GUIDELINES ON ANTI MONEY LAUNDERING, COUNTERING THE FINANCING OF TERRORISM AND COUNTER PROLIFERATION FINANCING PROGRAMME FOR INSURANCE COMPANIES AND BROKERING COMPANIES

Insurance Regulatory Commission of Sri Lanka (IRCSL)

Date of Issue: 25th July 2025

Index

Abbreviations

AML/CFT	- Anti-money Laundering and Countering the Financing of Terrorism
BO	- Beneficial Owner
CA	- Competent Authority
CBRN	- Chemical/Biological/Radio Active/Nuclear
CBSL	- Central Bank of Sri Lanka
CDD	- Customer Due Diligence
CSTFA	- Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005 (as amended)
CT	- Cash Transactions
CO	- Compliance Officer
ECDD	- Enhanced Due Diligence
EFT	- Electronic Fund Transfers
FATF	- Financial Action Task Force
FIU	- Financial Intelligence Unit of Sri Lanka
FTRA	- Financial Transactions Reporting Act, No. 6 of 2006
IAIS	- International Association of Insurance Supervisors
Insurers CDD Rules	- Insurers (Customer Due Diligence) Rules, No. 1 of 2019
IRCSL	- Insurance Regulatory Commission of Sri Lanka
ML	- Money Laundering
TF	- Terrorism financing
(PAE) Report	- Persons/Accounts/Entities Report
PEPs	- Politically Exposed Persons
SEC	- Securities Exchange Commission
STR	- Suspicious Transaction Report
UNSCR	- United Nations Security Council Resolutions

1. Introduction:

1.1 The Financial Transactions Reporting Act, No. 6 of 2006 (FTRA) and the Prevention of Money Laundering Act, No. 5 of 2006 (as amended), are applicable to all financial institutions, which include insurance companies and insurance broking companies. The application of anti-money laundering measures to insurance companies / insurance broking companies, has also been emphasized by international regulatory agencies as a key element in combating money laundering.

Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005 (as amended) (CSTFA) gives effect to Sri Lanka's obligations as a signatory to the International Convention on the Suppression of Terrorist Financing adopted by the United Nations on 10th January 2000. The Act prohibits the financing of terrorist acts, terrorists and terrorist organizations. Further, the CSTFA has provisions for freezing of terrorist financing related assets and forfeiture of such assets. CSTFA has been further strengthened through the amendments brought to the Act in 2011 and 2013.

Establishment of Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) programs by financial institutions is one of the central recommendations of the Financial Action Task Force and also forms part of the Insurance Core Principles of the International Association of Insurance Supervisors (IAIS).

The Financial Intelligence Unit of Sri Lanka (FIU) issued Insurers (Customer Due Diligence) Rules, No. 1 of 2019 (Insurers CDD Rules). Accordingly, the Insurance Regulatory Commission of Sri Lanka (IRCSL) has decided to revise the guidelines issued in 2006 to the Insurers and Brokers.

1.2 Insurance companies offer a variety of products aimed at transferring the financial risk of a certain event from the insured to the insurer. These products include life insurance products such as Linked Long Term, Annuities, Contracts for the Granting of Disability and Multiple Indemnity, Accident and Sickness Benefits, Permanent Health, Capital Redemption Policies, Pension Policies, Single Premium Short-Term Investment and non-life insurance such as marine, motor, fire, health and miscellaneous. These products are offered to the public through trained agents/sales staff of the insurance companies and insurance brokering companies and also through a number of alternate distribution channels like direct marketing, mobile platforms, bancassurance etc.

1.3 The obligation to establish an AML/CFT program applies to insurance companies / insurance broking companies. Hence the responsibility for guarding against insurance products being used to launder unlawfully derived funds or to finance terrorist acts, lies on each insurance company/insurance brokering company, which develops and bears the risks of its products, and each broking company.

2. What is Money Laundering?

2.1 Money Laundering (ML) is the action of disguising the source of assets in order to avoid detection of the illegal activity from which they were derived. 'Money laundering' is simply the use of illegally obtained funds. The offense of ML has been defined in Section 3 of the Money Laundering Act, No. 5 of 2006 as amended.

2.2 There are three common stages of money laundering as detailed below which are resorted to by the launderers and insurance companies / insurance broking companies which may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions: -

a. Placement - The initial stage of the process involves placement of illicitly earned funds into the financial system, usually through a financial institution. This can be accomplished by placing cash deposits into bank accounts or cash purchase of shares or insurance contracts. In the case of bank deposits large amount of cash are broken into smaller, less conspicuous amounts and deposited over time in different branches of a single financial institution or in multiple financial institutions.

b. Layering - The second money laundering stage, layering occurs after the ill-gotten funds have entered into the financial system, at which point the funds, securities or insurance contracts are converted or moved to other institutions further separating them from their criminal sources. Such funds could then be used to purchase other securities, insurance contracts or other easily transferable investment instruments and then sold through another institution; and

c. Integration - The third stage involves the integration of funds into the legitimate sector. This is accomplished through the purchase of assets such as real estate, securities, other financial assets or luxury goods such as cars, gems & jewelries etc.

2.3 If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. Financial institutions such as insurance companies/broking companies are therefore placed with a statutory duty to make a disclosure to the authorized officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of drug trafficking or of a predicated offence, or was or is intended to be used in that connection is passing through the institution. Law protects such disclosures, enabling the person with information to be able to disclose the same without any fear. Insurance companies / insurance broking companies likewise need not fear breaching their duty of confidentiality owed to customers.

3. What is Terrorist Financing?

Terrorism financing (TF) is the act of providing financial support to terrorists or terrorist organizations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organization.

While funds may come from criminal activities, they may also be derived from legitimate sources, for example, through salaries, revenue from legitimate business or donations including through non-profit organizations.

Similar to money laundering, there are generally stages in terrorism financing: raising, moving and using funds. Despite the different stages, the ways in which terrorism financing is done is similar and, in some cases, may be identical to the methods used to launder money. In both cases, the perpetrator seeks to misuse the financial or non-financial sectors for illegitimate purposes.

The offense of TF has been defined in section 3 of the Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005, as amended.

4. What is Proliferation Financing of Weapons of Mass Destruction?

Proliferation Financing of Weapons of Mass Destruction is providing funds for the rapid construction of weapons of mass destruction, closely associated with science and technological research projects (Chemical/Biological/Radio Active/Nuclear – CBRN).

5. What is the importance of an AML/CFT program to insurers/brokers?

- To protect the insurance companies / insurance broking companies from being used directly or indirectly for money laundering and terrorist financing purposes.
- To comply with the recommendations set out by the Financial Action Task Force (FATF).

6. AML/CFT Program:

In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing of terrorism, a company needs to have an AML/CFT program, which should, at a minimum, include:

6.1 Risk Management

6.2 Internal policies, procedures, and controls;

6.3 Appointment of a compliance officer;

6.4 Recruitment and training of employees/agents;

6.5 Internal Control/Audit;

6.6 Sanction Screening/ Targeted Financial Sanctions

The above said key elements of the AML/CFT programme are discussed in detail below:

6.1. Risk Management

6.1.1 Each company shall take appropriate steps to identify, assess and manage its money laundering and terrorist financing risks in relation to its customers, countries or geographical areas, products, services, transactions and delivery channels.

6.1.2 Each company shall document their risk assessments and findings and shall update the risk assessment through a periodic review.

6.1.3 Each company shall provide a timely report of its risk assessment, ML/TF risk profile of the company and the effectiveness of risk control and mitigation measures to its Board of Directors.

6.1.4 Each company shall comply with the Rules 4-13 of the Insurers (Customer Due Diligence) Rules, No.1 of 2019, as these Rules constitute an integral part of this guideline.

6.1.5 Insurance companies are required to carry out a comprehensive risk assessment in line with the above requirements, and the insurance brokering companies may carry out a risk assessment limited to its role as an intermediary.

6.2. Internal policies, procedures, and controls:

Each company shall formulate an internal policy approved by its Board of Directors subject to the written laws in force on AML/CFT.

Each company has to establish and implement policies, procedures, and internal controls, which would also integrate its agents in its AML/CFT program as detailed below.

6.2.1. Customer Due Diligence (CDD):

i. Customer Due Diligence (CDD) is the process of identifying and verifying information on customers including their beneficial owners (if any) to determine the risk they possess. A company should make reasonable efforts to determine the true identity of all customers requesting its services, in order to mitigate ML/TF risk. Hence effective procedures should be put in place to obtain requisite details for proper identification of new customers.

ii. Each company shall obtain following information for the purpose of conducting CDD, at minimum:
    a. purpose of the transaction;
    b. sources of funds;
    c. expected monthly turnover;
    d. expected mode of transactions (cash, cheque, etc.);
    e. expected type of counterparties (if applicable);

iii. Each company shall carry out Enhanced Due Diligence (ECDD), in terms of Rules 32 and 33 of the Insurers CDD Rules, where the assessed money laundering and terrorist financing risk for a customer has been rated as high risk.

iv. The documents to be verified at the time of entering the insurance contract to comply with CDD requirement for individuals and others should be in line with Rules 23 to 53 read with the Schedule of the Insurers CDD Rules. It is mandatory to obtain the said documents to clearly establish the customer identity (bearing a photograph of the customer) consistent with risk profile in respect of all new insurance contracts (Please also see 6.2.4 below).

v. Remittance of premium is an important stage of entering into contract, hence, cash transactions need more diligence and care (Please also see paragraph 6.2.10).

vi. Customer information should be collected from all relevant sources, including insurance agents and insurance brokering companies.

vii. Insurance premium paid by persons other than the person insured should be looked into to establish insurable interest.

viii. Beneficial owner (BO) means a natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a legal person or a legal arrangement. A Company shall identify the BO and take reasonable measures to verify the identity of the BO, using relevant information or data obtained from a reliable source.

ix. An insurance company should not enter into a contract with a customer 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 in terms of Rule 58 of the Insurers CDD Rules.

x. Insurance agents and insurance brokering companies play a critical role in AML/CFT by acting as a frontline for identifying suspicious activity, collecting customer information, and reporting potential ML concerns to the insurance company, as they often have direct interaction with clients and are privy to key details about transactions and policyholders; thus, their compliance with AML/CFT regulations is vital for the overall integrity of the insurance sector.

6.2.2. When should CDD be done?

i. Knowing New Customers:

a) In terms of Rules 26- 31 of the Insurers CDD Rules, CDD should be done before the issue of every new contract.
b) Special attention should especially, be paid to the 'non-face-to-face' business relationships which include Tele calling, Internet Marketing, Logging in of business or payment of premiums/lump sums at branches.

ii. Knowing Existing Customers:

In terms of Rules 37-40 of Insurers CDD Rules, each insurance company shall conduct CDD measures on its existing customers having regard to the assessment of materiality and risk of an existing customer.

6.2.3. On-Going Customer Due Diligence

In terms of Rules 34-36 of the Insurers CDD Rules, each insurance company shall conduct on-going customer due diligence and on-going transaction scrutiny in terms of the provisions of section 5 of the FTRA on continuing business relationship with the customer by:

- Regularly review and update the customer's risk profile including where necessary, the source of funds
- Monitor all business relationships with a customer on an ongoing basis
- Obtain information and examine the background and purpose of all complex, unusually large transactions and all unusual pattern of transactions

The frequency of on-going customer due diligence or enhanced on-going customer due diligence, shall be commensurate with the level of money laundering and terrorist financing risks posed by the customer based on the risk profile and the nature of transactions.

6.2.4. CDD and Risk Profiling of the Customer

In the context of managing a diverse customer base and the significant differences in the extent of risk posed by them, the companies shall conduct risk profiling on its customers, to decide upon the extent of due diligence, in terms of Rule 8 of Insurers CDD Rules.

i. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society, Government departments and Government owned companies, regulators and statutory bodies etc., In such cases, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Notwithstanding above, in case of continuing policies, if the situation warrants, as for example if the customer profile is inconsistent with his investment through top-ups, a re-look on the customer profile is to be carried out.

ii. For the high risk profiles, like for customers who are non-residents, high net worth individuals, trusts, charities, NGO's and organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher

due diligence and underwriting procedures should ensure higher verification and counter checks. In this connection insurers are also advised to carry out Enhanced Due Diligence (ECDD), in terms of Rule 32 of the Insurers CDD Rules. Further, please refer the following:

- Rules 23 - 31 of the Insurers CDD Rules – CDD in general
- Rules 41-44 of the Insurers CDD Rules - CDD for legal persons and legal arrangements
- Rules 45-47 of the Insurers CDD Rules - Non-Governmental Organizations, Not-for-Profit Organizations or Charities
- Rules 48-49 of the Insurers CDD Rules - Customers from High Risk Countries
- Rule 50 of the Insurers CDD Rules - Politically Exposed Persons
- Rules 51-53 of the Insurers CDD Rules – Reliance on Third Parties

6.2.5. Politically Exposed Persons (PEPs)

PEPs means an individual who is entrusted with prominent public functions either domestically or by a foreign country, or in an international organization and includes a head of a State or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a State owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals.

Each company shall implement appropriate internal policies, procedures and controls to determine whether the customer or the beneficial owner is a PEP.

Every insurance company shall where a PEP or an immediate family member and a close associate of PEP is a customer or a beneficial owner:

- obtain approval from the senior management of the insurance company, if any, to enter into or continue business relationship;
- identify, by appropriate means, the sources of funds and the sources of wealth; and
- Conduct enhanced CDD and ongoing monitoring of their business relationships with the insurance company.

Each company shall refer to the Guidelines on Identification of Politically Exposed Persons, No. 03 of 2019 issued by FIU on verification of PEPs.

6.2.6. Products to be covered:

The AML/CFT requirements focus on the vulnerability of the products offered by the insurance companies to any process of money laundering. Some vulnerable products are listed in **Annexure I.**

Please also refer to Rules 21-22 of the Insurers CDD Rules on Using New Technologies for both new and pre-existing insurance products.

6.2.7. Sources of Funds:

It is imperative to ensure that the insurance being purchased is reasonable. Accordingly, the customer's source of funds, his estimated net worth etc., should be documented properly, and the insurance agent or insurance brokering company or the employee of the insurance company shall obtain income proof as in **Annexure II**, to establish his need for insurance cover. Proposal form may also have questionnaires/declarations on sources of fund, and details of bank accounts. Large single premiums should be backed by documentation, to establish sources of funds.

6.2.8. Defining Suspicious Transactions:

The AML/CFT program envisages submission of Suspicious Transaction Reports (STR) to FIU to track possible money laundering attempts and for further investigation and action. It is extremely difficult to give an exhaustive list of suspicious transactions. An illustrative list of such transactions is however, provided in **Annexure III**. Suspicious activity monitoring programs should be appropriate to the company and the products it sells.

6.2.9. Reporting of Suspicious Transactions:

In terms of the provisions of section 7 of the FTRA, each company should report suspicious transactions immediately on identification. When such transactions are identified post facto the contract, a statement may be submitted to FIU within 2 working days of identification.

Insurance companies are required to submit STRs via goAML. The following two reports should be submitted in goAML system for STRs:

- Suspicious Transaction Report (STR)
- Persons/Accounts/Entities (PAE) Report (Follow-up report to STR to complete suspicion reporting)

It is important to note that submission of both the above reports (STR & PAE Report) are mandatory for the completion of STR reporting process to the goAML system, for every suspicious transaction, attempted transactions, or information.

Since insurance brokering companies are not reporting via goAML, STRs may be submitted in terms of the Schedule IV of the Suspicious Transactions (Format) Regulations of 2017, published in gazette extraordinary No. 2015/56, dated 21st April 2017.

Failure to identify and report STRs on time or failure to report STRs is punishable under the FTRA.

6.2.10. Monitoring and Reporting of Cash and Cheque Transactions:

In terms of the provisions of section 6 of the FTRA, insurance companies should report to FIU:

(a) any transaction of an amount in cash exceeding such sum as shall be prescribed by the Minister by Order published in the Gazette, or its equivalent in any foreign currency (unless the recipient and the sender is a bank licensed by the Central Bank); and
(b) any electronic funds transfer at the request of a customer exceeding such sum as shall be prescribed by regulation

in such form, manner, and within such period as may be prescribed by Rules issued by the FIU.

With a view to ensuring that premiums are paid out of clearly identifiable sources of funds, it has been decided that remittances of premium by cash should not exceed Rs. 1,000,000 /-. It would be advisable for the companies to evolve even lower thresholds for cash transactions. It is further advised that:

I. Premium/proposal deposits beyond Rs.1, 000,000/- should be remitted only through cheques, demand drafts, credit card or any other banking channels.
II. For integrally related transactions, premium amount greater than Rs.1,000,000/- in a calendar month should be examined more closely for possible angles of money laundering. This limit will apply at an aggregate level considering all the roles of a single person-as a proposer or life assured or assignee.
III. Insurance companies have to report any transactions of an amount in cash transactions (CT) and Electronic Fund Transfers (EFT) exceeding Rs.1,000,000/-or equivalent amount in any foreign currency to the goAML system within 31 days of the transaction's occurrence.

6.2.11. Verification at the time of redemption/surrender:

i. In life insurance business, no payments should be allowed to 3rd parties except in cases like superannuation/gratuity accumulations and payments to legal heirs in case of death benefits. All payments should be made after due verification of the bona fide beneficiary, through account payee cheques.

ii. Free look cancellations need particular attention of companies especially in clients/agents indulging in free look surrender on more than one occasion.

iii. AML/CFT checks become more important in case the policy has been assigned by the policyholder to a third party not related to him (except where the assignment is to Banks/Financial Institutions/Capital Market intermediaries regulated by CBSL/IRCSL/SEC).

6.2.12. Record Keeping:

Each company is required to maintain the records of types of transactions mentioned under Section 4 of Financial Transaction Reporting Act, No. 6 of 2006 and the copies of the Cash/Suspicious Transactions reports submitted to Income tax authorities, FIU and other local government authorities on request as well as those relating to the verification of identity of clients for a period of 06 years.

Please also refer to Rules 54 – 57 of the Insurers CDD Rules in this regard.

i. Sharing of information on customers may be permitted between different organizations such as banks, insurance companies/insurance broking companies, Income tax authorities, and local government authorities on request. Records can also be in electronic form.

ii. Companies should implement specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) to provide, if necessary, evidence for prosecution of criminal activity. In the case of long-term insurance, full documentary evidence is usually retained based on material completed at the initiation of the proposal of the contract, together with evidence of processing of the contract up to the point of maturity.

iii. Companies should retain the records of those contracts, which have been settled by claim (maturity or death), surrender or cancellation, for a period of at least 06 years after that settlement.

iv. In situation 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, companies are requested to seek and retain relevant identification documents for all such transactions and to report the offer of suspicious funds.

v. In case of customer identification data obtained through the customer due diligence process, account files and business correspondence should be retained for at least 06 years after the business relationship is ended.

6.2.13. Compliance Arrangements:

i. A detailed AML/CFT Policy should be drawn up encompassing aspects of Customer acceptance policy, Customer Identification procedure, Monitoring of transactions, Risk management framework as evolved by the company. The policy should have the approval of the Board of Directors. The policy should be reviewed annually and affect any changes based on experience.

ii. Responsibility on behalf of the agents:

The guidelines place the responsibility of a robust AML/CFT program on each insurance company/insurance broking company. Nonetheless, it is necessary that the following steps be taken to strengthen the level of control on the agents engaged by the insurance company/insurance broking company:

a. A list of rules and regulations covering the performance of agents must be put in place. A clause should be added making CDD requirements mandatory, and specific process documents can be included as part of the contracts.

b. The services of defaulting agents who expose the Insurance Company/Broking Company to AML/CFT related risks on multiple occasions should be terminated and the details reported to IRCSL for further action.

c. Insurance Company / insurance broking company when faced with a non-compliant agent should take necessary action to secure compliance, including when appropriate, terminating its business relationship with such an agent.

6.3. Appointment of Compliance Officer:

The Compliance Officer (CO) is required to have a comprehensive understanding of the provisions of the FTRA, Rules, Regulations, Directives, Orders and Guidelines issued thereunder.

6.3.1. Appointment:

In terms of Section 14 of the FTRA it is required to appoint a compliance officer being a senior management level officer, responsible for ensuring institutional compliance within the requirements of the FTRA.

6.3.2. Responsibilities:

The Compliance Officer should ensure the following:

a. Establish and maintain procedures and systems to:
    i. Identify the customers (CDD)
    ii. Record keeping
    iii. Aware of all officers on the relevant laws
    iv. Screen all persons before hiring for employment
b. Implement a system for reporting suspicious activities
c. Establishing of audit functions to test the procedures and systems of the compliance
d. Train the officers or employees and the relevant agents to recognize the suspicious transactions
e. Establish and maintain written internal procedures and systems to screen any designated list on targeted financial sanctions

Please refer to Rule 17 of the Insurers CDD Rules in this regard.

Insurance Brokering companies can appoint a suitable officer in the senior management or the Principal Officer as the Compliance Officer.

6.4. Recruitment and Training of employees/agents

6.4.1. As most of the insurance business is through agents/insurance brokering companies which brings in non-face to face business relationships with the policyholders, the selection process of agents should be monitored carefully. The committee monitoring the agents should monitor sales practices followed by agents and ensure that if any unfair practice is being reported then action is taken after due investigation; Periodic risk management reviews should be conducted to ensure company's strict adherence to laid down process and strong ethical and control environment. Companies should have adequate screening procedures when hiring employees. Instruction Manuals on the procedures for selling insurance products, customer identification, record keeping, acceptance and processing of insurance proposals, issue of insurance policies should be set out.

6.4.2. The concept of AML/CFT should be part of in-house training curriculum for agents.

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

i. New employees: A general appreciation of the background to ML/TF and the subsequent need for identifying and reporting of any suspicious transactions to the appropriate designated point should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority.

ii. 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 Insurer's policy on CDD and verification procedure, specially when dealing with non-regular customers, particularly where large transactions are involved, and the need for extra vigilance in these cases.

iii. Processing staff: Those members of staff who receive completed proposals and cheques for payment of a single premium contribution must receive appropriate training in the processing and verification procedures.

iv. Administration/Operations supervisors and managers: A higher level of instruction covering all aspects of ML/TF procedures should be provided to those with the responsibility for supervising or managing staff including the Board of Directors.

v. Ongoing training: It will also be necessary to make arrangements for refresher training at

regular intervals to ensure that staff do not forget their responsibilities, in order to implement the provisions of the FTRA and any Rules, Regulations, Guidelines made thereunder and internal policies and procedures relating to ML/TF risk management. This might be best achieved by a twelve or six-monthly review of training. The timing and content of training packages for various sectors of staff will need to be adapted by an individual institution for their own needs.

vi. Records of training imparted to staff in the various categories detailed above should be maintained.

6.4.4. The training material should be periodically updated with the latest developments in ML/TF. Please refer to Rule 17 (d) of the Insurers CDD Rules in this regard.

6.5. Internal Control/Audit:

Internal audit/inspection departments of Insurance companies should verify on a regular basis, compliance with policies, procedures and controls relating to AML/CFT activities. The reports should specifically comment on the robustness of the internal policies and processes in this regard and make constructive suggestions where necessary, to strengthen the policy and implementation aspects. Exception reporting under AML/CFT policy should be done to the Audit Committee of the company.

Please refer to Rule 17 (e) of the Insurers CDD Rules in this regard.

Insurance brokering companies may decide on conducting internal audits based on the complexity of the entity.

6.6. Sanction Screening/ Targeted Financial Sanctions

6.6.1 Each company shall verify whether any customer, prospective customer or beneficiary appears on any list of designated persons or entities issued under any regulation made in terms of the United Nations Act, No. 45 of 1968, with respect to any designated list on targeted financial sanctions related to terrorism and terrorist financing and proliferation of weapons of mass destruction and its financing or whether such customer, prospective customer or beneficiary acts on behalf of or under the direction of such designated persons or entities or for the

benefit of such designated persons or entities.

6.6.2 Obligations of each company:

- Not to provide any financial service or make available funds (and other assets) for the usage or benefit of designated persons and their associates.
- Formulate a policy on sanction screening (frequency, systems, alert management, notification channels, etc.) and practically use that policy in daily operations.
- Make the senior management, as well as all the employees of the company aware of the Institution's screening policy.

6.6.3 Obligations during operations:

- When a possible match is found (ID/Passport/exact name/exact address), during onboarding, refrain from accepting any funds and providing any financial services.
- When a possible match is found during trigger screening (upon FIU notification or customer details change), immediately freeze any funds you hold and terminate any financial service.
- When a possible match is found during transaction screening, immediately stop the transaction and freeze any funds you hold with regard to the transaction.
- When you are in doubt, you should immediately verify that from the Competent Authority (CA), which is established under regulation made in terms of the United Nations Act, No. 45 of 1968. You may continue provision of services to the person in question with enhanced due diligence until verified.
- Inform the freezing actions to the FIU and the CA.
- During onboarding, you can mention the designation as the reason for denial of services, as the designation is done publicly (no tipping off would occur).
- For freezing, you can (and should) inform the customer about the freezing after the funds are frozen.
- You should direct the designated person to the CA for any clarifications or further actions (false-positive cases, usage of frozen funds, appeals, etc.).
- You should have mechanism to immediately lift the freeze on funds when:
    - Informed by the CA
    - Delisted by United Nations Security Council (UNSC) or CA

6.6.4 Directives Issued by the Competent Authority:

a. UNSCR 1267 Implementation Practices and Enforcement Obligations, Directives No. 1 of 2013 - In relation to Taliban, ISIL (Da'esh) or Al-Qaida sanction list

b. UNSCR 1373 Implementation Practices and Enforcement Obligations, Directives No. 1 of 2014 – In relation to terrorism and terrorist financing in national level

c. UNSCR 1718 Implementation Practices and Enforcement Obligations, Directives No. 1 of 2019 - In Sanctions in relation to Democratic People's Republic of Korea

d. Directives Issued under the United Nations (Sanctions in relation to Iran) Regulations, No. 1 of 2018

6.6.5 Please refer Rule 58 of the Insurers CDD Rules.

The above guidelines on establishment of an effective AML/CFT regime would be effective immediately.

The Guidelines issued in 2006 is hereby repealed with immediate effect.

Annexure I

Vulnerable Products:

1. Linked long-term products which provide for withdrawals and unlimited top up premiums;
2. Single premium products-where the money is invested in lump sum and surrendered at the earliest opportunity;
3. Free look cancellations-especially the big ticket cases;
4. Insurance products that provide loan facilities;

Note: The list is only illustrative and not exhaustive

Annexure II

Income Proofs

Standard Income proofs:

Income tax assessment orders/Income Tax Returns

Employer's Certificate

Audited Company accounts

Audited firm accounts and Partnership Deed

Non-standard Income Proofs:

Chartered Accountant's Certificate

Bank Cash-flows statements

Pass-book

Note: The list is only illustrative and not exhaustive

Annexure III

Illustrative list of Suspicious Transactions:

1. Customer insisting on anonymity, reluctance to provide identifying information, or providing minimal, seemingly fictitious information
2. Cash based suspicious transactions for payment of premium and top ups over and above Rs.1,000,000/- per person per month.
3. Frequent free look surrenders by customers;
4. Assignments to unrelated parties without valid consideration;
5. Request for a purchase of policy in amount considered beyond his apparent need;
6. Policy from a place where he does not reside or is employed;
7. Frequent request for change in addresses
8. Inflated or totally fraudulent claims e.g. by arson or other means causing a fraudulent claim to be made to recover part of the invested illegitimate funds
9. Overpayment of premiums with a request for a refund of the amount overpaid.
10. Funds originating from a suspicious organization/individual (known terrorist front organizations, shell companies etc.) or a customer suspected of having terrorist links
11. Customer providing forged documents
12. Adverse news on media on predicated offenses of ML
13. Customers with ongoing court case/ police investigations
14. Frequent transactions below reporting threshold
15. Large, unexplained premium payments – when a policyholder makes unusually large premium payments without a clear source of funds.
16. Cash payments – policies purchased with cash or through third parties, especially in high amounts, are often indicators of ML.
17. Purchase of large single premium insurance - Suspicion is warranted when customers buy insurance contracts with a single large premium payment, especially if unusual payment methods like cash or cash equivalents are employed.
18. Disproportionate premium payment - Purchasing a single premium policy with cash, money orders, traveler's cheques, or cashier's cheques for an amount significantly disproportionate to the customer's income is suspicious.

19. Offshore premium payments - Entering into a substantial insurance contract with premiums paid from abroad, particularly from offshore financial centers, can raise red flags.
20. Third-party premium payments – payments made by a third party who is not the policyholder may be an attempt to obscure the true source of funds.
21. Unknown Source of Funds - Suspicion is raised when customers purchase insurance products with termination features using unknown or unverifiable sources of funds, such as cash, sequentially numbered money orders, traveler's cheques, and cashier's cheques.
22. Frequent policy changes – frequent alternations to a policy, such as increasing the death benefits or changing the beneficiary, may suggest an attempt to obscure the true nature of the policy.
23. Changing beneficiary without apparent connection - Changing the initial beneficiary during the life of the policy without an apparent connection to the policyholder can be suspicious.
24. Transferable ownership interests - Suspicion is warranted when policies allow the transfer of ownership interests without the insurance issuer's knowledge or consent, including secondhand endowment and bearer insurance policies
25. Unclear beneficial ownership – in situations where the true owner or beneficiary is not easily identifiable, further scrutiny may be necessary. Suspicion arises when there are indications or certainties that the involved parties are not acting on their own behalf and are attempting to conceal the identity of the actual customer.
26. Unusual policyholders – policies owned by shell companies, trusts or individuals with no obvious connection to the insured can be suspected.
27. Complex ownership structures – policies owned by complex corporate structures or chains of ownership can be used to obfuscate the beneficial owner.
28. Transactions involving tax havens or risk territories - Suspicion arises when transactions involve legal persons or arrangements domiciled in tax havens or high-risk regions, as these locations can be used to conceal financial activities.
29. Large transactions by recently created legal entities - Suspicion is warranted when recently established legal entities engage in large transactions that are disproportionate to their declared assets, as this may indicate an attempt to move or launder significant funds.
30. Policies in the name of minors – policies owned by or for minors that involve large sums of money may be used to launder funds.
31. Multiple small policies – money launderers may try to avoid detection by purchasing multiple small policies instead of one large one.
32. Sudden cancellation – a policy that is abruptly canceled after a short period may indicate a scheme to legitimize illicit funds. Cancelling an insurance contract and directing and the funds to a third party can indicate suspicious activity. A potential policyholder is more interested in a policy's cancellation terms than its benefits.

33. Disregarding tax or cancellation charges - Cancelling an insurance contract without concern for substantial tax or cancellation charges can indicate potential ML.
34. Repeated account opening - Suspicion arises when customers repeatedly open and close accounts with the same insurance company but under new ownership information.
35. Frequent policy lapses – policies that are frequently allowed to lapse without reason can indicate an attempt to launder money.
36. Lack of insurable interest – if there's no legitimate insurable interest between the policyholder and the insured, it could be a sign of ML.
37. No personal interaction – lack of any personal interaction with the insured, especially in cases of stranger-owned life insurance can be suspicious.
38. Inconsistent or missing documentation – discrepancies in the documentation submitted for policy applications, like identity documents or financial records, should raise concerns.
39. Securing policy loan and repaying with cash or monetary instruments - Suspicion arises when customers secure a policy loan against the cash value of a life insurance
40. policy shortly after the policy is issued and repay the loan with cash or various monetary instruments.
41. Frequent policy loans - Suspicion is warranted if the customer obtains policy loans frequently and settles them within a short interval.
42. Repaying the policy loans using a third party - repayments of the policy loans are made by third parties and/or using methods to which the customer might not have proper authorization such as corporate credit cards.

Note: The list is only illustrative and not exhaustive.