UNIVERSAL SIMPO GENERAL INSURACNE

ANTI-MONEY LAUNDERING (AML) POLICY AND GUIDELINESVERSION 4.0

Document Summary	
Authorisation, Ownership and Document Control	
Owner	Legal & Compliance Department shall be owner of this Policy
Approver and Date	Board
Validity of the Policy	This Policy shall be valid till the same is modified or revoked by the Board of Directors.
Periodicity of Review	This Policy should normally be reviewed annually
Effective Date	Date of approval

Review History			
Version	**Author**	**Date of Approval**	**Approved by**
4.0	**Chief Compliance Officer**	**8th August 2024**	**Board**
3.0	**Legal& Compliance Department**	**6th February 2024**	**Board**
2.0	**Legal & Compliance Department**	**3rd February 2023**	**Board**
1.14	**Legal & Compliance Department**	**23rd March,2022**	**Board**
1.13	**Legal & Compliance Department**	**11th May, 2021**	**Board**

1.12	**Legal & Compliance Department**	**10th December, 2020**	**Board**
1.11	**Legal & Compliance**	**23/07/2019**	**Board**

Table of Contents

1. Introduction

Money Laundering is a generic term used to describe any process that conceals the origin or derivation of the proceeds of crime so that they appear to have been derived from a legitimate source; it involves moving illegally acquired cash through financial systems so that it appears to be legally acquired. Driven by illegal activities, money laundering conceals the true source, ownership, or use of funds. This poses a serious threat to the financial systems of all countries, leading to the destruction of the sovereignty and character of the Company. Recognized at the international level, concerted efforts worldwide have been made to combat this ultra-criminal activity through stringent laws, regulations, and measures aimed at securing financial systems. A concrete step at the global level is the Financial Action Task Force (FATF), constituted in 1989.

In alignment with international efforts, the Prevention of Money Laundering Act (PMLA), enacted in 2002 and effective since July 2005, applies to all financial institutions, including insurance companies. Regulatory agencies emphasize the importance of Anti-Money Laundering (AML) measures for non-bank institutions, especially insurance companies, as a strong AML program is a core recommendation by FATF. The Insurance Regulatory and Development Authority of India (IRDAI), via circular IRDAI/IID/GDL/MISC/160/8/2022 dated August 1, 2022, issued Master Guidelines on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT), 2022, advising all insurance companies to establish a proper policy framework on AML/CFT. The adoption of this policy by Universal Sompo General Insurance aims to increase awareness of money laundering activities and their ill effects while contributing significantly to countering money laundering, including ensuring vigilance against such activities at all times. Good compliance is best facilitated by a willing adoption of best practices, which Universal Sompo General Insurance aims to implement through this policy.

2. Definitions

In these policies, unless the context otherwise requires, the terms herein shall bear the meanings assigned to them as below:

2.1	"Aadhaar Number"	Aadhaar Number shall have the meaning assigned to it under clause(a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, hereinafter referred to as „The Aadhaar Act".
2.2	"Act"	Act shall mean the Prevention of Money-Laundering Act, 2002.
2.3	"Authentication"	Authentication shall mean the process as defined under clause (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 as amended from time to time.

2.4	"Authority" or "IRDAI"	Authority or IRDAI shall mean the Insurance Regulatory and Development Authority of India established under sub-section 1 of Section 3 of the IRDA Act 1999.
2.5	"Beneficial Owner"	"Beneficial owner" shall have the same meaning as defined under sub clause (fa) of clause (1) of Section 2 of the PML Act.
2.6	"Board"	Board shall mean, the Board of Directors of Universal Sompo General Insurance.
2.7	"Central KYC Records Registry"	(CKYCR) means an entity defined under clause (ac) of sub rule (1) of Rule 2 of the PML Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.
2.8	"Client"	Client shall have the same meaning as defined under sub clause (ha) of clause (1) of Section 2 of the PML Act. The term client includes a customer/ person (Natural or Juridical) who may be a proposer or policyholder or master policyholder or assured or beneficiaries or assignees, as the case may be.
2.9	"Client Due Diligence"	Client Due Diligence(CDD) shall have the meaning assigned to it under sub clause (b) of clause (1) of Rule 2 of the PML Rules.
2.10	"Company"	Company for the purpose of this Policy shall mean the Universal Sompo General insurance.
2.11	"Designated Director"	Designated Director shall have the meaning assigned to it under sub clause (ba) of clause (1)of Rule 2 of the PML Rules.
2.12	"Digital KYC"	Digital KYC shall have the meaning assigned to it under sub clause (bba) of clause (1) of Rule 2 of the PML Rules.
2.13	"KYC Templates"	KYC Templates means templates prepared to facilitate collating and reporting the KYC datato the CKYCR, for individuals and legal entities.
2.14	"Policy" or "Anti-Money Laundering Policy"	Policy or Anti Money Laundering Policy shall mean this present Policy of the Company on Anti-Money Laundering.
2.15	"Principal Officer"	"Principal Officer" shall have the same meaning as defined under sub clause (f) of clause (1) of Rule 2 of the PML Rules. means an officer designated by the reporting entity who should be an officer at the management level

2.16	"Rule"	Rule shall mean the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

3. Rationale of the Policy

3.1 Money Laundering (ML) is the process which criminals engineer to cover the real origin and ownership of dirty or illegal money emanating from criminal illegal activities, and thereby render the prosecution and confiscation of funds so generated, impossible.

3.2 The rationale, therefore, would be to reflect the global resolve to prevent and fight Money Laundering (ML) activity, by establishing governing standards to insulate the Company from being used as a component of the financial system to launder money.

4. Applicability

This policy shall be applied to all the Branches and Offices of the Company. The Policy is drawn in line with the IRDAI Master Guidelines on Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT), 2022 issued by IRDAI on August 1, 2022 and amendments thereon made by PML act 2002.

5. Objectives

In the light of above, the objectives of AML Policy have been laid down as enumerated below:

5.1 Enable the Company to conduct clean, commercial business, conforming to standards set by IRDAI.

5.2 Enable the company to establish and implement policies, procedures and internal controls, which outline the actions to be undertaken by relevant employees/agents/intermediaries to prevent ML and FT while discharging their functional responsibilities;

5.3 To follow the internationally accepted standards used for KYC compliance.

5.4 To report and take suitable action upon detecting the suspicious activity involving shades of money laundering as directed by regulators from time to time.

5.5 To comply with applicable laws in India with reference to ML and adhere to standards accepted internationally.

The policy envisages AML aspects on the lines of recommendations given by Financial Action Task Force & IRDAI.

6. Money Laundering

6.1 Money Laundering activity is an involvement in any transactions/or series of transactions that is designed to disguise the nature/source of proceeds derived from illegal activities, which may comprise drug trafficking, terrorism, organized crimes, murders, fraud, etc.

6.2 The formal name of this rule is "Law about checking customer's identification by the financial institution.

6.3 There are three common stages of Money Laundering as detailed below which are resorted to by the launderers. The company may unwittingly get exposed to a potential criminal activity while undertaking normal business transactions. It is important for all staff members to be conversant and be absolutely familiar with the ML process (described below) as they must be vigilant all the time and should any ofthe aspects involved in ML process touch/surface our business they must be able to read the danger signaland blow the whistle.

6.3.1 Placement:

The first stage is successfully disposing of the physical cash received through illegalactivity. The

crooks accomplish this by placing this into traditional or non-traditional financialinstitutions

6.3.2 Layering:

The second stage concentrates on separation of proceeds from criminal activity through the use of various layers of monetary transactions. These layers are aimed at wiping audit trails, disguising the origin and maintaining anonymity for people behind the transactions.

E.g.: Fraudulent letters of credit transactions, over invoicing for goods transshipped from another country, using high value credit cards to pay for goods/services and accounting for the creditcard invoices with balances held in offshore banking secrecy havens.

6.3.3 Integration:

The final link in the money laundering process is called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency with a legitimate reason for querying the existence of money.

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.

Therefore, the Company should authorize a Principal Officer who shall bear the statutory duty to make a disclosure to the authorized officer on 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/ is intended to be used in that connection, is passing through the institution.

7. AML/ CFT Program

7.1 In order to discharge the statutory responsibility to detect possible attempts of money laundering or financing or terrorism, the Company needs to have an AML/ CFT program compromising of Internal policies procedures and controls. The AML/CFT program (Policy) needs to be reviewed and approved by the Board annually.

7.2 The AML/CFT policy needs to be communicated to all levels of management and relevant staff handling policyholder's information. The Procedures, SOPs & Office Orders shall be reviewed annually by the Chief Compliance Officer.

7.3 In case there is a variance in Client Due Diligence or AML/CFT standards specified by IRDAI, and the standards specified by regulators of the host country, foreign branches/majority-owned subsidiaries of the company shall adopt the more stringent requirements of the two. If the host country does not permit the proper implementation of AML/CFT measures consistent with the home country requirements, the company shall apply appropriate additional measures to manage the Money Laundering /Terrorist Financing risks and inform the Authority.

8. Responsibility of the Company

The guidelines place the responsibility of compliance on the Company. Nonetheless, it is necessary that the following steps are taken to strengthen the level of control on the intermediaries/representative of company engaged by the Company:

8.1 **Intermediaries/ representative of company engaged-**

a. The rules and regulations covering performance of intermediaries /representative of company must be put in place in the underlying contract. A clause should be added makingKYC norms mandatory and specific process documents can be included as part of the contracts.

b. Appropriate actions to be taken against defaulting intermediaries /representative of company who expose the Company to AML/CFT related risks on multiple occasions.

c. The selection process of intermediaries /representative of company should be monitored

scrupulously in view of set AML/CFT measures at the time of their onboarding.

8.2 **Compliance Certificate:**

An annual compliance certificate as prescribed in the IRDAI master guidelines needs to be submitted to the Authority within 45 days of the end of the Financial Year.

8.3 **Appointment of Designated Director**

a. A "Designated Director", who has to ensure overall compliance with the obligations imposed shall be appointed or designated by the company. The Managing Director shall be "Designated Director" ex-officio.

b. The contact details with mobile number and email id of the Designated Director and the Principal Officer or any changes thereon shall be communicated to Insurance Regulatory and Development Authority of India (IRDAI) and FIU-IND within 7 days of its effect.

8.4 **Appointment of Principal Officer:**

8.4.1 Appointment:

a. The Company shall appoint an official of senior cadre with sufficient operational experience and an investigative mind as the Principal Officer (PO). He would have the necessary freedom to act on his own authority and should report to the Managing Director.

b. Principal 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.

c. **Mr Sameer Patwardhan, Chief Compliance Officer** of the Company, has been designated as the PrincipalOfficer (PO).

Email Id: sameer.patwardhan@universalsompo.com

d. The Principal Officer shall ensure that the Board reviews and approves the AML Program. He shallalso report to the Board on its effective implementation.

8.4.2 Rights and Responsibilities:

a. The PO's role would be to maintain controls and procedures aimed at deterring criminal elements from using the products and services of the C om pa ny and implement this policy including monitoring compliance by the company's insurance agents with their obligations under the program.

b. He will also be instrumental in adhering to KYC principle and effective customer identification and should provide necessary guidance to operating staff.

c. His vigilance in computerized and non-computerized transactions and track patterns would be important.

d. He shall keep himself abreast of all latest developments in AML area in other organizations and countries and effect the changes in AML measures suitably to improve AML exercise. He shall ensure that employees /TPA's and other intermediaries of the insurance company have appropriate resources and are well trained to address questions regarding the application of the program in light of specific facts.

e. PO will:

i. Maintain up-to-date list of high-risk countries,

ii. Identify for the Company, the high, moderate and low risk activities from AML angle.

iii. Identify unusual transactions.

f. Depending on the Suspicious Transaction Report (STR), he shall co-ordinate with senior management to decide on continuing account relationship with increased caution/alert. In this context, on being satisfied that the transaction is suspicious, he would decide to furnish the information promptly in writing by fax or by electronic mail to the Reporting Authority (FIU) for the necessary actions.

g. PO will report to MD once in half-year, the progress and status of the AML measures in vogue and improvements & findings and Company's on-going preparedness on AML activity. The PO function is crucial and important, and a suitable person has to be designated.

8.5 Recruitment and Training

The concept of AML shall also be part of the induction training to the employees and in- house training curriculum for agents. The Company shall have adequate screening procedures while hiringemployees.

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

8.5.1 New employees training:

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 involved in the transactions, irrespective of the level of seniority and their area of operation.

8.5.2 Front Line staff training:

Members of staff who deal 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.

8.5.3 Those members of staff who interacts with the proposer/customer and receive completed proposals, KYC documents and cheques for payment of premium, requests of payment of Claims will be given appropriate training in the processing, KYC and verification procedures. They shall be specially trained to handle issues arising from lack of customer education.

8.5.4 Administration/Operations/Compliance supervisors and managers training: A higher level of instruction and training covering all aspects of money laundering procedures will be provided to those with the responsibility for supervising or managing staff.

8.5.5 Ongoing training: Annual refresher training will be provided to ensure that staff do not forget their responsibilities and also apprise them of any new developments / requirements. However, in the event of any major regulatory change additional refresher training will be conducted. Timing and content of training packages for various sectors of staff will be prepared in consultation with in-house and outsourced expertise. The overall training modules pertinent to PML would be reviewed at 6–12-month intervals.

8.5.6 Sales/ Advisory staff: The HR Department shall coordinate and maintain records of training materials and training imparted to staff in the various categories detailed above.

9. Internal Control/Audit

9.1 The Internal audit Department of the Company shall periodically verify compliance with the extant policies, procedures and controls related to money laundering activities on the basis of overall risk assessment. The Company shall also upgrade its questionnaire and system from time-to-time in accordance with the extant PMLA and PML Rules. 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. The Company shall submit audit notes and compliance to the Audit Committee.

9.2 Internal Audit department shall ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front-line staff, of their responsibilities in this regard. The internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

9.3 Internal audit shall verify on a regular basis compliance with policies, procedures periodic MIS on suspicious and Cash Transactions and controls relating to money laundering activities. The reports shall 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 policy shall be reported to Audit Committee of the Board periodically.

10. Customer Acceptance Policy (CAP)

10.1 No policy shall be issued in anonymous or fictitious/ benami name(s) and customers shallbe accepted only after verifying their identity and address, as laid down in Customer Identification Procedures. No transaction or account-based relationship shall be undertaken without following Customer Due Diligence (CDD) procedure as laid down below.

10.2 Parameters of risk perception as defined by the Company to be followed to classify customers as low and high risk keeping in view customer's identity, the nature of asset insured and mode of premium payment.

10.3 The Company shall not issue any policy or renew an existing policy when the Companyis unable to apply appropriate CDD measures due to non-cooperation of the customer or non-reliability of the data/information furnished.

10.4 It should be ensured that insurance coverages are not extended to any person or entity, whose name appears in the sanctions lists issued by UN Security Council (UNSC) and/orMinistry of Home Affairs (MHA) or any other list/negative list notified by the CompetentAuthority from time to time.

11. Customer Identification Procedure (CIP)

11.1 The Company shall verify the customers' identity by using reliable and authentic sources of documents, data or information to ensure that the insurance contracts are not under anonymous or fictitious names.

11.2 The Company shall determine the beneficial ownership and controlling interest in case of applicants who are not individuals, and the KYC of the beneficial owners shall be completed at claim stage.

11.3 For the purpose of verifying the identity of customers at the time of commencement of account-based relationship, the company shall at their option, rely on customer due diligence done by third party. The ultimate responsibility for customer due diligence and enhanced due diligence measures, as applicable, will be with the Company.

12. Know your Customer Norms (KYC)

12.1 Effective procedures should be put in place to obtain requisite details for proper identification of new/ existing customer(s). Special care has to be exercised to ensure that the contracts are not under anonymous or fictitious names.

12.2 Where a client is a juridical person, Company shall take steps to identify the client and its beneficial owner(s) and take all reasonable measures to verify his/her identity to their satisfaction so as to establish the beneficial ownership. Procedures for determination of Beneficial Ownership shall be as prescribed in the AML SOP read along with sub rule (3) of Rule 9 of PML Rules.

12.3 While implementing the KYC norms on juridical persons, Company will have to identify and verify their legal status through various documents as indicated in the company internal SOP read with sub-rule (6) to (9) of rule 9 of the PML Rules), to be collected in support of

12.3.1 The name, legal form, proof of existence,

12.3.2 Powers that regulate and bind the juridical persons,

12.3.3 Address of the registered office/ main place of business,

12.3.4 Authorized individual person(s), who is/ are purporting to act on behalf of such client, and

12.3.5 Ascertaining Beneficial Owner(s): No reporting entity shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

12.4 While implementing the KYC norms on juridical person the Company shall verify that any person purporting to act on behalf of such client is so authorised and verify the identity of that person.

12.5 Where a client is an individual person, the Company shall verify the identity, address and recent photograph in order to comply with the provision as specified in sub rule (4) of Rule 9 of the PML Rules.

12.6 No further documentation is necessary for proof of residence where the document of identity submitted also includes the proof of residence/address.

12.7 Where a customer submits Aadhaar for identification and wants to provide a current address different from the address available in the Central Identities Data Repository, the customer may give a self-declaration to that effect to the company.

12.8 Under Individual Policies, those individuals who are not able to undergo Aadhaar Authentication due to any injury, illness or old age or otherwise, or they do not wish to go for Aadhaar Authentication, they may submit their Officially Valid Documents (OVDs) at the time of commencement of Account based relationship.

12.9 Where there is no change in KYC information at the time of periodic updation and the existing documents are compliant with the extant PML Rules, then self-declaration of no change in KYC information may be obtained remotely from customer using registered email or SMS message or digital channels (such as mobile application, online portal) etc. to complete the updation process.

12.10 In case of change in KYC information of customers who were on-boarded as per the currently applicable Client Due Diligence requirements, scanned or digital documents, indicating changed KYC information, may be obtained. However, such scanned or digital documents should be furnished through secure online means such as mobile application, online portal, registered email id, etc.

12.11 **Company may perform KYC process by any of the following methods:**

12.11.1 Aadhaar based KYC through Online Authentication subject to notification by the Government under section 11A of PMLA Or

12.11.2 Aadhaar based KYC through offline verification Or

12.11.3 Digital KYC as per PML Rules Or

12.11.4 Video Based Identification Process (VBIP) as consent based alternate method of establishing the customer's identity, for customer or VBIP Or

12.11.5 By using KYC identifier" allotted to the client by the CKYCR Or

12.11.6 By using Officially Valid documents

12.11.7 PAN/Form 60 (wherever applicable) and any other documents as may be required by the company

12.12 Under all kinds of Group Insurance (General/Health), KYC of Master Policyholders / Juridical

Person / Legal Entity and the respective Beneficial Owners (BO) shall be collected. However, the Master Policyholders under the group insurance shall maintain the details of all the individual members covered, which shall also be made available to the Company as and when required.

12.13 Customer information should be collected from all relevant sources, including from agents/intermediaries.

12.14 Care must be exercised to avoid unwitting involvement in insuring assets bought out of illegal funds. It is imperative to ensure that the insurance premium should not be disproportionate to income/ assets.

12.15 At any point of time, where Company are no longer satisfied about the true identity and the transaction made by the customer, a Suspicious Transaction Report (STR) should be filed with Financial Intelligence Unit-India (FIU-IND) if it is satisfied that the transaction meets the criteria specified in sub clause (g) of clause (1) of Rule 2 of the PML Rules and any guidelines / indicators issued by IRDAI or FIU-IND.

12.16 **Client Due Diligence (CDD)**

Company shall undertake CDD as per the applicable provisions. Accordingly, the company shall undertake CDD as follows:

12.16.1 **Knowing New Customer/ Client**

In case of every new customer, necessary Client due diligence with valid KYC documents of the customer/ client shall be done at the time of commencement of account-based relationship.

12.16.2 **Knowing Existing Customer/Client**

a. The AML/ CFT requirements are applicable for all the existing customers/ clients. Hence, necessary Client due diligence with KYC (as per extant PML Rules) shall be done for the existing customers fromtime-to-time basis the adequacy of the data previously obtained such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients

b. In case of non- availability of KYC of the existing clients as per the extant PML Rules, the same shall be collected within 2 years for low-risk customers and within 1 year for other customers (including highrisk customers).

c. For continued operation of accounts of existing customers having insurance policy of not more than aggregate premium of Rs. 50,000/- in a financial year, PAN/Form 60 may be obtained by such date as may be notified by the Central Government.

12.16.3 **Ongoing Due Diligence**

a. Besides verification of identity of the customer at the time of initial issuance of contract, Risk Assessment and ongoing due diligence should also be carried out (if so required) at times when additional/ subsequent remittances are made.

b. Any change which is inconsistent with the normal and expected activity of the customer should attract the attention of the Company for further ongoing due diligence processes and action as considered necessary.

12.16.4 **Verification at the time of payout/claim stage (redemption/surrender/partial withdrawal/ maturity/ death/ refunds/reimbursement etc.)**

a. In insurance business, no payments should be allowed to third parties except as provided in the contract or in cases like superannuation/ gratuity accumulations and payments to beneficiaries/ legal heirs/assignees in case of death benefits.

b. Necessary due diligence should be carried out of the policyholders / beneficiaries/ legal heirs/ assignees, including beneficial owner, if any, before making the pay-outs. The company shall take reasonable measures to identify and verify the identity of the

beneficial owner of the beneficiary including Enhanced Due Diligence, if required, in case the Company determine that a beneficiary presents a higher risk, at the time of payout.

c. Necessary due diligence become more important in case the policy has been assigned by the policyholder to a third party not related to him (except where insurance policy is assigned to Banks/ FIs/ Capital market intermediaries regulated by IRDAI/RBI/ SEBI or Marine cargo insurance policies). Notwithstanding the above, Company shall be 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, necessary due diligence will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

d. Where company forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND."

13. Risk Assessment/ Categorization

13.1 The Guidelines require the Company to classify the customer into high risk and low risk based on the profile of the individual and product profile. The Guidelines further requires the Company to identify, assess, document and take effective measures to mitigate ML and TF risk for customers or geographic areas, products, services, nature and volume of transactions or delivery channels etc. as according to sub rule (13) of Rule 9 of PML Rules. The Guidelines also specify illustrative category of customers for classification purposes.

13.2 The majority of general insurance business is based on indemnity, wherein there is no investment component in the insurance contracts offered by general/health insurance companies and the payment is made at the time of claim(s) which not only is based on occurrence of the insured contingent event but also to the extent of actual loss suffered. Further, motor and health insurance constitute more than 50% of general insurance business and majority of claims are settled on cashless basis whereby the claim payment is directly made to the network hospital providers and/or garages, as the case may. All the claims are examined with respect to admissibility as per the terms of insurance policy and entitlement of the intended beneficiary.

13.3 The susceptibility of general insurance business to money laundering is minimal and the premium is highly disproportionate to the sum insured. Further, the vulnerability of customers on the basis of occupancy (ies) may not be relevant and suitable for the general insurance business.

13.4 Keeping in view the above, general insurance business is classified as low risk from an AML point of view, it will be appropriate to undertake risk categorization on the basis of underlying asset, quantum of sum insured and mode of premium payment apart from specified category of customers which may pose higher risk.

13.5 Basis of categorization:

13.5.1 Underlying asset

a. Type of asset (hypothecated or non-hypothecated)
b. When was the asset purchased and
c. Overall quantum of premium paid by the customer

13.5.2 Mode of Payment

a. Mode or multiple modes of payment of premium

13.5.3 Type of Customer

a. PEP
b. Residential status

14. **Simplified Due Diligence (SDD)**

14.1 Simplified measures as provided under sub clause (d) of clause (1) of Rule 2 of PML Rules are to be applied by the company in case of individual policies, where the aggregate insurance premium is not more than Rs 10000/ - per annum.

14.2 However, Simplified Client Due Diligence measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing or where specific high-risk scenarios apply, based on the Risk Assessment/categorization policy of the Company. Based on the robust risk assessment, Company may apply Simplified Due Diligence measures only in respect of customers that are classified as 'low risk'.

15. **Enhanced Due Diligence (EDD)**

15.1 Enhanced Due Diligence as mentioned in Section 12AA of PML Act. shall be conducted for high-risk categories of clients.

15.2 Company should examine, as far as reasonably possible, the background and purpose of all complex, unusual patterns of transactions, which have no apparent economic or lawful purpose.Where the risks of money laundering or terrorist financing are higher, Company should be required to conduct enhanced due diligence measures, consistent with the risks identified.

15.3 Company shall

15.3.1 Verify the identity of the clients preferably using Aadhaar subject to the consent of customer or;

15.3.2 Verify the client through other modes/ methods of KYC as specified in these guidelines.

15.4 Company shall examine the ownership and financial position, including source of the funds of the Client commensurate with the assessed risk of customer and product profile.

16. **Sharing KYC Information with Central KYC Registry (CKYCR)**

16.1 Government of India has notified the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI), to act as, and to perform the functions of the CKYCR vide Gazette Notification No. S.O. 31103(E) dated November 26, 2015.

16.2 Where a customer submits a “KYC identifier” for KYC, the Company shall retrieve the KYC records from CKYCR. In such case, the customer shall not submit the KYC records unless there is a change in the KYC information required by Company as per Rule 9(1C) of PML Rules.

16.3 If the KYC identifier is not submitted by the client / customer, the Company shall search (with certain credentials) for the same on CKYCR portal and record the KYC identifier of the client/ customer, if available.

16.4 If the KYC identifier is not submitted by the client/customer or not available in the CKYCR portal, company shall capture the KYC information in the prescribed KYC Template meant for „Individuals“ or „Legal Entities“, as the case may be.

16.5 Company shall file the electronic copy of the KYC records of the Client with CKYCR within 10 days after the commencement of account-based relationship with a client/ Customer (both Individual/ Legal Entities).

16.6 Once “KYC Identifier” is generated/ allotted by CKYCR, the Company shall ensure that the same is communicated immediately to the respective policyholder in a confidential manner, mentioning its

advantage/ use to the individual/legal entity, as the case may be.

In order to increase awareness and usage of Central KYC Records Registry for KYC following measures should be taken:

16.6.1 A one -time exercise shall be undertaken to inform the existing customers about their KYC Identifiers (CKYCR Identifier) through email/SMS messages, etc.

16.6.2 Display the KYC Identifier of a customer whenever he/she accesses any financial service online through internet portal, mobile application, etc. CKYCR Identifier may also be displayed on the policy of the customer.

16.7 The following details need to be uploaded on CKYCR if Verification/Authentication is being done using Aadhaar:

16.7.1 For online Authentication,

a. The redacted Aadhar Number (Last four digits)

b. Demographic details

c. The fact that Authentication was done

16.7.2 For offline Verification

a. KYC data
b. Redacted Aadhaar number (Last four digits)

16.8 At the time of periodic updation, it is to be ensured that all existing KYC records of individual/legal entity customers are incrementally uploaded as per the extant CDD standards. Company shall upload the updated KYC data pertaining to in force /paid-up policies against which "KYC identifier" are yet to be allotted/generated by the CKYCR.

16.9 Company shall not use the KYC records of the client obtained from Central KYC Records registry for purposes other than verifying the identity or address of the client and should not transfer KYC records or any information contained therein to any third party unless authorized to do so by the client or IRDAI or by the Director(FIU-IND).

17. Reliance on Third Party KYC

17.1 For the purposes of KYC norms under clause (Know Your Customer), while Company are ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable, Company may rely on a KYC done by a third party subject to the conditions -specified under sub-rule (2) of rule (9) of the Rules.

17.2 Where the Company relies upon third party which is a part of the same financial group, then they should obtain KYC documents or the information of the client due diligence within 15 days.

18. **Contracts with Politically Exposed Persons (PEPS)**

18.1 It is emphasized that proposals of Politically Exposed Persons (PEPs) in particular requires examination by senior management.

18.2 Company shall lay down appropriate on-going risk management procedures for identifying and applying enhanced due diligence measures on an on-going basis to PEPs and customers who are family members, close relatives/associates of PEPs. These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner(s).

18.3 If the on-going risk management procedures indicate that the customer or beneficial owner(s) is found to be PEP, or subsequently becomes a PEP, the senior management should be informed on this business relationship and apply enhanced due diligence measures on such relationship.

18.4 Company shall take reasonable measures to establish the source of wealth, and the source of funds of customers and beneficial owners identified as PEPs.

19. New Business Practices/Developments

19.1 Company shall pay special attention to money laundering threats that may arise from

19.1.1 Development of new products

19.1.2 New business practices including new delivery mechanisms

19.1.3 Use of new or developing technologies for both new and pre- existing products.

19.2 Company shall undertake ML/TF risk assessment prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks.

19.3 Special attention should especially, be paid to the „non-face-to-face" business relationships brought into effect through these methods.

19.4 Company should lay down systems to prevent the misuse of money laundering framework. Safeguards will have to be built to manage typical risks associated in these methods like the following:

19.4.1 Ease of access to the facility;

19.4.2 Speed of electronic transactions;

19.4.3 Ease of making multiple fictitious applications without incurring extra cost or the risk of detection;

19.5 The extent of verification in respect of such, non-face-to-face" customers will depend on the risk profile of the product and that of the customer.

19.6 Company shall have in place procedures to manage specific increased risks associated with such relationships e.g. verification of details of the customer through on-site visits.

20. Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA): -

20.1 The Company shall periodically check the Ministry of Home Affairs (MHA) website for an updated list of banned entities.

20.2 A list of individuals and entities subject to United Nations (UN) sanction measures under United Nations Security Council (UNSC) Resolutions (hereinafter referred to as "designated individuals/ entities") would be circulated to the insurers through/ General Insurance Council, on receipt of the same from the Ministry of External Affairs (MEA). This is in addition to the list of banned entities compiled by MHA that have been circulated to the insurers to date.

20.3 The Company should maintain an updated list of designated individuals/entities in electronic form and run a check on the given parameters on a regular basis to verify whether designated individuals/entities are holding any insurance policies with the insurers.

21. Contracts emanating from countries identified as deficient in AML/CFT regime

21.1 The Company shall conduct enhanced due diligence while taking insurance risk exposure to individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime.

21.2 Go beyond the FATF statements and consider publicly available information when identifying countries which do not or insufficiently apply the FATF Recommendations while using the FATF Public Statements, being circulated through the / General Insurance Council.

21.3 The Company shall take similar measures on countries considered as high risk from terrorist financing or money laundering perspective based on prior experiences, transaction history or other factors (e.g., legal considerations, or allegations of official corruption).

21.4 Agents/intermediaries/ employees shall be informed to ensure compliance.

22. Reporting Obligations

22.1 The Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML Rules in terms of Rule 7 thereof.

22.2 Director, FIU-IND shall have the power to issue guidelines for detecting transactions, direct the form and procedure for furnishing information, as per the Third Amendment Rules notified on September 22, 2015.

22.3 The Company shall take note of the reporting formats and guides released by FIU-IND and use the Report Generation Utility and Report Validation Utility to prepare reports.

22.4 The Company shall utilize the editable electronic utilities provided by FIU-IND for filing electronic Cash Transaction Reports (CTR) and Suspicious Transaction Reports (STR) if they lack suitable technological tools.

22.5 Principal Officers of the Company with non-computerized branches shall arrange to extract transaction details and feed them into electronic files using FIU-IND's utilities available at http://fiuindia.gov.in.

22.6 The illustrative list of suspicious transactions as shared by Authority through the /General Insurance Council shall be considered and also the Red Flag Indicators issued by FIU-IND

22.7 Delays in reporting or rectifying misrepresented transactions beyond the specified time limit shall be treated as separate violations.

22.8 The Company shall not restrict operations in accounts where an STR has been filed and shall keep the filing of an STR strictly confidential to avoid tipping off the customer.

22.9 Robust software shall be used to generate alerts when transactions are inconsistent with the risk categorization and updated customer profiles.

22.10 The Company shall leverage the broadest number of data points/records to implement alert generation systems for identifying and reporting suspicious activities and shall avoid arrangements with unregulated entities that could impair their reporting obligations.

23. Record Keeping

23.1 The Company along with its Designated Director, Principal Officer, and employees shall maintain records of all transactions and verification of client identity for five years, as per Rules 3 and 4 of PML Rules 2005. Records must be kept for five years from the date of the transaction or the end of the business relationship.

23.2 Records shall be kept in electronic or physical form. When using third-party service providers, the Company shall ensure:

23.2.1 The service provider has adequate capabilities and safeguards to protect data privacy and prevent unauthorized access.

23.2.2 Access to data processing systems, storage sites, and communication networks is controlled, monitored, and recorded.

23.2.3 Standard transmission, encryption formats, and non-repudiation safeguards for electronic data communication are established.

23.2.4 Compliance with relevant data protection statutes.

23.3 The Company shall have procedures to retain records of transactions to comply with information requests from authorities. Records shall permit reconstruction of transactions to provide evidence for prosecution if necessary. Contracts settled by claim or canceled should be retained for at least five years after settlement.

23.4 Records related to ongoing investigations or disclosed transactions shall be retained until the case is closed. Relevant identification documents should be sought and retained for such transactions.

23.5 Customer identification data, account files, and business correspondence shall be retained for at least five years after the business relationship ends.

24. Monitoring of Transactions

24.1 Regular monitoring of transactions is crucial for the effectiveness of AML/CFT procedures. The Company shall understand the normal activity of clients to identify deviations.

24.2 The Company shall pay special attention to all complex, large transactions or patterns that appear to have no economic purpose. Internal threshold limits may be specified for each class of client accounts, with special attention to transactions exceeding these limits. The background and purpose of such transactions, along with all related documents, should be carefully examined and findings recorded in writing. These records must be available to auditors, IRDAI, FIU-IND, and other relevant authorities during audits or inspections and preserved for five years from the date of the transaction.

24.3 The Principal Officer of the Company shall monitor and ensure that suspicious transactions are regularly reported to the Director, FIU-IND.

24.4 The compliance cell of the Company shall randomly examine a sample of transactions to assess whether they are suspicious.

25. Compliance Arrangements

The policy after the same is approved by the Board shall be filed with IRDAI for information. The Board will also review the same annually based on the experience and new business environment. The revisions in the policy will then be informed to IRDAI.

26. Review of the Policy

26.1 The Audit Committee and the Board shall review this Policy:

26.1.1 at least once every financial year, or

26.1.2 as and when the Board/Audit Committee considers it appropriate, or

26.1.3 as and when the underlying laws governing the Policy undergo any change