



---

**CUSTOMER DUE DILIGENCE & ANTI- MONEY LAUNDERING /  
COMBATING FINANCING OF TERRORISM / COUNTERING  
PROLIFERATION FINANCING (CDD & AML/CFT/CPF) POLICY**

---

**MCB SRI LANKA OPERATIONS**

**2023**

**Version 8.0**

The Policy document is for internal use of staff of MCB Bank Limited and should be accorded the same level of secrecy as required for other internal policies of the Bank. Copies of this document should not be shared prior to the approval of the Chief Compliance Officer and Head International Banking.

All Rights Reserved

### Document Control Sheet

Title Of Policy	Customer Due Diligence & Anti-Money laundering / Combating the Financing of Terrorism & Countering Proliferation Financing (CDD & AML/CFT/CPF) Policy – MCB Sri Lanka Operations
Associated Key Risks	Money Laundering / Financing of Terrorism / Proliferation Financing / Compliance / Operational / Legal / Regulatory / Reputational / Financial risks
Policy Owners	International Banking Compliance and Controls Group
Review Frequency	Once in a year or earlier as required.
First Approval Date	20 <sup>th</sup> October, 2015
Last Approval Date	16 <sup>th</sup> November, 2022
Current Review Date	October 2023
Next Review Date	October 2024
Version (Existing / New)	Existing (7.0) / New (8.0)
Reviewed by:	Operations Group International Banking Audit & Risk Assets Review (RAR) Group Risk Management Group Legal Affairs Group Compliance and Controls Group Oversight & Monitoring Group Human Resource Management Group
Concurred by:	President & Chief Executive Officer (CEO)
Recommended By	Compliance Review and Monitoring Committee (CR&MC)
Approved By	Board of Directors (BoD)

## Table of Contents

<b>1. INTRODUCTION .....</b>	<b>4</b>
<b>2. SCOPE.....</b>	<b>6</b>
<b>3. OBJECTIVES OF THE POLICY .....</b>	<b>7</b>
<b>4. GOVERNANCE .....</b>	<b>7</b>
<b>5. ORGANIZATIONAL CHART OF COMPLIANCE FUNCTION .....</b>	<b>9</b>
<b>6. KEY ELEMENTS OF CUSTOMER DUE DILIGENCE (CDD) .....</b>	<b>9</b>
<b>7. CORRESPONDENT BANKING and MONEY SERVICE BUSINESSES (MSBs) .....</b>	<b>17</b>
<b>8. TRADE BASED MONEY LAUNDERING .....</b>	<b>17</b>
<b>9. EMPLOYEE DUE DILIGENCE .....</b>	<b>17</b>
<b>10. RECORD KEEPING .....</b>	<b>18</b>
<b>11. E-COMMERCE .....</b>	<b>18</b>
<b>12. PROLIFERATION FINANCING .....</b>	<b>18</b>
<b>13. TRAINING.....</b>	<b>19</b>
<b>14. CDD &amp; AML/CFT/CPF HANDBOOK SRI LANKA OPERATIONS.....</b>	<b>19</b>
<b>15. APPLICABILITY &amp; PERIODICITY FOR REVIEW OF POLICY .....</b>	<b>19</b>
<b>16. GLOSSARY .....</b>	<b>20</b>

## 1. INTRODUCTION

MCB Bank-Sri Lanka (the Bank) is committed to combat Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF). Its commitment to the inhibition of ML / TF / PF is reflected in this policy in compliance with the legislative and regulatory requirements of authorities in Sri Lanka as well as with the requirements applicable on MCB Head Office in Pakistan as per methodology defined in SBP regulations / guidelines issued from time to time.

Management should ensure compliance with all relevant applicable laws, rules and regulations specifically the following (amended from time to time):

- Prevention of Money Laundering Act, No.05 of 2006 (PMLA);
- Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005 (CSTFA);
- Financial Transaction Reporting Act, No. 06 of 2006 (FTRA);
- Know-Your-Customer (KYC) and Customer Due Diligence (CDD) Rules prescribed by Financial Intelligence Unit (FIU) under Financial Transaction Reporting Act No. 06 of 2006 (FTRA) amended from time to time;
- SBP’s “Anti-Money Laundering, Combating the Financing of Terrorism & Countering Proliferation Financing (AML/CFT/CPF) Regulations” issued vide BPRD Circular Letter No. 33 of 2022 dated 28<sup>th</sup> November, 2022;
- SBP’s “Framework for Risk Management in Outsourcing Arrangements by Financial Institutions” issued vide BPRD Circular No. 06 of 2019 dated 17 December, 2019;
- SBP Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing issued vide FE Circular No. 04 dated 14 October, 2019;
- SBP’s “AML/CFT/CPF Regulations - Guidelines on Targeted Financial Sanctions (TFS) under UNSC Resolutions” issued vide BPRD Circular letter no. 44 of 2020 dated 30 September, 2020;
- High Risk Jurisdictions Rules, 2020 issued by Ministry of Finance, Government of Pakistan vide S.R.O. 951(I)/2020 dated October 01, 2020; and
- Applicable relevant AML/CFT/CPF Regulations / Guidelines issued by State Bank of Pakistan (SBP) / Central Bank of Sri Lanka (CBSL), from time to time.

In order to further strengthen the regulatory framework and to curb Money Laundering and Terrorist Financing risk(s), the Central Bank of Sri Lanka (CBSL) has published CDD Rules made by the FIU Sri Lanka cited as the Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016 covering the following aspects:

<b>Key Elements</b>	<b>Area(s) Covered</b>
Risk Based Approach and Risk Assessment	Banks must implement Risk Based Approach (RBA) in establishing AML/CFT/CPF Program prior to establishing business relationship and throughout the course of relationship with customers. Bank must take measures to identify, assess, monitor, manage and mitigate ML/TF/PF risks to which it is exposed.
Customer Due Diligence	CDD Measures for Identifying, Verifying and Accepting new customers and maintaining relationship with existing customers.
Correspondent Banking	CDD measures for establishing and maintaining relationship with Correspondent and Respondent Banks / Financial Institutions (FIs)
Wire Transfers / Fund Transfers	Responsibilities of Ordering, Intermediary and Beneficiary Institutions (as applicable) involved in processing wire transfers / fund transfers.
Maintenance of Accounts and General rules	All Measures prescribed by Central Bank of Sri Lanka under Licensed Banks and Registered Finance Companies KYC and CDD Rule No. 1 of 2016 and subsequent amendments issued by FIU, SL.  Financial Transactions Reporting Act No. 6 of 2006 is to be adhered to in letter and spirit.
Reporting of Suspicious Transactions (STRs)	Guidelines for Reporting of Complex, Unusually Large, and out of pattern Transactions.
Developing Technologies	Money Laundering, Terrorist Financing and Proliferation Financing risk(s) that may arise from the use of new and developing technologies especially those having features of anonymity or inconsistency with the basic principles of CDD Measures.
Penalty	Failure to comply with Anti-Money Laundering (AML) / Combating the Financing of Terrorism (CFT) & Countering Proliferation Financing (CPF) requirements may result in penal action(s) such as fines and imprisonment in accordance with the applicable laws, rules and regulations.
Internal Controls, Policies, Compliance, Audit and Training	Requirements relating to development of Controls, Policies, Procedures, Training programs to ensure compliance with AML/CFT/CPF laws, rules and regulations.
Beneficial Ownership	Determining and assessing the ultimate beneficial ownership structures of the Bank's customers.

In addition to the above, the international best practices such as Financial Action Task Force (FATF) Recommendations and Guidance on Correspondent Banking Services, Basel Committee on Banking Supervision (BCBS) guidelines on sound management of risk related to money

laundering, financing of terrorism, proliferation financing and Customer Due Diligence and United Nations Security Council (UNSC), European Union (EU), Office of Foreign Assets Control (OFAC) resolutions / concerning sanctions and any further development in the above from time to time should also be followed to prevent the possible use of the Bank as a conduit for money laundering, terrorist financing and/or financing for proliferation activities.

Amid increasing focus of banks and regulatory bodies on curbing Money Laundering (ML) / Financing of Terrorism (TF) and Proliferation Financing (PF) activities, banks are required to have comprehensive AML/CFT/CPF policy entailing guidelines on bank's ML/TF/PF risk management approach, to identify, assess, monitor, manage and mitigate these risks on an ongoing basis. Bank's Management should manage these risks throughout the life cycle of its customers related to channels / products / jurisdictions / services / transnational activities and relationships starting from onboarding of new business relationships till closure as well as for all walk in or occasional customers.

## **2. SCOPE**

This policy applies to each and every business segment of MCB Sri Lanka operations and all its employees to effectively mitigate the risk of ML/TF and PF. The document shall be read in conjunction with the AML/CFT/CPF Policy applicable in MCB (Pakistan) to ensure adherence to Regulation-13 (sub-section 6, 7, and 8) and other applicable sections of AML/CFT/CPF Regulations issued by State Bank of Pakistan (SBP) vide BPRD Circular Letter no. 33 of 2022 dated 28<sup>th</sup> November, 2022 as modified from time to time and Rule No.14 of (Customer Due Diligence) Rules, No. 1 of 2016 issued by FIU Sri Lanka.

Bank is prone to the risk of ML/TF/PF thereby being misused by criminal elements for their ulterior motives of conducting & facilitating terrorism incidents or aiming at concealing and/or changing the identity of illegally obtained money, so that it appears to have originated from legitimate sources. To address the risks stemming from such customers, this policy will be a guiding document for the Bank employees towards managing the customer risk in an effective way using the Risk Based Approach (RBA). Thus, the Customer Due Diligence process should involve the application of RBA Guidelines, through the introduction of sophisticated and quantified Risk Rating Sheet(s)/Customer Risk Profiling Form(s). The bank's management shall develop set of documents for various customer types to ensure CDD/EDD process for mitigation of associated ML/TF/PF risk and convey the same to the business units for compliance at their end.

Given the prevailing ML/TF/PF risks in Trade and Transnational transactions, international and local regulatory bodies have increased focus on management of Trade Based Money Laundering (TBML) risks and multiple regulations are coming into effect. SBP has also issued regulatory Framework for Managing Risks of TBML and TF that entails comprehensive guidelines for banks to be implemented to manage these risks. A comprehensive Manual/SOP should be developed for implementation of these guidelines and technology based solutions as specified in SBP's "AML/CFT/CPF Regulations" dated November 28, 2022 and "Framework for Managing Risks of TBML and TF" dated 14 October, 2019, amended from time to time as well as relevant instructions issued by CBSL,.

Bank's Management shall apply its AML/ CFT/ CPF policies in Sri Lanka Operations to the extent that laws, rules and regulations of the host country permit. Where the AML/ CFT/ CPF requirements in the host country or jurisdiction differ from those in Pakistan, management shall require its Sri Lanka operations to apply the higher of the two standards, to the extent that the law of the host country or jurisdiction so permits.

Where the law of the host country conflicts with the AML/ CFT/ CPF requirements of Pakistan so that the Sri Lanka Operations are unable to observe the higher standards, management through

Compliance & Controls Group (CCG) at Head office shall report this to SBP and comply with such further directions as may be issued.

The ultimate responsibility of ensuring effective AML/ CFT/ CPF controls rests with BoD. Therefore, management shall ensure provision of adequate, reliable, periodic information to the BoD through its Compliance Review & Monitoring Committee (CR&MC), for ensuring effective oversight, monitoring and accountability.

### **3. OBJECTIVES OF THE POLICY**

Objectives of the policy include the following in line with and subject to regulatory requirements of Central Bank of Sri Lanka and State Bank of Pakistan:

1. Compliance of all statutory, regulatory and legal obligations to manage and mitigate Legal, Regulatory, Reputational, Financial and risks emanating from the banking operations.
2. Acceptance of only bona fide and legitimate customers/transactions.
3. Verify the identity of customers using reliable and independent sources.
4. Conduct Ongoing Monitoring of customer accounts and transactions to prevent or detect potential ML / TF / PF activities.
5. Implement Customer Due Diligence process using risk-based approach.
6. Effectively manage customer-driven risks by using procedures laid down in CDD & AML/CFT/CPF Handbook of MCB Sri Lanka duly approved by the President.
7. To safeguard the bank from being used as a conduit in money laundering, terrorism financing, trade-based money laundering and proliferation financing.
8. To ensure implementation of Targeted Financial Sanctions (TFS) related to Terrorism Financing (TF) and Proliferation Financing (PF).
9. To put in place appropriate controls for prevention, detection and reporting of suspicious activities in accordance with applicable laws / rules / regulations / procedures.
10. To ensure that bank has implemented effective controls to mitigate the AML/CFT/CPF risks.
11. To maintain adequate record as per the legal, regulatory requirements as well as Bank's Record Management Policy.

### **4. GOVERNANCE**

#### **4.1. Board of Directors**

Bank shall define a proper mechanism to inform the board of directors (or a committee of the board) regarding status of AML/CFT/CPF program, compliance initiatives, compliance deficiencies and other regulatory requirements.

#### **4.2. Senior Management**

Bank's Senior Management will define ML/FT/PF risk appetite and ensure implementation of appropriate governance, internal policies, procedures, controls and operating systems; oversight of AML/CFT/CPF compliance program and application of directives of competent authorities. Detailed roles and responsibilities should be mentioned in CDD & AML/CFT/CPF Handbook Sri Lanka operations.

### 4.3. Department Head Compliance

The Bank shall appoint a Department Head Compliance in terms of Section 14 of the FTRA (Financial Transactions Reporting Act, No. 6 of 2006); who will be responsible for the overall management of regulatory and reputational risk of MCB Sri Lanka operations by effective implementation and ensuring compliance with the local requirements, the Applicable Laws and Regulations and the Bank's policies and procedures with special focus on ML/TF/PF risks throughout MCB Sri Lanka operations.

The Department Head Compliance shall specifically be responsible for the following:

- Ensuring the Bank's compliance with the requirements of FTRA No. 6 of 2006;
- Establishing and maintaining AML/CFT/CPF procedures/policies;
- Ensure compliance with the AML Laws and any other applicable AML/CFT/CPF legislation and regulations of home and host country;
- Ensuring day-to-day compliance with AML/CFT/CPF policies and procedures;
- To assist various business segments and support functions of the Bank in establishing and maintaining procedures and systems to:
  - Implement the customer identification requirements under section 2 of FTRA;
  - Implement procedures for the record keeping and retention requirements under section 4 of FTRA as well as those of Bank's Record Management Policy;
  - Implement the process of monitoring required under section 5 of FTRA;
  - Implement the reporting requirements under sections 6, 7, 8 and section 22 in relation to auditors and report all information to FIU as required in Section 7 of Financial Transaction Reporting Act No. 06 of 2006;
- Make its officers and employees aware of the laws, rules and regulations relating to money laundering, financing of terrorism and proliferation financing;
- Screen all persons before hiring them as employees;
- Ensure effective / continuous professional education and training / awareness programs are in place and accordingly adhered to at all levels.
- Ensure reporting of suspicious transactions (STR) as well as Cash and Financial Transaction Report, Electronic Fund Transfer In and Out in compliance with the relevant applicable laws, rules and regulations as well as CDD & AML/CFT/CPF Handbook Sri Lanka operations.
- Keep abreast with latest trends and developments in the field of compliance with special focus on ML/TF/PF.
- Ensure reporting of terrorism incidents and attempted transactions to the Combatting Financing of Terrorism (CFT) Desk, CCG at Head Office.
- Ensure conducting annual ML / TF / PF risk assessment of bank's Sri Lanka operations in line with the Regulation R-1 of the SBP's "AML/CFT/CPF Regulations" dated November 28, 2022, FIU Regulations on Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018 dated 11<sup>th</sup> January 2018 amended from time to time and any other relevant regulation(s).

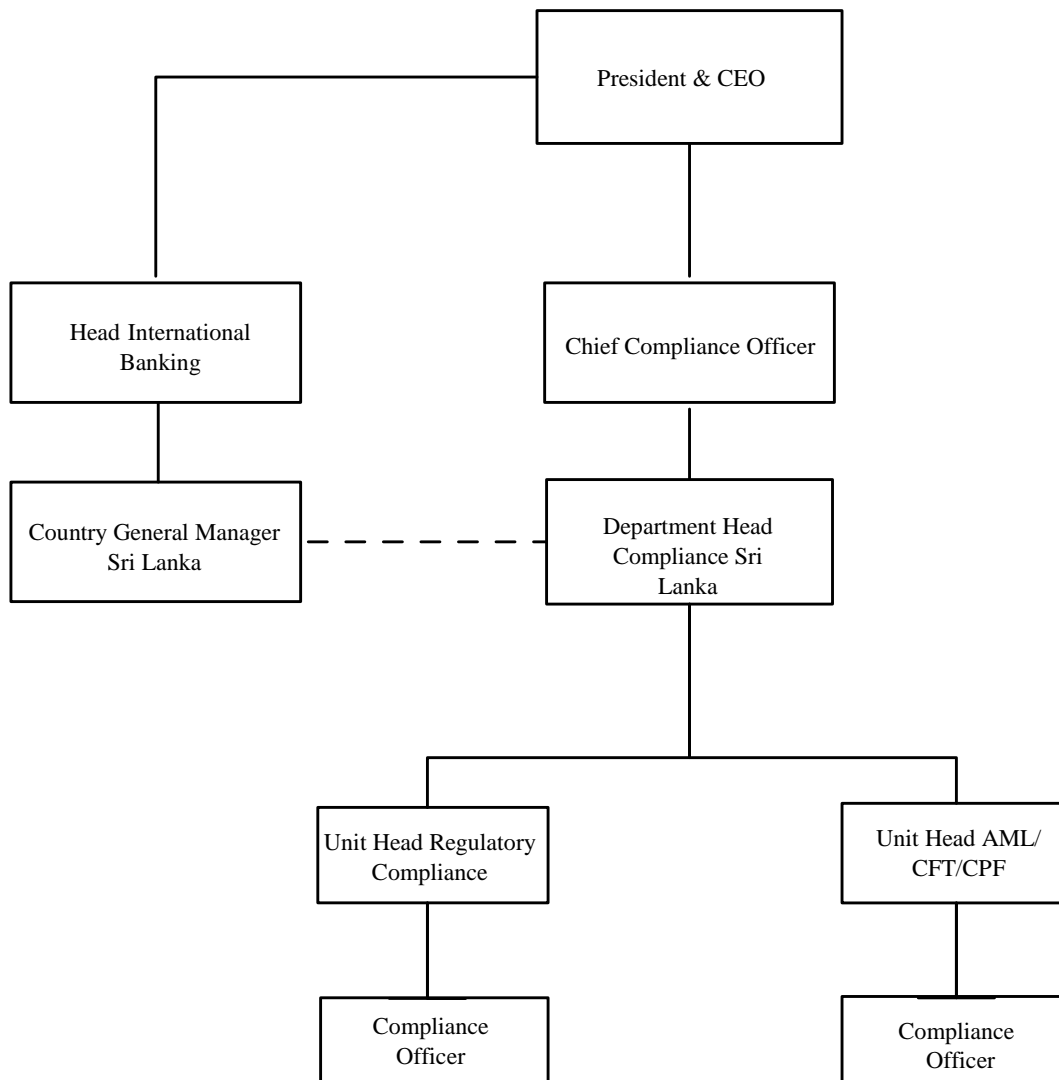


**4.4. Independent Audit Function**

Bank has in place an independent internal audit function to test the effectiveness and adequacy of internal polices, controls and procedures relating to combating the crimes of money laundering, financing of terrorism, of illegal organizations and proliferation financing. Detailed roles and responsibilities should be mentioned in CDD & AML/CFT/CPF Handbook Sri Lanka operations.

**5. ORGANIZATIONAL CHART OF COMPLIANCE FUNCTION**

**Organizational Chart**



**6. KEY ELEMENTS OF CUSTOMER DUE DILIGENCE (CDD)**

**6.1 CUSTOMER IDENTIFICATION:**

The Bank will serve only the genuine person(s) and all out efforts should be made to determine the true identity of every customer and record the information on KYC form/ Account Opening Form and relevant IT systems. Minimum set of documents shall be obtained from various types of customer(s), at the time of opening an account, as prescribed in Anti-Money Laundering,

Combating the Financing of Terrorism & Countering Proliferation Financing (AML/CFT/CPF) Regulations and other applicable laws, rules and regulations of State Bank of Pakistan (SBP) / Central Bank of Sri Lanka.

Customer relationship is only to be established on the strength of a valid Passport/ National Identity Card (NIC)/ Driving License (DL) number or where the customer is not a natural person, the registration/ incorporation number, business registration number or special resolution/authority, in case of Charity Accounts etc. (as applicable).

For walk-in-customers / Occasional customers, to establish and validate the true identity of the person(s) executing the transactions either for self or if the person is acting on behalf of some other person(s), complete originator information must be obtained and identities must be invariably verified.

For non-face-to-face customers, Bank's management shall put in place operational procedures in line with the FIU regulation Revised Guidelines for Non Face-to-Face Customer Identification and Verification Using Electronic Interface Provided by the Department for Registration of Persons, No. 3 of 2020 dated 30th December 2020 to mitigate the risk(s) attached with non-face-to face prospective customer(s) and establish identity of the client. Equally effective customer identification procedures for non-face-to-face customers shall be applied as for those available for interview.

In case Bank's Management is unable to satisfactorily complete required CDD measures for any potential customer, account shall neither be opened nor any service provided and consideration shall be given if the circumstances are suspicious so as to warrant the filing of an STR even though the account opening stands denied to the potential customer.

If the business unit is unable to satisfactorily complete CDD requirements of an existing customer, the relationship shall be terminated and reporting of suspicious transaction be considered as per law. Further, Bank's Management shall serve a prior notice and record cogent reasons for terminating business relationships in its systems. In cases where Bank's Management is suspicious of money laundering, terrorist financing, proliferation financing or other criminal activity, and it reasonably believes that performing the CDD process will tip-off the customer, it will not pursue the CDD process, and instead file an STR.

## **6.2 CUSTOMER VERIFICATION**

The Bank's Management shall identify the beneficial ownership of accounts/ transactions by taking all reasonable measures. Identification of the customer and beneficial owner will be verified using documents obtained from the customer as well as through available reliable sources and record the same in relevant IT system(s).

Extra care is essential where the customer is acting on behalf of another person, and reasonable steps must be taken to obtain sufficient identification data to verify the identity of that other person as well. For customers that are legal persons or for legal arrangements, management is required to take reasonable measures to ensure that:

- (i) The identity of the natural person(s) who ultimately have a controlling ownership interest in a legal person, and
- (ii) To the extent that there is doubt under (i) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s), or where no natural person exerts control of the legal person or arrangement through other means; and
- (iii) Where no natural person is identified under (i) or (ii) above, the identity of the relevant natural person who holds the position of senior managing official.

Identity documents, wherever required as per relevant AML/CFT/CPF Regulations and other applicable Laws, Rules and Regulations, are to be verified. Verification of the identity of the customer(s) and beneficial owner(s) shall be completed before business relationship is established or a transaction is processed.

### **6.3 CUSTOMER ACCEPTANCE**

Customer will only be accepted once the aforementioned formalities have been completed in letter and spirit and in accordance with the requirements of the applicable Laws, Rules and Regulations.

Following accounts will not be opened/maintained by MCB Bank where;

- a) Identity, beneficial ownership, or information on purpose and intended nature of business relationship is not clear.
- b) Name of the individual customer/organization (including such individuals who are authorized to operate account(s) and the members of governing body / directors / trustees of an entity) appears in the Proscribed / Designated / Sanctioned individuals / entities lists.
- c) Proscribed / Designated / Sanctioned entities and persons or to those who are known to be associated with such entities and persons, whether under the proscribed / designated / sanctioned name or with a different name.
- d) Anonymous / fictitious or numbered accounts.
- e) Shell Banks and Corporations.
- f) Client or business segment(s) black listed by the Bank and / or by the Regulators or sanctioned by any multilateral or treaty organizations.
- g) The Bank is unable to satisfactorily complete required CDD measures.
- h) Customers / account holders who transact / deal in Virtual currencies / Bitcoins etc.
- i) Any other activity forbidden by the law e.g. gambling, human smuggling etc.
- j) Government accounts opened in the name of Government Officials
- k) Illegal money value transfer services (MVTS) including unauthorized / unlicensed money changers/ prize bond dealers.
- l) Payable through accounts. (Definition: An account maintained at the correspondent bank by the respondent bank which is accessible directly by a third party to effect transactions on its own (Respondent bank's) behalf).
- m) Non-resident customers from high risk jurisdictions subject to a call for action by FATF.

### **Customers involving Additional Scrutiny & Approvals**

In addition to the above specified prohibitions, certain other types of customers pose higher level of ML/TF/PF risks. All such customers would require enhanced scrutiny / analysis from AML/CFT/ CPF perspective throughout their span of operations i.e. from onboarding till closure of account. Enhanced Due Diligence (EDD) measures must be applied on such account types including approval of the senior management as defined in the CDD/AML/CFT/CPF Procedural Handbook – Sri Lanka Operations. This enhanced scrutiny/ analysis should ensure that account behavior in these categories commensurate with the bank's knowledge of the account profile. Any deviation observed must be treated as per the prevailing regulations including filing of STR and termination of the business relationship. Examples of such High Risk customer types are as follows; however, bank's management may add on to this list by considering the criticality of ML/TF/PF risks associated with other types of customers:

- NGOs / INGOs / NPOs / Charities / Trust / Club / Societies / Madrassah / associations;
- Political Exposed Persons (PEPs);
- Money Service Businesses including Exchange Companies;
- Precious Metals Dealers (gold, silver, platinum, palladium & etc.);
- Embassies, Consulates and Diplomats Missions;
- Real Estate Dealers;
- Nationalist Groups;
- Customers from High Risk Countries;
- Arms and Ammunition dealers;
- Correspondent Banking Relationship;
- Pooled Funds etc.

Similarly, bank's management shall identify High Risk transactions wherein EDD measures will be applied as required under the updated AML/CFT/CPF Regulations from time to time.

Further, bank's management will ensure compliance with minimum standards prescribed by SBP and CBSL from time to time with regard to data privacy & protection of customer's information.

#### **6.4. ENHANCED DUE DILIGENCE**

There are certain high risk type of customers/businesses and other risk factors such as jurisdictions, products, services and delivery channels etc. that poses higher ML/TF/PF risks for which bank is required to undertake Enhanced Due Diligence (EDD) measures for better understanding of risk associated with such customer's / risk factor. Enhanced Due Diligence must be performed by obtaining additional information/documents for high risk customer / risk factors as per CDD/AML/CFT/CPF Procedural Handbook and in line with home and host country's laws, regulations & guidelines.

Bank's management may apply EDD measures which could include but not be limited to one or more of the following measures:

- Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial ownership.
- Obtaining additional information on the intended nature of the business relationship / transactions.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining additional information on the reasons for intended or performed transactions and purpose of transaction.
- Taking reasonable measures to establish the source of funds and wealth involved in the transaction or business relationship to be satisfied that they do not constitute the proceeds from / for crime.
- Obtaining the approval of senior management to commence or continue the business relationship or execute the high-risk financial transaction by the bank.

Where applicable, conducting enhanced monitoring of the business relationship by reviewing its nature and frequency of controls applied and selecting patterns of transactions that need further examination. Where available, requiring the first payment to be deposited through an account in the customer's name with a bank subject to similar CDD standards. EDD requirements may vary with the type of customers, products, channels, transnational activities and geographies; therefore, bank's Management shall take additional / appropriate measures. Negative EDD of customers may also

prompt appropriate action including termination of relationship/ filing of STR; in line with the prevailing law/rule/regulation.

## **6.5 ACCOUNTS AND TRANSACTION MONITORING**

Management should monitor transactions through Automated Transaction Monitoring System to identify suspicious transactions while paying special attention to every complex, unusually large and out-of-pattern transaction(s), which have no apparent economic or visible lawful purpose including but not limited to non-genuine trade finance transactions (e.g. non-genuine letters of credit/bills of lading), inflow or outflow of large amounts not consistent with the business, investment related transactions, secured or unsecured loan transactions etc. If the Bank's Management suspects or has reasonable grounds to suspect that the funds are the proceeds of criminal activity(ies) or have potential to be used for terrorist activity(ies), it shall report its suspicion to relevant authority at the Financial Intelligence Unit (FIU). Further, branch staff shall report transactions to Department Head Compliance, which is considered inconsistent with customer's known legitimate business or personal activities or with the normal business for that type of an account.

For Wire Transfers (both domestic and cross border), the Bank may act as Ordering Institution, Beneficiary Institution or Intermediary Institution while processing wire transfers / fund transfers. However, while conducting such operations, it shall be ensured that all requirements as described in the Bank's CDD & AML / CFT/CPF Handbook Sri Lanka operations are completed and other instructions, issued from time-to-time, are also adhered to in letter and spirit. SWIFT messages should be screened through Name Filtering Solution for possible name match against proscribed/designated/sanctioned entity(ies) and person(s).

The management shall maintain high standards consistent with FATF and BCBS guidance and all applicable laws, rules and regulations to ensure that all inherent risks accompanying cross-border wire transfers are identified and enhanced controls are applied to monitor transaction(s) that commensurate with the identified risks.

For customers whose accounts are dormant or in-operative, bank may allow credit entries without changing at their own, the dormancy status of such accounts. Debit transactions/ withdrawals shall not be allowed in dormant/ inoperative accounts (except for debit under recovery of loans, mark-up, regulatory/ government duties, levies and instructions issued under any law or from the court, any other permissible bank charges etc.) until the account holder fulfills requirements for activation of account and branch is satisfied with CDD of the customer.

In cases where bank's Management is suspicious of money laundering, terrorist financing or other criminal activity, and it reasonably believes that performing the CDD process will tip-off the customer, it will not pursue the CDD process, and instead file an STR. Further, bank's Management may terminate the relationship given the associated risks.

The employees of the bank are strictly prohibited to disclose the fact to any person including the customer that a Suspicious Transactions Report and/or related information have been reported to FIU or any other law enforcement agency.

The adequacy of staff posted for effective monitoring and reporting of suspicious transactions is a critical factor of Customer Due Diligence. Bank's Management shall place adequate number of analysts for monitoring and reporting purpose. Moreover, steps should be taken by bank's Management to develop knowledge and skills of their staff and utilize technology solutions required for effective Targeted Financial Sanctions (TFS) monitoring and reporting of suspicious transactions.

The reporting of suspicious transactions/currency transactions in the context of money laundering, financing of terrorism or proliferation financing shall not be assigned to outsourced employees.

Business shall update expected monthly credit/debit turnover limits in the system and / or revise CDD profile of customer(s) as per guidelines for ongoing review as required under applicable AML/CFT/CPF Regulations/guidelines along with international best practices, while the basis of revision shall be documented and customers may be consulted, if necessary. Such limits will be maintained to make sure that all transactions are consistent with the Bank's knowledge of the customer, its business and risk profile and are conducted in accordance with SBP, CBSL AML/CFT/CPF regulations and other international best practices.

Bank's management shall ensure Event Driven Review of the accounts in case of positive matches against any negative media. Relevant business unit will ensure EDD of these accounts on priority. Filing of Suspicious Activity Report (SAR)/STR on the accounts on the basis of given negative media will also be considered in order to safeguard the bank's interest.

High Value Cash transactions and Electronic Fund Transfers exceeding the prescribed limits as defined by FIU (of CBSL) shall also be reported to FIU through the Compliance Department Sri Lanka.

## **6.6 RISK MANAGEMENT**

In order to mitigate the money laundering, terrorist financing & proliferation financing risks; the bank shall take appropriate measures to assess, document and determine the level of overall ML, TF and PF risk along with the type of mitigation control to be applied. Additionally, the risk assessment shall be kept up-to-date through a periodic review and appropriate mechanism shall be put in place to provide risk assessment information to the supervisory authority(ies).

Bank should also identify and assess the ML, TF and PF risks that may arise in relation to the development of new products, services and business practices including delivery mechanisms and the use of new or developing technologies for both new and pre-existing products, especially those that have vulnerability with regard to ML/ TF/ PF risks specially identity theft, anonymity, inconsistency and cyber-crimes.

The intensity and extensiveness of risk management function shall be in compliance with the "risk based approach" and be proportionate to the nature, scale, and complexity of the bank's activities and money laundering, terrorist financing and proliferation financing risk profile. Furthermore, ML/TF/PF risk management shall be affiliated and integrated with the overall risk management of the bank.

All relationships shall be categorized with respect to their risk levels i.e. High, Medium and Low based on the quantified risk profiling of customer (through standard risk rating sheet, and as guided in CDD & AML/CFT/CPF Handbook Sri Lanka operations) for making effective decisions whether to perform Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) both at the time of opening and ongoing monitoring of business relationships. Bank's Management shall apply CDD requirements to existing customers on the basis of materiality and risk, and to conduct ongoing due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

The approval for opening of account of politically exposed persons (PEP) and Non-Governmental Organizations (NGOs/INGOs) / Non-Profit Organizations (NPOs), Charities, Embassies/Consulates & Diplomatic Missions shall be obtained from Department Head Compliance – Sri Lanka in accordance with Section 29(2)(C-ii) Financial Transaction Reporting Act No 06 of 2006 with Country General Manager's recommendation However, Country General

Manager shall report a list of such accounts opened on a monthly basis to Senior Management i.e. Head - International Banking and Chief Compliance Officer. Further, similar protocol shall also be adhered for opening of account of natural /legal person(s) from High Risk Countries and also transactions pertaining to such countries. Furthermore, bank's management shall also identify certain transaction types as High Risk as per Risk Based Approach (RBA) where the protocols for obtaining Senior Management's approval will be implemented.

Personal Accounts should not be allowed for charity, collection of donations and business purposes.

Customer KYC / CDD profile shall be reviewed and/or updated on the basis of the following predefined frequency contained in the CDD & AML / CFT/CPF Handbook Sri Lanka operations.

High Risk	At least Once in a Year or Need basis*
Medium Risk	At Least Once in 2 Years or Need basis*
Low Risk	At least Once in 3 Years or Need basis*

*\* In case of any material change in the relationship or deviation from customer profile, CDD will be conducted and customer profile will be updated immediately irrespective of the above defined period.*

Compliance Department of Sri Lanka (CDSL) will counter-examine the relationships to ensure that due diligence procedures are adhered to in letter and spirit by the concerned staff in business segments.

In line with FIU Guidelines No.02 of 2021 dated 20<sup>th</sup> July 2021, in order to enhance the operational risk management and safeguard banking operations against risks of being abused for money laundering and financing of terrorism, a robust CCTV system should be in place which is fully operational both within and outside of the bank premises. The business premises refer to the head office, branches, areas of Automated Teller Machines and any other places where Customer Due Diligence (CDD) is conducted.

The robustness of the Due Diligence process will be assessed independently through the Compliance function & Internal Audit function by adhering to the respective processes laid down in this regard. Internal Audit function of the Bank will specifically develop testing system to meet the requirement of FTRA.

## **6.7 CDD FOR ASSET SIDE/ TRADE FINANCE CUSTOMERS**

Bank's management shall also undertake CDD measures for assets side / trade finance customers and ensure monitoring of such customers with regard to ML/TF/PF risk.

## **6.8 CUSTOMERS FROM HIGH RISK JURISDICTIONS**

Bank shall apply Enhanced Due Diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from foreign jurisdictions for which this is called for by the FATF, notified by National Executive Committee (NEC) of Government of Pakistan constituted under AML Act 2010 and CBSL.

## **6.9. TARGETED FINANCIAL SANCTIONS (TFS) MANAGEMENT**

In order to comply with the Targeted Financial Sanctions regime, the bank's management will devise effective system and controls to safeguard the bank from being exploited by the terrorists for ML/TF/PF. In this regard, all relationships (customers & their beneficial owners, directors, members, trustees and authorized signatories, non-customers i.e. walk in customers, bank's

owner's/sponsors shareholders, directors, employees (permanent, contractual and outsourced) and third party service providers/vendors) shall be screened against the prescribed sanctioned lists; both local and international before establishment of the relationship through bank's Name List Screening system i.e. Safewatch and eName checker.

Accordingly, no customer/walk-in customer shall be facilitated in case if a person/entity is identified as proscribed/designated or is affiliated with Proscribed Person (PP)/ Designated Person (DP). Management shall ensure reporting of such cases to the FIU on immediate basis. Further, any sponsor shareholders/ beneficial owners, directors, presidents and key executives (all persons subject to Fit & Proper Test (FPT) etc. shall become disqualified if they are DP/ PP or associated directly or indirectly with any DP/ PP.

Management shall also ensure that all relationships are screened against sanctioned lists on periodic basis as per the frequency specified in bank's CDD & AML/CFT/CPF Procedural Handbook - Sri Lanka Operations.

## **6.10 REVIEW OF PRODUCTS AND SERVICES INCLUDING NEW TECHNOLOGIES.**

Bank's management shall identify and assess ML/TF/PF risks that may arise in relation to expansion of operations in different jurisdictions, development of new products, services, business practices including delivery mechanism and the use of new or developing technologies for both new and pre-existing products especially those that may favor anonymity. Furthermore, risk assessments shall be undertaken prior to the launch or use of such products, services and business practices and technologies. Appropriate measures should be taken to manage and mitigate the identified risks.

## **6.11 VENDORS, OUTSOURCING AND SERVICE PROVIDER'S DUE DILIGENCE**

Bank's management should ensure that regulatory guidelines as specified in Banking Act Direction no. 2 of 2012 'outsourcing of business operations of a licensed commercial bank and a licensed specialized bank' related to due diligence of its vendors and outsourced service providers are implemented.

## **6.12 COMPLIANCE REVIEW**

Compliance Department Sri Lanka (CDSL) shall perform the periodic review of branches to check their level of compliance with the provisions of the CDD & AML/CFT/CPF policy and procedures. Compliance Review Plan shall be approved by Chief Compliance Officer (CCO) on an annual basis.

## **6.13 INTERNAL RISK ASSESSMENT**

Bank shall conduct IRAR on an annual basis, as required under Regulation-1 of SBP's AML/CFT/CPF Regulations issued vide BPRD Circular no. 33 of 2022 dated 28 November, 2022 and FIU Regulation on Guidelines on Money Laundering & Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018 dated 11<sup>th</sup> January 2018 amended from time to time. IRAR shall cover ML/ TF/ PF risks including Transnational TF risks and other emerging risks. IRAR shall identify, assess, and understand ML/ TF/ PF risks for Sri Lanka Operations for customers, products, services, delivery channels, geographies, technologies, and different categories of employees etc.

It should be ensured that IRAR should be dynamically updated subject to any change of circumstances, relevant new threat or after any updating in the National Risk Assessment (NRA) Exercise conducted by Home and/or Host Country. The said document shall also include the recommendations for improvement along with time bound action plan for mitigation of any emergent ML/TF/PF risks highlighted therein.



The outcome of this exercise shall be shared with CCG (HO) to incorporate the same for arriving at a Bank level Risk Assessment and presenting to the BoD, through CR&MC, for its approval.

## **7. CORRESPONDENT BANKING and MONEY SERVICE BUSINESSES (MSBs)**

The Bank's Management will establish Correspondent Banking and MSB relationships with only those foreign banks/regulated MSBs that have adequate and effective AML / CFT/CPF systems and policies in line with the AML / CFT / CPF regulations relating to the country in which that Bank/MSB operates. Moreover, the Bank's Management shall ensure compliance of EDD measures when establishing or continuing correspondent / MSB relationship with banks/ financial institutions/MSBs except for Relationship Management Application (RMA). For RMAs, level of due diligence will depend on the risk profile which is derived from the bank's risk register in line with CDD and AML/CFT/CPF Procedural handbook – Sri Lanka Operations. RMA relationships shall be subject to EDD measures if the same are located or licensed in high risk countries as mentioned in the Counter Measures for High Risk Jurisdictions Rules, 2020 (as updated from time to time).

The Bank's Management shall adopt preventive measures consistent with FATF and BCBS Guidelines, Wolfsburg principles for correspondent banking and applicable laws, rules and regulations to effectively manage all high risk Correspondent Banking relationships, in particular, cross-border Correspondent Banking relationships involving the execution of third-party payments (e.g. nested /downstream and payable-through account services). Further, the reviews of the correspondents and MSBs' accounts shall be carried out as per risk based approach as defined in CDD & AML/CFT/CPF Procedural Handbook Sri Lanka operations.

Before establishing new correspondent banking relationship, approval from Head International Banking, Group Head RMG, Group Head TRY&FX and Group Head LAG shall be required. Any new induction shall also be cleared by CCO from regulatory perspective. Financial Institutions Division - Head Office shall conduct a proper due diligence of these relationships as per CDD & AML/CFT/CPF Handbook Sri Lanka operations. Ongoing Due Diligence of respondent/correspondent banks will be conducted using risk-based approach following the guidelines given in the CDD & AML/CFT/CPF Handbook Sri Lanka operations.

Bank shall not enter into or continue correspondent banking relationship with a shell bank and shall take appropriate measures when establishing correspondent banking relationship, to satisfy themselves that their respondent banks do not permit their accounts to be used with / by shell banks.

## **8. TRADE BASED MONEY LAUNDERING**

The Bank's Management should take adequate due diligence measures and transaction monitoring of the clients to counter money laundering and terrorist financing through trade transactions in line with local laws / regulations and "Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing" issued by SBP vide FE Circular no. 04 of 2019 dated October 14, 2019 amended from time to time.

## **9. EMPLOYEE DUE DILIGENCE**

The Bank's Management must develop and implement a comprehensive employee due diligence policy and procedure to be carried out at the time of hiring of all employees (permanent, contractual or hired through outsourcing). These procedures must include but are not limited to

verification of antecedents and screening procedures, on an ongoing basis, to verify that person being inducted / hired has a clean history and other controls are implemented to prevent criminals or their associates from being employed by the Bank. Further, Department Head Compliance- Sri Lanka should perform independent review of Employee Due Diligence process.

## **10. RECORD KEEPING**

The records of identification documents, account opening forms, KYC forms, verification documents, etc. along with records of account files and business correspondence, shall be maintained for a minimum period of ten years after the business relationship is ended.

The Bank's Management shall also maintain for a minimum period of ten years or more if required by local laws/rules/regulations, all necessary records on transactions for both domestic and cross border from the date of completion of transaction(s). The data relating to suspicious transactions and currency transactions (if mandated by the regulator) reported by the Bank to relevant Authority/ CBSL shall be retained for a period of at least ten years or more if required by local laws/rules/regulations from the date of such reporting.

However, records relating to customers, accounts or transactions shall be retained for a longer period, which involve litigation or is required by court of law or other competent authority until otherwise instructed by the relevant body(ies). Furthermore, all specimen signatures cards and documents indicating signing authorities, and other documents relating to the accounts/deposits or instruments surrendered to the CBSL, shall be kept in the bank's record till such time that the CBSL informs in writing that same need no longer to be preserved.

Further, MCB - Sri Lanka shall also follow the Bank's Record Management Policy, wherever applicable.

## **11. E-COMMERCE**

The Bank's Management shall ensure to take adequate measures to safeguard bank's channels from abuse by the criminal groups using e-Commerce businesses to send/receive payments for illicit transactions pertaining to ML/TF/PF activities. In this regard, regulatory instructions on Business-to-Consumer (B2C) E-Commerce Exports communicated vide SBP FE Circular No. 07 of 2020 dated December 02, 2020 (any amendment made therein from time to time) must be adhered with.

## **12. PROLIFERATION FINANCING**

Proliferation Financing is the act of providing funds or financial services which may be used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws / rules / regulations or, where applicable, international obligations.

Trade finance is considered as a common vehicle used to finance proliferation and bank should pay special attention to certain trade activities such as loans to facilitate export/ import transactions, factoring, providing of guarantees to or by financial institutions on behalf of exporters. Enhanced Due Diligence measures are to be implemented on trade finance transactions and relationships. Management shall ensure to take adequate measures to safeguard the bank from Proliferation Financing risk in line with this policy, CDD & AML/CFT/CPF Procedural Handbook for Sri Lanka operations and regulatory requirements.

### **13. TRAINING**

Suitable Employee Training Program will be put in place by Bank's Management at least on an annual basis to enhance staff capability, in order to effectively implement the regulatory / legal requirements, bank's own policy & procedural requirements relevant to AML/CFT/CPF including alerts, analysis, and possible reporting of suspicious transactions as well as to understand new developments in AML/CFT/CPF techniques, methods, and trends.

Further, Human Resource Management Group (HRMG) with support of CCG, wherever required, will continue assessment of Bank's employee's knowledge via Compliance Knowledge Assessment System (CKAS) test also covering AML / CFT / CPF area and its key regulatory requirements every alternate year.

### **14. CDD & AML/CFT/CPF HANDBOOK SRI LANKA OPERATIONS**

All procedures required for implementation of the guidelines related to CDD and AML/CFT/CPF shall be documented in the form of CDD & AML/CFT/CPF Handbook Sri Lanka operations. This document shall be prepared by Department Head Compliance Sri Lanka, and shall carry the recommendation of Country General Manager-MCB Sri Lanka, subject to review by Head International Banking and Chief Compliance Officer. The approving authority for this document shall be the President. Furthermore, it shall be reviewed at least on an annual basis and/or earlier on need basis.

### **15. APPLICABILITY & PERIODICITY FOR REVIEW OF POLICY**

This policy is applicable on Sri Lanka Operations of the Bank and shall be reviewed at least annually or earlier on need basis. This policy will be approved by the Board of Directors and all subsequent reviews of the document shall continue to be approved at the same level.

The primary responsibility for review and maintenance of this Policy rests with the Department Head Compliance Sri Lanka and Country General Manager – MCB Sri Lanka, subject to review by Head International Banking and Chief Compliance Officer.

## 16. GLOSSARY

AML	Anti-Money Laundering
BCBS	Basel Committee on Banking Supervision
BOD	Board of Directors
CDSL	Compliance Department Sri Lanka
CBSL	Central Bank of Sri Lanka
CCG	Compliance & Controls Group
CCO	Chief Compliance Officer
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CDD	Customer Due Diligence
CPF	Countering Proliferation Financing
CKAS	Compliance Knowledge Assessment System
CSTFA	Convention on the Suppression of Terrorist Financing Act
EDD	Enhanced Due Diligence
EU	European Union
FATF	Financial Action Task Force
FIs	Financial Institutions
FID	Financial Institutions Division
FIU	Financial Intelligence Unit
FTRA	Financial Transaction Reporting Act
GoP	Government of Pakistan
HRMG	Human Resource Management Group
IB	International Banking
IRAR	Internal Risk Assessment Report
KYC	Know Your Customer
ML	Money Laundering
MSB	Money Service Businesses

NGOs	Non-Governmental Organizations
NPOs	Non-Profit Organizations
OFAC	Office of Foreign Assets Control
PEPs	Politically Exposed Persons
PF	Proliferation Financing
PMLA	Prevention of Money Laundering Act
RBA	Risk Based Approach
SBP	State Bank of Pakistan
SDD	Simplified Due Diligence
STRs	Suspicious Transaction Reports
SAR	Suspicious Activity Report
TBML	Trade Based Money Laundering
TF	Terrorism Financing
UNSC	United Nations Security Council
LAG	Legal Affairs Group
RMG	Risk Management Group
TRY&FX	Treasury and Forex Group