Edme Insurance Brokers Ltd.

edme
Clarity in Complexity

Edme Insurance Brokers Limited Anti-Money Laundering (AML), Know Your Customer (KYC) & Combating Financing Terrorism (CFT) Policy

Edme Insurance Brokers Ltd.
(Formerly Aditya Birla Insurance Brokers Ltd.)
Corporate Office: One World Centre, Tower 1, 7th Floor, Jupiter Mills Compound, 841
Senapati Bapat Marg, Elphinstone Road, Mumbai 400 013, Maharashtra, India
T: +91 22 4356 8585 | E: care@edmeinsurance.com | W: www. edmeinsurance.com
Registered Office: Indian Rayon Compound, Veraval 362 266, Gujarat, India

CIN: U99999GJ2001PLC062239 | IRDAI Registration Number: 146 | License Validity: 9th April, 2027 | Broker Category: Composite Broker
ISO 9001 Quality Management Certificate certified by Intertek Certification Ltd. Under certificate number 0145476
ISO 27001 Information Security Management Certificate certified by BSI under certificate number IS738839

POLICY DETAILS

Policy Title	*EDME – Anti-Money Laundering Policy*
Policy Owner	*Risk & Compliance*
Policy Author	*Risk & Compliance*
Document Reference Code	*EDME/AMLPOL/003/2024-25*
Approved by	*Board of Directors*
Approval Date	*November 26, 2024*
Effective Date	*November 26, 2024*
Version Number	*3.0*
Issue Date	*November 26, 2024*

Version Control

Date	Prepared / Modified by	Reviewed By	Approved by	Version #	Nature of Change
25.03.2020	Apurv Mehta	Punit Pancholi and Arpit Patel	Board of Directors	1.0	New Policy
26.07.2023	Ishita Dhotre	Punit Pancholi	Board of Directors	2.0	Revision in Policy based on review
26.11.2024	Jaibind Sahu	Anurag Dharnidharka	Board of Directors	3.0	Annual Review

1. INTRODUCTION

Money Laundering is moving illegally acquired cash through financial systems so that it appears to be legally acquired. Terrorists' attacks have made the subject of money laundering much more relevant to the stability of modern world. Criminals including terrorists use techniques and tools of money laundering to sustain and finance their operations. Today money laundering is a global problem. As a dire need to combat terrorist financing EDME has formulated a CFT and KYC measure as a part of a standard due diligence mechanism. EDME

In accordance with Section 3 of the Prevention of Money Laundering Act, 2002:

Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering.

2. DEFINITIONS

1. "Beneficial Owner" means: -
(a) Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has a controlling ownership interest or who exercises control through other means.

Explanation- For the purpose of this sub-clause-
(i) "Controlling ownership interest" means ownership of or entitlement to more than twenty-five per cent. of the shares or capital or profits of the company;
(ii) "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(b) Where the customer/ client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than fifteen per cent. of capital or profits of the partnership;

(c) Where the customer / client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of the unincorporated association or body of individuals;

***Explanation*:** The term 'body of individuals' includes societies. Where no natural person is identified under (a) to (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

(d) Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

2. "Beneficiary Institution" means the financial institution that receives the wire transfer from the ordering institution, directly or through an intermediary institution, and makes the funds available to the wire transfer beneficiary.

3**. "Customer" or "Client"** for the purpose of these Guidelines shall mean a person who is engaged in a financial transaction or activity with a Regulated Entity and includes a person on whose behalf the person engaged in the transaction or activity, is acting.

4.. "Designated Director" *"Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes -;*

(i) the Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,
(ii) the managing partner if the reporting entry is a partnership firm,
(iii) the proprietor if the reporting entity is a proprietorship concern,
(iv) the managing trustee if the reporting entity is a trust
(v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

5. "FATCA" means Foreign Account Tax Compliance Act, 2010 of the United States of America (USA) which, inter-alia, requires reporting financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

6. "**Money Laundering"** shall have the meaning assigned to it under section 3 of the Act and "Anti-Money Laundering" shall be construed accordingly, and shall include Counter-Terrorist Financing and other related measures.

*7. "**Principal Officer** " means an officer designated by a reporting entity who shall be responsible for furnishing information as required;*

8. "**Regulated Entity"** means a unit/entity which has been granted license, recognition, registration or authorisation by the Authority.

9. **"Senior Management" means:**
(a) In relation to a Regulated Entity,
(i) for an incorporated entity in International Financial Services Centre in India, every member of the Regulated Entity's Governing Body;
(ii) for a branch, the person or persons who control the day-to-day operations of the Regulated Entity in an IFSC and may include such other persons as may be designated by the Regulated Entity.
(b) In relation to a customer, that is a legal person, every member of its Governing Body and the person or persons who control its day-to-day operations.

10. "Suspicious Transaction" means a "Transaction" as defined in these Guidelines, including an attempted transaction, which to a person acting in good faith-
(a) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the
Schedule to the Act, regardless of the value involved; or
(b) appears to be made in circumstances of unusual or unjustified complexity; or
(c) appears to have no economic rationale or *bona-fide* purpose; or
(d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Explanation: Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist

acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

I. OBJECTIVE

One of the core principles of Edme Insurance Brokers Limited (Formerly known as Aditya Birla Insurance Brokers Limited) hereinafter referred to as "*EDME*" is that we are committed in complying with all the Laws and Regulations which govern the operations in our country. We are committed to operating our businesses conforming to the highest moral and ethical standards.

Our Company believes in acting professionally, fairly and with integrity in all its business dealings and relationships wherever it operates, and to implementing and enforcing effective systems to counter Anti-Money Laundering activities. Our Company is equally committed to the prevention, deterrence and detection of Anti – Money Laundering (hereinafter to be referred to as "AML"), Combating Financing Terrorism (hereinafter to be referred to as "CFT") & Know your Customer (hereinafter to be referred to as "KYC") activities and other corrupt business practices.

EDME constantly benchmarks itself against international practices, regulations and conventions to theextent reasonable and practicable. EDME has therefore established Anti Money Laundering Policy (AML), CFT, KYC to participate in the international efforts against Money Laundering and Combating Finance Terrorism and ensure that EDME is not used as a vehicle for Money Laundering or any Terrorist financing activities

The Prevention of Money Laundering Act, hereinafter referred to as *"PMLA*", 2002 brought into force with effect from 1st July 2005. Further to the above said guidelines, the Authority notified additional amendments under the Prevention of Money Laundering (Amendment) Act, 2012, the Prevention of Money Laundering (Maintenance of Records) Amendments Rules, 2013 and the latest being, the Prevention of Money Laundering (Maintenance of Records) Second Amendment Rules, 2017 dated June 01 2017, issued by the Authority. The application of Anti-Money Laundering measures has been emphasized by international regulatory agencies as a key element in combating money laundering.

1.1. The Money Laundering process

Money Laundering means "any act or attempted act to disguise the source of money or assets derived from criminal activity". The purpose of Money Laundering is to turn 'dirty money' into 'clean money' through a series of financial transactions so that criminal origins of the funds becomes difficult to trace.

Money can be obtained illegally from various criminal activities like drug trafficking, terrorism, organized crime and fraud. As criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities and provide a legitimate cover for their source of income, they usually follow three stages:

"Placement": means placing currency into the financial system to convert illicit funds from cash straight into a financial instrument or a bank account.

For Example, A criminal having huge crime proceeds in form of cash, can deposit this cash in bank accounts maintained with different banks, in the name of his relatives, friends and associates, in small amounts. Alternatively, he can also invest in insurance policies by paying premium in cash.

"Layering": Now having successfully placed money into the financial system, the second stage is layering.

Layering involves converting the proceeds of crime into another form and creating complex layers of financial transactions to hide the original source. It also involves the movement of funds from

institution to institution to hide the source and ownership of the funds, conceal the audit trail and break the link with the original crime.

At this stage criminal can invest in insurance products, thus changing the form of crime proceeds from bank account to insurance product. Then surrender the insurance policy under the free look period to get a payment from insurance company in cheque, he can layer this transaction by investing these funds in security markets or mutual funds. Sell off securities in short span of time and invest in some other assets.

Thus, he can layer the original source by converting the crime proceeds from one form to another and moving them from institution to institution.

"Integration": Now, having successfully layered the funds at integration stage criminal can invest funds in assets like businesses, house, cars, financial assets, etc.

Thus, Integration means the reinvestment of those funds in an apparently legitimate business so that no suspicion of its origin remains and to give the appearance of legitimizing the proceeds.

1.2. Money laundering in India

With the growing financial sector, India is vulnerable to money laundering activities. Some common sources of illegal proceeds in India are narcotics trafficking, illegal trade in gems, smuggling, corruption and income tax evasion. Large portions of illegal proceeds are laundered through the alternative remittance system called “hawala”. Under this system, individuals transfer funds from one country to another or from one state to another, often without the actual movement of currency.

The Prevention of Money Laundering Act (PMLA), 2002 brought into force with effect from 1st July 2005, is applicable to all the financial institutions, which include insurance institutions. The application of anti-money laundering measures to insurance companies, has also been emphasized by international regulatory agencies as a key element in combating money laundering. Establishment of anti-money laundering programs by financial institutions is one of the central recommendations of the Financial Action Task Force (FATF) and forms part of the Insurance Core Principles of the International Association of Insurance Supervisors (IAIS). Accordingly, Insurance Regulatory and Development Authority of India (IRDAI) have set out following regulatory guidelines/instructions to the Insurers and Intermediaries as part of an Anti-Money Laundering Program for the insurance sector.

EDME INSURANCE BROKERS LIMITED (EDME) solicits variety of products offered by different insurers / reinsurers with an aim of transferring the financial risk of a certain event from the insured to the insurer. These products are offered through trained Brokers Qualified Personnel (BQP) and also through a number of alternate distribution channels like direct marketing, bancassurance etc. The guidelines are therefore of importance to the intermediaries also, to the extent indicated in the guidelines.

Punishment for money-laundering.—Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine which may extend to five lakh rupees: Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words “which may extend to seven years”, the words “which may extend to ten years” had been substituted.

MONEY LAUNDERING RISK

EDME is aware that it is exposed to several risks if an appropriate AML Framework is not established. Types of Risk include:

- **Reputation Risk** Reputational risk is a threat or danger to the good name or standing of a business or entity.
- **Compliance Risk**- Risk of loss due to failure of compliance with key Regulations governing the EDME's operations
- **Operations Risk-** Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.
- **Legal Risk**- Risk of loss due to any of the above risk or combination thereof resulting into the failure to comply with Law and having a negative legal impact. The specific types of negative legal impacts could arise by way of fines, confiscation of illegal proceeds, criminal liability etc.
- **Financial Risk-** Risk of loss due to any of the above risks or combination thereof resulting into the negative financial impact on EDME.

OVERVIEW

Considering the potential threat of usage of financial services by a money launderer, EDME shall make reasonable efforts to determine the true identity of all clients requesting for its services. Where a client is a juridical person, verification of identity is required to be carried out on persons purporting to act and is authorized to act on behalf of a client. Special care has to be exercised to ensure that the contracts are not anonymous or under fictitious names.

EDME shall not enter into a contract with a clients whose identity matches with any person with known criminal background or with banned entities and those reported to have links with terrorists or terrorist organizations. Considering the potential threat of usage of financial services by a money launderer, EDME shall make reasonable efforts to determine the true identity of all clients requesting for its services. Where a client is a juridical person, verification of identity is required to be carried out on persons purporting to act and is authorized to act on behalf of a client. Special care has to be exercised to ensure that the contracts are not anonymous or under fictitious names.

- While carrying out the KYC norms, special care which includes determination of the true identity of all the customers requesting for its services, shall be exercised to ensure that the contracts are not anonymous or under fictitious names.
- All the transactions shall be carried out through account payee cheques, bank drafts direct credit or NEFT or by pay order only.
- Care has to be exercised to avoid unwitting involvement in insuring assets bought out of illegal funds.
- While carrying out the KYC norms, special care which includes determination of the true identity of all the customers requesting for its services, shall be exercised to ensure that the contracts are not anonymous or under fictitious names.

1. **AML Program**

In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing of terrorism, EDME has an AML program, which includes:

- Internal policies, procedures, and controls;
- Designating a Principal Compliance officer;
- Recruitment and training of employees/agents
- Internal Control/Audit

EDME has designed an AML program to report suspicious transactions. Weightage is given more on design and implementation of a program, rather than isolated instances failing to report suspicious transactions. The AML program also envisages submission of Suspicious Transaction Reports (STR) to a Financial Intelligence Unit-India (FIU-IND) set up by the Government of India for further investigation and action. Formal instructions on the manner of submission of Suspicious/Cash Transaction Reports (STR/CTR) to the Financial Intelligence Unit are issued by IRDAI. EDME to report all the suspicious transactions to FIU-IND in the format given by IRDAI.

This program has been implemented in August 2006 and is applicable to all the Policies coming in to force on or after 1st January 2006. The key elements of the AML program are discussed in detail below:

2.1. INTERNAL POLICIES, PROCEDURES AND CONTROLS

Know Your Customer (KYC)

Considering every potential threat of usage of the financial services by a money launderer, EDME shall make reasonable efforts to determine the true identity of all customers requesting insurance services through effective procedures for obtaining identification from new customers to establish his or her genuine need for an insurance contract. While prescribing the guidelines the IRDAI has considered the large distribution network of agents required by the insurers, geographical spread of insurance, the customers and the product design so that the program has the needed flexibility while addressing the main requirements.

Customer's KYC procedures is divided into

2.1.1. Customer Acceptance Procedure (CAP)

For the purpose of KYC guidelines, 'customer' is defined as-

- A person or entity that maintains policy and/or has a business relationship with the Insurance Company
- One on whose behalf the account/policy is maintained (beneficiaries/assignees)
- Professional intermediaries or power of attorney holders, carrying out transactions under the policy as permitted under the laws and regulations

2.1.2. Customer Identification Procedure (CIP)

This can be explained as the Due Diligence Process carried out to decide whether to accept a Prospect as customer and candidate as employee. Once the decision is taken to accept a customer, business partner and employee, identification process will take place.

- The measures may differ based on the type of Prospect. However, following guidelines can be regarded as the guiding principles:

  - ✓ KYC should be carried out before every new policy contract, agency agreements, empaneling brokers.
  - ✓ Customer information should be collected from all relevant sources.
  - ✓ Due diligence measures on legal persons based on risk perception should include verification of natural persons who have controlling interest and comprise the mind and management of the legal persons.
  - ✓ Documents collected towards the identity and address of the customer should be duly certified by an authorized person as identified on an ongoing basis.
  - ✓ No policy should be issued where company is unable to apply appropriate due diligence measures i.e. company is unable to verify the identity and /or obtain documents required as per the risk categorization due to noncooperation of the customer or non-reliability of the data/information furnished. It may, however, be necessary to have suitable built in safeguards to avoid harassment of the customer.
  - ✓ EDME may avail e- KYC services of the Unique Identification Authority of India (UIDAI) for KYC verification as prescribed by the IRDAI or other Statutory Authorities subject to certain conditions as specified by the Authority from time to time.

- Due diligence process for agents are as per agent's recruitment process followed at Direct Sales Force and Alternate Channels (here in after it includes Dealers, POSPs and Contract employees)
- New Employee's due diligence process is as per recruitment process followed at Human Resources Function.

2.1.2.1. Essentials of KYC

- ✓ Essential components of effective KYC are obtaining and verifying authenticity of information provided by the applicant. To ensure effective KYC, EDME shall collect documentary evidence to establish the identity of the applicant along with source of funds. A list of documents to be verified and obtained at the time of accepting the risk for compliance with the KYC requirements for individuals and others is defined in the AML Operational Manual
- ✓ The application forms and the enclosed supporting documents are scanned for electronic storage and hard copies stored at an offsite location
- ✓ In case of non-face to face business that includes tele calling, internet marketing, etc collection of applicable documentation shall be completed before logging of the policy with the company.
- ✓ Compliance to conduct surprise scrutiny of newly received application forms to check if the KYC procedures and third-party payment identification process is in place and followed.

KYC Procedures

EDME shall endeavor to undertake Due Diligence Process for Vendors, Reinsurance Brokers and Reinsurance Entities.

Documentation seeked from Outsourced Vendors – ANNEXURE I

Documentation seeked from Reinsurance Brokers – ANNEXURE II

Documentation seeked from Reinsurers – ANNEXURE III

As a general practice EDME shall send Service Provider Requisition Sheet hereinafter to be referred to as "*SPRF*" herewith annexed under ANNEXURE – I, which would be in the form of questionnaire / declaration to all the outsourced third - party service providers. EDME should take appropriate measures as a part of due diligence measures which may include conducting Independent enquiries on the details collected by the Service Providers.

EDME shall maintain relevant records and details in such a way that it enables verification at a later date and support the fact of having established sources of funds involved in the insurance contract.

AML checks will not be done where assignment is to Banks / Financial Institutions / Capital Market intermediaries regulated by IRDAI / RBI / SEBI.

Where assignments are made to nonrelated third parties, AML checks would be higher.

Notwithstanding the above, EDME is required to ensure that no vulnerable cases go undetected. Especially where there is suspicion of money laundering or terrorist financing, or where there are factors to indicate a higher risk, AML/Combating the Financing of Terrorism hereinafter referred to as *"CFT"* checks will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

Assignment

The assignee needs to submit KYC documents as defined in the AML Operational Manual. Income proof requirement shall be raised as per the due diligence measures applied on customer

Claim Settlement

It is imperative besides verification of identity of the customer at the time of initial issuance of the policy. KYC should be carried out at the claim payout stage, if EDME receives request to facilitate settlement of claim. Identification of the claimant needs to be established. Hence the claimant needs to provide KYC documents as defined in the AML Operational Manual.

Address change

All address change requests should be accompanied with proof of the revised address as defined in the AML Operational Manual.

2.1.2.2. Blacklisted customers

Company will not enter into a contract with a customer whose identity matches with any person with known criminal background/with banned entities/those reported to have links with terrorists or terrorist organizations.

2.1.2.3. NRI Insurance

Compliance approved controls have been built at Underwriting stage to ensure compliance with all applicable laws and regulations.

2.1.2.4. Reliance on Third Party KYC

- ✓ EDME may rely on third party and insurers subject to complying with conditions as specified by the Authority from time to time.

2.1.3. MONITORING TRANSACTIONS

2.1.3.1. Third Party Payment

- Insurance premium paid by person other than insured should be looked into establish insurable interest.
- Insurable interest is a basic requirement of any contract of insurance unless it can be, and is, lawfully waived. At a general level, this means that the party to the insurance contract who is the insured or policyholder must have a relationship with the subject matter of the insurance, whether that be a life or property or liability to which he might be exposed. The absence of required relationship would render the contract illegal, void or simply unenforceable, depending on the type of the insurance.

✓ **Control**

i. Receipt of premium from a person other than the insured is considered third party payment and is subject to EDME's Third Party Payment Process
ii. Receipt of premium via Demand Draft is accepted along with a declaration from the client confirming the source of funds

2.1.3.2. Suspicious Transactions:

It is difficult to define what constitutes a suspicious transaction and a complete list is next to impossible. However, a suspicious transaction will often be one which gives rise to a reasonable suspicion that it may involve the laundering of money or is inconsistent with a customer's known, legitimate business or personal activities. An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behavior. Suspicious transactions also include "Attempted Transactions" which is of suspicious nature.

- **Monitoring Suspicious Transactions**

Adequate procedures are developed, implemented, controlled and enhanced to identify suspicious transactions and to report to FIU-IND setup by the Government of India. Suspicious Transactions are to be reported within 7 working days of identification of such transaction to FIU-IND.

Besides the above, employees shall be responsible to report any suspicious transactions that are noticed by them to the Money Laundering Reporting Officer of for further analysis and reporting.

2.1.3.3. Confidentiality

Directors, officers and employees (permanent and temporary) of EDME INSURANCE BROKERS LIMITED shall be prohibited from disclosing the fact that a suspicious Transaction Report or related information of a policyholder/ prospect is being reported or provided to the FIU-IND.

2.1.4. RISK MANAGEMENT

EDME may devise procedures for creating Risk Profiles of their existing and new customers and apply various AML and CFT measures keeping in view the risks involved in a transaction, account or business relationship.

Risk Assessment:

EDME shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk, severally and together, for customers, countries or geographic areas including countries or jurisdictions are subject to sanctions, embargos or similar measures, and products, services, transactions or delivery channels etc. as prescribed by Authority.

In the context of the very large base of insurance customers and the significant differences in the extent of risk posed, EDME shall classify the customers/clients into high risk, medium risk, low risk, based on the individual and product profile to decide upon the extent of due diligence.

2.1.4.1. Enhanced Due Diligence (EDD):

EDME shall ensure Enhanced Due Diligence (EDD) where the risk of money laundering or terrorist financing is higher such as the background and purpose of all complex, unusually large transactions and all unusual pattern of transactions, which have no apparent economic or lawful purpose.

2.1.4.2. Simplified Due Diligence (SDD):

'Simplified Due Diligence' shall be applied in the case of 'Low risk' and ‘Medium risk’ customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.

- In situation where the records relate to ongoing investigations, or transactions, which have been the subject of a disclosure, EDME shall retain until it is confirmed that the case has been closed.

- As per IRDAI Guidelines, sharing of information on customers is permitted between different organizations such as banks, insurance companies, Income tax authorities, and local government authorities on request. Records can also be in electronic form.

- In case of customer identification data obtained through the customer due diligence process (e.g. copies of records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence after the business relationship is ended for a period approved by the Designated Director and Principal Compliance Officer in line with the changes made in the PMLA or any other regulatory authority from time to time.

PERIODIC UPDATION

A Regulated Entity shall adopt a risk-based approach for periodic updation of Customer Due Diligence (hereinafter to be referred to as "CDD"). The periodicity of updation from the date of opening of the account / last CDD updation for different categories of customers is as follows: -

(i) Annually- for high-risk customers;
(ii) once in three years- for medium risk customer; and,
(iii) once in every five years- for low-risk customers.

(a) Individual Customers:

(i) No change in CDD information:
In case of no change in the CDD information, a self-declaration from the customer in this regard may be obtained through mobile number registered with the Regulated Entity or through digital channels (such
as online banking / internet banking, e-mail or mobile application of Regulated Entity).

(ii) Change in address:

(aa) In case of a change only in the address details of the customer, a self-declaration of the new address
may be obtained from the customer through customer's email-id registered with the Regulated Entity, customer's mobile number registered with the Regulated Entity, digital channels (such as online banking internet banking, e-mail or mobile application of the Regulated Entity). The declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.

(bb) Further, a Regulated Entity shall obtain a copy of OVD or the equivalent e-documents thereof for
the purpose of proof of address declared by the customer at the time of periodic updation. Such requirement, however, shall be clearly specified by the Regulated Entity in its internal KYC policy, duly approved by its Governing Body.

(b) Customers other than Natural Persons:

(i) No change in CDD information:
In case of no change in the CDD information of a customer, which is a non-natural person, a self declaration
through email id registered with the Regulated Entity, digital channels (such as online

banking / internet banking, mobile application of Regulated Entity), a letter duly signed by authorised
official and requisite resolutions in this regard shall be obtained from the customer. Further, a Regulated
Entity shall ensure that Beneficial Ownership (BO) information available with them is accurate and upto-
date.

(ii) Change in CDD information:

In case of change in CDD information, Regulated Entity shall undertake fresh CDD process as is applicable for on boarding a new customer which is a non-natural person.

In case expiry of documentation from Vendors / Foreign Brokers / Reinsurers as prescribed under ANNEXURE I,II,III, EDME shall endeavor to undertake fresh CDD process equivalent to that applicable for on boarding a new
customer.

RECORD KEEPING

EDME shall maintain the records (either in electronic or in paper from) of types of transactions mentioned under Rule 3 of PMLA Rules 2005 and the copies of the Cash / Suspicious Transactions reports submitted to FIU for a period of 5 years from the date of transaction between the client and the EDME as well as those relating to the verification of identity of clients for a period of 5 years from the date of cessation of relationship with the client in order to enable EDME to comply swiftly with information requests from the competent authorities. Such records shall be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity.
Records can be maintained in electronic form and/or physical form.

a. EDME shall be satisfied about the organizational capabilities, and that technology, systems and measures are in place to safeguard the privacy of the data maintained and to prevent unauthorized access, alteration, destruction, disclosure or dissemination of records and data.

b. The physical or electronic access to the premises, facilities, automatic data processing systems, data storage sites and facilities including back-up sites and facilities and to the electronic data communication network of the service provider is controlled, monitored and recorded;

c. EDME has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

d. In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been

closed where practicable, EDME is required to seek and retain relevant identification documents for all such transactions and to report such transactions of suspicious funds.

e. As per IRDAI Guidelines, sharing of information on customers is permitted between different organizations such as banks, insurance companies, Income tax authorities, and local government authorities on request. Records can also be in electronic form.

f. In case of customer identification data obtained through the customer due diligence process (e.g. copies of records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence after the business relationship is ended for a period approved by the Designated Director and Principal Compliance Officer in line with the changes made in the PMLA or any other regulatory authority from time to time.

IMPLEMENTATION OF SECTION 51A OF THE UNLAWFUL ACTIVITIES (PREVENTION) ACT, 1967

By virtue of Section 51A of UAPA, the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism.

EDME – AML FUNCTION

As part of the Internal Control System, EDME shall establish an AML/CTF function, as a specialised unit of the Legal & Compliance Function that focuses on the prevention of Money Laundering. The AML function's mission is to:

- Design and implement an effective AML/CTF compliance programme;
- Give advice and report to the Board of Directors on AML/CTF risks;
- Investigate and assess suspicious activity reports and report to the relevant authorities;
- Monitor and respond to Legal and Regulatory developments in relation to AML/CTF;
- Monitor and test the AML/CTF controls to evaluate and ensure their effectiveness;
- Define appropriate remediation actions when deficiencies have been identified.

2.2. DESIGNATING A DESIGNATED DIRECTOR AND PRINCIPAL OFFICER

2.2.1. Designated Director

EDME has appointed "Designated Director" to ensure overall compliance with the anti-money laundering laws, regulations and policies under the PMLA Act and Rules as defined from time to time. The Designated Director must be Managing Director or a whole-time Director duly authorized by the Board of Directors.

2.2.2. Principal Compliance Officer:

- Appointment

The Board of EDME would appoint “Principal Compliance Officer” for AML who is responsible for ensuring day-to-day compliance with the anti-money laundering laws, regulations and policies. The Principal Compliance Officer serves as a single reference point to whom staff and agents/representatives shall be instructed to report suspected money laundering transactions promptly and shall be responsible for reporting any suspicious or large cash transactions to FIU-IND, where appropriate. The Principal Compliance Officer for AML guidelines and staff assisting him in execution of AML guidelines should have timely access to customer identification data, other KYC information and records.

- Duties of the Principal Compliance Officer

i. Be the point of contact with FIU-IND with respect to money laundering matters;
ii. Approve any new or revised procedures for combating money laundering within a business unit;
iii. Review and investigate any suspicions of money laundering identified by employees, agents and/or Business Unit Compliance Officers;
iv. Determine when a transaction constitutes a suspicious transaction or large cash transaction requiring reporting to FIU-IND;
v. Reporting of the Suspicious Transactions and AML activities to FIU and Authorities (IFSCA / IRDAI / SEZ)
vi. Ensure cash transaction where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions are reported to FIU-IND as required;
vii. Maintain a system for reporting suspicious and prescribed transactions to the FIU-IND as required;
viii. Ensure no transaction (financial or otherwise) is permitted in any insurance contract freezed under Section 51A of UAPA Act;
ix. Carry out, on a periodic basis, in accordance with the local policy and procedures, an examination of a sample of client transactions to determine whether appropriate anti-money laundering and client identification procedures were followed;
x. Take reasonable steps to establish awareness and training programs for local staff with respect to anti-money laundering laws; and
xi. Maintain up-to-date information on money laundering laws and regulations and communicate such to relevant stakeholders.
xii. EDMEcarrying out, or overseeing the carrying out of, ongoing monitoring of business relations for
compliance with these Guidelines;
xiii. promoting compliance of these Guidelines and taking overall charge of all AML/CFT matters
within the organisation;
xiv. informing employees, officers and representatives promptly of regulatory changes;
xv. ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
xvi. reporting or overseeing the reporting of suspicious transactions;
xvii. advising and training employees, officers and representatives on developing and implementing
internal policies, procedures and controls on AML/CFT;

xviii. reporting to Senior Management on the outcome of reviews of the Regulated Entity's compliance with these Guidelines & risk assessment procedures; and

xix. reporting regularly on key AML/CFT risk management and control issues, and any necessary remedial actions, arising.

BOARD OF DIRECTORS AND SENIOR MANAGEMENT ROLE

The Board of Directors / Senior Management of EDME are ultimately responsible for defining the strategies, directives and policies for the effective management of the company's AML/CTF risks. The Board of Directors/Senior Management shall:

- ✓ Ensure that an effective AML/CTF compliance culture thrives and operates at all levels of the business and that this is supported by an active AML/CTF compliance awareness and monitoring process;
- ✓ Appoint Designated Director and Principal Officer and establish an independent, permanent and effective AML/CTF Function;
- ✓ Approve the AML/CTF Policy and oversee its implementation;
- ✓ Review the reports prepared by the AML/CTF Function.;
- ✓ Ensure that AML/CTF-related issues are resolved effectively and expeditiously by Senior Management, with the assistance of the AML/CTF Function;
- ✓ Ensure the effectiveness and adequacy of the AML/CTF risk management system and issue instructions for the definition of corrective measures identified by the AML/CTF Function;

DUTIES OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT

AML Program: In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing of terrorism the Board of Directors and the Senior Management shall discharge the following duties:

- ✓ Set and follow the highest standards of integrity leading by example and demonstrating an open and receptive attitude towards AML/CTF;
- ✓ Ensure that the all the company policies are communicated, implemented and adhered to and that the minimum standards set are met;
- ✓ Build AML/CTF awareness through ensuring that all staff receive appropriate AML/CTF training;
- ✓ Create an environment of accountability in which the staff is not only assessed on productivity measures, but also rewarded for their ability to proactively manage AML/CTF risks;
- ✓ Provide the AML/CTF function with sufficient resources, management support and access they need to detect and manage AML/CTF risks;
- ✓ Inform the Principal Officer of any changes that may impact AML/CTF risk in the business;

Any change in details of the Designated Director and Principal Officer for AML/ CFT Guidelines shall be communicated to IRDAI / IFSCA / SEZ and FIU IND within the timelines prescribed by the Authority.

RECRUITMENT AND TRAINING OF EMPLOYEES

2.2.3. Anti-Money Laundering Training

The following training requirements are considered essential based on the class of employees.

2.2.3.1. New employees:

A general appreciation of the background to money laundering, and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point shall be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority. Impact of money laundering will be part of new employee's induction module in consultation with Human Resources.

2.2.3.2. Sales/Advisory staff:

Members of staff who are dealing directly with the public (whether as members of staff or agents) are the first point of contact with potential money launderers and their efforts are therefore vital to the strategy in the fight against money laundering. It is vital that "front-line" staff is made aware of the insurance institution's policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases. AML Policy and its impact will be a part of in-house training curriculum..

2.2.3.3 Processing staff:

Those members of staff who receive completed proposals and cheques for payment of the premium contribution shall receive appropriate training in the processing and verification procedures. EDME's ready reckoner will be modified accordingly.

2.2.3.4 Administration/Operations supervisors and managers:

A higher level of instruction covering all aspects of money laundering procedures shall be provided to those with the responsibility for supervising or managing staff.

2.2.3.5 Ongoing training:

It will also be necessary to make arrangements for refresher training at regular intervals to ensure that staff does not forget their responsibilities. Timing and content of training packages for various sectors of staff will need to be adapted. Compliance shall make training module and put to test the employees on ongoing basis.

Department wise records of training imparted to staff in the various categories detailed above shall be maintained. Compliance would do surprise check on those training records.

2.3. POLICY REVIEW

AML Policy should be reviewed as and when prescribed by the Authority and changes there of shall be incorporated. The same shall be approved by the Board. the AML Operational Manual should be as and when prescribed by the authority and changes there off shall be incorporated. The same shall be approved by the Principal Compliance Officer.

AUDIT

(a) A Regulated Entity shall maintain an audit function that is adequately resourced and independent, that is able to regularly assess the effectiveness of the Regulated Entity's internal policies, procedures and controls, in compliance with regulatory requirements and these Guidelines..

(b) A Regulated Entity's AML/CFT framework should be subjected to periodic audits. Such audits should be performed not just on individual business functions but also on a Regulated Entity-wide basis.

Auditors should assess the effectiveness of measures taken to prevent ML/TF. This would *inter-alia* include —

(i) Determining the adequacy of the Regulated Entity's AML/CFT policies, procedures and controls, ML/TF risk assessment framework and application of risk-based approach;

(ii) Reviewing the content and frequency of AML/CFT training programmes, and the extent of employee's, officer's and representative's compliance with established AML/CFT policies and procedures; and

(iii) Assessing whether instances of non-compliance are reported to Senior Management on a timely basis. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the Regulated Entity's business.

****