Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) Policy

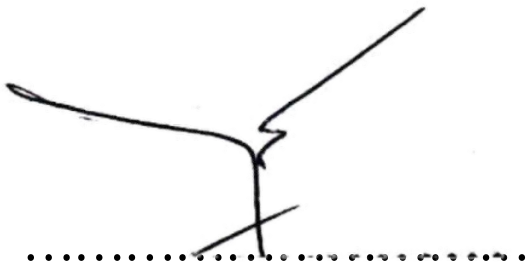
Legal, Compliance and Secretary Department

March 2025

MYANMA APEX BANK LIMITED

POLICY ON ANTI-MONEY LAUNDERING (AML) AND COMBATING THE FINANCING OF TERRORISM (CFT)

APPROVED BY



KYAW NI KHIN

DIRECTOR/ CHIEF EXECUTIVE OFFICER

Contents

Anti-Money Laundering and Combating the Financing of Terrorism Policy

1. Introduction

Myanma Apex Bank Limited (**MAB**) actively undertakes both local and international financial services with both domestic and international organizations since MAB has been granted a "Authorized Dealer License" in 2010 from the Central Bank of Myanmar (**CBM**).

Every Financial Institution has to comply with the laws, rules, regulations, orders, directives, guidelines and recommendations relating to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) in its banking and financial sector.

In this regard, MAB shall have its own Anti-Money Laundering and Combating the Financing of Terrorism policy and procedure of internal control, overseen by an appointed knowledgeable compliance officers well trained in AML/CFT related matters to effectively manage and mitigate such risks in MAB's operations.

2. Key Compliance Principles

(a) Abiding by the laws, rules and regulation relating to our business operations as well as the prevention of money laundering and terrorist financing;

(b) Observing values such as fairness, honesty, good social ethics etc. and also provides confidence and a sense of sensitivity for both internal customers as well as external customers;

(c) Compliance starts at the top management level from the board of directors and down to the lowest level of bank's staff and thus, every employee must keep compliance in their minds and refrain from any dishonest act, unethical behaviors and corruption.

3. Money Laundering

Money laundering refers to:

(a) converting of illegal funds and assets into legitimate funds and assets;

(b) concealing of financial resources obtained through criminal activities; and

(c) transferring of funds from one account to another account repeatedly in order to make the funds appear as if they were obtained through legitimate transactions.

The money laundering process typically encompasses three stages - **Placement, Layering, and Integration.**

(a) **Placement**: the first stage of Money Laundering is criminals transform the cash obtained through illegal means into legitimate financial system.

(b) **Layering**: the second stage is to continue to work on segregating the proceeds of offenses or crimes under the Anti-Money Laundering Act 2014 using various financial instruments to transform them with the intention of concealing the original form and the name of the original owner behind the operations.

(c) **Integration**: the last stage is to return the laundered or cleaned money to legitimate financial system managed by end user, through legal channels.

The following offences are prescribed as predicate offences under the Anti- Money Laundering Law:

(a) Offences relating to terrorism and financing of terrorism

(b) Offences relating to trafficking in humans and migrant smuggling

(c) Offences relating to illicit trafficking of narcotic drugs and psychotropic substances

(d) Offences relating to illicit arms trafficking

(e) Offences relating to trafficking of stolen and other illicit goods

(f) Offences relating to corruption and bribery

(g) Offences relating to fraud

(h) Offences relating to counterfeit money

(i) Offences relating to counterfeit goods

(j) Offences relating to murder or causing grievous bodily harm

(k) Offences relating to kidnapping, illegal restraint and taking hostage

(l) Offences relating to robbery or theft

(m) Offences relating to smuggling

(n) Offences relating to extortion

(o) Offences relating to forgery

(p) Offences relating to converting or transferring any money and property knowing, or having reason to believe, that is obtained from the commission of any offence, in order to disguise or conceal the source of such money and property, or with the intention of aiding a person involved in a predicate offence or after its commission to avoid the legal consequences of his actions

(q) Concealing or disguising the proceeds of crime of their true nature, source, location, inherent property, conversion or ownership, knowing or having reason to believe that they are obtained from committing an offence

(r) Obtaining, keeping in possession or using such profits, knowing or having reasons to believe at the time of receipt that they are proceeds of crime

(s) Attempting or conspiring, aiding, supporting, facilitating, abetting, providing, recruiting, managing, associating with counseling the commission of an anti-money laundering offence including the abovementioned offences

(t) Being a member of an organized crime group that commits, attempts to commit or conspires to commit a money-laundering offence including abovementioned offences

(u) Inciting a person to commit a money-laundering offence, or conspiring with or deliberately facilitating a person or persons to commit money-laundering

(v) Laundering money and property in Myanmar that is derived from committing an offence abroad where the act constitutes an offence in that country and would have constituted any of the abovementioned offences had the same act been committed in Myanmar.

4. Terrorist Financing

Terrorist Financing is the act of providing financial support for terrorist activities. Fund may originate from both legal and illicit sources. Funds raised to finance terrorism are usually laundered and the anti-money laundering process in the banks through tracking terrorist financing is, therefore, most effective way to combat the terrorism.

MAB's AML/CFT Policy is established to protect MAB from being used or implicated in money laundering or terrorist financing activities. All MAB staff, wherever located, aware of the bank's Anti-Money Laundering (AML) policy and procedures and must be vigilant in the fight against money laundering and must not allow MAB to be used for money laundering activities.

5. Financing of Proliferation

The financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes.

MAB will fully comply and implement with the United Nations Security Council Resolutions, FATF Recommendation 7 and Orders or directives issued by the Central Committee for Conter Terrorism relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

6. Governance and Responsibilities

6.1. The Responsibilities of Board of Directors (BOD)

The Board of Directors (BOD)) has the overall responsibility for the effective implementation of the AML/CFT policy and for ensuring that the bank's anti-money laundering and counter-financing of terrorism efforts comply with both local and international legal requirements. The BOD ensures that sufficient resources, infrastructure, and expertise are allocated to AML/CFT functions within the organization.

6.2. Compliance Officer and Compliance Function

The Chief Compliance Officer (CCO) is independent and appointed at a senior management level. He/she has appropriate experience and qualifications in respect of AML/CFT matters with the authority to act independently and directly report to the board of directors.

MAB shall provide the CBM and the CBM's Myanmar Financial Intelligence Unit (**MFIU**) with details of the chief compliance officer including name, details on qualifications, address, contact number and email address. MAB shall promptly inform the CBM and MFIU of any change in the chief compliance officer.

The responsibilities of the Chief Compliance Officer include, but is not limited to, the following:

(a) Implementing the Bank's AML/CFT policy and its procedures. This includes any sanctions policies;

(b) Stating the requirements of all AML/CFT matters in the Bank's AML/CFT Policy;

(c) Working internally with bank employees at all levels and externally government regulator;

(d) Supervising operations of the respective department to make sure its accounting, investment and lending practices comply with local laws;

(e) Assisting and training employees on regulatory issues, and updating such training from time to time as where necessary and advisable;

(f) Monitoring any suspicious transactions;

(g) Liaising in the verification of suspicious accounts maintained in MAB, and addressing any inquiries raised by the MFIU, CBM or any competent authority;

(h) Attending workshops, seminars, forums and meeting that are organized by the CBM, MFIU and foreign banks held at Nay Pyi Taw and Yangon;

(i) Monitoring and screening daily Threshold Transaction Report (**TTR**) and Reporting Suspicious Transaction Report (**STR**) online reporting to MFIU;

(j) Leading any KYC or counterparty questionnaires issued by international correspondent banks as well as Western Union recertification processes;

(k) Maintaining and updating MAB's data base related to sanctioned Entities or Persons and PEPs (as defined in accordance with Foreign Exchange and Foreign Trade Act);

(l) Coordinating compliance within MAB's individual branches. For the avoidance of doubt, branch managers and division managers are equally responsible for AML/CFT compliance, and will be directly responsible for AML/CFT compliance at their individual branch and department level;

(m) Establishing AML/CFT compliance department, assigning skillful and experienced senior staff official of AML/CFT for the task of the department and forming the compliance unit at each department and bank branch;

(n) Approving Customers' Accounts Freezing for CBM AML/CFT letters which investigate into Core Banking System;

(o) Undertaking periodic reporting to the Board or MAB's Executive Management Committee, which should contain:

(1) All suspicious transactions detected, and the implications on MAB during such reporting period

(2) Measures taken by compliance staff to strengthen the bank's AML/CFT policies, procedures, systems and controls of the Bank.

(3) Results of any independent audit of AML/CFT systems

(4) Results of any onsite inspections conducted by the CBM or MFIU

(5) Statement on remedial actions required to be implemented by the Bank.

The Head of Legal, Compliance and Secretary Department will have the following authority:

(a) Overseeing the compliance officers and ensuring that such officers submit the report of the transactions of deposit, encashment, transfers that exceed the threshold amount to MFIU within 24 hours if it is situated in an urban centre and within three working days if it is situated in a remote district.

(b) Filling STR in compliance with the applicable laws, rules and regulations;

(c) Maintaining the number of STRs files along with a brief summary as to the local currency or foreign currency account of the suspicious activities which shall be reported to Senior Management and the Board;

(d) Ensuring all supporting evidence for STR shall be maintained for a minimum of 5 years and stored securely;

(e) Once the suspicious activity is discovered, reviewing and making a recommendation as to whether a STR should be filed;

6.3. Responsibilities of Compliance and Risk Management Committee (CRMC)

The Compliance and Risk Management Committee is regularly monitor to ensure compliance with the laws, regulations and other relevant regulators, particularly the

Financial Institutions Law and the directives and notifications issued by the Central Bank of Myanmar, and to ensure the performing the regularly risk assessments on operations.

6.4. Responsibilities of Legal, Compliance and Secretary Department (LCSD)

The Legal, Compliance and Secretary Department is responsible to undertake the following responsibilities:

(a) Monitoring of the bank's compliance with AML/CFT laws, regulations, and internal policies;

(b) Monitoring of branches on a regular basis to ensure full compliance with AML/CFT and WMD laws, regulations, directives and internal policies;

(c) Keeping the bank up to date with any changes in AML/CFT and WMD laws, regulations and instructions;

(d) Monitoring transactions for suspicious activities and ensuring adherence to Know Your Customer (KYC), Customer Due Diligence (CDD) and Enhance Due Diligence (EDD) procedures;

(e) Conducting training and awareness programs for employees to ensure they understand their obligations under the AML/CFT framework.

6.5. Responsibilities of Internal Audit

The Internal Audit provides independent verification of the effectiveness of the bank's AML/CFT controls and procedures and is responsible for:

(a) Conducting regular internal audits to assess the effectiveness of AML/CFT controls, systems, and compliance;

(b) Providing detailed reports to the Board of Directors (BOD) on audit findings, including any identified weaknesses or deficiencies in AML/CFT procedures;

(c) Making recommendations for improvements to strengthen the bank's AML/CFT framework.

7 Risk Assessment

This Section deals with the risk assessment process to determine certain risk category of customer accounts for the purpose of CDD. All accounts must be assigned with a risk category for CDD purpose. The risk category must be assigned prior to account opening. The risk level will determine the level of due diligence required to be performed in the account hence proper risk assessment of the accounts is necessary and important. In the case of existing customers maintaining an account and/or doing transactions before implementation of this procedure, the customer shall be identified, sufficiency shall be reviewed, and risk grading shall be done.

While assigning risk categories, MAB shall give consideration to factors such as:

(a) Customer risk

(b) Country or Geographic region risk (i.e. countries or geographic areas in which customers operate or the place of origination or destination of transactions);

(c) Products and services risk (i.e. the risks that arise from the products and services offered); and

(d) Delivery channel risk (i.e. the risks that arise from the channels used to deliver products).

(each an "**Assessment Criterion**").

The risk assessment should take place *prior* to the launch of new products, business practices or the use of new or developing technologies. The risk assessment will be performed by the senior management on an annual basis. MAB shall identify, assess and take appropriate measures to manage and mitigate any money laundering or terrorism financing risks that may arise in relation to:

(a) The development of new products and new business practices including new delivery mechanisms for products and services; and

(b) The use of new or developing technologies for both new and pre-existing products.

7.1. How to Perform a Risk Assessment

As a general overview, the Risk Assessment is conducted by consolidating the relevant information for each of the Assessment Criterion. Upon the processing the statistics, an internal risk assessment is undertaken to evaluate the Assessment Criterion on a risk scale from “Low”, Medium” to “High”.

Based on the identified level of risk, if a particular Assessment Criterion is assessed to be of “High” risk, the senior management will put into place measures to mitigate and/or to address the risk.

For example, if it is identified based on the risk assessment that the customers in the previous year are primarily from a foreign background, and the identified countries of such foreign customers are mostly from high-risk and/or monitored jurisdictions based on the Financial Action Task Force (**FATF**) public lists, then practical measures should be put into place to enhance customer due diligence with respect to customers from such foreign jurisdictions as part of our ongoing ML/FT compliance.

MAB has developed a risk profile on customers and transaction established and documented based on the following:

(a) The purpose of an account or relationship;

(b) The customer's anticipated business with the bank;

(c) The source of funds and source of wealth of the customer;

(d) Knowledge of the customer and beneficial owner;

(e) Enhance the customer who communicate with high-risk customers;

(f) Update more regularly the information on all customers;

(g) Monitor the amount, type and frequency of customer transactions; and

(h) Adopt other measures as may be prescribed by the CBM, the Central Body or the MFIU.

7.2. Risk Factors

MAB stated on a risk scale from “Low”, Medium” to “High”.

The following includes the general context for each Assessment Criteria:

(A) Customer Risk Factors

(1) The business relationship is conducted in unusual circumstances

(2) Non-residents not holding Myanmar Identification Card or Myanmar Passport.

(3) Legal persons or arrangements that manage the assets of third parties.

(4) Companies that have nominee shareholders or shares in bearer form.

(5) Activities those are cash-intensive or susceptible to money laundering or terrorism financing

(6) The ownership structure of the legal person appears unusual or excessively complex with no visible economic or lawful purpose given the nature of the company’s business.

(7) Business relationships conducted in or with countries as identified by the Myanmar Financial Intelligence Unit (MFIU).

(8) Persons who are prominent and entrusted with public activities locally or abroad, his/her family members and persons closely co-operating with them.

(9) High net worth customers, or customers whose source of income or assets is unclear.

(10) Businesses/activities identified by the FIU, the Central Body, the CBM or the FATF as of higher money laundering or financing of terrorism risk.

(B) Country or Geographic Region Risk Factors

(1) Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.

(2) Countries identified by the FATF, Central Body, MFIU or CBM as high risk.

(3) Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.

(4) Countries classified by credible sources as having significant levels of corruption or other criminal activity.

(5) Countries or geographic areas classified by credible sources as providing funding or support for terrorist activities, or that United Nations have designated terrorist organisations operating within their country.

(C) Products, Services and Delivery Channel Risk Factors

(1) Private banking

(2) Anonymous transactions

(3) Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.

(4) Payment received from unknown or un-associated third parties.

(5) Complex trade financing products.

7.3. Classification of Risk

(A) Customer Risk

(a) Low Risk

(b) Government departments and government owned companies (state and central).

(c) Person Resident whose income structures are well defined.

(d) Salaried Employee

(e) Pensioner

(f) Student

(g) Manufacturing Business

(h) Retail and Wholesale

(i) Transportation and Logistics

(j) Agriculture and Farming

(k) Tourism

(l) Medical and Health Care

(m) All customers not classified either as High Risk and/or Medium Risk.

(b) Medium Risk

(1) Telecommunication service providers

(2) Information Technology and Communication

(3) Import/Export

(4) Aviation/Aerospace

(5) Industrial Estate

(6) Religious Association

(7) Legal Persons (Company, Association)

(c) High Risk

(1) Non-resident customers

(2) Politically Exposed Persons ("PEP") or customers linked to a PEP

(3) NGO/ INGO/ Association

(4) Business relationships conducted in or with countries as identified by the MFIU

(5) Non-face-to-face, virtual customers

(6) Money Changers

(7) Money Remittance Company

(8) Lawyers and Accountants

(9) Real Estate Company Agents

(10) Jewelry/Dealer in Gems and Metals/Gold Shop

(11) High Net Worth Customers

(12) Arms and Ammunition Dealer

(B) Country or Geographic Region Risk

Myanmar's locations of states and regions that are prone to conducting AML/CFT with low, medium, and high risk, which are assessed based on the indicators of urbanization and concentration of financial institutions.

(C) Products, Services and Delivery Channel Risk

MAB will categorize the types of products based on low, medium and high risk according to products and services risk and the delivery channel risk based on low, medium and high risk according to customer's use of transaction on channels.

Please refer to **Appendix 1** for a Customer Type form as per guidance of Central Bank of Myanmar.

8. Know Your Customer (KYC)

KYC means Know Your Customer, a term used for Customer Identification Process. It involves making reasonable efforts to determine the true identify and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business etc; which in turn helps the banks to manage their risk prudently.

MAB adopts a Know Your Customer policy to be complied with by all MAB staff. This policy is founded on three key policies:

1. Customer Acceptance Policy
2. Customer Due Diligence Measures
3. Ongoing Monitoring of High-risk transactions and Accounts

8.1. Customer Acceptance Policy

All staff should be aware of the existing policies and procedures regarding the opening of accounts for new customers including the types of customers that are eligible for opening of an account:

(a) Types of customers acceptable

1. Individuals who are Myanmar citizens
2. Non-Citizen Individuals with a permanent residence in Myanmar
3. Non-Citizen Individuals with an employment/secondment in Myanmar or having apparent economic or commercial interest in Myanmar
4. Sole-Proprietorship registered with the Ministry of Commerce
5. Private/Public Limited Company registered with DICA
6. Non-Profit Organizations with formal registration and with formal recognition the by authorized Ministry of the Government
7. Political Parties which are legally approved by the Union Election Commission
8. Embassies / Consulates/ Diplomatic Missions in Myanmar to the extent that such customers do not originate from high risk or FATF countries

(b) Types of customers NOT acceptable

1. Non-Resident Individuals with Tour Visa or Non-Business Purpose Visa
2. Non-Resident Individuals **NOT** in employment/ secondment in Myanmar or having **NO APPARENT** economic or business interest in Myanmar
3. Companies or Organizations which have no formal/legal recognition by the authorities of Myanmar Government
4. Resident or Non-Resident or Companies or Organizations with incomplete KYC information which are requested accordingly to the rules and regulations of Myanmar

5. Non-face-to-face customers
6. Customers with an unknown identity or fictitious name

(c) Types of High-risk customers acceptable with the approval of MAB's Compliance Department

1. Government or Government Agencies
2. Political Parties
3. Customers from high-risk regions
4. Politically Exposed Persons
5. Customers who are high-level public officials and their family members, and well-known personalities wishing to open e-wallet accounts (PEPs)
6. Money Services Business
7. Banks or Financial Institutions
8. Casino / Gaming
9. Hedge Funds
10. Charity Foundation, Non-Government Organization and Non-Profit Organization
11. Trading or Selling Business with Jewelry/ Gems/ Precious Metals or Stones
12. Defense Contractors/ Arms & Munitions Manufacturers
13. Cash Intensive Business
14. Embassies/ Consulates/ Diplomatic Missions save for customers who come from high-risk FATF countries
15. Customers who are engaged in the multi-level marketing, pyramid scheming and networking business

For avoidance of doubt, the aforementioned group of high-risk customers may only be onboarded after enhanced due diligence has been undertaken.

8.2. Customer Due Diligence (CDD) Measures

The Bank shall undertake the CDD measures, in the following circumstances:

(1) Prior to establishing business relationship, such as opening accounts, taking stocks, bonds or other securities into safe custody, granting safe-deposit facilities or engaging in any other business dealings;

(2) Prior to identifying the beneficial owners and taking reasonable measures to verify the identities of beneficial owners such that the financial institution is satisfied that it knows who the beneficial owner is. Beneficial owners of corporation, trusts, nominee, fiduciary accounts and other legal entities are to be identified;

(3) In the case of a representative acting on behalf of an individual, company, organization or legal arrangement, to verify whether the individual has been duly authorized to do so. This includes verifying the identify of the representative, the legal status of the representative, obtaining information about the legal arrangement, and reviewing relevant documents evidencing the person's authority to act on behalf of the individual, company, organization or as such pursuant to the legal arrangement;

(4) Prior to carrying out occasional or one-off transactions including wire-transfers, that involve a sum in excess of amount as defined by the supervisory authority; identification information accompanying wire transfers shall contain the name and address of the originator, and where an account exists, the number of that account. In the absence of an account, a unique reference number shall be included;

(5) If the reporting entity has a suspicion of money laundering or financing of terrorism irrespective of the sum involved in the transaction;

(6) If the reporting entity has any doubts about the veracity or adequacy of previously obtained customer identification data; and

(7) Updating the customers' information regularly to ensure that the records of customers are kept up-to-date and relevant.

For the avoidance of doubt, if unable to perform the customer due diligence measures for any reason, MAB should not carry out the provision of services or terminate the provision of such services with the relevant individual, company or organization and report the situation to the MFIU.

MAB shall obtain the following customer identification requirements from customers depending on the types of customers as required and obtain and verify the information required using independent source documents and/or reliable data. If there are any suspicions over the course of the CDD raised MAB shall ask for additional documentary evidence as necessary and/or escalate these red flags to the Head of Compliance as soon as practicable.

In the event where a customer is unable to produce an original document, a bank may consider accepting as an alternative a copy of the document, only if it is:

(a) certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant); or

(b) confirmed by an independent bank staff that he has sighted the original document

8.2.1. Customer Identification Requirements

A. Natural Persons

1. Full Name, including any aliases
2. National Registration Card/ Citizen Scrutiny Card/Passport
3. Permanent and mailing address
4. Date of Birth
5. Nationality

6. Occupation
7. Phone Number
8. Recent Photo
9. Name and account numbers of two introducers (existing account holders)

For Joint Accounts, if the account holders are customer of the Bank, those all-joint account holders shall be checked with customer due diligence (CDD) measures by the bank.

B. Legal persons and Legal Arrangements including partnerships, limited liability partnerships and trusts

1. Name of Company
2. Address of head office
3. Full address (including phone, fax)
4. Certificate of Incorporation, Memorandum of Association, Article of Association
5. Partnership Agreement
6. Trust Deed
7. Name and address of Board of Directors (phone number, if available)
8. Identification documents of Directors/Shareholders/Partners
9. Identification documents of Settlors, Trustees, Protectors and beneficiaries with respect to trusts
10. Board resolution authorizing opening and operation of the account
11. Authorization by Board of Directors to Chief Executive Officer or other officers for conducting financial transactions
12. Identification documents to identify the person authorized to present the company/business in its dealings with the bank

MAB shall verify the authenticity of the information provided by the company/business with the Directorate of Investment and Company Administration (DICA).

For foreign incorporated or foreign registered business entities, comparable documents should be obtained. Bank shall make all efforts to verify the documents supplied including requiring that they be certified by the Office of Foreign Affairs and endorsed by the Embassy of Myanmar.

C. Non-Government Organization

1. Name of Non-Government Organization
2. Head Office Address
3. Certification of registration
4. Constitution of the NGO
5. Name and address of Executive committee
6. Telephone No
7. Name and address of senior management
8. Registered address, if different from the principal place of business
9. Executive committee's decision regarding opening of account
10. Identification documents of directors/ senior officers of the NGO
11. Authorization for the operation of accounts financial transactions
12. Identification documents to identify the person authorized to represent the NGO in its dealing with the banks

8.3. Ongoing Monitoring of High-risk Transactions and Accounts

(a) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting entities, knowledge of the customer, their business and risk profile including, where necessary, the source of funds.

(b) The bank monitors transactions on an ongoing basis and to update customer profiles on the basis of risk.

(c) The bank reviews unusual or large transactions and keep a record of findings

(d) The bank maintains up to date customer profiles to assist bank staff to identify transactions which are not consistent with the customer's business/stated for the relationship.

(e) The reports of the customers should be updated once a year.

9. Delayed Customer Identification Verification

MAB shall engage in the business relationship with the customer prior to the completion of the customer verification process if the following circumstances are met:

(a) when the verification occurs as soon as reasonably practicable;

(b) when it is essential not to interrupt the normal conduct of business; or

(c) when the money laundering and terrorist financing risks are effectively managed.

Additionally, MAB should include in its risk management procedures concerning delayed customer verification, a set of minimum requirements such as a limitation on the number, types or amount of transactions that can be performed by the customer.

Where MAB is unable to complete the customer identification or verification within 30 business days, MAB shall not commence or continue business relations with any customer, or undertake any transaction for any customer. MAB shall at all times consider if the circumstances are suspicious so as to warrant the filing of a STR.

10. Non-Face to Face Services

As a general rule, MAB shall always perform a face to face CDD when operating new account opening. Account opening will be completed after doing face to face CDD with the branch compliance officer or branch manager at the bank. Unless face to face CDD is performed, no provision of banking services to the customer will be allowed.

11. Politically Exposed Persons (PEPs)

11.1. Definition

Domestic PEPs: Individuals who are or have been entrusted domestically with prominent public functions within the country and family member or close associates of such persons, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Foreign PEPs: Individuals who are or have been entrusted with prominent public functions by a foreign country and family member or close associates of such persons, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials

International organizations PEPs: A director, a deputy director, a member of the board of directors and a senior member of an international organization, a member who has the similar position who been entrusted with such function and family member or close associates of such persons.

MAB has established appropriate risk-management systems to determine whether a customer or beneficial owner is a PEP, or a family member or close associate of PEP. Overall measures for indicating a PEP should include:

(a) seeking relevant information from the customer;

(b) screening information about the customer;

(c) referring to commercial electronic databases of PEPs; and

(d) taking reasonable measures to determine whether the beneficial owner is a PEP.

11.2. Risk Management System for each PEP

Determining if each type of customer as a PEP

Foreign PEPs: Referring to the Recommendation 12 of the FATF, an appropriate risk management system to determine whether customers or beneficial owners is a foreign PEP. MAB is to take proactive steps such as:

(a) Assessing customers on the basis of risk assessment criteria, risk profiles, the business model, verification of information under the process of CDD or MAB's own.

(b) Foreign PEPs are considered high risk and require the application of the ECDD for high-risk customers. Overall, the following ECDD measures apply:

(1) obtaining senior management approval before establishing or continuing a business relationship;

(2) taking reasonable measures to identify the source of wealth and funds;

(3) Applying enhanced ongoing customer due diligence and monitoring of the business relationship.

Domestic and international organization PEPs: The Recommendation 12 of the FATF also requires domestic and international organizations to take reasonable measures based on the assessment level of risk to determine whether the customer or beneficial owner is a domestic PEP. The measures include:

(a) Reviewing, according to the relevant risk assessment factors and CDD data collected. For instance, to gather sufficient information to understand the

characteristics of the public functions that the PEP has been entrusted with.

(b) The assessment is to be based on risk factors to determine if the business relationship with the PEP is of higher risk. To refer to the Assessment Criteria set out in Section 7 above and Section 7 of the CRP.

(c) If the risk assessment establishes that the business relationship with the domestic/international organization PEP presents a normal or low risk, MAB is not required to apply ECDD measures.

If he/she is defined as PEP, enhanced customer due diligence shall be done on those customers or beneficiaries. Where higher risks are identified, in addition to performing ECDD, the relevant bank officer shall:

(a) seek approval of the Head Legal and Head of Compliance or any other senior management prior to any payout of proceeds; and

(b) conduct enhanced scrutiny of the business relationship with the customer and consider submitting a STR (where applicable) to the MFIU.

For detail ECDD measures, please refer to the content out in Section 11, ECDD below.

12. Enhanced Customer Due Diligence (ECDD)

MAB shall enhance the customer due diligence of identified high-risk customers. MAB is required to undertake ECDD measure in the following circumstances:

(a) If the transactional amount is equal to or above the threshold of Kyat or any other currencies equivalent of USD 15,000 [1]/ (or as otherwise amended from time to time by the CBM), including situations where the transaction is carried out in a single operation or in several operations that appear to be linked.

1/ Pursuant to Section 17 of CBM Directive 18/2019

(b) When carrying out occasional transactions of a customer who has no established relationship with the bank.

(c) The transaction relates to a foreign country that has been designated by the FATF as requiring ECDD measures.

(d) The customer is (or has a beneficial owner who is) a foreign PEP

The minimum requirements of ECDD are as follows:

(a) Obtaining approval of the Head of legal, Compliance and Secretary Department before establishing or continuing a business relationship.

(b) Taking customers' information and data, the source of wealth and funds.

If the customer is confirmed as PEP or customers of high-risk categories, the following actions shall be in place:

(a) Examining as far as reasonably possible the background and purpose of all complex, unusual large transactions and all unusual patterns of transactions, which have on apparent economic or lawful purpose;

(b) Increasing the degree and nature of monitoring of the business relationship regarding the transactions or performance in order to determine whether transactions or activities appear unusual or suspicious;

(c) 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 owner;

(d) Obtaining additional information on the intended nature of the business relationship;

(e) Obtaining information on the source of funds or source of wealth of the customer;

(f) Obtaining information on the reasons for intended or performed transactions;

(g) Obtaining the approval of senior management to commence or continue the business relationship;

(h) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;

(i) Creating a customer profile or monitoring in place to be able to support identification of unusual transactions for higher risk customers including PEPs;

(j) Carrying out customer due diligence measures on the first transaction conducted through the account opened with the customer's name;

For customers who are unable to be physically present for the face-to- face ECDD, additional measures should be taken, including:

(a) Requesting for certification of documents in accordance with applicable laws; and

(b) Requesting for other independent verification measures which includes contacting the customer directly.

MAB shall apply the ECDD measures to higher-risk customers at each stage of the CDD process and on an on-going basis.

MAB shall routinely review and keep its risk assessment process up-to-date.

If the customer is from a high-risk or FATF jurisdiction, ECDD measures as set out in **Appendix 2** will be applied.

13. Simplified Customer Due Diligence (SCDD)

MAB may apply SCDD procedures to customers that have been identified as low risk through a documented risk assessment. The SCDD measures should be commensurate with the risk factors and are limited to the following:

(a) Reducing the frequency of customer identification updates;

(b) Reducing the degree of on-going monitoring and scrutinizing transactions;

(c) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship

MAB shall not apply SCDD measures whenever there is a suspicion of money laundering or terrorism financing, or when the customer has a business relationship with or is in countries not applying sufficient measures to prevent money laundering and terrorist financing or those who have been listed by the FATF or identified by the FIU as being high risk or where higher risk scenarios apply as identified by MAB.

14. Know Your Employee (KYE)

Know Your Employee (KYE) program means that the institution has a program in place that allows it to understand and employee's background, conflicts of interest and susceptibility to money laundering complicity. These employees have the necessary capacity and suitability to perform their responsibilities being upright. They must be screened for potential conflicts of interest, including their financial situation, and the elimination of money laundering and terrorist financing.

MAB shall verify all employees, including the bank's board of directors (BOD) and senior management, to ensure the criteria of suitability. Before appointed as permanent employee, Legal, Compliance and Secretary Department shall screen with Sanction list, PEP list, CBM blacklist and HR blacklist which was from other banks by using the acuity link(C-link). People and Culture Department shall incorporate the provisions of KYE in the recruitment process and undertake a periodic review of employees' information. The

Employee information form and a copy of the identification documentation shall be retained by People and Culture Department and these files must be kept for five years after the employee resigns.

15. Determination of Beneficial Owner

If MAB determines that the customer is acting on behalf of one or more beneficial owners, MAB should verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source such that MAB is satisfied that it knows the identity of the beneficial owner.

The information to be obtained on a beneficial owner should be consistent with the requirements set out in clause 8 above.

For the avoidance of doubt, the requirement above includes accounts opened by lawyers or law offices on behalf of their customers and by trustees. MAB will apply CDD measures on the beneficial owners in such cases.

Customers which are companies listed on the stock exchange

If a customer is a company listed on a stock exchange, MAB is not required to identify and verify the identity of any shareholder or beneficial owner of the company provided that the company is subject to adequate disclosure requirements to ensure transparency of beneficial ownership. In such a scenario, MAB should only obtain customer identification documents on the company itself and obtain the relevant identification data from public register or if not available from a public register, the reporting organization shall obtain the information from the customer.

Customers that are legal persons or arrangements

If a customer is a legal person or in a legal arrangement, MAB should take adequate measures to understand their ownership and control structure. In particular, identification should be made of each natural person that:

(a) Owns or controls directly or indirectly more than 20 percent of the legal entity or exercises control of the legal person or arrangement through other means; or

(b) Is responsible for the management of the legal entity.

With respect to legal arrangements, identification should be made of the Settlor, trustee, protector, beneficiary or of persons in similar positions and any other person exercising ultimate effective control including through a chain of control/ownership.

MAB shall not establish any business relationship or carry out an occasional transaction equal to or above USD 15,000 before the trustee provides MAB with the requisite information about its details, and information on the beneficial ownership and assets of the trust to be held or managed under the terms of the business relationship.

16. Maintenance of Customer Information

MAB shall gather and maintain its customer and beneficial owner(s) information throughout the course of the business relationship. Documents, data, or information and business correspondence collected under the CDD process should be kept up to date and relevant by undertaking reviews of existing records at appropriate times as determined by MAB when:

(a) A significant transaction is to take place;

(b) There is a material change in the way the account is operated; and

(c) Information held on the customer is insufficient to enable the bank to understand the nature of the banking relationship or transactions being conducted.

17. Ongoing Monitoring of Customer Information

MAB should adopt procedures, such as computerized automated systems, to monitor on an ongoing basis customer transaction and the relationship with the customer. The monitoring undertaken by MAB shall include the scrutiny of customer transactions to ensure that they are being conducted according to the bank's knowledge of the customer,

the customer's commercial activities, the customer risk profile and, where necessary, the source of funds and wealth, and shall include predetermined limits on the amount and volume of transactions and type of transactions.

18. Shell Banks and Cross Border Correspondent Banking Relationships

MAB shall not enter into or continue a correspondent or business relationship with a shell bank that as defined by the CBM's Directive No (21/2015) and (18/2019) and 3(h) of the Anti-Money Laundering Law (2014). Accordingly, business relationship with the banks or financial institutions in a foreign country that allows its accounts to be used by a shell bank shall not be done.

Before entering into a cross-border correspondent banking relationship or other similar relationship or other similar relationship, in addition to performing normal customer due diligence measures, MAB shall:

(a) gather sufficient information about the respondent bank as required;

(b) understand the nature of the respondent bank's business as required;

(c) evaluate the anti-money laundering and the control measures to combat the financing of terrorism implemented by the respondent bank;

(d) based on publicly available information, evaluate the reputation of the respondent institution and the quality of supervision to which it is subject based on publicly available information;

(e) obtain prior approval from Head Legal, or Head of Compliance before establishing new correspondent relationships;

(f) to document clearly the AML and CFT responsibilities of each bank; and

(g) be required to satisfy themselves that the respondents have performed CDD obligations on customers with direct access to the accounts and that respondents can provide relevant CDD information upon request.

The bank shall emphasize verifying the following documents obtained from customers for ECDD:

(a) The documents obtained when opening and closing of accounts;

(b) The documents obtained when utilizing the accounts for banking services;

(c) The documents obtained when accessing the service of Safe Deposit Box;

(d) The documents obtained when operating the remittance by wire transfer or e-fund transfer;

(e) The documents obtained when operating the remittance between Myanmar and abroad countries;

(f) The documents obtained when submitting credit application;

(g) The documentary evidence relating to the customers; and

(h) Background history and types of transferring cash or cheque for each transaction.

19. Policies and Procedures on Wire or Electronic Transfers

Wire transfer is a method of electronic funds transfer from one person or entity to another. A wire transfer can be made from one bank account to another bank account within the national boundaries of a country or from one country to another. Wire transfers does not involve actual movement of currency, they are considered a secure method for transferring funds from one location to another.

19.1. Carrying out Domestic Wire or Electronic Transfer

Information on wire or electronic transfers shall be made available by the ordering bank within three business days of receiving the request from the beneficiary or from the MFIU. If the identity has not been previously verified, in order to maintain the information in accordance with the record keeping requirements, a beneficiary bank shall verify the identity of the beneficiary.

For wire or electronics transfers, either the ordering bank or the beneficiary bank is required to report the following transactions to the MFIU:

(a) A domestic wire or electronic transfer in excess of 100 million kyats or the amount as required and determined by the Central Body from time to time; or

(b) A transfer where the originator's information is incomplete or unavailable.

For the purposes of this Section, domestic wire or electronic transfer shall include the originator information for cross border wire or electronic transfers unless such information can be made available to the beneficiary institution and competent authorities through other means. The ordering financial institutions need only include the originator account number or if no such account number exists, a unique transaction or reference's number that allows the transactions to be traced back to the originator or the beneficiary.

19.2. Carrying out Cross-Border Wire or Electronic Transfer

For Cross-Border wire or electronics transfers, bank processing an intermediary element of the payment chain shall keep all wire or electronic transfer information including originator and beneficiary information.

For cross border wire or electronic transfers, it should include the following information and ensure that the information remains with the wire or electronic transfers and related messages throughout the payment chain:

(a) Accurate originator and recipient information including the full name of the originator;

(b) The originator account number where such an account is used to process the transaction;

(c) The originator's address, customer identification, date and place of birth;

(d) The name of recipient and the recipient account number where such an account is used to process the transaction; and

(e) The transaction is *bona fide* and there are proper supporting and documentary evidence to illustrate the payments, and the payor-payee details correspond with such documentary evidence.

If MAB is unable to comply with the specifications prescribed above, it shall not execute the wire or electronic transfer.

For wire or electronics transfers either the ordering bank or beneficiary bank is required to report a cross border wire or electronic transfer in excess of USD 10,000 or the amount as required and determined by the Central Body from time to time. Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire or electronic transfers from remaining with related domestic wire or electronics transfers information, the intermediary bank shall keep a record of all the information received from the ordering bank or another intermediary bank for at least five years.

Foreign Exchange Management Regulation 2014

It is an obligation of MAB as a foreign exchange dealer license holder to request and scrutinize documentary evidence that is relevant to trading or the immediate or in-advance purchase and sale of foreign currency in order to do their business thoroughly. The documentary evidence shall be the most relevant evidence in internationally recognized commercial or accounting procedures and internationally recognized trading or legal procedures for the purposes below.

(a) Scrutinizing and approving the category, class and characteristic of the relevant foreign currency businesses.

(b) Obtaining, scrutinizing and approving evidence that the applicant is genuine, and the application by domestic residents to pay and transfer foreign currency to residents abroad is genuine.

(c) Acquiring, scrutinizing and approving evidence that the application by foreign residents to pay and transfer foreign currency to domestic residents is genuine.

(d) Obtaining, scrutinizing and approving evidence as to the required time to put the accounts together and the amount of money regarding the payment and transfer of foreign.

(e) Recording personal data of persons who are involved in the payment and transfer of foreign currency.

MAB shall if there is an official agreement in writing between domestic residents and residents abroad, comply with the items and also obtain, scrutinize and approve the following documentary evidence when performing a payment and transfer of foreign currency.

(a) Original agreement in writing personally signed by the relevant persons or their representatives.

(b) Documents related to such payment and transfer; these documents should support, accounting procedures, trading or legal procedures, the payment and transfer, and should be usable as additional evidence for the payment and transfer.

(c) Supplementary or additional documents, such as the relevant purchase order, delivery notice, receipt for goods, shipping document or other title documents of different types, contractual documents for transportation costs, money transfer records, insurance documents, permits, licenses and other documentary evidence related to the payment and transfer.

(d) As minimum requirement, the original agreement and the supplementary or additional documents have to be scrutinized in order to determine whether the payment and transfer of foreign currency is done correctly.

If MAB cannot obtain original documentary evidence as set out above, it may obtain a certified true copy, or documentary evidence sent by fax or an electronic system.

If MAB doubts the purpose and characteristics of the customer when performing a foreign currency business, it shall submit this case to the CBM for it to decide.

MAB can after scrutinizing the documentary evidence as to whether the payment and transfer is permissible, perform the following foreign currency transfers from abroad to the country and from the country to a destination abroad at the request of an individual domestic resident if the amount used per year is not more than USD 10,000 or other types of foreign currency in an equivalent amount:

(a) Gifts

(b) Donations

(c) Repair and maintenance fees

(d) Inheritances

(e) Cash from the transfer of real estate

(f) Other types of financial support or monetary aids except the financial support or monetary aids which are granted by the Union Government.

MAB can act only after obtaining permission from the Central Bank if someone requests a unilateral transfer or payment of more than USD 10,000 or other types of foreign currency in an equivalent amount.

20. Suspicious Transaction Reporting (STR)

It is impossible to exhaustively define all the activities that would qualify as suspicious. As a general guideline, transactions that are not part of a customer's normal operational management or deviate from the customer's normal operational management or deviate from the customer's profile are considered as suspicious activity. Suspicious activities can happen anytime during the account opening as well as throughout the customer relationship with the bank. Examples or red flags of suspicious activities shall be referred to in the transaction monitoring policy and procedures.

Suspicious or unusual transaction reporting process includes:

(a) Procedures to identify suspicious or unusual transactions or activity through various channels including employee observations or identification, inquiries from law enforcement or alerts generated by transaction monitoring systems;

(b) A formal evaluation of each instance, and continuation, of unusual transactions or activity;

(c) Documentation of the suspicious transaction reporting decision (i.e. irrespective of whether a report was submitted to the authorities);

(d) Procedures to periodically notify senior management or the board of directors of suspicious transaction submissions; and

(e) Employee training on detecting suspicious transactions or activity.

Red Flags / Examples of Suspicious Activity ("SA") and Suspicious Transaction ("ST")

Suspicious Customer Behavior

(a) Overly secretive customer;

(b) Customer refuses to provide information;

(c) Customer shows familiarity with process;

(d) Customer has used/changed a number of advisors in short space of time;

(e) Customer appears disinterested with outcome;

(f) Customer is prepared to pay substantially abnormally high fees;

(g) Customer shows inadequate knowledge of transactions;

(h) Customer uses multiple bank accounts;

(i) Customer requests an unusual short or deferred repayment schedule;

(j) Customer does not want to receive correspondence to home address; and

(k) Customer avoids face-to-face meetings.

Suspicious Customer Identification Circumstances

(a) Customer provides counterfeit documents;

(b) Customer only provides copies rather than original documents;

(c) Customer only provides foreign, unverifiable identity documents; and

(d) Customer only acts through a third party.

Suspicious economic profile;

(a) There is lack of sensible/commercial/financial or legal reason for business;

(b) Absence of documentation to support a customer's claims;

(c) Business cannot be found on the internet;

(d) Creation of complicated ownership structures;

(e) Funds invested in dormant companies; and

(f) Transactions involve non-profit or charitable organizations for which there appears to be no logical economic purpose.

Suspicious Transactions

(a) Large cash transactions/exchange of small bills for large ones;

(b) Multiple transactions in a short period of time;

(c) Finance is not provided by a credit institution;

(d) Transfer of large amounts of money to or from overseas locations with instructions for payments in cash;

(e) Cash deposits/withdrawals that fall consistently below the relevant transaction threshold;

(f) Mortgages are repeatedly repaid quickly;

(g) Unusual source of funds;

(h) Request for payments to third parties;

(i) Customer receives high injection of capital; and

(j) Back-to-back property transactions

Suspicion of terrorist financing and weapon proliferation

(a) Customer conducts uncharacteristic purchases (camping gear, weapons, hydrogen peroxide);

(b) Customer trades in commodities that may be dual used in chemical and biological weapons; and

(c) Customer donates to a cause that is subject to derogatory publicly available information (NPO's, NGO's, charities).

Suspicious Customer Relations

(a) Customer conducts uncharacteristic purchases (camping gear, weapons, hydrogen peroxide);

(b) Parties connected without an apparent business reason;

(c) Customer is known to have convictions or currently under investigation;

(d) Age of parties is unusual for type of transactions;

(e) Customer has known connections with criminals regardless of whether they are reported or otherwise;

(f) Customer is engaging in a complex, unusually large transaction, or has an unusual pattern of transaction with no apparent or visible economic or lawful purpose; and

(g) The customer is from or in a country which does not apply sufficient measures to prevent money laundering and financing of terrorism.

In making a decision on whether to make a report, the following factors will need to be taken into account:

(a) Whether or not the activities/transactions in question consist of instances of reportable (suspected) ML/TF;

(b) Whether the information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege;

(c) Whether unusual activity appears during the ongoing monitoring of a customer's information (i.e. the activity of the customer is not in line with the initially documented economic profile); and

(d) A STR may also be required when there are "reasonable grounds" to know or suspect. This is an objective test, i.e. the standard of behavior expected of a reasonable person in the same position. A claim of ignorance or naivety does not constitute defense. Additional monitoring and investigation of transactions should be performed prior to submitting a STR.

The bank shall report if there is a suspicious transaction within 24 hours if it is situated in an urban centre and within three working days if it is situated in a remote district.

Threshold Transaction Activity (TTA)

Any transactions one hundred million kyat (for a Myanmar currency transaction or a property transaction [2]/) and over within the country shall be reported to MFIU as a TTA through a TTR. Any foreign remittance inward/outward transactions of USD 10,000 and over (whether by single or several linked transactions) or equivalent foreign currencies shall be reported to MFIU as a TTA through the TTR. For the avoidance of doubt, such TTRs must be submitted to MFIU even where there is no AML/CFT suspicion of the customers.

Audit for Compliance with the Policy

21. Bank branches shall be audited at least once a year by internal or external auditors to ensure that they comply with the policies, procedures and instructions related to combating money laundering, and that they scrutinize the threshold transactions, and that they effectively analyze the suspicious transactions identified. The audit report, containing the findings and recommendations, shall be distributed to the bank's board of directors (BOD), senior management and relevant stakeholders and shall be maintained in the Legal, Compliance and Secretary Department.

2/ Section 14 (b) of AML/CFT Guideline on Wire Transfer (2010) issued by Central Bank of Myanmar

21. Record Keeping Requirements

The bank shall maintain records of the following information for at least five years after the business relationship has ended:

(a) Documents and copies of all records obtained through the customer due diligence process;

(b) Documents obtained from scrutiny and evidencing the identities of customers and beneficial owners, account files and business correspondences;

(c) A transaction with customer who does not have an established business relationship with the bank;

(d) All records of transactions as above (a) and (b), both domestic and international, attempted or executed; and

(e) Copies of reports and related documents made to MFIU.

MAB must ensure that the records and underlying information above are readily available to the MFIU and other authorities and the records should be sufficient for the reconstruction of individual transactions.

22. Staff Training

MAB shall provide an ongoing training program that educates the banks employees on AML/CFT responsibilities. Trainings shall be provided to all levels of employees including the top management. MAB will also arrange face to face trainings and online trainings which will be conducted for the following employees:

(a) Senior Management of the Bank

(b) Officers of Bank including compliance officers

(c) Front and Back-office staff

MAB shall conduct its training schedule based on its nature of the business and operation. The AML/CFT Compliance training for new employees or staff shall be included in the

training program. Ongoing training programs including information of money laundering and terrorist financing techniques for existing employees shall be provided periodically.

The compliance officer shall not only assure that appropriate training occurs for all new and existing employees, but also that the training is documented. Documentation requires making a record of who was trained, training log, certificate of completion, training materials and report. Online training programs shall be arranged for existing and new employees within the appropriate time.

23. Offences and Penalties

Whoever violates the provisions contained in this policy shall be liable for any penalties provided in the following laws for such offences:

(a) the Anti-Money Laundering Law (The Pyidaungsu Hluttaw Law No.11, 2014),

(b) the Counter Terrorism Law (2014),

(c) CBM notifications and related laws, directives and guidelines enacted from time to time.

Bank branches of MAB breaching the provision of this policy shall be liable to the penalties and actions as reasonably determined by their respective managers. Any person, including staff, senior management, supervisors who fail to comply with the obligations under this policy may be subject to one or more of the following supervision or measures:

(a) Written warnings

(b) Remedial actions as determined by MAB;

(c) Dismissal;

(d) Other appropriate measures.

Appendix 1

Customer Type Form

Breakdown of Customer Type

Types of Customer(s)	Number of Customer(s)	Total Deposits
1.Natural Persons		
Resident		
Non-Resident		
Of which are residents of "high-risk" jurisdictions as defined by the FATF, APG, Myanmar and/or MAB		
2.Legal Persons		
Resident		
Non-Resident		
Of which are residents of "high-risk" jurisdictions as defined by the FATF, APG, Myanmar and/or MAB		
3.Money Remittance Companies (including agents)		
4.Money Changers		
5.NGOs – Domestic		
6.NGOs – Foreign		
7.Real Estate Companies (including agents)		
8.Dealers in precious metals, stones and jewelry shops		
9.Lawyers and Accountants		

Appendix 2

Enhanced Customer Due Diligence (ECDD) Measures

MAB shall obtain the following information and documents from the customers as part of the **Enhanced Customer Due Diligence (ECDD)** as per FATF's recommendation.

(a) Additional information such as occupation and ownership, including beneficial owner if applicable, from other public and reliable internet sources

(b) Nature and purpose of transaction

(c) Source of fund and source of wealth

(d) Supporting documents for transactions

(e) Management approval for starting business relationship and transaction

(f) Enhanced monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination

(g) Customer due diligence measures on the first transaction conducted through the account opened with the customer's name.

The bank shall also perform the following steps as required from AML Central Committee for FATF high-risk countries.

(a) Enhanced relevant reporting mechanisms, or systematic reporting of financial transactions

(b) Not allowing the establishment of any subsidiary, branch or representative offices of financial institutions from the countries of such FATF high-risk regions/countries to open in Myanmar

(c) Not allowing Myanmar financial institutions to establish a subsidiary, branch or representative office in such FATF high-risk regions/countries

(d) Restrict the financial transactions and business activities with the individuals and entities from such FATF high-risk regions/countries

(e) Prohibiting financial institutions from relying on third parties located in FATF high-risk regions/countries to conduct elements of the customer due diligence process

(f) Requiring financial institutions to review, amend, and if necessary, terminate correspondent banking relationship with the bank and financial institutions from those FATF high-risk regions/ countries

(g) Enhanced due diligence and performing external audit for subsidiaries and branches of financial institutions from those FATF high-risk regions;

(h) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in FATF high-risk regions/countries.

Acronyms

AML - Anti-Money Laundering

BOD - Board of Director

CBM - Central Bank of Myanmar

CCO - Chief Compliance Officer

CDD - Customer Due Diligence

CEO - Chief Executive Officer

CFT - Combating the Financing of Terrorism

WMD - Weapons of Mass Destruction

DICA - Directorate of Investment and Company Administration

ECDD - Enhanced Customer Due Diligence

FATF - Financial Action Task Force

INGO - International Non-Governmental Organization

KYC - Know Your Customer

KYE - Know Your Employee

MAB - Myanma Apex Bank Limited

MFIU - Myanmar Financial Intelligence Unit

NGO - Non-Governmental Organization

NPO - Non-Profit Organization

PEP - Politically Exposed Person

SA - Suspicious Activity

SCDD - Simplified Customer Due Diligence

ST - Suspicious Transaction

STR - Suspicious Transaction Report

TTA - Threshold Transaction Activity

TTR - Threshold Transaction Report