; (d) Date of deposit/date of renewal; (e) Duration and the maturity date of each deposit; (f) Rate of interest and the basis of payment of interest (monthly or at maturity); (g) The amount of accrued interest (if any); (h) Date and amount of each payment (principal and/or interest); (I) Serial number of the certificate			
28	Does the company issue upon acceptance of savings deposits , a document containing the terms governing the operations of savings accounts in all three languages and a pass book for recording the operations of the account including the following particulars :– (a) Registered name and address of the finance company; (b) Name of the branch; (c) Name, date of birth, National Identity Card number and the address of the account holder; and (d) Account number			
29	Does the company maintain following records in respect of each savings account? a) Name, date of birth, national identity card number and the address of the account holder ;(b) Account number ;(c) Date, amount and description of every credit or debit made to the savings account; and(d) Outstanding balance at any particular time.			

	DIRECTIONS	Compliance Status	Comments	
	Business Transactions with Directors and their Relatives(2 of 2007)			
30	Has the company conducted any business transactions with a director of the company or a relative of a director of the company where the total value of transaction/s exceeds Rs.50, 000 per month or Rs.500, 000 for a financial year? (N/A to time and savings deposits)			
31	If so has the approval of the director of the Department of Supervision of Non-bank financial institutions been obtained?			
	Insurance of Deposit Liabilities (2 of 2010)			
32	Has the company insured deposit liabilities in the Deposit Insurance Scheme?			
33	Has the company disclosed to the public in advertisements soliciting deposits, the fact that eligible deposit liabilities have been insured with the Sri Lanka Deposit Insurance Scheme on payment of the applicable premium for compensation up to a maximum of Rs. 600,000.00 per depositor?			
	Information systems security Policy (4 of 2012)			
34	Does the company maintain an Information Systems Security Policy (ISSP) as stipulated by the Central Bank?			
35	Does the company classify all information and data within the finance company to reflect its level of confidentiality or importance to the organization and implement security measures according to the level of confidentiality needed?			

36	Does the company create adequate training and awareness programs on aspects such as information systems security, access controls, procurement and maintenance procedures, network management, business continuity plan, information system audits and software licensing?			
37	Has the company clearly identified and listed assets associated with processing and communication of information (i.e. hardware, software and communication equipment), and has assigned the responsibility of securing all information system assets to an individual who has been authorized by the management?			
38	Does the company have procedures for purchasing and maintaining commercial software?			
39	Does the company have a security policy for network management?			
40	Does the company have a Business Continuity Plan (BCP) covering disaster management and risk analysis, which has been implemented after testing and acceptance?			
41	Does the company conduct periodic information system audits? If so who is responsible for the audit? (Responsibilities of the audits should be assigned to a separate unit or external personnel, independent of the IT department).			
	DIRECTIONS	**Compliance Status**	**Comments**	
42	Does the company comply with legal and policy requirements relating to software licensing?			

Interest Rates (No 4 of 2020)

43

Tenure of Deposit	Maximum Interest Rate per annum	Remark
Savings and other deposits of a tenure of less than 01 month or maturity is not specified	Standing Deposit Facility Rate [SDFR] – To be reviewed quarterly. The reference rate of SDFR for the quarter will be the SDFR as at the end of the immediately preceding quarter.	The maximum rate payable for savings deposits of children under the age of 18 shall be 0.5% higher than the normal interest rate.
Term Deposits		
01 month > 03 months	Weighted average yield applicable to 364 – day Treasury Bills	The Annual Effective Rate should not exceed the specified maximum interest rate, if any periodic interest payments are made on term deposits during the tenure of the deposit.
03 months > 06 months	Weighted average yield applicable to 364 – day Treasury Bills +0.25	
06 months > 01 year	Weighted average yield applicable to 364 – day Treasury Bills +0.50%	
01 year > 02 years	Weighted average yield applicable to 364 – day Treasury Bills + 2.00%	
02 years > 03 years	Weighted average yield applicable to 364 – day Treasury Bills + 2.75%	
03 years >05 years	Weighted average yield applicable to 364 – day Treasury Bills + 3.25%	

	05 years	Weighted average yield applicable to 364 – day Treasury Bills + 4.25%				
	Does the company comply with the above interest rates as defined by the Direction?					
44	Does the company comply with the regulation that the maximum rate payable for term deposits with tenure of 01 year or more of senior citizens shall be 0.5% higher than the normal interest rate?					
	DIRECTIONS			**Compliance Status**	**Comments**	
45	Does the company comply with the regulation that the maximum rate of interest which may be paid by a finance company on a debt instrument shall not exceed the maximum upper limit of interest rates for maturity periods set out below; I. mature in less than one year - The quarterly weighted average yield applicable to 364-day Treasury Bills issued + 0.50% II. maturity between one year and less than 02 years - The quarterly weighted average yield applicable to 364-day Treasury Bills issued + 2.75% III. maturity between 02 years and less than 03 years -The quarterly weighted average yield applicable to 364-day Treasury Bills issued + 3.25% IV. maturity between 03 years and less than 05 years - The quarterly weighted average yield applicable to 364-day Treasury Bills issued + 3.75% V. maturity in 05 years or more - The quarterly weighted average yield applicable to 364-day Treasury Bills issued + 4.25%					
46	In the instance of a pre-mature withdrawal does the company comply with the regulation that the interest payable on the deposit up to the date of withdrawal shall be computed on the basis of the lower of, the published					

	interest rate of the LFC applicable to the completed period prevailing at the time of withdrawal or at a rate of 100 basis points less than the contracted rate?			
47	Does the finance company furnish details of the interest rates in accordance with the monthly web based return on NBD-MF-06-ID-Rate of Interest/Deposits?			
	Corporate Governance			
48	Does the Board of Directors of the company; a) approve and oversee the finance company's strategic objectives and corporate values and ensure that such objectives and values are communicated throughout the finance company?			
	b) Approve the overall business strategy of the finance company, including the overall risk policy and risk management procedures and mechanisms with measurable goals, for at least immediate next three years?			
	c) Identify risks and ensuring implementation of appropriate systems to manage the risks prudently?			
	d) Approve a policy of communication with all stakeholders, including depositors, creditors, share-holders and borrowers?			
	e) Review the adequacy and the integrity of the finance company's internal control systems and management information systems;			
	f) Identify and designate key management personnel, who are in a position to: (i) significantly influence policy; (ii) direct activities; and (iii) Exercise control over business activities, operations and risk management?			
	DIRECTIONS	**Compliance Status**	**Comments**	
	g) Define the areas of authority and key responsibilities for the Board and for the key management personnel?			

	h) Ensure that there is appropriate oversight of the affairs of the company by key management personnel that is consistent with the finance company's policy?			
	i) Periodically assess the effectiveness of its governance practices, including: (i) the selection, nomination and election of directors and appointment of key management personnel; (ii) the management of conflicts of interests; and (iii) the determination of weaknesses and implementation of changes where necessary?			
	j) Ensure that the finance company has an appropriate succession plan for key management personnel?			
	k) Meet regularly with the key management personnel to review policies, establish lines of communication and monitor progress towards corporate objectives?			
	l) Understand the regulatory environment?			
	m) Exercise due diligence in the hiring and oversight of external auditors?			
49	Is it ensured that a director who has not attended at least two-thirds of the meetings in the period of 12 months immediately preceding or has not attended the immediately preceding three consecutive meetings held, shall cease to be a director unless participated through an alternate director?			
50	Has the Board appointed a company secretary whose primary responsibilities are handling the secretarial services to the Board and shareholder meetings and carrying out other functions specified in the statutes and other regulations?			
51	Do all directors have access to advice and services of the company secretary?			
52	Does the company secretary maintain the minutes of Board meetings? Does the minutes clearly contain or refer to the following: (a) a summary of data and information used by the Board in its deliberations; (b) the matters considered by the Board; (c) the fact-finding discussions and the issues of contention or dissent which may illustrate whether the Board was carrying out its duties with due care and prudence; (d) the explanations and confirmations of relevant executives which indicate compliance with the Board's strategies and policies and adherence to relevant laws and regulations; (e) the Board's knowledge and understanding of the risks to which			

	the finance company is exposed and an overview of the risk management measures adopted; and (f) the decisions and Board resolutions			
	Composition of the Board			
53	Are the number of Directors of the Board more than 5 and less than 13? (the number of independent non-executive directors of the Board shall be at least one fourth of the total numbers of directors) (Criteria applicable to independent non-executive directors)			
54	At each Board meeting held, is at least one half of the number of directors that constitute the quorum at such meeting non-executive directors?			
	DIRECTIONS	**Compliance Status**	**Comments**	
55	Does the company identify independent non-executive directors expressly in all corporate communications that disclose the names of directors of the finance company?			
56	Does the company disclose the composition of the Board, by category of directors, including the names of the chairman, executive directors, non-executive directors and independent non-executive directors in the annual corporate governance report as part of its Annual Report.?			
57	Is there a formal, considered and transparent procedure for the appointment of new directors to the Board and for the orderly succession of appointments to the Board?			
58	Are all directors appointed to fill a casual vacancy, subject to election by shareholders at the first general meeting after their appointment?			
59	Does any person over the age of 70 years serve as a director of the finance company?			

60	Does any director hold office as a director or any other equivalent position in more than 20 companies/societies/bodies corporate, including associate companies and subsidiaries of the finance company?			
61	Does the Board delegate any matters to a Board Committee, Chief Executive Officer, executive directors or key management personnel, to an extent that such delegation would significantly hinder or reduce the ability of the Board as a whole to discharge its functions			
62	Does the Board review the delegation processes in place on a periodic basis to ensure that they remain relevant to the needs of the finance company?			
63	Is the role of the Chairman and Chief Executive Officer performed by the same person or separated?			
64	Is the Chairman a non-executive director? (Criteria applies(pg. 35))			
65	Does the Board include in the finance company's corporate governance report, the name of the Chairman and the Chief Executive Officer and the nature of any relationship [including financial, business, family or other material/relevant relationship(s)], if any, between the chairman and the chief executive officer and the relationships among members of the Board?			
	Board appointed Committees			
66	Does the company have at least an Audit Committee and Integrated Risk Management Committee?			
67	Does each committee report directly to the Board?			
68	Does each committee have a secretary to arrange its meetings, maintain minutes, records and carry out such other secretarial functions under the supervision of the chairman of the committee?			

	DIRECTIONS	Compliance Status	Comments	
	Audit Committee			
69	Is the chairman of the Audit Committee a non-executive director who possesses qualifications and experience in accountancy and/or audit?			
70	Are the Board members who are appointed to the committee Non-Executive Directors?			
71	Does the committee make recommendations on (i) the appointment of the external auditor for audit services to be provided in compliance with the relevant statutes; (ii) the implementation of the Central Bank guidelines issued to auditors from time to time; (iii) the application of the relevant accounting standards; and (iv) the service period, audit fee and any resignation or dismissal of the auditor, provided that the engagement of an audit partner shall not exceed five years, and that the particular audit partner is not re-engaged for the audit before the expiry of three years from the date of the completion of the previous term.			
72	Does the committee review and monitor the external auditor's independence and objectivity and the effectiveness of the audit processes in accordance with applicable standards and best practices?			
73	Has the committee developed and implemented a policy with the approval of the Board, on the engagement of an external auditor to provide non-audit services that are permitted under the relevant statutes, regulations, requirements and guidelines?			
74	Does the audit Committee discuss and finalize with the external auditors the nature and scope of the audit before the commencement of the audit?			
75	Does the audit Committee review the financial information of the finance company?			

76	Does the committee discuss issues, problems and reservations arising from the interim and final audits, and any matters the auditor may wish to discuss including those matters that may need to be discussed in the absence of key management personnel, if necessary?			
77	Does the committee review the external auditor's management letter and the management's response?			
78	Does the committee meet at least once in six months, with the external auditors without the presence of the executive directors?			
79	Does the committee have; (i) explicit authority to investigate into any matter within its terms of reference; (ii) the resources which it needs to do so; (iii) full access to information; and (iv) authority to obtain external professional advice and to invite outsiders with relevant experience to attend, if necessary.			
80	Does the committee disclose in the Annual Report, i) details of the activities of the audit committee; (ii) the number of audit committee meetings held in the year; and (iii) details of attendance of each individual member at such meetings.			
81	Does the secretary to the committee record and keep detailed minutes of the committee meetings?			
	DIRECTIONS	**Compliance Status**	comment	
	Board Integrated Risk Management Committee			
82	Does the committee consist of at least one non-executive director, CEO and key management personnel supervising broad risk categories, i.e., credit, market, liquidity, operational and strategic risks?			
83	Does the committee meet at least on a quarterly basis? Does the committee submit a risk assessment report within a week of each meeting to the Board?			

84	Does the company have a Compliance function and a dedicated Compliance Officer selected from key management personnel?			
	Related party transactions			
85	Does the Board ensure that the finance company does not engage in transactions with a related party in a manner that would grant such party "more favorable treatment" than that is accorded to other similar constituents of the finance company?			
	Disclosures			
86	Does the Board ensure that ; (a) annual audited financial statements and periodical financial statements are prepared and published in accordance with the formats prescribed by the regulatory and supervisory authorities and applicable accounting standards, and that (b) such statements are published in the newspapers in an abridged form, in Sinhala, Tamil and English			
87	Are the following disclosures made in the annual report?			
	a) A statement to the effect that the annual audited financial statements have been prepared in line with applicable accounting standards and regulatory requirements, inclusive of specific disclosures. b) A report by the Board on the finance company's internal control mechanism that confirms that the financial reporting system has been designed to provide a reasonable assurance regarding the reliability of financial reporting, and that the preparation of financial statements has been done in accordance with relevant accounting principles and regulatory requirements. c) The external auditor's certification on the effectiveness of the internal control mechanism in respect of any statements prepared or published after March 31, 2010. d) Details of directors, including names, transactions with the finance company.			

	e) Fees/remuneration paid by the finance company to the directors in aggregate, in the Annual Reports published after January 1, 2010. f) Total net accommodation as defined in paragraph 9(4) outstanding in respect of each category of related parties and the net accommodation outstanding in respect of each category of related parties as a percentage of the finance company's capital funds. g) The aggregate values of remuneration paid by the finance company to its key management personnel and the aggregate values of the transactions of the finance company with its key management personnel during the financial year, set out by broad categories such as remuneration paid, accommodation granted and deposits or investments made in the finance company. h) A report setting out details of the compliance with prudential requirements, regulations, laws and internal controls and measures taken to rectify any non-compliance. i) A statement of the regulatory and supervisory concerns on lapses in the finance company's risk management, or noncompliance with the Act, and rules and directions that have been communicated by the Director of the Department of Supervision of Non-Bank Financial Institutions, if so directed by the Monetary Board to be disclosed to the public, together with the measures taken by the finance company to address such concerns. j) The external auditor's certification of the compliance with the Act and rules and directions issued by the Monetary Board in the annual corporate governance reports published after January 1, 2011			
	Assessment of fitness and propriety of directors and officers performing executive functions (3 of 2011)			
88	Has the company submitted to the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka,an affidavit and declaration from respective directors or officers selected for appointment? (In respect of every continuing director, a finance company shall obtain and submit affidavits and declarations to the Director annually before the Annual General Meeting of the respective finance company if such directors are nominated for re-appointment)			
89	Has the company obtained a letter from the institution/company in which a director or officer held office immediately preceding the appointment, regarding the level of performance of duties assigned to him/her in the particular institution and submitted to the director ?			

	Reporting Requirements (2 of 2011)			
90	Has the company submitted all information to the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka, according to the formats provided under the Central Bank Financial Information System by the due dates as specified? Has the company paid any penalty due to delayed submission?			
	Audited Accounts (16 of 1991)			
91	Has an auditor been appointed to audit the following? (a) balance sheet as at the last working day of each financial year; (b) profit and loss account in respect of such year.			
	DIRECTIONS	**Compliance Status**	**Comments**	
	Other Directions			
	Transfer of Assets (4 of 1991)			
92	Have any assets of the company been transferred or alienated for any consideration other than for a monetary consideration which should pass in favor of the transferor?			
	Fixed Assets (11 of 1991)			
95	Has the company purchased any immovable property or any right title or interest exceeding : (i) the aggregate (at any time) of the amount outstanding on the loans obtained for the specific purpose of purchasing ; or			

	(ii) 50 % of the capital funds of the finance company without the prior approval of the Director?			
	Accrued Interest (15 of 1991)			
96	In accrued interest calculation, does PLC take into account accrued interest for the loans on which interest and/or capital repayments are in arrears for six months or more?			
97	Does the company segregate when maintaining books of accounts all outstanding accommodations (loan, credit facility or any type of financial accommodation) in arrears for over six months, under separate control accounts in the general ledger?			
	Deposit incentive scheme (5 of 2001)			
98	Has the prior approval of the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka, been obtained in writing for every incentive scheme used for soliciting deposits?			
	DIRECTIONS	**Compliance Status**	**Comments**	

99	Are all incentive schemes for soliciting deposits; i) Within the accepted practices of financial institutions? ii) Bestow on the depositors a real benefit and not something illusory? (iii) Not lead to unfair and unethical competition among other financial institutions? (iv) Not weaken prudential requirements? (v) Are operated directly by the company or where it is undertaken in association with another company, the company providing the benefits is not an affiliate or subsidiary company of the finance company concerned or a party of a group to which the finance company belongs; and (vi) Not have an adverse impact on the profitability of the company through excessive increase in costs of mobilizing deposits.			
	Closure of office/s for business (Direction No. 06 of 2020 – Business Expansion and Operation)			
100	Has the finance company during the year, closed its offices for business on any day of the week from Monday to Friday, which is not a holiday declared by the Ceylon Chamber of Commerce, without the prior approval in writing of the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka,?			
	Structural changes (No 1 of 2013)			
101	Has the company complied with obtaining prior approval for any of the following structural changes of the company? a) Establishing any subsidiary or associate company b)commencing a new business activity which is not directly related to finance business, hire purchase or pawning; c)enhancing or reducing issued capital; d)selling its business;			

	e)acquiring whole or part of the business of any other finance company; f)changing the Memorandum of Association or Articles of Association; g)amalgamating, consolidating or merging the company with any other finance company; h)restructuring the management of the company			
102	Has the Company obtained the prior approval in writing of the Director for any of the followings? a) Enhance or reduce its share capital b) Enhance its investment in share capital of a subsidiary or an associate company c) Sell whole or part of the business of a subsidiary or an associate company d) Change its Articles of Association e) Transfer or sell any of its assets of a book value of more than Rupees Five Million , at a price less than the prevailing market value f) Change the designation of any member of the Board of Directors and CEO.			
	DIRECTIONS	**Compliance Status**	**Comments**	
103	Has the Company transferred or sold any of its assets other than for monetary consideration that should be passed in favor of the transferor?			
104	Does the Company comply with the policy that no member of the Board of Directors and CEO shall without prior approval of the Director resign from the Company?			
	Direction No. 06 of 2020 – Business Expansion and Operations			

105	Has the company complied with obtaining prior approval from the Monetary Board for any of the following?			
	(a) Opening a branch or an ATM;			
	(b) changing the location of any business places; or			
	(c) Closing any of its business places.			
106	Does the company have Board approved prudent policies on Annual Branch Expansion Plan (ABEP)?			
	Opening of new branches/ ATM's			
107	Does the company submit an economic feasibility study for each branch to be opened along with the application? Does the company obtain Board approval prior to submission of such application for opening of new branches/ ATM's?			
108	Does the company ensure that they commence business operations within 3 months from the date of announcement of decision by the Monetary Board?			
109	Does the company notify the Director the date of the new branch opened within 10 business days after opening the new branch?			
	Closure of Business places			
110	Does the company submit an application for closing of existing business places to the Director at least 45 days before the expected date of closure with the approval of the Board of Directors?			
111	Does the company ensure that they notify the Director the date of the closure within 10 business days after the closure?			

	Relocation of business places			
112	Does the company submit a request with prior approval of the BOD, to effect a change in the location of any existing business place to the Director at least 45 days before the expected date of the relocation?			
	DIRECTIONS	**Compliance Status**	**Comment**	
	Deposit Mobilization /Issuing of Debt Instruments			
113	Does the company ensure that deposit mobilization is conducted only at branch offices?			
	Loan to value ratio for loans and advances in respect of motor vehicles (03 of 2020)			
114	Does the company adhere to the direction that Licensed Finance Companies (LFC's) are restricted from granting loans and advances for the purpose of purchase or utilization of motor vehicles as follows? [In respect of unregistered vehicles and registered vehicles which have been used in Sri Lanka for less than one year after the first registration.]			

Vehicle Category	Vehicle class of Department of Motor Traffic	Electric Ve
Commercial Vehicles	CI,C,CE,DI,D,DE,GI,G	90%
Motor Cars, SUVs and Vans	B (Other than light trucks and single cabs)	90%

	Locally Assembled motor cars , Suvs & vans	(Other than light trucks & single cabs)	90%		70%			
	Three Wheelers	B1	90%		25%			
	Any other vehicle	A1,A, light trucks and single cabs categorized under B	90%		70%			
	Hybrid Motor Cars, Vans and SUVs	B (Other than light trucks and single cabs)		50%				
	80% in respect of registered vehicles which have been used in Sri Lanka for more than one year after the first registration.							

	DIRECTIONS	Compliance Status	Comments	
	RULES			

	Advertisements (No 1 of 2006)			
115	Does every advertisement published in **print media** (excluding hoardings, bill boards and banners) directly or indirectly soliciting deposits from the public, contain; (a) that the company has been registered by the Monetary Board of the Central Bank of Sri Lanka under the Finance Companies Act, No. 78 of 1988; (b) the date of incorporation of the company; (c) credit rating for the entity assigned to the company by a credit rating agency acceptable to the Central Bank of Sri Lanka; (d) periodicity of payment of interest and the annual effective rate of interest in respect of all maturities; and (e) terms and conditions subject to which deposits are accepted			
116	Does the company forward to the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka, a copy of any advertisement to be published at least 2 working days prior to the publication of such advertisement?			
117	Does every advertisement transmitted or broadcasted through **audio or audio-visual media** (including websites posted on the internet) directly or indirectly soliciting deposits from the public contain :– (a) that such company has been registered by the Monetary Board of the Central Bank of Sri Lanka under the Finance Companies Act, No. 78 of 1988; (b) credit rating for the entity assigned to the company by a credit rating agency acceptable to the Central Bank of Sri Lanka; and (c) if interest rates are indicated, the annual effective rates of interest.			
118	Does the company forward to the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka, through electronic means a copy of any advertisement to be transmitted, at least, 3 working days prior to the first transmission or broadcast of such advertisement?			
119	Does every advertisement displayed by the finance company through **hoardings, bill boards and banners** soliciting deposits directly or indirectly from the public state the fact that the company has been registered by the Monetary Board of the Central Bank of Sri Lanka under the Finance Companies Act, No. 78 of 1988?			
120	Has the company prior to the display of an advertisement on a hoarding, billboard or banner, inform the Director, Department of Supervision of Non-Bank Financial Institutions, Central Bank of Sri Lanka, the contents of such advertisement and the locations of such hoardings or billboards?			

	PUBLICATION OF HALF YEARLY FINANCIAL STATEMENTS			
121	Does the company publish key financial data key performance indicators for 12 month period ended 31 March and 6 months period ended 30 September, every year, in accordance with the format given by the Director of the Department of Supervision of Non-Bank Financial Institutions of the Central Bank of Sri Lanka?			
	MAINTENANCE OF SAVINGS ACCOUNTS FOR MINORS			
122	Does the company include the following clauses in the terms / conditions pertaining to opening, operating and maintaining of savings accounts for minors :–			
	(a) The balance lying to the credit of an account of a minor may be transferred upon instructions of a parent or a legal guardian of the minor, to an account maintained in the name of the minor in an authorized deposit taking institution, upon completion of sixty months from the date of the first deposit or at any time thereafter. (b) The balance lying to the credit of an account of a minor may be withdrawn by a parent or a legal guardian of the minor, for a justifiable reason such as meeting the cost of medical treatment or education of the minor or for any other reason acceptable to the RFC.			
	DIRECTIONS	**Compliance Status**	**Comments**	
123	Are the contents of the above two clauses informed to the parent or legal guardian of the minor at the time of opening the savings account? (If the account is opened by a person other than a parent or legal guardian, the parent or the legal guardian should be informed by the RFC, of the contents of the above two clauses, within one month from the opening of the account.)?			
	Other circulars/ guidelines			
124	Are the external auditors used by the company included in the panel of external auditors appointed by the Central Bank of Sri Lanka?			
	OTHER			

	Investment fund account			
125	Does the company operate an Investment Fund Account?			
126	Does the company pay the premium on deposits to the Sri Lanka Deposit Insurance Fund and forward the details as required to the director of Bank Supervision?			
127	Does the company maintain a proper system of information to support the accuracy of the calculation of premium?			
	FIU Regulations			
128	Does the company report the following to the Financial intelligence Unit of the Central Bank;			
	All Cash transactions amounting to Rs.1,000,000/- or it's equivalent in foreign currency			
	All Electronic Fund transfers done at the insistence of the customer of Rs. 1,000,000/- or its equivalent in foreign currency			
	Any suspected transaction or attempted transaction may be related to the commission of any unlawful activity or any other criminal offence			
	Information that it suspects may be relevant 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; 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.5 of 2006 and the Convention on the Suppression of Terrorist Financing Act, No.25 of 2005			
	DIRECTIONS	**Compliance Status**	**Comments**	
129	Does the company adhere to KYC and CDD rules and regulations issued by the FIU? Specially on;			
	*Appointment of a compliance officer			
	*Establishment of an audit function			
	*Awareness of staff (training)			

130	Has the company established and maintain procedures and systems to implement the reporting requirements under the Section 7 of the FTRA and train its officers, employees and agents to recognize suspicious transactions?			
	Credit Ratings (No 01 of 2018)			
131	Has the company entered in to an agreement with a Credit Rating agency and informed the CBSL accordingly within the prescribed time period.			
132	Disclose the Credit Rating in all the advertisements			
133	Has the company updated Credit Ratings at least annually and has informed D/SNFBI within one month from the date of the report?			
	Financial Customer Protection Framework (No .01 of 2018)			
134	Has the Company followed the minimum standards on customer protection as per CBSL Directions no 01 of 2018 on Financial Customer Protection Framework			
	Valuation of Immovable Property (No.04 of 2018)			
135	Is the Company in compliance with regulatory requirements issued under the Finance Leasing Act, No 56 of 2000?			
136	Are Board approved prudent policies and procedures on valuation of immovable property in place?			
137	Ensure periodical review of the Policy			
138	Ensure the eligibility criteria for valuers as defined in the CBSL Direction No. 01 of 2021 of Valuation of Immovable Properties			
139	Has the company established an appropriate threshold for internal and external valuation in respect of immovable property?			
	DIRECTIONS	**Compliance Status**	**Comments**	

	Maximum Rate of Interest on Micro finance Loans [No 08 of 2018 & No 10 of 2018]			
141	Does the Company comply with the rule that no LFC shall charge a rate exceeding 35% per annum (effective annual interest rate), inclusive of all other charges on Micro finance loans?			
142	Does the Company report Micro finance loans under code 3.1.4.9.0.0 / 1.1.4.12.0.0-Micro finance Loans in the Financial Information Network (FInNet) return NBL-MF-03-Balance Sheet?			
	Out Sourcing of Business Operations [No 07 of 2018]			
143	Does the Company adhere to the rule that outsourcing arrangements are not directly related to provisions of financial services?			
144	Does the Company comply with the rule that the LFC shall at all times enter into a legally binding agreement with the outsourcing service provider and thus selected Service providers have specialized resources , capacity and expertise or perform such functions/operations or activities?			
145	Have any of the out sourcing arrangements that were entered into have any Director, employee and/or close relative of a Director or an employee of the LFC who has an interest in it?			
146	Does the Company comply with the provisions made in the Related Party Transactions stipulated in Finance Companies (Corporate Governance) Direction No 3 of 2008 [or as amended] in instances where the outsourcing service provider is the parent company or other related company of the LFC?			
147	Does the Company maintain an up-to-date register of all outsourcing arrangements?			
148	Has the Company outsourced any of the following functions and if so, does the Company comply with Finance Business Act Directions No 07 of 2018?			

Staff Circular No……

Annual Declaration to be submitted by all employees of People's Bank, for the year 2023.

We, at People's Bank are committed to execute our business in compliance with the highest standards of good governance and it has always been the belief and policy of the employees of People's Bank to conduct their activities and transactions with transparency.

It is the responsibility of each and every employee to uphold high standards of personal integrity, conduct and professionalism during their career at People's Bank.

In light of this, you are kindly requested to complete the attached Annual Declaration for 2023 and submit it to Assistant General Manager (Human Resources- Administration) on or before 31st of January, 2023.

Please acknowledge the receipt of this Circular to the Assistant General Manager (Compliance).

Clive Fonseka
Actg. Chief Executive Officer/General Manager

People's Bank
Head Office,
Colombo 02.

2nd January, 2023.

EMPLOYEE ANNUAL DECLARATION 2022

I

……

……

S/No.…… of

……

……

declare as follows:

1) That I am the (declarant) above named and I am an employee of People's Bank, a Banking Corporation duly established by People's Bank Act No.29 of 1961 (as amended) and which is a Licensed Commercial Bank in terms of the Banking Act No.30 of 1988 (as amended) and that I am currently a ……..……. (***present post/grade***) attached to ……. (***dept/branch***).

2) That I am a citizen of Sri Lanka and I am not a citizen or Permanent Resident (PR) of any other country save and except as follows:

……..

……..

3) That I am honest in my dealings with

- my employer
- my superiors, subordinates and peers at my work place
- all internal and external customers in regard to my work
- all other parties who have dealing with me

and that I carry out my functions at work with integrity and act with proper decorum at all times.

4) That I am not in default in payments of Bank loans/facilities/credit card payments etc from the People's Bank.

5) That I have no accounts/loans/facilities from any other Bank or Financial Institution save and except for the following :

……..

……..

…….

and I further declare that I am not in default with regard to payments in respect of any of the above.

6) That I do and will at all times act with responsibility and uphold the standards of conduct being entrusted with the protection of the reputation of the People's Bank.

7) That there is no finding of any regulatory or supervisory authority, professional association, any Commission of Inquiry, Tribunal or other body established by law in Sri Lanka or abroad, to the effect that I have committed or have been connected with the commission of, any act which involved fraud, deceit, dishonesty or any other improper conduct;

8) That I am not involved in any business or employment other than for my employment at People's Bank and I have no additional income save and except as follows:

……

……

……

9) That the following are the only business ventures of my spouse and children

……

……

……

……

10) That the Business Ventures set out above have no business dealings with the People's Bank either as customer, supplier or any other capacity save and except as follows:

…… ……..

(Name of Business) (Type of Business Dealing)

11) That the following are the Taxes paid by me for the year 2022

…….. …….

(Type of Taxes paid) (File No.)

12) That I have signed the Declarations of Secrecy as required by the Banking Laws of Sri Lanka.

13) That presently I am not subject to an investigation or inquiry consequent upon being served with notice of a charge involving fraud, deceit, dishonesty or other similar criminal activity, by any regulatory authority, supervisory authority, professional association, commission of Inquiry tribunal or other established by law, in Sri Lanka or abroad.

14) That I am not an undischarged insolvent nor have I been declared bankrupt in Sri Lanka or abroad;

15) That I have not failed to satisfy any judgment or order of any court whether in Sri Lanka or abroad, or to repay a debt;

16) That I have not been declared by a court of competent jurisdiction in Sri Lanka or abroad, to be of unsound mind;

17) That I have not been removed or suspended by an order of a regulatory or supervisory authority from any previous/present service

18) That I am committed to complying with all external/statutory laws and regulations and all internal policies and procedures of the People's Bank.

19) That I will exercise utmost care in respect all business functions with our various stake holders.

20) That I will use the Assets of the People's Bank for authorized purposes only.

21) That I verily believe that I am a fit and proper person to be an employee of People's Bank.

Declared by …….. on this …… day of ……..…….. 2023 at ……..

…….

Signature of Declarant

Witnesses

1…….. ……..

(Name) (Service No.) Signature

2. …….. ……..

(Name) (Service No.) Signature

To : Deputy General Manager/ Human Resources

From : Assistant General Manager/ Compliance

Date : 02.01.2023

Ref : agmc/sam

EMPLOYEE ANNUAL DECLARATION 2023

As instructed by CEO/GM an Annual Declaration – 2023 has been issued to all employees of the Bank to fill out and submit to you on or before **31st January 2023.**

Please make arrangements to file the signed declaration of each and every employee in their Personal Files.

Samanthi Senanayake
Assistant General Manager- Compliance

µ&ß<æ ëæÜµÙßç à'æ:

´{íù ý`'æÝµÓ &Ú× ´ µ&ß<æ µ&ßÑæ$<ùß Ñ&Úùß
2023 <&Ø µ<ùÔµ<ùß á÷ÀÚÍûõß æÙ×ÔõÝ <$ÌÂÚæ ûÜæ$Á×

´{íù ý`'æÝ µ&ß<µ×ß ùÚØõ àû, ×{ûõß û$Ùù×æß {$ à÷À$Ù ÑÁÚÂßñõ´ ûÜÆõÛùß àùÔæÞÙ< <]$û$Íæ æð×ÔõÝ û<õß<$ µèù ×$´ð à`û æ`û Ò &Ú®ù àõØ, &|´ Ñµðæ´ ´{íù ý`'æÝ µ&ß<æ×ùµèß ÑÁß<$&× {$ ûÜõÚûõßõÚ× <Õµ×ß ÷À å<Ôùµèß æÜÚ×$æ$ØæÈ {$ èóÔµ÷ÀùÔ û$Ø÷À#Á]õ$<×æÚùß ×ÔõÝ< û<õß<$ èõ ×ÔõÝ ý<×.

äûÍ÷ÀÚ ´{íù ý`'æÝ µ&ß<µ×ß ùÚØõ &´&ßö æ$Ù× õÝÙ à<'æý<, ×{û`<`õß´ {$ <#õßõÚ×õ$< à÷À$Ù ÑÁÚÂßñõ´ ûÜÆõÛùß µù$µ<ù&ß< û<õß<$ è`ùÛ´ &|´ µ&ß<æ µ&ßÑæ$<æµèß´ <èæÛ´ µ<×Ú.

µ´´ õõß<× &`}æÚÙßÙð èùÚÆùß µÈ &´ê à´Ôó$ à`õÚ <$ÌÂÚæ ûÜæ$Áù× 2023 <&Ø µ<ùÔµ<ùß &ÈûÕÌó æØ 2023 íù<$Í ´& 31 ÷ÀÚù µ{$ß âð ûÜö´ &{æ$Ø &$´$ù]$½æ$Î (´$ù< &Èûõß) µ<õ á÷ÀÚÍûõß æØù µ´ùß æØ`ó$µ<ùß áÙßÙ´Ô.

æØ`ó$æØ µ´´ ëæÜµÙßç× Ù÷À ý`Ó &{æ$Ø &$´$ù]$½æ$Î (àùÔæÞÙõ$) µ<õ õ{<ÔØ` æØùßù.

æßÙ×ÚÓ µ\$ùßµ&ßæ$
<`. ý. ûÜø$ù Ñø$×æ ùÚÙø$Î/ &$´$ù]$½æ$Î.

´{íù ý`'æÝ<
ûÜø$ù æ$Ì×$Ù×
µæ$}Ö 02.

2023.01.02

<$ÌÂÚæ µ&ß<æ ûÜæ$Á× - 2023

..... {Ú û÷ÀÚ'¥ (µ&ß<$ à'æ× .....) ..... <ù ´´ û{õ ÷À`æßµ<ù ûÍ÷ÀÚ ûÜæ$Á æØ &Ú®Æ.

1. ´$ (ûÜæ$Áæ) á{õ ùÈ &úÀ{ùß à× <ù àõØ, &'µÁ$ß½õ 1961 à'æ 29 ÷ÀØó ´{íù ý`'æÝ ûùõÚùß ùÚ&Ú ûÍ÷ÀÚ &ßö$ûÚõ ý`'æÝ &´$è´×æß <ù {$, &'µÁ$ß½õ 1988 à'æ 30 ÷ÀØó ý`'æÝ ûùµõß ùÚ×´×ùð àùÔ< ÙÚ×$û÷ÀÚ'¥ æØù Ù÷À <$óÚí ý`'æÝ<æß <ù ´{íù ý`'æÝµÓ µ&ß<æµ×æß <ù àõØ, ÷À`ùð ´$ ..... (÷À`ùð ÷ÀØó õùõÝØ /µÁÜßóÚ×) <Áµ×ùß ..... (µ÷ÀûÌõµÈùßõÝ< / Á$ç$<) àùÔ×Ôæßõ< &Ú®ù ý<õß,

2. ´$ ÁÜÛ Ù'æ$µÓ ûÔØ<`&Úµ×æÝ ý<õß, û{õ &úÀ{ùß à$æ$Øµ×ùß {`µØùßùð µ<ùõß æÝ´ù µ{$ß Øðæ ûÔØ<`&Úµ×æÝ µ{$ß ùÚõ] û÷ÀÚ'¥æØ`µ<æÝ µ{$ß µù$<ù ý<õß,
   .....
   .....

3.

- ´$µèß µ&ß<$ µ×$ßíæ ,
- ´$µèß µ&ß<$ &ßö$ùµ×ß ûÜø$ùÛùß, ãû µ&ßÒùß {$ &´ µ&ßÒùß,
- ´$µèß µ&ß<$ {$ à÷À$} &Ú×Ï àþ]ùßõÍæ {$ ý${ÚØ èóÔµ÷ÀùÔæØ`<ùß,
- ´$ &´ê èóÔµ÷ÀùÔ æØùÔ Ùýù àµùæÝõß &Ú×Ï û$ÌÁ<×ùß,
  &´ê û<õß<ùÔ Ùýù ´$µèß &Ú×Ï èóÔµ÷ÀùÔ <Ù÷ÀÛ ´$ à<'æ <ù ý<õß,

  Ø$íæ$Î {$ à÷À$} ´$µèß æ$Ì××ùß &#íÔ ýÑùß ×ÔõÝ< áðÔ æØù ý<õß,
  &|´ Ñðæ´ &÷À$ë$Ø$õß´æ< æð×ÔõÝ æØù ý<õß,

4. ´$ ´{íù ý`'æÝµ<ùß Ùý$ µèù à`õÚ ý`'æÝ ó× / û{&ÔæÈ / ó× æ$³ûõß à$÷ÀÚ× à÷À$Ù µèÒÈ àõû&Ô æØ {Úê {ÚðÔ<$ µù$´`õÚ ý<õß

5. û{õ ÷À`æßµ<ù à$×õù×ùß &´ê {`µØùßùð, æÚ&Ú×È µ<ùõß ý`'æÝ<æß µ{$ß ´ÔÙ] à$×õù×æß &´ê èÚóÔÈ / ó× / û{&ÔæÈ ´$ ùÆùß µù$û<õßù$ ý<õß,

.....

.....

á{õ &úÀ{ùß æÝ´ù µ{$ß û{&Ôæ´æß &Èýùßøµ×ùß µèÒÈ àõû&Ô µæ$ð {Úê {ÚðÔ<$ µù$´`õÚ ý<õß, ´´ õ<÷¸Øðõß ûÜæ$Á æØ &Ú®Æ.

6. ´$ &Ú×Ï à<&ßö$<ùß{Ú÷ÀÛ´ <èæÛ´æÚùß ×ÔõÝ< æÜÚ×$ æØù ý<õß, ´{íù ý`'æÝµÓ æÛÌõÚ× à$ØæßÂ$ æØÆùß, ´$ µ<õ û<ØùÔ Ù`ý à`õÚ ×{ûõß û`<`õß´ð à÷À$} ûÜÆõÛùß û<õß<$ èùÚÆùß æð×ÔõÝ æØù ý<õß ûÜæ$Á æØÆ.

7. æÚ&Ú×È ùÚ×$´ù µ{$ß à¾æßÂó à½æ$Í×æß, <#õßõÛ´× &´$è´×æß, æÚ&Ú×È Ñ´ÌÁù µæ$Æ&´æß, ÁÜÛ Ù'æ$µÓ µ{$ß Ñµ÷ÀßÁ×æ µ{$ß ùÛõÚ× ´èÚùß &ßö$ûÚõ ÑùÚÁßë× &þ$<æß µ{$ß ´óßòÙ×æß Ñ&Úùß , <'ëù×æß, ´ÔÙ$ æÚÎ´æß, <'æþ$<×æß µ{$ß àùß æ<Ø µ{$ß à$æ$Ø×æ à<ëÌ×<æß &ÈýùßØ <Ø÷Àæß ´$ Ñ&Úùß &Ú÷¸ æØùÔ Ù`ý à`õÚ ý<ð µ{$ß <Ø÷Àæð &ÈýùßØ Ò à`õÚ ý<ð æÝ´ù µ{$ß à½è´ù×æß &Ú÷¸ µæ$ð µù$´`õÚ ý<õß,

8. ´ Ñ&Úùß ´{íù ý`'æÝµ<{Ú &Ú÷¸ æØùÔ Ùýù 'æÚ×$< {`µØùßùð µ<ùõß æÝ´ù µ{$ß <]$û$Ø×æ µ{$ß 'æÚ×$<æ ´$ ùÚØõ µù$<ù ý<õß, û{õ ÷Àæß<$ à`õÚ à$æ$Ø×ð {`µØùßùð µ<ùõß àõÚµÌæ à$÷À$×´æß ´$ µù$Ùýù ý<õß,

.....

.....

9. ´$µèß æÙõÜ×$ {$ ÷ÀØ`<ùß Ñ&Úùß û<õß<$ µèù ×ùÔ Ùýùßµùß û{õ &úÀ{ùß <]$û$Ø û´óæß ý<õß,

.....

.....

10. û{õ ÷Àæß<$ à`õÚ à$æ$Øµ×ùß {`µØùßùð, á{õ ÷Àæß<ù Ù÷À <]$û$Ø Ñ&Úùß ´{íù ý`'æÝ< &´ê èóÔµ÷ÀùÔæØ`µ<æÝ <Áµ×ùß µ{$ß &`û×ÔÈæØ`µ<æÝ <Áµ×ùß µ{$ß àù] à$æ$Ø×æÚùß µ{$ß <]$û$Íæ èóÔµ÷ÀùÔ û<õß<ùÔ µù$Ùýù ý<õß,

....

(<]$û$Ø ù$´×) (<]$û$Ø èóÔµ÷ÀùÔ &ß<þ$<×)

11. 2022 <&Ø à÷À$}< ´$ Ñ&Úùß µè<ù Ù÷À ý÷¸ û{õ ûÍ÷ÀÚ <ù ý<õß,

....
(µè<ù Ù÷À ý÷¸ &ß<þ$<×) (ÙÚûÚµè$ùÔ à'æ×)

12. ÁÜÛ Ù'æ$µÓ ý`'æÝ ùÛõÚ× ´èÚùß àµûßæßÂÚõ ûÍ÷ÀÚ , Ø{&]õ$ ÷ÀÚ<ÔØ`È ûÜæ$Á×ùð ´$ àõß&ùß õý$ à`õÚ ý<õß,

13. æÚ&Ú×È ùÚ×$´ù à½æ$Í×æß µ{$ß à¾æßÂó à½æ$Í×æß, <#õßõÛ´× &´$è´æß, æÚ&Ú×È Ñ´ÌÁù µæ$Æ&´æß, ÁÜÛ Ù'æ$µÓ µ{$ß Ñµ÷ÀßÁ×æ µ{$ß ùÛõÚ× ´èÚùß &ßö$ûÚõ ÑùÚÁßë× &þ$<æß µ{$ß ´óßòÙ×æß Ñ&Úùß <'ëù×æß, ´ÔÙ$ æÚÎ´æß, <'æþ$<×æß µ{$ß µ<ùõß &´è$Ç &$ûØ$¾ æÜÚ×$<æß à÷À$} <Õ µë$ß÷Àù$µØ$ßûó×æß þ$Ø÷ÀÛ´ µ{ßõÝµ<ùß &Ú÷¸ µæµØù Ñ´ÌÁù×æð µ{$ß ûÎæßÂó×æð ´$ ×ðõß< µù$&Ú®ù ý<õß,

14. ´ÕÙ] æ}´ù$æØó× µ{$ß ëÍõ ÷¼Âó× µ{$ß &Èýùßø àûØ$ø×æð ÁÜÛ Ù'æ$µÓ µ{$ß Ñµ÷ÀßÁ×æ µ{$ß æÝ´ù à$æ$Ø×æ µ{$ß à½æØó×æß Ñ&Úùß ´´ µ÷À$ßÂó× æØ µù$´`õÚ ý<õß,

15. ´$ àù$æßÂÚûßõ ýÔùß<õß <Õµ<æÝ µù$<ù ý<õß, ÁÜÛ Ù'æ$µÓ µ{$ß Ñµ÷ÀßÁ×æ µ{$ß ûÜæ$ÁÚõ ý'æµÙ$õßæØ`µ<æÝ µù$<ù ý<õß,

16. ÁÜÛ Ù'æ$µÓ µ{$ß Ñµ÷ÀßÁ×æ æÝ´ù µ{$ß à½æØó×æß ´èÚùß ùÚæÝõß æ} ÑùÚ&Ô´æß µ{$ß ùÚµ×$ßè×æß µ{$ß ó× ´Ô÷ÀÙæß à$û&Ô µèÒ´æß µ{$ß áðÔ æÚÎ´ ´$ û`{`Ø {`Ø µù$´`õÚ ý<õß,

17. ´$ ÑæÙ &Ú{Úµ×ùß ×ÔõÝ ý<ð ÁÜÛ Ù'æ$µÓ µ{$ß Ñµ÷ÀßÁ×æ µ{$ß ÁæßùÔ<ùß ùÛõÚ´× ýÙ à½æ$Í×æß Ñ&Úùß ûÜæ$Á æØ µù$´`õÚ ý<õß,

18. æÝ´ù µ{$ß ùÚ×$´ù µ{$ß à¾æßÂæ à½æ$Í×æß Ñ&Úùß ùÚæÝõß æ} ùÚµ×$ßè×æß ´õ æÚ&Ú×È ûÕÌ</ ûÜ<Ìöù µ&ß<$<æÚùß ´$ á<õß æØùÔ Ù`ý µ{$ß àõß&ÚðÔ<ùÔ Ù`ý µ{$ß µù$´`õÚ ý<õß,

19. &Ú×Ï ý${ÚØ / <]<&ßö$ûÚõ ùÛõÚ {$ ùÚ×$´ù×ùß÷À, ´{íù ý`'æÝµÓ &Ú×Ï àþ]ùßõØ ûÜõÚûõßõÚ {$ æÜÚ×$ û®û$¯ùß÷À àùÔ< æð×ÔõÝ æÚÎ´ð ´$ ý`úÀÛ à`õÚ ý<õß,

20. àûµèß ÑÑø$æ$Ø<Õ ûØ÷¸õýùßùùß {$ &Ú÷¸ µæµØù &Ú×Ï <]$û$Íæ æ$Ì××ùß{Ú÷ÀÛ ãûÍ´ ûÜµÓÁÈ &{èõ ý<æÚùß ×ÔõÝ< ´$ æð×ÔõÝ æØù ý<õß,

21. ´$ ´{íù ý`'æÝ<ð à×õß <õßæÈ ýÙ×Ùõß à<Á]õ$ &úÀ{$´ û´óæß ûÜµ×$ßíù×ð èùßù$ ý<õß,

22. ´´ ´{íù ý`'æÝµÓ µ&ß<æµ×æÝ Ò´ð õØÈ µ×$ßè] {$ ùÚ&Ú ûÔ÷ÀßèÙµ×æÝ <ùßµùÆ ×`×Ú &`ý`Ñùß´ ÑÁß<$& æØù ý<õß, ´´ ûÜæ$Á æØÆ.

..... Ñ&Úùß 2023 ..... ´&..... ÷ÀÚù ..... ÷ÀÛ ûÜæ$Á æØù Ù÷ÀÛ.

.....
ûÜæ$ÁæØ`µèß àõß&ù.

&$æßÂÚ:-

1. ....
(ù´ {$ µ&ß<$ à'æ×) àõß&ù.

2. ....
(ù´ {$ µ&ß<$ à'æ×) àõß&ù.

Copah; Rw;WepUg ,y:……..

kf;fs; tq;fpapd; midj;J Copah;fspdhYk; 2023 Mk; Mz;Lf;fhf rkh;g;gpf;fg;gl Ntz;ba tUlhe;j “ntspg;gLj;jy;;”

kf;fs; tq;fpapy; NritapyPLgl;Ls;s ehk;> ey;yhl;rpf;Fk; Fwpj;j kpfr;rpwe;j juq;fSf;Fk; Vw;g flikfis Nkw;nfhs;tjw;Fk;; vk;ik mh;g;gzpj;Jf;nfhz;Ls;s mNj Neuj;jpy; kf;fs; tq;fp Copah;fspd; eltbf;iffSk; nfhLf;fy; thq;fy;fSk; ntspg;gilj;jd;ikAld; ,Ug;gNj mth;fspd; ek;gpf;ifahfTk; nfhs;ifahfTk; ,Uf;f Ntz;Lk;.

MfNt kf;fs; tq;fpapy; NritapyPLgl;Ls;s Neuj;jpy; Neh;ik> ed;dlj;ij> njhopy;rhh; jpwik vd;gtw;iwg; Ngz Ntz;baJ xt;nthU CopahpdJk; nghWg;ghFk;.

,e;epiyiaf; fUj;jpw;nfhz;L ,j;Jld; ,izf;fg;gl;Ls;s tUlhe;j gpufldj;ij 2023 Mk; Mz;Lf;fhfg; G+h;j;jp nra;J 2023 rdthp khjk; 31Mk; jpfjpad;W my;yJ mjw;F Kd;dh; cjtp nghJ Kfhikahsh; (kdpj tsk;) mth;fsplk; rkh;g;gpf;Fk;gb jathff; Nfl;Lf; nfhs;fpd;Nwhk;.

jaTnra;J ,r;Rw;WepUgk; fpilj;jikgw;wp ,zf;f mYtyhplk; mwptpf;fTk;.

fpist; nghd;Nrfh
gjpw; flikahw;Wk; gpujhd epiwNtw;W mjpfhhp / nghJKfhikahsh;

kf;fs; tq;fp>
jiyik mYtyfk;>
nfhOk;G 02

02.01.2023

tUlhe;j Copah; ntspg;gLj;jy; 2023

…….…….. tjpAk; (**Copah; ,y:……)**
……..… **Mfpa ehd; gpd;tUk**h**W ntspg;gLj;JfpNwd;**

1. NkNy ngah; Fwpg;gplg;gl;l (ntspg;gLj;Jeh;)) Mfpa ehd;> 1961Mk; Mz;bd; 29Mk; ,yf;f jpUj;jg;gl;l kf;fs; tq;fp rl;lj;jpd;%yk; xOq;fhdKiwapy;];jhgpf;fg;gl;l tq;fp epWtdkhd kw;Wk; 1988Mk; Mz;bd; 30Mk; ,yf;f(jpUj;jg;gl;l) tq;fpr; rl;lj;jpd; epakq;fspd; gpufhuk; gjpT nra;ag;gl;l th;j;jf tq;fpahd kf;fs; tq;fpapd; Copauhf ,Uf;fpd;w mNjNeuj;jpy;> jw;nghOJ ehd; ……(jw;nghOJ tfpf;Fk; gjtp/juk;)Mf..…….,y;(jpizf;fsk;/fpis) ,ize;jpUf;fpd;Nwd; vd;gijAk;>

2. ehd; ,yq;ifg; gpuir vdTk;> fPNo Fwpg;gpl;Ls;s tpjj;ijj; jtph;j;J NtW ve;jnthU ehl;bYk; gpuirahf my;yJ epue;ju FbAhpik ngw;wtuhf ,Uf;ftpy;iy vd;gijAk;**>**

   .....
   .....

3.

   - vdJ njhopy; jUeh;

   - vd;Dila Nrit epiyaj;jpd; jiyth;fs;> Jiz Copah;fs; rkepiy Copah;fs;>
   - vd;Dila NritAld; rk;ge;jg;gl;l midj;J cs;sf> Gw thbf;ifahsh;fs;>
   - vd;Dld; nfhLf;fy; thq;fy;fis Nkw;nfhs;fpw Vida midj;J jug;gpdh;>
     MfpNahUld; elj;Jfpw midj;J nfhLf;fy; thq;fy;fspd;NghJk; ehd; Neh;ikahf ,Uf;fpNwd; vd;gijAk;
     flikAld; rk;ge;jg;gl;;l gzpfis Neubahf epiwNtw;WtjhfTk;> vg;nghOJk; xOf;f tpOkpaq;fSld; Nritahw;WtjhfTk;

4. ehd; kf;fs; tq;fpapypUe;J ngw;Wf; nfhz;Ls;s tq;fpf; fld; trjpfs;/ fld; ml;il Nghd;wit rk;ge;jg;gl;l nfhLg;gdTfisj; jhkjg;gLj;jp epYitahf itf;ftpy;iy vd;gijAk;>

5. fPo;f; Fwpg;gplg;gl;Ls;s epWtdq;fisj; jtph;j;J. NtW ve;jnthU tq;fpAlDk; my;;yJ epjp epWtdj;JlDk; fzf;Ffs;/fld; trjpfs; vd;Dila ngahpy; ,y;iy vd;gijAk;>
   .....
   .....
   .....
   Nkw; Fwpg;gpl;l ve;jnthU trjp njhlh;ghfTk; nfhLg;gdTfisj; jhkjg;gLj;jp epYitahf itf;ftpy;iy vd;gijAk;> ehd; NkYk; ntspg;gLj;JfpNwd;.

6. ehd; midj;J re;jh;g;gq;fspYk; nghWg;Gld; nrayhw;WfpNwd; vd;gijAk;> kf;fs; tq;fpapd; ew;ngaiug; ghJfhj;J> vd;trk; xg;gilf;fg;gl;Ls;s ey;y nraw;ghLfs; rk;ge;jkhd juq;fisg; Ngzp nrayhw;WfpNwd; vd;gijAk; ntspg;gLj;JfpNwd;.

7. VNjDk; xOq;FgLj;jy; my;yJ fz;fhzpg;G mjpfhurig> njhopy;rhh; epWtdk;> tprhuiz Mizf;FO> ,yq;ifapy; my;yJ ntspehnlhd;wpy;

rl;lj;jpd;%yk;];jhgpf;fg;gl;l epaharig my;yJ Vida rig Mfpatw;wpdhy;> Nkhrb> Vkhw;Wjy;> Neh;ikapd;ik my;yJ NtNwNjDk; tpjj;jpyhd Kiwaw;w elj;ij njhlh;gpyhd jtnwhd;iw ehd; Ghpe;Js;sjhf my;yJ jtnwhd;wpy; ehd; njhlh;Ggl;Ls;sjhf fz;Lgpbf;fg;gltpy;iy vd;gijAk;>

8. ehd; kf;fs; tq;fpapy; nra;Ak; njhopiy jtph;j;J NtW ve;jnthU njhopypy;
my;yJ tpahghuj;jpy; <Lgltpy;iy vd;gijAk;> fPNo fhl;lg;gl;Ls;s tpjj;ijj; jtph;j;;J Vida Nkyjpf tUkhdk; ngwtpy;iy vd;gijAk;>
.....
.....
.....

9. vd;Dila tho;f;ifj; JizAk; gps;isfSk; gpd;tUk; tpahghuj;ij khj;jpuk; elj;Jfpd;wdh; vd;gijAk;>
.....
.....
.....

10. fPNo fhl;lg;gl;Ls;stpjj;ijj; jtph;j;J> NkNy Fwpg;gplg;gl;Ls;s
tpahghuj;jpdhy; kf;fs; tq;fpAld; thbf;ifahsuhf my;yJ tpepNahf];juhf my;yJ NtW ve;jtpjj;jpYk; th;j;jf nfhLf;fy; thq;fy;fis elj;jtpy;iy vd;gijAk;>

....
(tpahghuj;jpd; ngah;) (tpahghu nfhLf;fy; thq;fy; tif)

11. 2022 Mk; Mz;Lf;fhd gpd;tUk; thpfs; vd;dhy; nrYj;jg;gl;Ls;sd vd;gijAk;>

....
(nrYj;jg;gl;l thpfspd;tif) (Nfhg;G ,y.)

12. ,yq;ifapy; tq;fpr; rl;lj;jpdhy; Ntz;lg;gLfpd;w ,ufrpafhg;G cWjp nkhopapy; ifnahg;gkpl;Ls;Nsd; vd;gijAk;>

13. VNjDk; xOq;FgLj;jy; mjpfhurig my;yJ fz;fhzpg;G mjpfhurig>
njhopy;rhh; epWtdk;> VNjDk; tprhuiz Midf;FO> ,yq;ifapy; my;yJ ntspehnlhd;wpy; rl;lj;jpd;%yk;];jhgpf;fg;gl;l epaharig my;yJ Vida rig Mfpatw;wpdhy; Nkhrb> Vkhw;Wjy;> Neh;ikapd;ik my;yJ Vida Fw;wtpay; eltbf;if njhlh;gpyhd Fw;wr;rhl;Lf;F mwptpj;jiy xg;gilj;jjd; fhuzkhf Nkw;nfhs;sg;gLfpd;w Gydha;Tf;F my;yJ tprhuizf;F ehd; cs;shftpy;iy vd;gijAk;.

14. epjp Kfhikj;Jtk; my;yJ xOf;ff;NfL njhlh;gpyhd Fw;wr;nraypy; ehd; <Lgl;ljhf ,yq;ifapy; my;yJ ,yq;iff;F ntspapy; my;yJ Ntnwe;j tpjj;jpYk; ePjpkd;wnkhd;wpdhy; Fw;wj; jPh;g;gspf;fg;gltpy;iy vd;gijAk;.

15. ehd; fldpWf;f tifaw;wth; my;y vd;gijAk; ,yq;ifapy; my;yJ ntspehnlhd;wpy; ntspg;gLj;jg;gl;l tq;FNwhj;jhdth; my;y vd;gijAk;

16. ,yq;ifapy; my;yJ ntspehnlhd;wpy; ePjpkd;wnkhd;wpdhy; toq;fg;gl;l jPh;g;ig my;yJ fl;lisia my;yJ fld; kPsspg;ig ehd; epiwNtw;wj;
jtwtpy;iy vd;gijAk;>

17. ehd; rpj;jRthjPdkw;wth; vd ,yq;ifapy; my;yJ ntspehnlhd;wpd; jFjp tha;e;j epahahjpf;fj;jpdhy; ntspg;gLj;jg;gltpy;iy vd;gijAk;

18. ve;jnthU xOq;FgLj;jy; my;yJ Nkw;ghh;f;Fk; mjpfhu rigapdhy; toq;fg;gl;l fl;lisapd; kPJ vdJ Kd;ida NritapypUe;J / jw;Nghija NritapypUe;J ehd; ePf;fg;gltpy;iy my;yJ ,ilepWj;jg;gltpy;iy
vd;gijAk;

19. midj;Jtpjkhd Gw /cs;sf epajpr;rl;lq;fs; kw;Wk; xOq;Ftpjpfs; kw;Wk; kf;fs; tq;fpapd; midj;J cs;sf nfhs;iffs; eilKiwfs; vd;gtw;iwg; gpd;gw;wp nrayhw;w fl;Lg;gl;;Ls;Nsd; vd;gijAk;

20. vkJ gy;NtW tifahd giza nghUshsh;fSld; Nkw;nfhs;sg;gLfpd;w midj;J tpahghu mYty;fisAk; kpf ftdkhf Nkw;nfhs;Ntd; vd;gijAk;

21. kf;fs; tq;fpapd; nrhj;Jf;fis mjpfhukspf;fg;gl;l NjitfSf;fhf khj;jpuk; gad;gLj;JNtd; vd;gijAk;

22. ehd; kf;fs; tq;fpapd; Copauhf Nritahw;Wtjw;F nghUj;jkhd rhpahd egh; vd;gij jplkhf ek;GfpNwd; vd;gijAk;> ntspg;gLj;Jfpd;Nwd;.

..... My; 2023 ..... khjk; ..... jpfjp ..... ,y; ntspg;gLj;jg;gl;lJ.

.....
ntspg;gLj;Jehpd; ifnahg;gk;

rhl;rp:-

1. ....
(ngah;;) (Nrit ,yf;fk;) ifnahg;gk;

2. ....
(ngah;); (Nrit ,yf;fk;) ifnahg;gk;

Schedule I

Assessing Fitness and Propriety of Chief Executive Officer[1] and Officers Performing Executive Functions of Licensed Banks

AFFIDAVIT

Section I: Information to be submitted in terms of Sections 42(2), 44A and 76H of the Banking Act, No. 30 of 1988 (As amended)

Passport size photo *(Taken within last 6 months)*

Name of the Bank: People's Bank

I ..... holder of National Identity Card No. ..... and Passport No. ..... of ..... being a ..... do hereby solemnly declare and affirm/ make oath and state as follows

(1) I am the deponent/affirmant above named and I have been proposed to be appointed as ..... of People's Bank which is a licensed commercial bank under the Banking Act No. 30 of 1988.

(2) I state/affirm that my personal details are as follows:

2.1	(i) Name with Initials:					
	(ii) Title:				(iii) Age as at date of signing the affidavit: **yy/mm/dd**	
	(iv) Date of Birth:				(v) Gender:	
	(vi) Civil Status:		(vii) Nationality:		(viii) Citizenship:	
					(ix) Local/ expatriate:	
2.2	Contact Details	Permanent Address:				
		Residential Address:				
		(i) Telephone	Mobile			
			Fixed line			
			Fax			
		(ii) E-mail	Personal			
			Official			
2.3	(i) Proposed Post/ Designation in the bank:				(ii) Date of appointment to the Post/ Designation **dd/mm/yyyy**	
2.4	(i) Details of Appointment of Chief Executive Officer/ Officers Performing Executive Functions					
	New Appointment		Contract Basis	√	Lateral Move	
	Promotion		Renewal of		Other *(Please specify)*	

			Contract			
2.5	2.5.1 Details of close relations in terms of Section 86 of the Banking Act					
	(i) Full name of the Spouse:					
	3.1 **NIC No:**				(iii) Passport No	
	2.5.2 Details of dependent children					
	(i) Full Name				(ii) NIC No:	(iii) Passport No.

(3) I state/affirm that I possess the following academic and/ or professional qualification/s:

Qualification (Academic	Relevant discipline	Country	Name of the Institution	Year of Completion
BSc in MIS (Management Information Systems)				
Qualifications (Professional)				
Higher Diploma in Computer Based Information Systems				
Diploma in Computer Systems Design				

(4) I state/affirm that the effective experience that I possess in banking, finance, business or administration or of any other relevant discipline is as follows:

Current Positions	Name of the Institution/own business	Designation/ Position	Nature of Appointment (as per item 2.4 as applicable)	Work Specialization	Date of Appointment (dd/mm/yyyy)	Service period (dd/mm/yyyy to dd/mm/yyyy)
Directorships						
(i) Specified Business Entities						
(ii) Other						
Other Positions						

Previous Positions						
Directorships						
(i) Specified Business Entities						
(ii) Other						
Other Positions						

(5) In addition to the above information, I state/affirm that I possess the following additional qualifications:

Special Assignments/ Consultancy	Name of the Institution	Description	Service Period (dd/mm/yyyy to dd/mm/yyyy)
(i)			
(ii)			
Outstanding Contributions (Publications, Seminars Conducted, Research etc.)			
Topic of the Research/ publication		Institute/ Place	Year

(6) I state/affirm that I do hold shares in licensed banks & their related companies (Subsidiaries, Associates and Other Companies), finance companies, leasing companies and primary dealers registered with/ licensed by the Central Bank of Sri Lanka.

Name of the Institution/s	Voting/ Non-voting	No. of Shares		Percentage holding	
		Direct	Indirect	Direct	Indirect

(7) Business Transactions

7.1. I state/affirm that I have deposits with the bank, its subsidiaries or associate companies. (if yes, please state name of the institution/s).

7.2. I state/affirm that I currently have the following business transactions with the licensed bank & its related companies (Subsidiaries, Associates and Other Companies), finance companies, leasing companies and primary dealers registered with/ licensed by the Central Bank of Sri Lanka.

Name of the Institution/s	Date of Transaction (dd/mm/yyyy)	Amount as at dd/mm/yyyy (Rs.mn)		Classification (performing/ non-performing)	Type and Value of Collateral (Rs.mn)	% of Bank's regulatory Capital
		Limit	Outstanding			

Borrowings					-	
Investments						

(8) **Appointments, Shareholdings and Business Transactions of Close Relations**

8.1. I state/affirm the following details of my close relations presently employed as Directors, Chief Executive Officers or Officers Performing Executive Functions of any licensed bank, its related companies (Subsidiaries, Associates, and Other Companies), finance companies, leasing companies and primary dealers registered with/ licensed by the Central Bank of Sri Lanka.

Name of the Close Relation	Name of the Institution	Position Held

8.2. I state/affirm the following details of direct or indirect share ownership in the licensed bank, its related companies (Subsidiaries, Associates, Other Companies), finance companies, leasing companies and primary dealers registered with/ licensed by the Central Bank of Sri Lanka, if any, presently held by any close relation.

Name of the Close Relation	Name of the Institution	No. of Shares		Percentage Holding	
		Direct	Indirect	Direct	Indirect

8.3. I state/affirm that the close relation of mine currently has the following business transactions with the licensed bank, its related companies (Subsidiaries, Associates and Other Companies), finance companies, leasing companies and primary dealers registered with/ licensed by the Central Bank of Sri Lanka

Name of the Close Relation	Name of the Institution	Date of Transaction (dd/mm/yyyy)	Amount as at dd/mm/yyyy (Rs.mn)		Type and value of collateral (Rs.mn)	% of Bank's regulatory capital
			Limit	Outstanding		
Borrowings						
Investments						

(9) I state/affirm that there is no finding of any regulatory or supervisory authority, professional association, any Commission of Inquiry, tribunal or other body established by law in Sri Lanka or abroad, to the effect that I have committed or have been connected with the commission of any act which involves fraud, deceit, dishonesty or any other improper conduct.

(10) I state/affirm that I am not subject to an investigation or inquiry consequent upon being served with notice of a charge involving fraud, deceit, dishonesty or other similar criminal activity, by any regulatory authority, supervisory authority, professional association, Commission of Inquiry, tribunal or other body established by law, in Sri Lanka or abroad.

(11) I state/affirm that I have not been convicted by any Court in Sri Lanka or abroad in respect of a crime committed in connection with financial management or of any offence involving moral turpitude.

(12) I state/affirm that I am not an undischarged insolvent and have not been declared a bankrupt in Sri Lanka or abroad.

(13) I state/affirm that I have not failed, to satisfy any judgment or order of any Court whether in Sri Lanka or abroad, or to repay a debt.

(14) I state/affirm that I have not been declared by a Court of competent jurisdiction in Sri Lanka or abroad, to be of unsound mind.

(15) I state/affirm that I have not been removed or suspended by an order of a regulatory or supervisory authority from serving as a Director/ Chief Executive Officer/ Officer performing Executive Functions or any other officer in a licensed bank or any other financial institution or corporate body, in Sri Lanka or abroad.

(16) I state/affirm that I have not been a Director, Chief Executive Officer or have not held any other position of authority in any bank or financial institution –

(i) Whose license has been suspended or cancelled; or
(ii) Which has been wound up or is being wound up, or which is being compulsorily liquidated; whether in Sri Lanka or abroad.

(17) I state/affirm that I am aware of the provisions of the Banking Act on assessment of fitness and propriety of my position and confirm that the above information is to the best of my knowledge and belief true and complete. I undertake to keep the bank fully informed, as soon as possible, of all subsequent events, which are relevant to the information provided above.

(18) I state/affirm that I am not prevented by any written law from being appointed to the above post.

(19) I state/affirm that to the best of my knowledge I am a fit and proper person to be appointed or nominated as ..... of a licensed commercial bank in terms of the provisions of the Banking Act.

The averments contained herein were read over to the deponent/affirmant who having understood the contents hereof and having accepted same as true, swore/affirmed to and placed his/her signature at Colombo on this ..... day of ..... 2021.

.....

Affix Stamps as applicable

Before me

JUSTICE OF THE PEACE /

COMMISSIONER FOR OATHS

Section 2: To be filled by the Company Secretary

1. Corporate Information

Recommendation of the Nomination Committee/ Appointing Authority for the Chief Executive Officer and Officers Performing Executive Functions	
Assessment Criteria (Please specify the specific knowledge/ skills considered by the Nomination Committee/ Appointing Authority)	
Recommendation (Please attach minutes of the resolution/ decision of the Nomination Committee/ Appointing Authority)	

2. Remarks of the Board of Directors
   (1) Any other explanation/ information regarding the details furnished above.
   (2) Approval has been granted by the Board of Directors for above proposed appointment at the meeting dated

Name:

Date:

Signature of the Company Secretary and the official stamp

Section 3:
For Chief Executive Officer (Local banks) – To be filled by the Chairman
For Chief Executive Officer/ Country Head (Foreign banks) – To be filled by the Regional Head
For Officers Performing Executive Functions – To be filled by the Chief Executive Officer
Declaration:

(1) Any other explanation/ information regarding the details furnished above and other information considered relevant for assessing the suitability of the Chief Executive Officer/ Officer Performing Executive Functions of the bank.

(2) I confirm that, in terms of Section 44A/ Section 76H read with Section 44A of the Banking Act, No.30 of 1988, the officer referred to above is fit and proper to be appointed as the Chief Executive Officer/ an Officer Performing Executive Functions of People's Bank.

Date:

Signature of the Chairman/ Regional Head/ Chief Executive Officer and the official stamp