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

2024

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 is 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."

DOCUMENT CONTROL SHEET

Title of the Policy	Customer Due Diligence & Anti-Money Laundering / Combating Financing of Terrorism / Countering Proliferation Financing (CDD & AML/CFT/CPF) Policy – Pakistan
Associated Key Risks, if any	Money Laundering, Financing of Terrorism, Proliferation Financing, Regulatory, Legal, Financial and Reputational Risks
Policy Owner	Compliance and Controls Group (CCG)
Review Frequency	Annually or earlier on need basis
First Approval Date	2009
Last Approval Date	February – 2023
Current Review Date	February – 2024
Next Review Date	February – 2025
Version (Existing / New)	Existing (7.0) / New (8.0)
Reviewed By	• Legal Affairs Group • Risk Management Group • Operations Group • Audit and Risk Assets Review Group • Oversight and Monitoring Group • Human Resource Management Group • Retail Banking • Wholesale Banking Group • Treasury & FX Group
Concurred by	President & Chief Executive Officer (CEO)
Recommended By	Compliance Review and Monitoring Committee (CR&MC)
Approved By	Board of Directors
Distribution List	MCB's all branches, offices and subsidiaries in Pakistan

Table of Contents

1. PURPOSE

Formulation and revision of this policy is in line with requirements of:

- Anti-Money Laundering (AML) Act 2010 (as updated from time to time);
- Anti-Terrorism Act (ATA) 1997
- Applicable SBP Anti Money Laundering (AML) / Combating Financing of Terrorism (CFT) / Countering Proliferation Financing (CPF) Regulations & Guidelines on Risk based approach amended from time to time;
- United Nations Security Council (Freezing & Seizure) Order, 2019;
- United Nations (Security Council) Act, 1948 (UNSC Act);
- Ministry of Foreign Affairs (MOFA) Guidelines on the Implementation of UNSC Resolutions concerning Targeted Financial Sanctions, Travel Ban, and Arms Embargo (UNSC 1267);
- Ministry of Foreign Affairs (MOFA) Guidelines on the Implementation of UNSC Resolutions concerning Targeted Financial Sanctions on Proliferation Financing (UNSC 2231 & 1718);
- National Counter Terrorism Authority (NACTA) Guidelines on Actions to be taken by Competent Authorities for Implementation of United Nation Security Council Resolution No. 1373;
- Counter Measures for High Risk Jurisdictions Rules, 2020 amended from time to time;
- Recommendations of National Risk Assessment (NRA) conducted by Government of Pakistan (GoP) from time to time along with international best practices to prevent the possible use of MCB Bank as a conduit for Money Laundering or Terrorist Financing or Proliferation Financing activities; and
- Any other applicable laws, rules and regulations with respect to AML/CFT/CPF.

Amidst 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, manage and mitigate these risks on an ongoing basis. Banks are required to manage these risks throughout the life cycle of its customers' relationship related to channels / products / jurisdictions / services / transnational activities starting from onboarding till closure as well as for all walk-in or occasional customers.

In addition to the above, the international AML / CFT / CPF standards such as Financial Action Task Force (FATF), Basel Committee on Banking Supervision (BCBS) Guidelines on Customer Due Diligence, and United Nations (UN) resolutions concerning sanctions are to be followed to prevent the possible use of the Bank as a conduit for money laundering, terrorist financing and proliferation financing activities.

To further strengthen the regulatory framework for curbing Money Laundering, Terrorist Financing and Proliferation Financing, State Bank of Pakistan (SBP) has issued AML/CFT/CPF

Regulations for SBP REs vide BPRD Circular Letter no. 33 of 2022 dated November 28th, 2022 covering the following aspects;

Regulation	Areas Covered
Regulation -1 Risk Based Approach to AML/CFT	Internal Risk Assessment Report [IRAR] of the bank to identify, assess and understand ML/TF/PF & Transnational risks at entity level for customers, products, services, delivery channels, technologies and their different categories of employees etc.
Regulation -2 Customer Due Diligence (CDD)	CDD measures for identifying, verifying and onboarding new customers, continuing relationship with existing customers, protocols for marking active accounts to dormant and activation thereof through different channels available to customers.
Regulation -3 Reliance on 3rd Party Financial Institutions For CDD Measures	Responsibility for CDD measures to remain with the bank despite reliance on 3rd party financial institutions as allowed by the regulator.
Regulation -4 Targeted Financial Sanctions Under UNSC ACT, 1948 AND ATA, 1997	Bank to undertake Targeted Financial Sanctions (TFS) obligations with regard to Designated Persons / Proscribed Persons; entities owned / controlled directly or indirectly by it and individuals / entities acting on its behalf or its direction.
Regulation -5 Politically Exposed Persons [PEPs]	Bank to implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP or a closed associate or a family member of a PEP, both prior to establishing a business relationship and / or conducting transactions throughout the course of business relationship. This stipulates certain EDD measures to establish, continue business relationship and executing financial transactions in PEP accounts.
Regulation -6 NGO/NPO/Charity/Trust Accounts	The bank to ensure EDD measures as specified in the regulation while establishing relationship / execution of financial transactions with NGOs/NPOs, Charities & Trusts.
Regulation -7 Reporting of Transactions [STRs / CTRs]	The bank to file STR & CTR with Financial Monitoring Unit (FMU) as required under Section 7 of the AML Act 2010 (amended from time to time).
Regulation -8 Record keeping	The bank to ensure compliance of the instructions as given in AML/CFT & CPF regulations with regard to record keeping.

Regulation -9 Correspondent Banking	The bank to ensure EDD measures as outlined in the prevailing SBP AML/CFT & CPF regulations before entering/continuing Correspondent Banking relationships with other banks / FIs
Regulation -10 Money Value Transfer Service [MVTS] / Exchange Companies	The bank to ensure compliance of regulatory guidelines as envisaged in said regulation.
Regulation -11 Wire Transfers / Funds Transfers	The bank to discharge its responsibilities being an Ordering Institution or a Beneficiary Institution or an Intermediary Institution, as applicable, in terms of SBP guidelines.
Regulation -12 New Technologies	The bank to identify and assess ML/TF & PF risks before acquiring, adopting or developing of new products, technologies, services and business practices etc.
Regulation -13 Internal Controls	The bank's Internal Risk Assessment Report [IRAR] to recommend measures to BOD through time-bound Action plan to ensure adequate introduction and implementation of AML/CFT & CPF controls and preventive measures to mitigate potential ML/TF/PF risks posed to it. Furthermore, relevant guidelines relating to Compliance Function, Audit, Foreign Branches & Subsidiaries, Employee Due Diligence and Training Programs to be adhered.
Regulation -14 Counter Measures For High Risk Jurisdictions	The bank to comply with the obligations mentioned in the Counter Measures for High Risk Jurisdictions Rules, 2020 as amended from time to time.
Regulation -15 Regulation & Supervision	The bank to ensure screening of all its sponsor shareholders / beneficial owners, directors, president and key executives [all persons subject to Fit and Proper test (FPT)to verify that no person is linked to any criminal activity(ies) or DP/ PP directly or indirectly with any DP/PP; or affiliated with any terrorist organization. Further, in case of corporate group the bank shall implement; i. Policies and procedures for sharing CDD and Risk Management related information at group level. ii. Provision of compliance, audit and/ or AML/CFT functions iii. Confidentiality and use of information exchange at group level.

In addition to the AML/CFT/CPF regulations, SBP has also issued various Frameworks / regulations / guidelines such as:

- "Framework for Managing Risk for Trade Based Money laundering and Terrorist Financing" *vide FE circular no. 04 of 2019 dated October 14th, 2019,*
- "Branchless Banking Regulations for FIs" *vide BPRD circular no. 10 of 2019 dated December 30th, 2019,*
- *"Framework for Remote/ Digital Onboarding of Non Resident Pakistani (NRP)" issued vide BPRD letter No. BPRD/AML-01/2020-9124 dated August 13th, 2020,*
- *"Implementation of Cash Management & Single Treasury Account Rules, 2020" issued vide BPRD Circular No. 01 of 2021 dated April 06, 2021, and*
- *"Customers' Digital Onboarding Framework" issued vide BPRD Circular Letter No. 15 of 2022 dated April 30th, 2022.*
- *"Framework for Freelancers Accounts" issued vide BPRD Circular No. 05 of 2023 dated October 23th, 2023.*

The above stated Regulations/framework/guidelines as updated from time to time should be emphasized in bank's procedural manuals for meticulous compliance as the bank maintains zero tolerance for regulatory non-compliance.

2. SCOPE

This policy applies to each and every business / support segment and all employees of MCB Bank Limited – Pakistan to effectively mitigate the risks of ML / TF/ PF. As Bank is prone to the risk of being misused by criminal elements for their ulterior motives, this policy will be a guiding document for employees to address the risks stemming from customers or transactions in an effective way using risk-based approach.

Management shall continuously refine its Customer Due Diligence processes using the risk-based approach, through implementation of system-based Risk Rating environment for Customer Risk Profiling. Standard Operating Procedures (SOPs) along with various guidance documents (including guidance regarding red flag indicators of suspicious transactions relating to various areas emanating ML/TF/PF risks) and systems should be provided to the branches / field offices from time to time to ensure effective execution of the processes to identify and mitigate ML / TF / PF risks.

Considering the challenges of undocumented sector in the economy, execution of due diligence process is complex and time consuming. However, for compliance of regulatory requirements and to contain the customer related risks, bank's management, in addition to strict compliance of related laws/rules/regulations, shall make best efforts to conduct proper due diligence of every existing and prospective customer.

Moreover, the bank's management shall handle TF as separate risk and shall regularly conduct Internal Risk Assessment to identify threats posed by Terrorism Financing and to gauge efficacy of the controls to mitigate the inherent risks in such activities. Accordingly, existing controls shall be regularly evaluated in light of prevailing and emerging risks and additional appropriate actions/controls to identify, assess and mitigate the risks; will be implemented.

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, which entails comprehensive guidelines for banks to be implemented to manage these risks. Bank's management shall implement these guidelines through comprehensive SOPs and technology based solutions.

Policy Breaches:

Any breach of this policy by any employee may be treated as a disciplinary issue subject to disciplinary action as per bank's HR policy / procedures.

3. OBJECTIVES

- To prevent criminal elements from using the bank for money laundering activities from any of its branches and/or channels.
- To safeguard the bank from being used as a conduit in Terrorism and Proliferation financing.
- Ensuring that only bona fide and legitimate customers are accepted.
- Verifying the identity of customers using reliable and independent sources.
- Ensuring that proscribed/designated individuals or entities and their affiliates or associates are not having any banking relationship or being provided any service from the bank.
- Ongoing Monitoring of customer accounts and transactions to prevent or / and detect potential ML / TF / PF risks/activities.
- Implementing Customer Due Diligence process using risk-based approach.
- To ensure implementation of Targeted Financial Sanctions (TFS) related to Terrorism & Proliferation Financing (TF & PF).
- Managing reputational, operational, legal, financial and regulatory risks etc.
- To put in place appropriate controls for prevention, detection and reporting of suspicious activities in accordance with applicable laws/rules/regulations/laid down procedures.
- To comply with the applicable laws, rules, regulatory requirements and guidelines etc.

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

Senior Management shall define a proper mechanism to periodically inform the Board of Directors (BOD) (or its relevant sub-committee(s)) i.e. Compliance Review and Monitoring

Committee (CR&MC) regarding status of AML/CFT/CPF program, compliance initiatives, compliance deficiencies and other regulatory requirements.

4.2. SENIOR MANAGEMENT

Bank's Senior Management shall define ML/TF/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.

Further, Senior Management shall ensure efficacy of the AML/CFT/CPF controls embedded in Fintechs and RegTechs systems for supporting bank's operations.

4.3. COMPLIANCE FUNCTION

The Bank has in place an independent Compliance Function to ensure overall management of legal, regulatory, operational, financial and reputational risks associated with the Bank's 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 risks throughout the Bank's operations.

4.4. INDEPENDENT AUDIT FUNCTION

Bank has in place an independent audit function to test the effectiveness and adequacy of internal policies, controls and procedures relating to combating the crimes of money laundering, financing of terrorism and proliferation financing.

5. ELEMENTS OF CUSTOMER DUE DILIGENCE

5.1. CUSTOMER IDENTIFICATION

MCB Bank will serve only the genuine person(s) and all out efforts would be made by the management to determine true identity of its customers. Minimum set of documents and information shall be obtained from various types of customer(s), at the time of account opening, as prescribed in updated Anti-Money Laundering/ Combating the Financing of Terrorism/ Countering Proliferation Financing (AML/CFT/CPF) Regulations for SBP REs.

Customer relationship shall only be established on the strength of valid CNIC / SNIC / Passport / NICOP / SNICOP/ POC / ARC / POR / Form B / Juvenile Card number (as applicable) or where the customer is not a natural person, the registration/ incorporation number, business registration number or special resolution/authority, in case of government accounts/autonomous entities (as applicable).

For **non-face-to-face** customers, Bank's management shall put in place suitable operational procedures to mitigate the risk(s) attached with non-face-to-face prospective customer(s) and establish identity of the client. For "Due Diligence" of customers onboarded through digital channels, the management shall ensure to utilize available technological resources for customer

identification and verification, while complying with the SBP's Digital Onboarding Framework along with all applicable laws, rules and regulations including but not limited to AML Act 2010, AML/CFT/CPF Regulations, Foreign Exchange Regulations and Enterprise Technology Governance & Risk Management Framework for Financial Institutions, as amended from time to time.

The bank can rely on third party financial institutions for CDD measures, however the same shall be done by putting in place a comprehensive procedural document duly approved by the President. It may also be noted that as per the regulations, the ultimate responsibility for CDD measures shall remain with the bank relying on the third party financial institutions.

5.2. CUSTOMER VERIFICATION

Management shall identify the beneficial ownership of accounts/ transactions by taking all reasonable measures. Identity(ies) of the customer and beneficial owner shall be verified using reliable independent sources including biometric verification. Verification of the identity of the customers and Ultimate Beneficial Owners (UBO) shall be completed before business relations are established.

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 entity or for legal arrangements, branches shall take reasonable measures to identify and verify the beneficial owners:

(i) By identifying the natural person(s) who has ultimate effective control of a customer (as defined under relevant laws / rules / regulations); 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 through ownership interests, the identity of the natural person(s) (if any) exercising 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 updated AML/CFT/CPF Regulations, shall be verified by utilizing on-line facility of biometric verification and / or NADRA VERISYS. Verification of the identity of the customers and beneficial owners shall be completed before business relationship is established or a transaction is processed.

Further, wherever required, bank shall use mitigation measures in digital channels against identity theft such as live picture or video, electronic/ digital signatures, two-factor authentication through registered email and mobile number, and biometric verification of customers.

5.3. CUSTOMER ACCEPTANCE

Customer will only be accepted once above given formalities have been completed in letter and spirit. Following accounts shall not be opened/maintained by the bank where;

i. Identity, beneficial ownership, or information on purpose and intended nature of business relationship is not clear.

ii. 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 / Sanctioned / Specially Designated Nationals (SDNs) entities lists.

iii. Proscribed/Designated entities and persons or those who are known to be associated with such entities and persons, whether under the proscribed name or with a different name.

iv. Customers or transactions to / from sanctioned / designated countries including Israel.

v. Non-resident customers from high risk jurisdictions subject to call for action / Black listed by FATF.

vi. Anonymous / Fictitious / Benami or Numbered accounts.

vii. Banks that are not able to satisfactorily complete required CDD measures.

viii. Financial Institutions or corporations that do not have a physical presence in any country i.e. Shell Banks / Corporations

ix. Government accounts opened in the name of Government Officials

x. Government accounts mentioned in Federal Government's Treasury Single Account (TSA) list without Finance Division's NOC.

xi. Customers / account holders who transact / deal in Virtual Assets (VA), Virtual currencies (VC), i.e. Bitcoins, Etherium, Tether etc. and Virtual Assets Service Providers (VASPs).

xii. Illegal Money Value Transfer System (MVTS) such as Hawala/Hundi including unauthorized/ unlicensed money changers / prize bond dealers.

xiii. Offshore Foreign Exchange Trading, Margin Trading, Contract for Difference (CFD) Trading Websites / Apps / Platforms e.g. OctaFX, Easy Forex etc. and individuals who intend to transact in such apps through Person to Person (P2P) mode. Any other activity forbidden by the law e.g. gambling, human smuggling etc.

xiv. Unauthorized/ unlicensed digital lending platforms (individuals or businesses)

Customers requiring 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 as specified in the updated AML/CFT/CPF Regulations must be applied on such account types including approval of the senior management as prescribed in SBP's prevailing AML/CFT/CPF Regulations. This enhanced scrutiny/ analysis is to 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 STR and termination of the business relationship in line with the prevailing laws / rules / regulations. 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:

- NGOs/INGOs/NPOs/Charities/Trust/Club/Societies/Madaris/Masajid/ Dargah/ Darbar / Associations;
- Political Exposed Persons (PEPs);
- Money Service Businesses including Exchange Companies;
- Relationship Management Accounts (RMAs) from High Risk Jurisdictions;
- Precious metals dealers (gold, silver, platinum, palladium etc.) / Jewelers;
- Embassies, consulates and diplomats missions;
- Real Estate Dealers;
- Nationalist Groups/ Political Parties;
- Customers from High Risk Countries;
- Arms and ammunition dealers;
- Correspondent Banking Relationship;
- Accounts wherein the funds were sourced under Amnesty schemes of Government of Pakistan;
- Exchange Companies (MSBs);
- Electronic Money Institutions (EMI), Payment Service Providers (PSP)/Payment Service Operators (PSO) and Digital Banks;
- Non-Banking Finance Companies (NBFCs)
- Employees of NGOs / NPOs / Trusts, Masajids / Madrassahs and Exchange Companies.

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

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

5.3.1. ENHANCED DUE DILIGENCE

Customers that pose higher ML/ TF/ PF risks are subject to enhanced scrutiny, or EDD. This enhanced level of scrutiny provides bank with a more comprehensive level of understanding of the risks associated with the customer profiles.

Bank 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 and carrying out additional scrutiny (i.e. verifiable adverse media searches).
- 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(s) 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 CDD/EDD of customers may also prompt appropriate action including termination of relationship / filing of STR; in line with the prevailing laws/rules/regulations.

5.3.2. CDD FOR WALK-IN CUSTOMERS

Walk-in customers shall only be entertained, once due diligence measures for transactions relating to such customers as prescribed by the applicable SBP's AML/CFT/CPF Regulations/guidelines along with international best practices have been complied with.

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; using reliable, independent source of information, i.e. biometric verification or NADRA Verisys in line with SBP's Frequently Asked Questions (FAQs) on use of Biometric Technology.

Further, name clearance should also be obtained against sanctioned lists through E-Name Checker Module / Sanction Screening for walk in customer executing the transaction to ensure that the person is not a proscribed person / entity.

5.3.3. CDD FOR ASSET SIDE/ TRADE FINANCE CUSTOMERS

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

5.3.4. CUSTOMERS FROM HIGH RISK JURISDICTIONS

Bank's management shall also apply Enhanced Due Diligence (EDD) including Senior Management's (as defined by the regulator) approval, proportionate to the risks to business relationships and transactions with individuals and entities including Financial Institutions from high risk foreign jurisdictions in compliance of latest AML/CFT/CPF Regulations for SBP REs and Counter Measures for High Risk Jurisdictions Rules, 2020 issued by Ministry of Finance, vide SRO 951(I)/2020 dated October 01, 2020 (as updated from time to time). High risk countries will be identified on the basis of communication by the National Executive Committee (NEC) through Financial Monitoring Unit (FMU), Government of Pakistan (GoP).

5.4. TARGETED FINANCIAL SANCTIONS (TFS) MANAGEMENT

In order to comply with the Targeted Financial Sanctions regime, the bank's management will devise effective systems and controls to safeguard the bank from being exploited by the terrorists for 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 owners/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 on real time basis before establishment of the relationship.

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 FMU on immediate basis. Further, any sponsor shareholders / beneficial owners, directors, president and key executives (all person(s) subject to 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 i.e. atleast once per anum (preferably twice per anum).

5.5. ACCOUNTS AND TRANSACTIONS MONITORING

Business Groups, as applicable, 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 SBP's 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 the SBP AML/CFT/CPF Regulations for SBP REs, instructions of Financial Monitoring Unit (FMU) and other applicable local /international bodies.

Business groups / functions must ensure that complete originator information along with unique transaction identifier is available with every domestic and cross border transfer.

SWIFT MESSAGES shall be screened through name filtering solution to prevent utilization of bank's channels by individuals / organizations in Proscribed/Sanctioned lists.

Financial transactions should be monitored through automated Transaction Monitoring System (TMS) based on pre-defined scenarios and thresholds.

Management shall pay special attention to every complex, unusually large and out-of-pattern transaction, which has no apparent economic or visible lawful purpose. If management suspects or has reasonable grounds to suspect that the funds are the proceeds of criminal activities or have potential to be used for terrorist activities, it shall report its suspicion to Financial Monitoring Unit (FMU) through Compliance and Controls Group (CCG). In case of suspicion, management shall raise Suspicious Transaction Report in line with the requirement highlighted under AML Act 2010, AML / CFT / CPF regulations and Guidelines of the Financial Monitoring Unit (FMU) issued/updated from time to time. Accordingly, management should devise procedures to meet these requirements. Given the ML/TF/PF risks associated with the suspicion, business units may not commence business relations or perform the transaction; or shall terminate the business relationship if any, in line with section 7D of AML Act 2010, updated from time to time.

Bank's management shall also focus on emerging ML/TF/PF risk emanating from Freelancers and their inward remittances / payments against contracts with foreign agents or companies/entities/organizations.

For customers / clients whose accounts are dormant, branches shall not allow debit entries in such accounts (except for those allowed under AML/CFT/CPF Regulations) until formal request from the customer is received from channels specified in AML/CFT/CPF Regulations for SBP REs updated from time to time. Bank should perform Verisys/ Biometric as per their respective internal control arrangements and a copy (digital or hard copy) to be retained in record. Further, bank shall ensure that accounts without valid Identity Document are treated as per the relevant regulations.

Bank's employees are strictly prohibited to disclose the fact to the customer that a Suspicious Transaction Report (STR) / Currency Transaction Report (CTR) or related information has been reported to FMU or any other Law Enforcement Agency (LEA).

Currency Transactions (i.e. CTR) exceeding the prescribed limits as defined in AML Act 2010 and its subsequent amendments from time to time will be reported to FMU through CCG.

In order to adopt additional measures to further strengthen the CDD regime, CDD/EDD Assessment of Top 100 depositors of each branch will be conducted as required by the regulator. The branches shall conduct assessment of such accounts regarding compliance of the CDD/EDD requirements and identify deficiencies and make necessary efforts to regularize the deficiencies identified during the assessment process.

5.6. WIRE TRANSFER

Bank may act as Ordering Institution, Beneficiary Institution or Intermediary Institution while processing wire transfers/fund transfers. However, Business / concerned support Group/Function shall ensure that all requirements as described in SBP's AML/CFT/CPF regulations along with international best practices are complied. Besides, transactions with incomplete originator/beneficiary information and unclear purpose shall not be executed and if required may be reported to the Financial Monitoring Unit (FMU) under section 7 of the AML Act 2010, amended from time to time. For Home remittance transactions under Pakistan Remittance Initiative (PRI), bank shall follow risk based approach for execution/termination of transactions

where no information can be made available other than the originator name for screening; in line with the Frequently Asked Questions (FAQs) on Targeted Financial Sanctions (TFS) Obligations circulated vide BPRD Circular Letter No. 02 of 2022 and any subsequent amendment thereto.

5.7. RISK MANAGEMENT

All relationships shall be categorized with respect to their risk levels i.e. High, Medium and Low based on the risk profiling of customer through e-KYC/CDD application and as guided in SBP's AML/CFT/CPF Regulations/guidelines and international best practices for making effective decision whether to perform Simplified Due Diligence (SDD), Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) both at the time of establishing and ongoing monitoring of business relationship.

CCG shall counter-examine High Risk relationships requiring Senior Management's approval; to ensure that due diligence procedures are adhered to in letter and spirit by the concerned staff in business segments.

Further Personal accounts will not be allowed to be used for organized charity purposes/collection of donations. Moreover, these accounts shall not be used for business purposes unless otherwise directed under SBP's AML/CFT/CPF Regulations.

Customer KYC / CDD profile will be reviewed and/or updated on the basis of below mentioned pre-defined frequency, in accordance with the risk profile of the customer:

High Risk	*Atleast Once in a Year or on need basis**
Medium Risk	*At least Once in 2 Years or on need basis**
Low Risk	*Atleast 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 without lapse of above defined period.

While formulating procedures and controls, management shall take into consideration Money Laundering, Financing of Terrorism and Proliferation Financing threats that may arise from the use of new or developing technologies, especially those having features of anonymity or inconsistency with the spirit of SDD/CDD/EDD measures.

5.8. REVIEW OF PRODUCTS AND SERVICES INCLUDING NEW TECHNOLOGIES

Bank's management shall identify, assess and manage the ML/TF/PF risks that may arise in relation to expansion of operations in different jurisdictions, the development of new products, services, business practices including delivery mechanism 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 risks specially identity theft, anonymity and cyber-crimes.

5.9. INTERNAL RISK ASSESMENT

Bank's management shall ensure an entity level Internal Risk Assessment Report (IRAR) on annual basis, as required under Regulation-1 of SBP's AML/CFT/CPF Regulations issued vide BPRD Circular letter no. 33 of 2022 dated November 28th, 2022 updated from time to time. IRAR shall cover ML/ TF/ PF risks including Transnational TF risks and other emerging risks. IRAR shall also identify, assess and understand ML/TF/PF risks for customers, products, services, delivery channels, geographies, technologies and different categories of employees.

It should be ensured that IRAR is dynamically updated subject to any change of circumstances, relevant new threats or after any updation in the NRA exercise conducted by the Government of Pakistan. IRAR shall be presented to the BoD for approval. 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.

Bank's policy for application of SDD, CDD and EDD will be based on the levels of ML/ TF/ PF risks identified as low, medium, or high in IRAR. Further, bank's policies / controls / procedures / preventive measures shall be developed / updated / implemented proportionate to the level of ML / TF / PF risks as evaluated in IRAR.

6. RECORD KEEPING

The records of identification documents, account opening forms, KYC forms, verification documents (information obtained digitally or in hard form) and other relevant documents 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 as stipulated in bank's Record Management Policy.

Management shall maintain all necessary records of transactions, both domestic and international, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions) and shall also keep and maintain all record related to STRs and CTRs filed by it for a minimum period of ten years from completion of the transaction.

However, records relating to customers, accounts or transactions will be retained for 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 signature cards and documents indicating signing authorities, and other documents relating to the account/deposit or instrument surrendered to SBP / any other competent law enforcing agency (duly authorized by law/court), shall be kept in the bank's record till such time that SBP / competent law enforcing agency (duly authorized by law/court) informs in writing that same need no longer to be preserved.

7. CORRESPONDENT BANKING & MONEY SERVICE BUSINESSES [MSBs]

The Bank's management will establish correspondent banking 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 for SBP RE's relating to the country in which that bank/MSB operates. Moreover, the Bank shall ensure EDD measures when establishing or continuing correspondent / MSB relationship with banks/ financial institutions/MSBs except for Relationship Management Application (RMA) relationships, whose risk factors as per the bank's risk register will define the level of due diligence in line with CDD and AML/CFT/CPF Procedural handbook. Further, RMA relationships will 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).

Management shall undertake preventive measures consistent with FATF and Basel Committee on Banking Supervision (BCBS) Guidelines, *Wolfsberg's principles for correspondent banking,* applicable laws, rules and regulations to effectively manage all high risk correspondent banking relationships involving the execution of 3rd party payments [e.g. nested/downstream and payable-through account services]. Further, opening and reviews of the correspondents and MSBs accounts are to be carried out as per risk-based approach in line with the prevailing AML/CFT/CPF Regulations issued by the regulator.

Regarding approval matrices for Correspondent Banking, following are the details.

- Nostro accounts are approved by the President upon recommendation of the Group Head, Treasury & FX Group.
- Vostro & RMA from High Risk jurisdictions will be approved by the Chief Compliance Officer upon recommendation of the Group Head, Treasury & FX Group, while their periodic reviews will be approved by respective Division Head in Compliance & Controls Group upon recommendation of the Division Head, Financial Institutions Division.

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	*Atleast Once in a Year or earlier if any happening / event/situation so demands**
Medium Risk	*Atleast Once in 2 Years or earlier if any happening / event/situation so demands **
Low Risk	*Atleast 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, EDD will be conducted and customer profile will be updated immediately. Material change in relationship in the context of correspondent banking would mean that the conduct of the account does not commensurate with the stated profile of the correspondent or respondent bank and can also be triggered owing to some geo-political situation under sanctions regime.*

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

8. TRADE BASED MONEY LAUNDERING

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 the regulations and regulatory "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. E-COMMERCE

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 FE Circular No. 07 of 2020 dated December 02, 2020 amended from time to time must be adhered.

10. 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 or, where applicable, international obligations as well.

Management shall ensure to take adequate measures to safeguard the bank from Proliferation Financing risk emanating from trade transactions. Further, bank's management must ensure that the automated controls exist in the bank for mitigation of such risks.

11. FOREIGN BRANCHES AND SUBSIDIARIES

Bank's management shall pay particular attention to their branches and subsidiaries located in countries, which do not or insufficiently comply with FATF Recommendations (as determined by FATF or identified by SBP) and ensure that their AML/ CFT/ CPF policy is observed by branches and subsidiaries in those countries as per their CDD & AML/CFT/CPF Procedural handbook.

Where the law of the host country conflicts with the AML/ CFT/ CPF requirements of Pakistan so that the overseas branch or subsidiary is unable to observe the higher standards, CCG shall report this to SBP and comply with such further directions as may be issued. However, management shall conduct assessment of home country's AML/CFT/CPF regulations vis-à-vis host country's AML/CFT/CPF regulations to ascertain higher of the two standards and maintain such inventory for ready reference by respective overseas jurisdictions as well as by CCG at Head Office.

In addition to the above, for subsidiaries in a corporate group (Corporate group means a group that consists of a parent entity exercising control or management on branch or subsidiary that are subject to AML/CFT/CPF policies and procedures at the group level). Bank's management shall ensure the following in line with AML/CFT/CPF Regulations for SBP REs issued vide BPRD circular letter no. 33 of 2022 dated November 28th, 2022 amended from time to time:

- Development and implementation of procedures for sharing information at a group level required for the purposes of CDD and risk management;
- The provision of information of customer, account, and transaction information from branches and subsidiaries when necessary for AML & CFT purposes, for group-level compliance, audit, and/or AML & CFT function.
- Adequate safeguards on the confidentiality and use of information exchanged at group-level, including safeguards to prevent tipping-off.

12. EMPLOYEE DUE DILIGENCE

In line with SBP's AML/CFT & CPF regulations, Bank's management must develop adequate screening procedures to ensure high standards while hiring employees whether contractual or permanent or hired through outsourcing. These procedures must include controls to prevent criminals or their associates from being employed by the bank.

In this respect, bank's management shall ensure that:

- All employees are screened against lists of designated and proscribed individuals, on an ongoing basis, and maintain proper record of screening. Accordingly, employees shall become disqualified if they are designated/ proscribed or associated directly or indirectly with DPs/ PPs.
- No employee is or has been convicted/ involved in any fraud/ forgery, financial crime etc.
- No employee is or has been associated with any illegal activity concerning banking business, foreign exchange business, financial dealing and other business or employment.
- Bank management will comply with SBP's Fitness and Proprietary Test (F&PT) criterion required for sponsor shareholders & board approval and senior management appointment.

13. VENDORS, OUTSOURCING AND SERVICE PROVIDER'S DUE DILIGENCE

Bank's management should ensure that regulatory guidelines as specified in SBP's "Framework for Risk Management in Outsourcing Arrangements by Financial Institutions" issued vide BPRD circular no. 06 of 2019 dated December 17, 2019 (amended from time to time); related to Due Diligence of its vendors and outsourced service providers are implemented.

14. TRAININGS AND CAPACITY BUILDING

Suitable Employee Training Program will be put in place by bank's management on an annual basis to enhance staff capability, to effectively implement the regulatory 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 ML/TF/PF techniques, methods, and trends.

Further, as required in AML/CFT/CPF Regulations, bank's management will chalk out and implement suitable Annual Training Program, which may be developed after formal Training Need Assessment in area of AML/ CFT/ CPF annually. Bank's management shall ensure that the Annual Training Program adequately covers training sessions for Sponsor Shareholders, BoD, Senior Management, Line Management, and Field Staff. Special emphasis shall be given for officials directly/ indirectly responsible for ensuring Governance/ Oversight/ Supervision/ Monitoring of risk mitigation of ML/ TF/ PF risk and ensuring AML/ CFT/ CPF preventive measures as per the AML Act 2010 (amended from time to time) and latest Regulations including on TFS for TF & PF and STR/ CTR as per their required need and relevance of job.

Furthermore, bank's management, wherever required, will continue assessment of Bank's employee's knowledge via Compliance Knowledge Assessment System (CKAS) test also covering AML / CFT/ CPF and TFS areas and its key regulatory requirements in each alternate year.

15. COMPLIANCE REVIEW

CCG shall perform the periodic review of branches and non-branch entities to check their level of compliance with the provisions in the CDD & AML/CFT/CPF Policy and procedures according to their scope/framework.

16. CDD & AML/CFT/CPF PROCEDURAL HANDBOOK

All procedures required for implementation of the guidelines related to SDD/CDD/EDD and AML/CFT/CPF shall be documented in the form of CDD and AML/CFT/CPF Procedural Handbook. This document shall be prepared by CCG and shall carry the recommendations of all stakeholders i.e. RB, OPG, RMG, WBG LAG etc. subject to final review by Chief Compliance Officer. The approving authority for aforesaid document shall be President. Furthermore, it shall be reviewed at least on an annual basis and / or earlier on need basis.

The bank shall ensure keeping this document up to date for maintaining effectiveness of its AML/CFT/CPF controls [preventive measures] including implementation of TFS related to TF & PF and reporting of STRs / CTRs.

17. POLICY REVIEW PERIOD

The CDD & AML / CFT/ CPF policy will be reviewed on as and when required basis but not later than one year.

GLOSSARY

AML/CFT/ CPF	Anti-Money Laundering/ Combating the Financing of Terrorism/ Countering Proliferation Financing
AMLD	Anti-Money Laundering Department
ARC	Aliens Registration Card
B2C	Business-to-Consumer
BCBS	Basel Committee for Banking Supervision
BOD	Board of Directors
BPRD	Banking Policy and Regulations Department
CCG	Compliance and Controls Group
CCO	Chief Compliance Officer
CDD	Customer Due Diligence
CNIC	Computerized National Identity Card
CKAS	Compliance Knowledge Assessment System
CRMC	Compliance Review and Monitoring Committee
CTR	Currency Transaction Report
DP	Designated Person
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FCCM	Financial Crime & Compliance Management
FID	Financial Institutions Division
FMU	Financial Monitoring Unit
F&PT	Fitness and Proprietary Test
GoP	Government of Pakistan
HRMG	Human Resource Management Group
IRAR	Internal Risk Assessment Report
KYC	Know Your Customer
LAG	Legal Affairs Group
MOFA	Ministry of Foreign Affairs
MSB	Money Service Business
NACTA	National Counter Terrorism Authority
NADRA	National Database & Registration Authority
NEC	National Executive Committee
NICOP	National Identity Card For Overseas Pakistanis
NRA	National Risk Assessment
NRP	Non Resident Pakistanis
OFAC	Office of Foreign Assets Control
OPG	Operations Group
POR	Proof of Registration (For Afghan Nationals)
PEP	Politically Exposed Person
POC	Pakistan Origin Card
PP	Proscribed Person
RBA	Risk Based Approach
REs	Regulated Entities

RBG	Retail Banking Group
RMG	Risk Management Group
SBP	State Bank of Pakistan
SDD	Simplified Due Diligence
SNIC	Smart National Identity Card
SNICOP	Smart National Identity Card for Overseas Pakistanis
SNIC	Smart National Identity Card
SRO	Statutory Regulatory Orders
STR	Suspicious Transaction Report
TBML	Trade Based Money Laundering
TFS	Targeted Financial Sanctions
TSA	Treasury Single Account
UBO	Ultimate Beneficial Owners
UNSCR	United Nations Security Council Resolutions
VASPs	Virtual Assets Service Providers