

Anti Money Laundering Policy
Of
Prime Islami Life Insurance Limited

1.0 Anti Money Laundering Policy of Prime Islami Life Insurance Limited.

1.1 Overview

Money Laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities. The term "Money Laundering" is also used in relation to the financing of terrorist activity (where the funds may, or may not, originate from crime).

In conducting business with due skills, care and diligence, company should comply with relevant laws, rules, regulations, codes and standards of good practice and 'anti money laundering procedures should be strictly followed. Because Company employees may personally be liable if any deviation is found in his assigned duties.

The financial institution recognizes that the fight against money laundering is a team effort and has drawn a policy to combat this threat.

1.2 Policy Objective

BROAD OBJECTIVE

The objective, therefore, would be to present and fight against money laundering activities, by establishing and governing standards to insulate the institution from being used as a component of financial system to launder money.

SPECIFIC OBJECTIVE

Beside these broad objectives, the specific objectives include:

1. Enable the institution to conduct clean, commercial business, conforming to standards set by Financial Institute and Insurance industry; within the framework designed by regulations and Head Office.
2. Build up awareness amongst the staff
3. Focus on methods of prevention of Money Laundering
4. Prevent use of institution's products or services for money laundering.
5. Prevent damage to the institution's name and reputation by associating with money launderers.
6. Ensure that the institution complies with money laundering legislation/regulations.
7. Comply with applicable laws in Bangladesh in reference to Money Laundering and adhere to standards accepted internationally by the financial world on the subject.

1.3 Policy Scope

This policy addresses the responsibility of management and employees for:

- Preventing, detecting, monitoring and reporting suspected, confirmed, detected money laundering issues;
- Client identification and verification ("Know Your Customer") or KYC;
- Record keeping;
- Money laundering control training;
- Monitoring of accounts, activities, policies, procedures and plans;

1.4 Policy Statements

- Following are the minimum standards to be observed while conducting business:
- Customer identity must be ascertained before issuing a policy
- Issuance of policy generally subjected to a detailed interview to ascertain purpose of purchasing a policy, sources of funds etc.
- All suspicious transactions to be noted and escalated to senior management whenever appropriate.
- Ensure suspicious transactions are reported to the Chief Anti Money Laundering Compliance Officer at Head Office (CAMLCO) who will determine whether the report is required to be sent to the regulators.
- Provide the Compliance Officer at the Head Office with all reasonable access to information that may be of assistance to him in carrying his duties.
- Records are kept for all data obtained for the purpose of identification.
- Employees are trained on a regular basis on anti-money laundering measures.

1.5 Procedure

As financial organizations are committed to the prevention of money laundering, the management of PILIL has taken the following program:

- 1.5.1 Formation of Central Compliance Unit (CCU) at Head Office headed by Chief Anti Money Laundering Compliance Officer (CAMLCO). He will examine the report received from branches and if deemed necessary will report to Bangladesh Financial Intelligence Unit (BFIU) for information & necessary action.
- 1.5.2 Senior desk officer of all corporate zonal office would act as Branch Anti Money Laundering Compliance Officer (BAMLCO) at branch level. He is the main point of contact and all suspicious activities are to be reported to him directly. He will oversee the day-to-day activities at the branch and confirm compliance of Bangladesh Financial Intelligence Unit (BFIU) instructions.

- 1.5.3 Know Your Customer (KYC) (Appendix-a) is an integral part of a business relationship. They are mandatory and a vital reference point to all business relationships.
- 1.5.4 Appropriate customer identification, record keeping and reporting are primary points of consideration. The institution has a policy to keep all related documents/records for five years of AML Act 12 years as per insurance Act after the settlement of all sorts of claim.
- 1.5.5 Head Office regularly collects information /statements from branches as per requirement of BFIU and issues various circulars to the branches related to AML.
- 1.5.6 Workshops and Seminars are regularly being arranged to keep all related workforce updated with the skills of AML procedures.
- 1.5.7 Leaflets/Festoons are printed explaining the laws, regulations and penalties for the policy holders and general public to create awareness.
- 1.5.8 The institution also collects AML information from foreign re-insurance institutions with whom the institution has a relationship.

Compliance is the responsibility of each employee. Therefore, all guidelines related to AML/CFT are regularly updated and circulated and ensured that all staffs are aware of the local AML/CFT laws, internal guidelines and other policies and procedures.

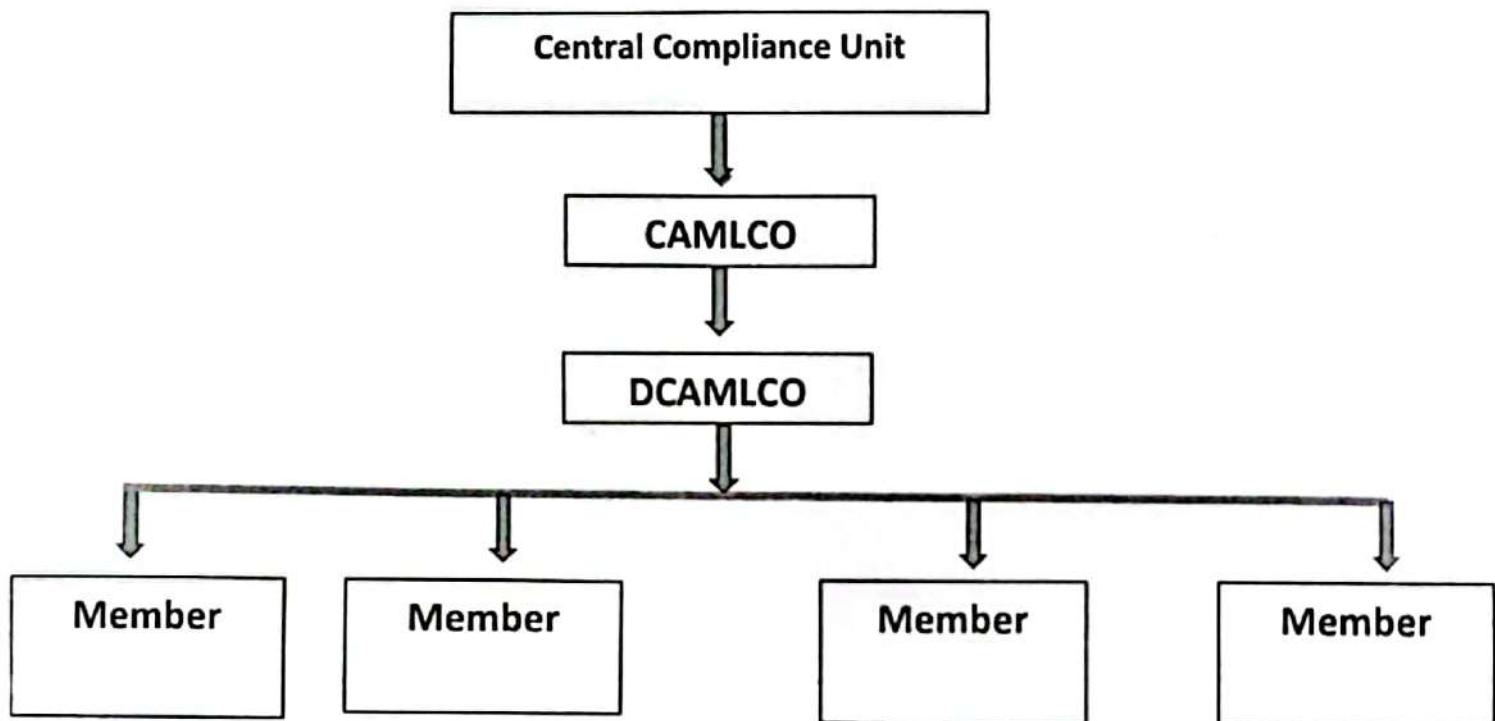
1.6 Central Compliance Unit

A Central Compliance Unit (CCU) consisting of five (5) members has been formed at Head Office headed by Chief Anti Money Laundering Compliance Officer (CAMLCO). The members of the unit are:

DMD/AMD/CFO	CAMLCO
Head of Underwriting Dept.	DCAM LCO
Head of Finance & Accounts Dept. Member	Member
Head of Information & Technology Dept.	Member
Head of Internal Audit Dept.	Member
Head of Claims & Policy Servicing Dept.	Member
Mid Level Employee	Anti Money Laundering Department

The terms of reference of the unit are as follows:

- i) Shall evaluate all reports and statements received from branches; prepare a consolidated evaluation report and submit to the Managing Director along with comments and recommendations if any.
- ii) Shall also evaluate the reports of Internal Audit Department conducted during last quarter, prepare a consolidated evaluation report and submit to the Managing Director along with comments and recommendations if any.



1.7 Guideline for Branches & All Employees

1.7.1 Commencement of Business Relationship

- i) Individual Customer shall fill in the Proposal Form. Documents which are obtained as prescribed in the check list shall be attached along with the Proposal Form (PF).
- ii) Corporate Customers shall fill in the Company/Intuitional Proposal Form. Documents which are obtained as prescribed in the check list shall be attached along with the Proposal Form (PF).
- iii) While accepting the policy the staff shall ensure the identification, source of income, reason of purchasing policy of the customer with any one of the documents referred in the check list of the forms.
- iv) Inspection of all documents should be carefully done. The photo, name, address, telephone. no/fax/email, signature, document expiry dates, etc. Should be carefully verified.
- v) While dealing with corporate entities, the following details should be obtained, recorded and attached with the Proposal form:
 - a) Entity name
 - b) Full registered address
 - c) Type of business activity
 - d) Trade license details
 - e) Names and photographs of Directors/Partners/Proprietor etc and their personal details.
 - f) Board Resolution for purchasing policy
 - g) Memorandum & Articles of Association /by laws / Trust Deed etc.
 - h) Any other relevant documents.
- vi) The customer in the presence of the designated officer of PILIL shall sign the Proposal form.
The branch in-charge or officer in charge shall sign the above documents.
- vii) Address of the customer must be verified at the commencement of the business relationship.
- viii) For all transactions the identity of the customer and counter checking the same with the information available in the system should be done.

1.8 Customer Due Diligence:

Customer Due Diligence (CDD) is a fundamental principle of all anti-money laundering controls. Each staff of the PIIIL is required to perform due diligence on all prospective clients prior to selling a policy. This process is completed by fulfilling the documentation requirements and also a "Know Your Customer" profile which is used to record a client's source of wealth, expected transaction activity at its most basic level.

Obligations for institution's staff to perform customer due diligence have been strengthened with the introduction of a five step process. The steps are:

- Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information determining whether the customer is acting on behalf of another person. If so then the reasonable steps should be taken to obtain sufficient identification data to verify the identity of the person behind.
- Identifying the (ultimate) beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurer is satisfied that it knows who the beneficial owner is. For legal persons and arrangements insurers should take reasonable measures to understand the ownership and control structure of the customer.
- Obtaining information on the purpose and intended nature of the business relationship and other relevant factors.
- 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 insurer's knowledge to the Customer and /or beneficial owner, their business and risk profile, including, where necessary , the source of funds.

The inadequacy or absence of KYC standard can subject institutions to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks, It is worth noting that all these risks are interrelated, However, any one of them can result in significant financial cost to institutions (e.g. through the withdrawal of funds by depositors, the termination of inter-institution facilities, claims against the institution, investigation costs, asset seizures, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

Reputational risk poses a major threat to institutions, since the nature of their business requires maintaining the confidence of depositors creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a institution's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Institutions are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective KYC program.

Operational risk can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of institutions programs, ineffective control procedures and failure to practice due diligence. A public that a institution is not able to manage its operational risk effectively can disrupt adversely affect the business of the institution,

Legal risk is the possibility that lawsuits, adverse judgments or contracts that turn out to be unenforceable can disrupt to adversely affect the operations of a institution. Institutions may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practice due diligence. Consequently, institutions can, for example, suffer fines criminal liabilities and special penalties imposed by regulators. Indeed, a court case involving a institution may have far greater cost implications for its business than just the legal costs, institutions will be unable to protect themselves effectively from such legal risk if they do not engage in due diligence in identifying their customers and understanding their business.

Supervisory concern about concentration risk mostly applies on the assets side of the balance sheet. As a common practice, supervisors/regulators/ not only require institutions to have information systems to identify credit concentrations but most also set prudential limits to restrict institutions exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers will not be possible for a institution to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

1.8.1 Risk Categorization – Based on Activity /KYC Profile

When establishing the business relationship, the concerned staff/officer must assess the risk that the relationship could be used for 'money laundering' and must classify the relationship as either High Risk or Low Risk.

Factors to consider when assessing risks, which are not set out in any particular order of importance and which should not be considered exhaustive, include (where appropriate):

- Type and background of customer and/or beneficial owner
- The nature of the activities
- The means of payment as well as the type of payment (cash, or other means of payment)
- The source of funds
- The source of wealth
- The frequency and scale of activity
- The type and complexity of the business relationship
- Whether or not payments will be made to third parties
- Whether a business relationship is dormant
- Suspicion or knowledge of money laundering & financing of terrorism or other crime.

1.9 Detection of suspicious Transactions

Money Laundering Prevention Act, 2012 'suspicious transaction' means transactions –

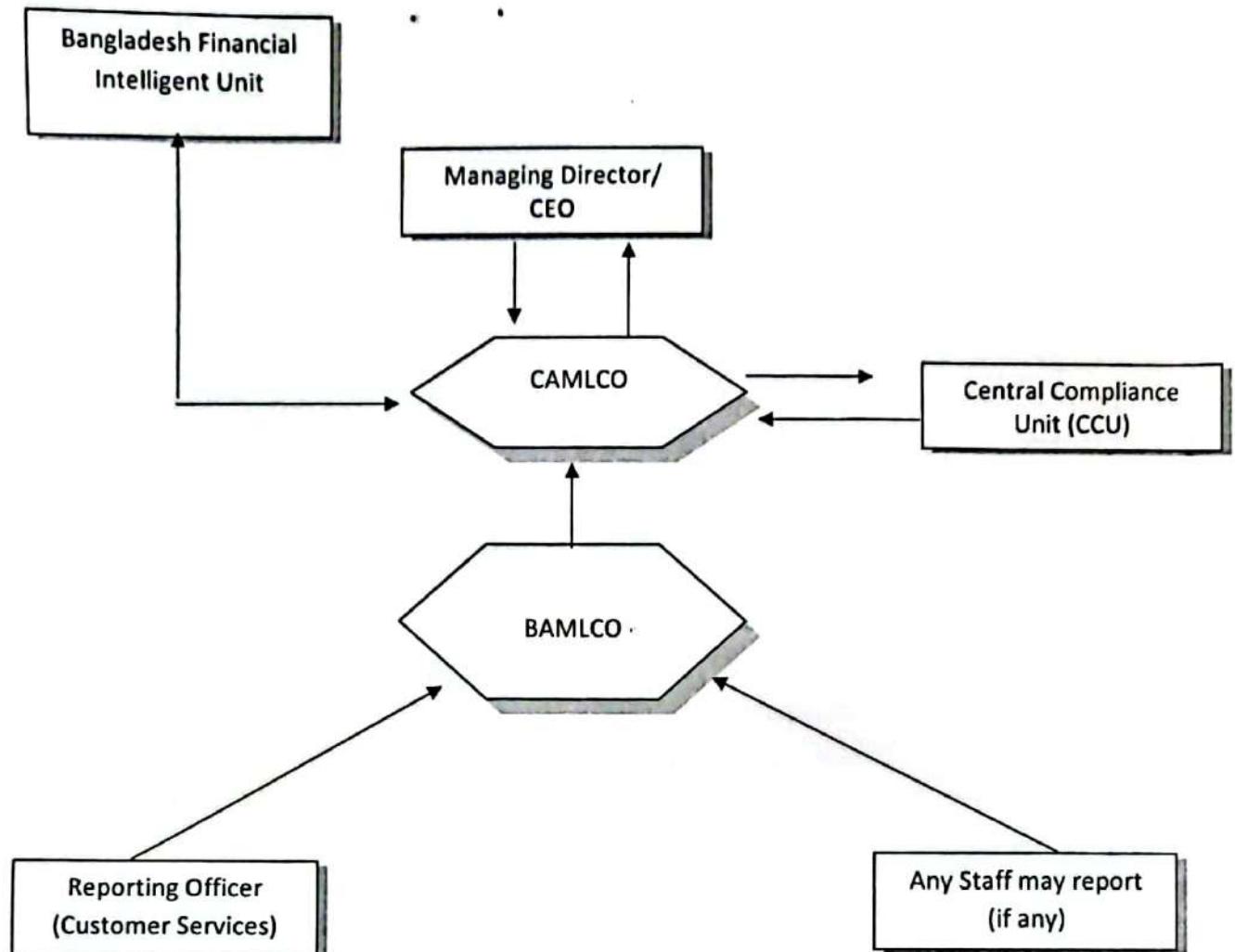
- i) Which deviates from usual transaction;
- ii) Of which there is ground to suspect that.
 - 1) The property is the proceeds of an offence,
 - 2) It is financing to any terrorist activity, a terrorist group or an individual terrorist;
- iii) Which is, for the purpose of this Act, any other transaction or attempt of transaction delineated in the instructions issued by Bangladesh Financial Intelligence Unit from time to time.
 - ❖ Transactions are found inconsistent with the KYC profile and there is no valid reasonable explanation;
 - ❖ Monitoring customer transactions;

1.10 Reporting of Suspicious Transactions

- 1.10.1 Any employee who identifies any activity or transaction which he deems to be suspicious must report that suspicion to the Anti Money Laundering Compliance Officer at the branch and to the branch manager, who in their turn and after agreeing with the employee's finding, will report it, through a written Suspicious Transaction Report (STR) to the Chief Anti Money Laundering Compliance Officer at the Head Office.
- 1.10.2 All Suspicious reported to the AMLCO should be documented (in urgent cases this may follow an initial, discussing by telephone). The report should include the full details of the customer and as a full statement as possible of the information – giving rise to the suspicion, The AMLCO should acknowledge receipt of the report.
- 1.10.3 STRs should not be discussed with anyone other than the Anti Money Laundering Compliance Officer at the branch and at the Head Office and with the branch including the customer and other staff members to avoid the risk of “tipping off”
- 1.10.4 The Head Office maintains a register for recording the Suspicious Transactions Reports.
- 1.10.5 Failure to report suspicious and unusual transaction to the Central Compliance Unit shall tantamount to gross negligence of duty and disciplinary action.
- 1.10.6 The Chief Anti Money Laundering Compliance Officer at the Head Office will review the STRs submitted by the branches and decide whether they should be reported to the relevant authorities.
- 1.10.7 Following the submission of a suspicious activity report, the branch is not precluded from subsequently terminating its relationship with a customer, provided it does so for normal reasons. It must not alert the customer to the fact of the disclosure as to do so would constitute a “tipping –off” offence.

1.11 Reporting To Bangladesh Financial Intelligent Unit

If any Suspicious Transaction Report (STR) is placed before the central Compliance Unit (CCU) the unit pursues the following procedures to report of Bangladesh Financial Intelligent Unit.



1.12 Maintaining & Updating Information

- 1.12.1 The objective of Maintaining & Updating Information is to ensure that we are able to provide the basic Information about customer and to reconstruct the individual transactions undertaken at the request of the relevant authorities at any given time.
- 1.12.2 In accordance with Anti – Money Laundering Prevention Act’ 2012, Money Laundering Information and documents will be stored at Least a 3 years period.
- 1.12.3 The information relating to customers (personal details, proof of beneficial ownership, transaction profile etc...) should be kept up-to –date.
- 1.12.4 The Compliance Unit at Head Office will ensure, from time to time, that detailed and concerted renewal efforts are made.

1.12.5 When a report of suspicious activity has been submitted to Bangladesh Financial Intelligence Unit or where it knows that a client or transaction is under investigation, any relevant records should not be destroyed without the agreement of the Bangladesh Financial Intelligence Unit even though the five year limit may have been reached.

1.13 Staff Training

The management of Prime Islami Life Insurance Ltd. ensures ongoing training of the staff and the participation of all officers involved in frontline operations. Relevant seminars, workshops and lectures are held in order to keep abreast of money laundering -fighting method.

The training the following:

- a) Responsibility of the employees in line with Bangladesh Financial Intelligence Unit regulations for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering.
- b) Procedure for reporting of suspicious transactions.
- c) Potential effect of the company, of its employees and customers if there is any breach of law or regulation.
- d) Ways to identify suspicious transactions.
- e) Storing and updating records.
- f) Duties and responsibilities of the CAM LCO, BAMLCO and other officers.

1.14 Our Responsibilities at a glance

- i) Reporting of suspicious transactions and monitoring are not the sole responsibility of BAMLCO and business procurement officer. This is a collective responsibility of all concerned.
- ii) All officers must have thorough knowledge on KYC and its application. They should always be aware of circulars issued by Bangladesh Financial Intelligence Unit and Head Office time to time.
- iii) KYC mandatory for all new and existing clients.
- iv) Source of funds to be ascertained and verified for all clients.
- v) Before allowing any facility to any customer, branch to ensure, up-to -date KYC has been maintained.

- vi) First detecting officer of any Money Laundering issue will be treated as Reporting Officer. A Reporting Officer will keep his observations secret and only communicate with BAMLCO through Suspicious Transaction Report (STR) from. BAMLCO will keep all AML report in his personal safe custody maintaining highest secrecy. He will not discuss this matter even with his fellow colleagues. If the report warrants CALMCO's attention then the BAMLCO will report it to CAMLCO;
- vii) Appropriate questions to be asked but not to alarm or tip off the customer.
- viii) It is wise not to deal with the clients who work beyond your command area (there may be exceptions).
- ix) It is wise to obtain Head Office approval before involving with a customer (existing or prospective) who has political connection/influence.
- x) We should be aware and cautious about the customer's behavior, attitude, social/political association, suspicious transactions, unlawful activities and undue approaches.
- xi) Meeting the requirements of this Policy is considered of paramount importance and takes precedence over other commercial aspects of managing our customer relationships. The management of PILIL is fully aware that the financial for criminal activities Therefore. co-ordination and co-operation between the concerned parties are essential its success.

Effective AML/CFT activities have beneficial consequences for financial institutions. Taking effective action against Money Laundering and terrorist financing makes a positive contribution to the well being and safety of the institution and its employees and shareholders.

We should all come forward to combat this evil force by implementing anti Money Laundering Measures complying with the law of the land.