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

MCB SRI LANKA OPERATION

2025

Version 10.0

Document Control Sheet

Title Of Policy	Customer Due Diligence (CDD) & Anti-Money Laundering (AML) / Combating Financing of Terrorism (CFT) / Countering Proliferation Financing (CPF) Policy – MCB Sri Lanka Operations
Associated Key Risks	Money Laundering / Trade Based Money Laundering / Financing of Terrorism / Proliferation Financing / Compliance / Legal / Regulatory / Reputational / Financial / Operational
Policy Owners	1. International Banking 2. Compliance and Controls Group
Review Frequency	Annual or earlier on need basis
First Approval Date	October 20, 2015
Last Approval Date	October, 2024
Current Review Date	October 2025
Next review date	October 2026
Version (Existing / New)	Existing (9.0) / New (10.0)
Reviewed by:	1. Operations Group 2. International Banking 3. Audit & RAR Group 4. Risk Management Group 5. Legal Affairs 6. Compliance and Controls Group 7. Human Resource Management Group 8. Treasury & Forex Group (T&FXG) 9. Oversight & Monitoring 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

1. INTRODUCTION

MCB Bank-Sri Lanka (the Bank) is committed to combat Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF). Its commitment towards the prevention of ML/TF/PF/Trade based money laundering (TBML) risks 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 to MCB Pakistan as per methodology defined in State Bank of Pakistan (SBP) Regulations / Guidelines issued from time to time.

The bank's management should ensure compliance with all applicable laws, rules and regulations, as issued / amended / updated from time to time, specifically the following:

- Convention on the Suppression of Terrorist Financing Act, No.25 of 2005 (CSTFA) as amended from time to time
- Prevention of Money Laundering Act, No.05 of 2006 (PMLA) and its amendments
- Financial Transaction Reporting Act, No. 06 of 2006 (FTRA) and its amendments
- 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) as amended from time to time.
- Prevention of Terrorism (Proscription of Extremist Organizations) Regulations No 1 of 2019.
- Banking Act Determination No. 01 of 2019 as amended from time to time.
- SBP's "Framework for Risk Management in Outsourcing Arrangements by Financial Institutions" issued vide BPRD Circular no. 06 of 2019 dated December 17, 2019 as amended from time to time.
- 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 September 30, 2020 as amended from time to time.
- High Risk Jurisdictions Rules, 2020 issued by Ministry of Finance, Government of Pakistan vide S.R.O. 951(I)/2020 dated October 01, 2020 as amended from time to time.
- SBP's "Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Regulations" issued vide BPRD Circular Letter no. 20 of 2021 dated June 08, 2021 as amended from time to time.
- SBP's "Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Regulations" issued vide BPRD Circular Letter No.33 of 2022 dated November 28, 2022.
- Anti- Corruption Act, No. 9 of 2023, including requirements relating to reporting of corruption related to suspicious transaction etc.
- Proceeds of Crime Act 05 of 2025
- SBP's Consolidated Customer Onboarding Framework Issued vide BPRD Circular No. 01 of 2025 dated July 25, 2025 (where applicable)
- SBP Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing issued vide EPD Circular No. 08 dated August 12, 2025 as amended from time to time.
- Applicable relevant AML/CFT/CPF Regulations/ Guidelines issued by State Bank of Pakistan / CBSL, from time to time.

In order to further strengthen the regulatory framework and to curb Money Laundering, Terrorist Financing and Proliferation Financing risks, 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 and other applicable laws, rules and regulations covering the following aspects:

Key Elements	Area(s) Covered
Risk Based Approach and Risk Assessment	Bank's management must implement Risk Based Approach (RBA) in establishing AML/CFT/CPF Programs prior to establishing business relationship and throughout the course of relationship with customers. Bank's management must take measures to identify, assess, monitor, manage and mitigate ML/TF/PF/TBML risks to which it is exposed. Further, the Bank Management will conduct internal ML/TF/PF/TBML risk assessment of the bank on periodic basis to identify, assess, and understand ML/TF/PF/TBML risks for Sri Lanka Operations for customers, products, services, delivery channels, geographies, technologies, and different categories of employees etc.
Customer Due Diligence	CDD/ EDD 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 Rules 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 and Terrorist financing and Proliferation Financing risks, 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.
Tipping off	All employees are strictly prohibited to disclose to any person including customers that a certain transaction is being scrutinized for possible involvement in suspicious money laundering operations and/or terrorist financing.
Penalty	Failure to comply with Anti-Money Laundering (AML) / Combating the Financing of Terrorism (CFT) and Counter Proliferation Financing (CPF) requirements may result in penal action(s) such as fines and imprisonment in accordance with the applicable laws.
Internal Controls, Policies, Compliance, Audit and Training	Requirements relating to development of Controls, Policies, Procedures, Training programs to ensure compliance with AML/CFT/CPF regulations.
Beneficial Ownership	Determining and assessing the ultimate beneficial ownership structures of the Bank's customers.
Record Keeping	Maintenance and Retention of Customer Due Diligence, Transactions Record, Compliance Records and Training Records.

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), Trade Based Money Laundering (TBML), Financing of Terrorism (TF) and Proliferation Financing (PF) activities, banks are required to have comprehensive CDD & AML/CFT/CPF policy entailing guidelines on Bank's ML/TF/PF/TBML 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 / technologies / 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 risks of ML/TF/PF/TBML. This policy document shall be read in conjunction with the CDD & AML/CFT/CPF Policy applicable to MCB (Pakistan) to ensure adherence to its 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 November 28, 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.

The Bank is prone to the risks of ML/TF/PF/TBML thereby being misused by criminal elements for their ulterior motives of conducting and 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 or transactions, this policy will be a guiding document for concerned employees towards managing the customer risk in an effective way by 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). Under the Customer Due Diligence process, various sets of documents should be developed and provided to the Relationship Managers (RMs) / concerned staff at the Branches/Office(s) from time to time to ensure execution of the processes and identification of risks attached to each customer for effective mitigation of ML/TF/PF/TBML risks.

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. CBSL issued guidance on Trade Based Money Laundering and 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 shall be developed for implementation of these guidelines and technology-based solutions as specified in SBP's "AML/CFT/CPF Regulations" issued vide BPRD Circular Letter No. 33 of 2022 dated November 28, 2022 and "Framework for Managing Risks of TBML and TF" issued vide Circular Letter No. 08 of 2025 dated August 12, 2025 as amended/updated from time to time as well as relevant instructions issued by CBSL

The latest National risk assessment of Sri Lanka has highlighted Drug Trafficking, Bribery and Corruption, and Trade-Based Money Laundering (TBML) as significant vulnerabilities. To effectively address these critical vulnerabilities, the policy mandates that all relevant personnel must undergo

regular training and participate in continuous awareness programs, ensuring they are well-informed and fully prepared to handle these threats.

Bank's management shall apply its CDD & 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 stringent of the two standards, to the extent that the laws of the host country or jurisdiction so permits.

Where the laws, rules and regulations of the host country conflicts with the AML/CFT/CPF requirements of Pakistan so that the Sri Lanka Operations are unable to observe the stringent standards, bank's management through CCG at Head office shall report this to SBP and comply with such further directions as may be issued. The Head of Compliance will ensure retaining the MIS of comparative analysis of home and host country's regulations/guidelines.

The ultimate responsibility of ensuring effective AML/CFT/CPF controls rests with BoD. Bank's management shall ensure provision of adequate, reliable, periodic information to the BoD through its Compliance Review and 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 (wherever applicable):

1. To identify, assess, understand and mitigate ML/TF/PF/TBML risks.
2. To put in place adequate management and information systems, internal controls, policies, procedures to mitigate risks and monitor implementation.
3. Compliance of all statutory, regulatory and legal obligations to manage and mitigate Legal, Regulatory, Operational, Compliance, Reputational, Financial and risks emanating from the banking operations.
4. Acceptance of only bona fide and legitimate customers/transactions.
5. Verify the identity of customers using reliable and independent sources.
6. Conduct ongoing monitoring of customer accounts and transactions to prevent or detect potential ML/TF/PF/TBML risks / activities.
7. Implement Customer Due Diligence process using risk-based approach.
8. Effectively manage customer-driven risks by using procedures laid down in CDD & AML/CFT/CPF Handbook of MCB Sri Lanka (as updated annually or earlier on need basis) duly approved by the President & CEO.
9. To safeguard the bank from being used as a conduit in money laundering, terrorism financing, trade-based money laundering and proliferation financing.
10. To ensure implementation of Targeted Financial Sanctions (TFS) related to Terrorism Financing (TF) and Proliferation Financing (PF).
11. To put in place appropriate controls for prevention, detection and reporting of suspicious activities in accordance with applicable laws / regulations / procedures.
12. To ensure that bank has implemented effective controls to mitigate the AML/CFT/CPF risks.

13. To ensure that the Bank has implemented effective AML/CFT/CPF controls (preventive measures) including Targeted Financial Sanctions (TFS) related to TF, PF and reporting of STRs in line with UN Security Council decisions and as per the directives of Competent Authorities
14. To maintain adequate record as per the legal, regulatory requirements as well as Bank's Record Management Policy.
15. Appointment and responsibilities of Compliance Officer.
16. To maintain adequate record as per the regulatory requirements.

4. GOVERNANCE

Compliance framework of the Bank is based on a well-defined governance structure to ensure effective and strong compliance culture. The structure is broadly based on the following:

4.1. BOARD OF DIRECTORS

The BoD shall approve ML/TF/PF/TBML risk appetite and policy guidelines for ensuring effective oversight, monitoring and accountability relating to AML/CFT/CPF programs through Compliance Review and Monitoring Committee (CR&MC), (a sub-committee of the Board).

CR&MC shall also ensure the effectiveness of internal controls, systems and mitigation measures put in place for managing ML/TF/PF/TBML risks.

4.2. SENIOR MANAGEMENT

Bank's Senior Management shall define ML/TF/PF/TBML risks 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. Bank's management shall define a mechanism to inform the board of directors (or its relevant sub-committee i.e. Compliance Review and Monitoring Committee (CR&MC) regarding status of AML/CFT/CPF program, compliance initiatives, compliance deficiencies and other regulatory requirements.

Senior Management shall also ensure efficacy of the FinTech's (Computer programs and other technology used to support or enable banking and financial services) implemented by the Bank. In this regard, the following actions will be ensured by the Senior Management:

- An effective Transaction Monitoring program that ensures the quality and completeness of data drawn from the Bank's Core banking and transactional systems and databases.
- Assess the functionality of sanctions screening systems and processes, including threshold settings, screening rules, and the accuracy and completeness of data used in the screening process.
- Assessment of ML/TF/PF/TBML risks should be updated at periodic intervals (at least annually or otherwise as appropriate and justified by the required circumstances) and also upon the occurrence of "trigger events," such as material changes in the MCB Sri Lanka's business or risk profile or the legal and regulatory environment.
- In order to identify patterns of potentially suspicious or illegal activity spanning multiple transactions, the bank's management should group individual Transaction Monitoring (TM)

parameters and thresholds into multi-factor risk scenarios in order to more precisely target transaction patterns and behaviors consistent with known illicit financing typologies.

4.3. THREE LINES OF DEFENSE

The bank's management shall clearly define roles across the three lines of defense: operational units (1st), independent Compliance and Risk Management (2nd), and Internal Audit (3rd), ensuring their independence, authority, and adequate resourcing.

4.4. HEAD OF COMPLIANCE FUNCTION

The bank's management shall appoint a Head of Compliance(Senior most officer) 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 applicable laws, rules and regulations and the Bank's policies and procedures with special focus on ML/TF/PF/TBML risks throughout MCB Sri Lanka operations.

The Head of 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;
    - 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 as amended from time to time;
- Disseminate the laws, rules, and regulations related to money laundering, financing of terrorism, and proliferation financing to relevant employees to enhance and update their awareness. Ensure effective / continuous professional education and training / awareness programs related to AML/CFT/CPF are established and consistently followed at all levels. Ensure reporting of suspicious transactions (STR) as well as Cash Transaction Report, Electronic Fund Transfer (EFT and IFT) in compliance with the 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/TBML risks.
- Ensure reporting of terrorism incidents and attempted transactions to the Combating Financing of Terrorism (CFT) Desk, CCG at Head Office.

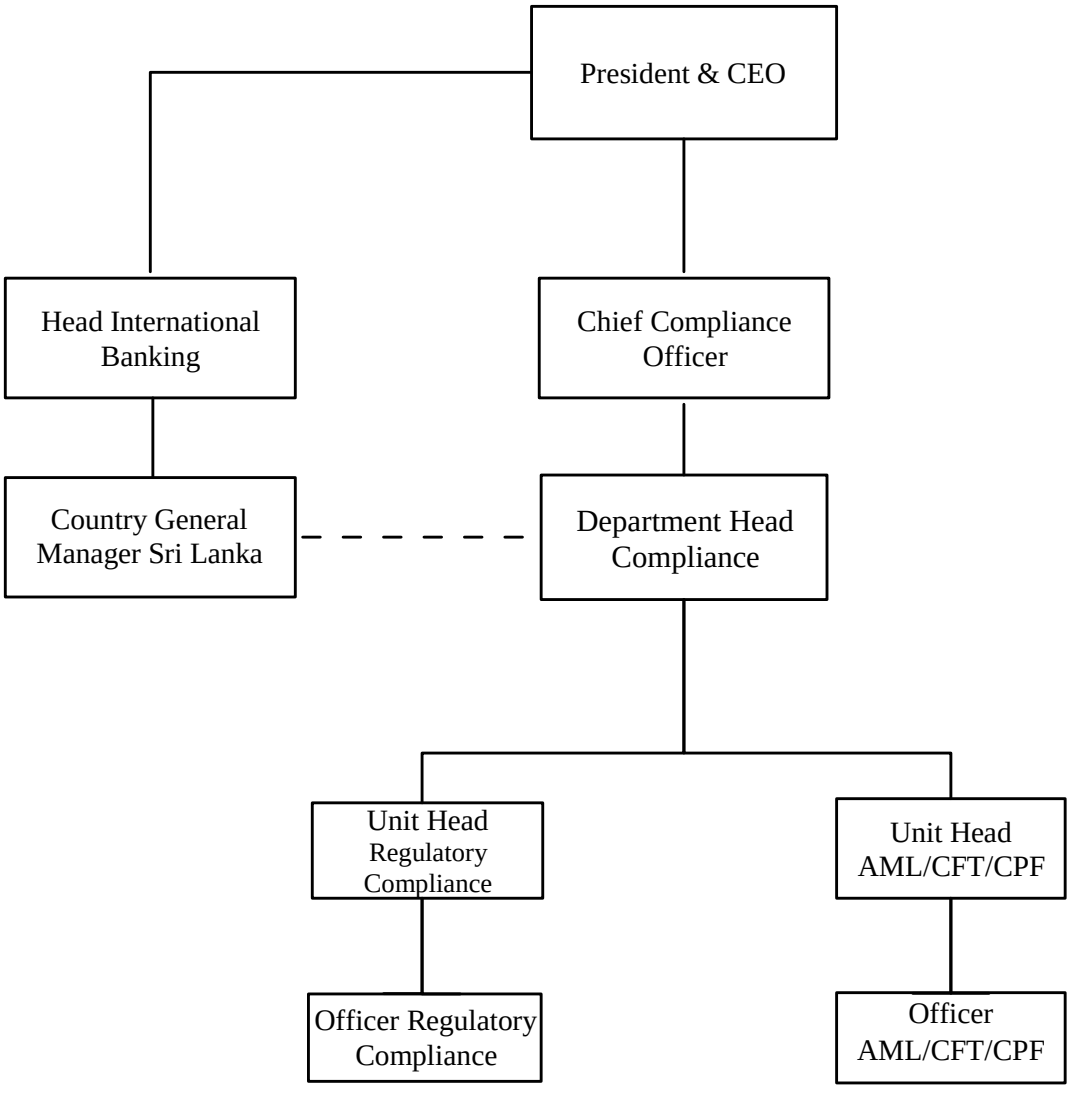
- Prompt reporting of Suspicious Transaction Reports related to ML/TF/PF/TBML risks to relevant authorities as per CBSL guidelines.
- Ensure conducting annual ML/TF/PF/TBML risk assessment of bank's Sri Lanka operations in line with the Regulation R-1 of the SBP's "AML/CFT/CPF Regulations" issued vide BPRD Circular No. 33 of 2022 dated November 28, 2022, FIU Regulations on Guidelines on Money Laundering and Terrorist Financing Risk Management for Financial Institutions, No.01 of 2018 dated January 11, 2018 and any other relevant laws, rules and regulations as issued / updated / amended from time to time.
- Acting as main point of contact in respect of handling and reporting of compliance related matters to concerned offices of host as well home country.
- Keep abreast with latest trends and developments in the field of compliance with special focus on ML/TF/PF/TBML risks. Ensure effective/ continuous professional education and training/awareness programs are in place and accordingly adhered to at all levels.
- Ensure that policies and procedures are kept updated and effectively implemented at all levels on a continuous basis.
- Ensure that necessary systems of internal controls are effectively and continuously in operations with special focus on Anti-Money Laundering, Combating Financing of Terrorism and Countering of Proliferation Financing measures and on-boarding of customers.
- In general, to carry out all necessary steps to ensure Bank's operations carry minimal regulatory and reputational risk with special focus on compliance with all applicable laws, rules and regulations.

4.5. 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 and proliferation financing to ensure that it is adequate and functioning to counter ML/TF/PF/TBML risks.

5. ORGANIZATIONAL CHART OF COMPLIANCE FUNCTION

Organizational Chart



6. KEY ELEMENTS OF CUSTOMER DUE DILIGENCE (CDD)

The bank's management shall implement robust Customer Due Diligence (CDD) procedures, including the identification and verification of customers and beneficial owners, to assess and mitigate the risk of money laundering and terrorist financing. The bank's management shall comply with FIU Circulars 01–04 of 2024 relating to Customer Due Diligence (CDD) and reporting requirements under the Financial Transactions Reporting Act (FTRA), including timely submission of Suspicious Transaction Reports (STRs), Threshold Transaction Reports (TTRs), and other mandated regulatory returns.

6.1 CUSTOMER IDENTIFICATION

Bank's management will serve only the genuine person(s) and all out efforts should be made to determine the true identity of every customer, beneficial ownership 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 Central Bank of Sri Lanka's directives / guidelines and SBP's Consolidated Customer Onboarding Framework, Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Regulations (whichever are relevant) and other applicable laws, rules and regulations as well as MCB's CDD& AML/CFT/CPF Procedural Handbook – Sri Lanka Operations.

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/Registration number with the National Secretariat for Non-governmental organizations, in case of Charity Accounts etc. (as applicable), as stipulated in CBSL and SBP regulations and all other applicable laws, rules and regulations, required for various nature of accounts.

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 as directed under the regulations issued / updated / amended from time to time; using reliable, independent source of information.

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 December 30, 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 other customers.

In case bank's management is unable to satisfactorily complete required CDD measures for any potential customer and existing customer, account shall neither be opened nor any service be 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. Further, if required, the existing customer relationship shall be considered for termination as per the prevailing laws without pursuing the CDD process to avoid tipping-off the customer and Suspicion shall be considered for filing of STR. In such a case, bank's management shall serve a prior notice to the existing customers and record cogent reasons for terminating business relationship.

6.2 CUSTOMER VERIFICATION

The bank's management shall identify the customer and beneficial ownership of accounts/ transactions by taking all reasonable measures in accordance with the guidelines of CBSL/SBP and all other applicable laws/rules/regulations and directives issued/updated/amended from time to time. 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, branch 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 / are 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 or on-boarded once customer identification and verification formalities have been completed in letter and spirit, in accordance with the requirements of the applicable laws, rules and Regulations.

Following accounts/transactions will not be opened/maintained/allowed by MCB Sri Lanka 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. As per International Sanction laws and guidelines, permissible/exempted Transactions with such countries may be considered on a case-to-case basis.

g) The Bank is unable to satisfactorily complete required CDD measures.

h) Customers / account holders who transact / deal in Virtual Assets (VA) / Virtual currencies (VCs) / Bitcoins, Ethereum etc. as well as Virtual Assets Services Providers (VASPs).

i) Accounts/ customers involved in any other activity forbidden by the law e.g. gambling, human smuggling etc.

j) Government accounts opened in the personal name of Government Officials
k) Illegal money value transfer services (MVTS) including unauthorized / unlicensed money changers..
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) Customers from high risk jurisdictions subject to a call for action/ black listed by FATF.
n) Customers or transactions to/ from sanctions/ designated countries subject to available advisories.

o) Individual accounts opened for charity purpose.

p) Unauthorized/ Unlicensed digital lending platforms (individuals or businesses).

High Risk Customers' Approvals

In addition to the above specified prohibitions, certain other types of customers pose higher level of ML/TF/PF/TMBL 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/TMBL risks associated with other types of customers:

- NGOs / INGOs / NPOs / Charities / Trust / Club / Societies / Madrassah / associations;
- Politically Exposed Persons (PEPs);
- Money Service Businesses including Exchange Companies;
- Precious metals dealers (gold, silver, platinum, palladium etc.);
- Embassies, consulates and diplomat's missions;
- High Net Worth Individuals (HNWI) with no clearly identifiable source of income;
- Real Estate Dealers;
- Nationalist Groups/Political Parties;
- Customers from High Risk Countries;
- Arms and ammunition dealers;
- Correspondent Banking Relationship;
- Pooled Funds;
- Electronic Money Institutions (EMI), Payment Service Providers/ Payment Service Operators/ Digital Banks;
- Non-Banking Finance Companies (NBFCs);
- Accounts wherein the funds were sourced under Tax Amnesty schemes of Government Similarly, bank's management shall identify High Risk transactions wherein EDD measures will be applied as required under the updated CDD & AML/CFT/CPF Regulations from time to time.

Further, bank's management will ensure compliance with minimum standards prescribed in the Sri Lanka's Personal Data Protection Act, No. 9 of 2022 and SBP (wherever relevant), when collecting, processing, and retaining customer due diligence data, ensuring confidentiality and security of customer information. with regard to data privacy and 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 pose higher ML/TF/PF/TBML 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 – Sri Lanka Operations and in line with home and host country's laws, rules, regulations and guidelines.

Bank's management shall apply EDD measures which could include but not 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.
- Taking specific measures to identify the source of the first payment in customer's account and applying RBA to ensure that there is a plausible explanation in any case where the first payment was not received from the same customer's account.

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 laws/rules/regulations.

6.5 CDD FOR WALK-IN/ OCCASIONAL CUSTOMERS

Walk-in / Occasional customers are customers who do not maintain account with the Bank. Bank's management shall not conduct transactions on behalf of walk-in / occasional customers.

Walk-in-customers shall only be entertained for conducting transactions to or from customer accounts that are allowed legally and by the regulators, including cheque deposit, cheque withdrawal, cash deposit, submission of transactions requests by the customer. The aforementioned transactions shall be conducted once due diligence measures for transactions relating to such customers as prescribed in MCB's CDD & AML/CFT/CPF Procedural Handbook for Sri Lanka Operations in line with the applicable AML/CFT/CPF regulations/guidelines/frameworks along with international best practices have been complied with.

6.6 ACCOUNTS AND TRANSACTION MONITORING

Management must perform risk assessment of the customer prior to and during the establishment of business relationship and on an ongoing basis throughout the life of its relationship with the customer. Bank's management must review and update customer's risk profile regularly as per

frequency defined in CDD & AML/CFT/CPF Procedural Handbook for MCB Sri Lanka Operations and shall update expected monthly credit/ debit turnover limits in the system based on consultation with the customers in line with customers' profile and such limits will be maintained/ updated to make sure that all transactions are consistent with the Bank's knowledge of the customer, its business and risk profile.

Management should monitor transactions through automated Transaction Monitoring System (TMS) 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/transport documents), 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) and or have potential to be used for terrorist activity(ies), it shall report its suspicion to the Financial Intelligence Unit (FIU), CBSL. Further, branch/Dept. staff shall report transactions, to Head of Compliance of MCB's Sri Lanka Operations, 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).

Bank's 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. Management must ensure that complete originator and beneficiary information along with unique transaction identifier is available with every domestic and cross border transfer.

For customers whose accounts are dormant or in-operative, bank' management 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/interest, 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 respective customer.

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. Further, bank 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 the 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 based on consultation with the customer. 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 CBSL, SBP 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.

6.7 RISK MANAGEMENT

In order to mitigate the money laundering, terrorist financing, proliferation financing and trade based money laundering risks; bank's management shall take appropriate measures to assess, document and determine the level of overall ML/TF/PF/TBML risks 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's management should also identify and assess the ML/TF/PF/TBML 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 existing products, especially those that have vulnerability with regard to ML/TF/PF/TBML risks specially identity theft, anonymity, inconsistency and cyber-crimes.

The intensity and extensiveness of risk management functions 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/TBML 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 Procedural Handbook Sri Lanka operations) for making effective decisions whether to perform Simplified Due Diligence (SDD) or Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) both at the time of opening and ongoing monitoring of business relationships as per defined frequency. Bank's management shall apply CDD requirements to existing customers on the basis of risk (keeping in view its risk appetite), 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) / Not-for-Profit Organizations (NPOs), Charities shall be obtained from Head of Compliance in accordance with Section 29(c ii) Financial Transaction Reporting Act No 06 of 2006 and Banking Act Determination No. 01 of 2019 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. Furthermore, 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. As per FIU Circular

01/2019 and 01/2025, the bank's management shall implement Enhanced Due Diligence measures for Non-Governmental Organizations (NGOs), Non-Profit Organizations (NPOs), and Charities, including verification of registration, funding sources, and monitoring of transactions.

Personal Accounts should not be allowed for charity, collection of donations and business purposes. Customer KYC / CDD / EDD 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 (Preferably 6 months) or on Need basis*
Medium Risk	At Least Once in 2 Years or on Need basis*
Low Risk	At least Once in 3 Years or on 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 20th July 2021, in order to enhance the operational risk management and safeguard banking operations against risks of being abused for money laundering, financing of terrorism and proliferation financing, 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 main 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 and Internal Audit functions 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.

6.8 CDD FOR ASSET SIDE/ TRADE FINANCE CUSTOMERS

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

6.9 CUSTOMERS FROM HIGH RISK JURISDICTIONS

Bank's management shall apply Enhanced Due Diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from high risk foreign jurisdictions. Management must take adequate precautions and risk mitigation measures before onboarding non-resident customers from high risk jurisdictions. Management must not accept non-residents customers from high risk jurisdictions subject to a call for action by FATF.

6.10 TARGETED FINANCIAL SANCTIONS (TFS) MANAGEMENT

In order to comply with the Targeted Financial Sanctions regime, the bank's management will devise effective system(s) and controls to safeguard the bank from being exploited by the terrorists for ML/TF/PF/TBML risks. In this regard, all relationships (customers and 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 Filtering system i.e.

Safewatch and eName checker. Where a customer, beneficial owner, or transaction is identified as a match with designated persons or entities, the bank's management shall immediately freeze the related funds/assets without prior notice and report to the FIU within 24 hours, in accordance with FIU Guidelines on Targeted Financial Sanctions.

Management shall further ensure that no relationship or transaction is allowed related to the Dual-Use Goods without proper authorization from the competent authority.

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 and CBSL on immediate basis. Further, any sponsor shareholder/ beneficial owner, director, President and key executive (all person's subject to Fit & Proper Test (FPT) etc. shall become disqualified if he is 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.

6.11 REVIEW OF PRODUCTS AND SERVICES INCLUDING NEW TECHNOLOGIES

Bank's management shall identify and assess ML/TF/PF/TBML 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-exiting 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.

6.12 VENDORS, OUTSOURCING AND SERVICE PROVIDER'S DUE DILIGENCE

Bank's management should ensure that regulatory guidelines as specified in CBSL's Banking Act Direction no. 2 of 2012 updated / amended from time to time on the subject of '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.

6.13 COMPLIANCE RISK REVIEW

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

6.14 INTERNAL RISK ASSESSMENT

Bank's management shall conduct and document IRAR on an annual basis, as required under Regulation-1 of SBP's AML/CFT/CPF Regulations issue / amended / updated from time to time and FIU Regulation on Guidelines on Money Laundering and Terrorist Financing Risk Management for Financial Institutions, No. 01 of 2018 dated January 11, 2018 amended/updated from time to time. IRAR shall cover ML/TF/PF/TBML risks including Transnational TF risks and other emerging risks. IRAR shall identify, assess, and understand ML/TF/PF/TBML risks for MCB-Sri Lanka Operations for

customers, products, services, delivery channels, geographies, technologies, and different categories of employees etc.

It should be ensured that IRAR is dynamically updated subject to any change of circumstances, relevant new threats or after any updating in the 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/TBML risks highlighted therein.

The outcome of this exercise shall be shared with CCG (HO) to incorporate the same for arriving at an overall bank wide Bank Level Risk Assessment and presenting to the BoD for its approval through its Compliance Review & Monitoring Committee (CR&MC).

Bank's policy for application of CDD and EDD will be based on the levels of ML/TF/PF/TBML risks identified as low, medium, high or very high in Internal Risk Assessment Report (IRAR) and in line with regulatory requirements of CBSL/FIU/SBP etc. Further, bank's policies / controls /procedures / preventive measures shall be developed / updated / implemented by the management proportionate to the level of ML/TF/PF/TBML risks as evaluated in IRAR.

7. CORRESPONDENT BANKING AND MONEY SERVICE BUSINESSES (MSBs)

The Bank will establish Correspondent Banking and MSB relationships with only those 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 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 for MCB Sri Lanka Operations.

The below matrix will be followed for onboarding and periodic reviews of Correspondent Banking relationships:

Category / Account Type	Review Type	Initiated By	Recommended By	Approving Authority
NOSTRO	Onboarding*	Country General Manager (After review of Head of Compliance Sri Lanka)	Head International Banking and GH T& FX	President & CEO
VOSTRO				Chief Compliance Officer
RMAs (High Risk)				
RMAs (Medium & Low Risk)			Division Head, FID	Division Head AML & CRR
VOSTRO	Periodic**	FID	Division Head, FID	Division Head AML & CRR
RMAs (High, Medium & Low Risk)				

**In case of onboarding; MCB Compliance Sri Lanka is responsible to seek approval from Approving Authority.*
***FID will share details and documents with MCB Compliance Sri Lanka for review/screening before recommending as per above matrices.*

MCB Compliance Sri Lanka will ensure compliance with local regulatory requirements related to NOSTRO, Vostro and RMAs onboarding and periodic reviews.

Similarly, bank's management shall formulate approval matrices for MSBs and make the same a part of the CDD & AML/CFT/CPF Procedural Handbook for Sri Lanka Operations.

Ongoing Due Diligence of respondent/correspondent banks and Money Service Businesses (MSBs), will be conducted using risk-based approach following the guidelines given in below table.

High Risk	At least Once in a Year or earlier if any happening / event/situation so demands*
Medium Risk	At least Once in 2 Years or earlier if any happening / event/situation so demands*
Low Risk	At least Once in 3 Years or earlier if any happening / event/situation so demands *

**In case of any material change in the relationship or deviation from customer profile, CDD/EDD will be conducted and customer profile will be updated immediately without lapse of above defined period.*

Bank' management 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

Bank's management should take adequate due diligence measures and transaction monitoring of the clients to counter money laundering, terrorist financing and proliferation financing through trade transactions in line with local laws/ rules / regulations and Regulatory "Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing" issued by SBP vide EPD Circular no. 08 of 2025dated August 12, 2025 updated/amended from time to time.

Bank's management shall put in place SOPs as per the provisions stipulated in the updated regulatory framework for; onboarding of trade customers, processing of trade transactions which includes price verification of underlying contracts/ screening of trade customers and their counterparties/ goods (including dual used goods), escalation matrix and, post fact monitoring of trade transactions.

The bank's management shall periodically identify and assess the ML/TF/PF/TBML risks arising out of trade transactions and document their findings in their IRAR document. The assessment should consider, at a minimum, the factors as stipulated in the above-mentioned regulatory circular(s). The risks thus identified will be presented to the designated committee of BoD i.e. Compliance Review & Monitoring Committee (CR&MC) as a part of the Internal Risk Assessment Report (IRAR). Additionally, periodic reviews of trade customers will be concluded as per risk-based approach following the guidelines given in below table.

High Risk	At least Once in 12 months or earlier if any happening / event/situation so demands*
Medium Risk	At least Once in 15 months or earlier if any happening / event/situation so demands*
Low Risk	At least Once in 18 months or earlier if any happening / event/situation so demands*

**In case of any material change in the relationship or deviation from customer profile, CDD/EDD will be conducted and customer profile will be updated immediately without lapse of above defined period.*

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, Head of Compliance-Sri Lanka (Senior Most Officer) 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 (10) Years or more if required by local law after the business relationship is ended.

MCB Sri Lanka Operations shall also maintain transactions record for a minimum period of ten years or more if required by local law, for all necessary records on transactions including both domestic and cross border from the date of completion of transaction(s). The data relating to suspicious transactions and currency transactions reported by the bank's management to relevant Authority/ CBSL shall be retained for a period of at least ten years or more if required by local law 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. Furthermore, all specimen signatures cards and documents indicating signing authorities, and other documents relating to the accounts/deposits or instruments surrendered to the CBSL, if required 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. The Personal Data Protection Act, No. 9 of 2022 Sri Lanka, when collecting, processing, and retaining customer due diligence data, ensuring confidentiality and

security of customer information with regard to data privacy and protection of customer's information shall be adhered in letter and spirit.

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/TBML 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 (as amendment / updated from time to time) must be adhered to.

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, transshipment, 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 or, where applicable, international obligations.

Trade finance is considered as a common vehicle used to finance proliferation and bank's management shall 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. Bank's management shall ensure to take adequate measures to safeguard the bank from Proliferation Financing risks 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 Human Resources Department – Sri Lanka in coordination with Head of Compliance – Sri Lanka, at least on an annual basis to enhance staff capability, in order to effectively implement the regulatory / legal requirements and also bank's own policy and 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, HRMG-Pakistan with support of CCG-Pakistan, wherever required, will continue assessment of Bank's employee's knowledge via CKAS test also covering AML/CFT/CPF area and its key regulatory requirements every alternate year.

The bank's management shall establish effective arrangements to regularly train with role-specific programs for all staff on AML/CFT/CPF matters, ensuring they understand the institution's inherent ML/TF/PF/TBML risks and the measures in place to mitigate them.

14. CORRUPTION AND BRIBERY

Corruption and Bribery being a predicate offense as per updated National Risk Assessment of Pakistan & Sri Lanka; bank shall maintain zero tolerance approach towards corrupt practices. Bank's management must ensure robust control environment to take appropriate disciplinary action (including termination of employment) against bank's staff involved in supporting corrupt practices / other predicate offences. All bank's staff should act professionally, fairly and with integrity in all business interactions and relationships.

15. CDD & AML/CFT/CPF PROCEDURAL HANDBOOK FOR MCB 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 Procedural Handbook Sri Lanka operations. This document shall be prepared by Head of Compliance Sri Lanka, duly reviewed by all relevant stakeholders and shall carry the recommendations of Country General Manager-MCB Sri Lanka, Head International Banking and Chief Compliance Officer. The approving authority for this document shall be the President & CEO. Furthermore, it shall be reviewed on an annually or earlier on need basis.

16. APPLICABILITY AND PERIODICITY FOR REVIEW OF POLICY

This policy is applicable to 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 development, review and maintenance of this Policy rests with the Head of Compliance Sri Lanka and Country General Manager – MCB Sri Lanka, subject to review by Head International Banking and Chief Compliance Officer.

17. ACRONYMS / 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
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
IRAR	Internal Risk Assessment Report
KYC	Know Your Customer
ML	Money Laundering
MSB	Money Service Businesses
NGOs	Non-Governmental Organizations
NPOs	Not-for-Profit Organizations
OFAC	Office of Foreign Assets Control
PEPs	Politically Exposed Persons
PF	Proliferation Financing
PMLA	Prevention of Money Laundering Act
POCA	Proceeds of Crime 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
LA	Legal Affairs
RMG	Risk Management Group
TRY&FX	Treasury and Forex Group
HRD	Human Resources Department