Anti-Money Laundering Policy

Corporate Office:

Narayana Health Insurance Limited
261/A, Bommasandra Industrial Area, Anekal Taluk,
Bommasandra Industrial Estate,
Bangalore South, Karnataka
India-560099

Document Summary					
Document Title	**Anti-Money Laundering Policy**				
Document Id	NHIL-004	**Current Version**	1.0	**Date of Release**	26-Mar-2024
Classification	Internal		**Storage Location**	NHIL Corporate office	
Administrating Function / Department	Finance Function				
Document Owner's Name & Designation	Mr. Anil Kumar Taneja				

Document Approvers			
Version No	**Name**	**Designation**	**Date**
1.0	Sheela Ananth	CEO	

Revision History			
Version No	**Date of Revision**	**Pages Affected**	**Description of Change**
-	-	-	-

Table of Content

Table of abbreviation

Following are the full forms of the abbreviations used in the policy.

Serial no	Abbreviation	Full description
1	AML	Anti-Money Laundering
2	CFT	Combating Financial Terrorism
3	ML and TF	Money Laundering and Terrorist Financing
4	FIU-IND	Financial Intelligence Unit, India
5	KYC	Know your customer
6	CKYCR	Central KYC Records Registry
7	CDD	Client Due Diligence
8	SDD	Simplified Due Diligence
9	EDD	Enhanced Due Diligence
10	FATF	Financial Action task Force
11	IRDAI	Insurance Regulatory and Development Authority of India
12	PAN	Permanent Account Number
13	UAPA	Unlawful Activities (Prevention) Act, 1967
14	NREGA	National Rural Employment Guarantee Authority
15	CCR	Counterfeit currency
16	STR	Suspicious Transaction Report
17	CTR	Cash Transaction Report
18	PEP	Politically Exposed Person
19	IAIS	International Association of Insurance Supervisors
20	OVDs	Officially Valid Documents
21	NGO	Non-Govt organization
22	PO	Principal Officer
23	VBIP	Video-Based Identification Process

1. Background

The Prevention of Money Laundering Act, 2002, brought into force with effect from 1st July 2005, is applicable to all financial institutions including Health Insurance Companies. The application of anti-money laundering measures to non-depository financial institutions generally, and to insurance companies, has also been emphasized by international regulatory agencies as a key element in combating money laundering. The establishment of AML programs by Financial Institutions is one of the recommendations of the FATF and also forms part of the Insurance Core Principles of the International Association of Insurance Supervisors (IAIS). Accordingly, the Company has decided to put in place an **AML Programme (AML)** for its business.

The obligation to establish an Anti-Money Laundering program applies to an insurance company. Hence the responsibility for guarding against insurance products being used to launder unlawfully derived funds or to finance terrorist acts, lies with the insurance company, which develops and bears the risks of its products.

IRDAI has been issuing Guidelines regarding AML/CFT standards to be followed by Insurance Companies and measures to be taken to prevent Money Laundering.

In accordance with the Master Guidelines on Anti-Money Laundering/ Counter Financing of Terrorism (AML/CFT), 2022, Insurance Companies are required to put in place an AML/CFT program comprising policies and procedures, for dealing with Money Laundering (ML) and Terrorist Financing (TF) reflecting the current statutory and regulatory requirements., duly approved by its Board of Directors. The policy covers the minimum aspects of customer acceptance, customer identification procedure, monitoring of transactions, and Risk Management framework. This policy document has been prepared in line with the extant IRDAI Guidelines.

2. Definitions:

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.	**"Authentication",**	"Authentication" shall mean the process as defined under clause (c) of section 2 of the Aadhaar Act as amended from time to time.
2.3	**"Beneficial owner"**	"Beneficial owner" shall have the meaning assigned to it under subclause (fa) of clause (1) of Section 2 of the PML Act.
2.4.	**"Central KYC Records Registry" (CKYCR**)	"Central KYC Records Registry" (CKYCR) shall mean 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.

2.5.	**"Client"**	"Client" shall have the meaning assigned to it under subclause (ha) of clause (1) of Section 2 of the PML Act. Explanation: The term client includes a customer/ person (Natural or Juridical) who may be a proposer or policyholder, or master policyholder or life assured or beneficiary or assignees, as the case may be.
2.6.	**"Client Due Diligence"**	"Client Due Diligence" (CDD) shall have the meaning assigned to it under subclause (b) of clause (1) of Rule 2 of the PML Rules.
2.7	**"Company"**	'Company' shall mean the Narayana Health Insurance Limited including its constitution and operation at its registered office, corporate office or branch office or any other place where Narayana Health Insurance Limited shall be considered to be carrying on its business.
2.8.	**"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.
2.9	**"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.
2.10	**"KYC Templates"**	"KYC Templates" shall mean templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.
2.11	**"KYC Records"**	"KYC Records" shall have the meaning assigned to it under sub clause (cd) of clause (1) of Rule 2 of the PML Rules.
2.12	**"Offline verification"**	"Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of theAadhaar Act.
2.13	**"On-going Due Diligence"**	"On-going Due Diligence" shall mean regular monitoring of transactions to ensure that they are consistent with the customers' profile and source of funds.
2.14	**"Officially valid document**	"Officially valid document" shall have the meaning assigned to it under sub clause (d) of clause (1) of Rule 2 of the PML Rules. (Annexure II)
2.15	**"Politically Exposed Persons (PEPs)"**	"Politically Exposed Persons (PEPs)" are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important

political party officials.

2.16	**"Principal Officer"**	"Principal Officer" shall have the meaning assigned to it under sub clause (f) of clause (1) of Rule 2 ofthe PML Rules.
2.17	**"Suspicious Transaction"**	"Suspicious Transaction" shall have the meaning assigned to it under sub clause (g) of clause (1) ofRule 2 of the PML Rules.
2.18	**"Video Based Identification Process (VBIP)"**	"Video Based Identification Process (VBIP)" shall mean an alternative (optional)electronic process of Identification/ KYC in paperless form, carried out by the insurer/authorized person (person authorized by the insurer and specifically trained for face-to-face VBIP) by undertaking seamless, secure, real-time, consent based audio-visual interaction with the customer/beneficiary to obtain identification information including the necessary KYC documents required for the purpose of client due diligence and to ascertain the veracity of the information furnished by the customer/ beneficiary.
2.19	"**Non-profit organization" (NPO)**	"Non-profit organization" (NPO) shall mean any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)

3. Scope:

This AML Policy establishes the standards of AML/CFT compliance and is applicable to all activities & employees of the Company.

4. Objective of the Policy:

The primary objective is to prevent the Company from being used intentionally and/or unintentionally by criminal elements for money laundering activities or terrorist financing activities. Other key objectives of the policy are:

4.1. To lay down the detailed AML/CFT Framework of Narayana Health Insurance Company Ltd.

4.2. To ensure compliance with relevant statutory and regulatory requirements

4.3. To co-operate with the relevant law enforcement authorities, including the timely disclosure of information

4.4. To lay down AML/CFT compliance norms for the employees of the Company

5. Review:

The Audit Committee and the Board shall review this Policy:

a. at least once in every financial year, or

b. as and when the Board considers it appropriate, or

c. as and when the underlying laws governing the Policy undergo any change including any relevant change in the laws mentioned in the Governing Law section of this Policy.

6. AML/CFT Framework:

As required by IRDAI Master guidelines, the Company's AML/CFT Framework is broadly divided into the following main components:

6.1. AML/KYC Standards

6.2. Appointment of Designated Director and Principal Officer

6.3. Recruitment and training of employees / agents

6.4. Internal Control / Audit

6.1. AML/KYC Standards

a. Know Your Customer (KYC) Norms

The Company shall verify the customers' identity by using reliable and authentic sources of documents and data/information to ensure that the insurance contracts are not under anonymous or fictitious names. It is imperative to ensure that the insurance premium should not be disproportionate to income/ assets.

At any point in time, when the Company is no longer satisfied with the true identity and the transaction made bythe customer, a Suspicious Transaction Report (STR) should be filed with the Financial Intelligence Unit-India (FIU- IND).

b. KYC of Natural Person

In the case of a new customer, KYC and CDD shall be done at the time of commencement of the new account-based relationship and in accordance with the regulatory prescriptions as may be issued by the Authorities from time to time. The Company shall verify the identity, address, and recent photograph of the individual person.

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

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

submits an 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.

Under Individual Policies, those individuals who are not able to undergo Aadhaar Authentication due to any injury, illness, old age, or otherwise, or they do not wish to go for Aadhaar Authentication, may submit their Officially Valid Documents (OVDs) as mentioned in Annexure III at the time of commencement of the Account-based relationship.
The Company may use any of the following modes to perform the KYC process:

- Aadhaar-based KYC through Online Authentication Or
- Aadhaar-based KYC through offline verification Or
- Digital KYC Or
- Video-Based Identification Process (VBIP) as a consent-based alternate method of establishing thecustomer's identity, for the customer. Or
- By using the KYC identifier' allotted to the client by the CKYCR Or
- By using Officially Valid documents (a list of documents to be verified and collected for individuals isgiven in Annexure III)
- PAN/Form 60 (wherever applicable) and any other documents as may be required by the Company.

c. KYC of Juridical Person

In the case of a juridical person, the 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 beneficial ownership.

The Company will have to identify and verify the legal status of the Juridical Person through various documentsto be collected in support of:

- The name, legal form, proof of existence,
- Powers that regulate and bind the juridical persons,
- Address of the registered office/ main place of business,
- Authorized individual person(s), who is/ are purporting to act on behalf of such client, and ascertainingbeneficial owner(s)

The Company shall verify the identity of the authorized person purporting to act on behalf of the Juridical Person. The list of documents to be obtained in the case of a Juridical Person is given in Annexure III
The Company shall determine the beneficial ownership and controlling interest in case of Juridical Person and the KYC of the beneficial owners shall be obtained. Necessary information with respect to the identification and KYC of the beneficial owner(s) is given in Annexures III & IV.

d. KYC of Group Policyholder

Under all kinds of Group Insurance, the KYC of Master Policyholders / Juridical Person / Legal Entity and the respective beneficial owners shall be collected. However, the details of all the individual members covered under the group insurance need to be maintained by Master Policyholders. The concerned business function needs to ensure that the details of beneficiaries are made available to the Company as and when required.

e. Knowing Existing Customers/Clients

Basis the adequacy of the data previously obtained, CDD and KYC shall be done for the existing customers from time to time.

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 high-risk customers).

For the continued operation of accounts of existing customers having an insurance policy of not more than an 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.

f. Reliance on third-party KYC

The Company may rely on a third party subject to the following conditions:

- The third-party immediately submits necessary information of CDD carried out by it.
- The Company takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.
- The Company is satisfied that such third party is regulated, supervised, or monitored for, and has measures in place for compliance with CDD and record-keeping requirements in line with the requirements and obligations under the Act read with IRDAI AML/ CFT guidelines on record-keeping.
- The third party is not based in a country or jurisdiction assessed as high risk.
- The Company is ultimately responsible for CDD and undertaking EDD measures, as applicable

g. Verification at the time of payout/claim stage (claim/refunds/reimbursement etc.)

The mandates are as follows:

- Payments to third parties shall not be allowed except as provided in the contract.
- Necessary due diligence should be carried out of the policyholders/beneficiaries/ legal heirs/assignees before making the payouts.
- Frequent Free Look cancellations on more than one occasion at short intervals

need the particularattention of the Company.

Necessary due diligence becomes more important in case the policy has been assigned by the policyholder to a third party not related to him (except where the insurance policy is assigned to Banks/ FIs/ Capital market intermediaries regulated by IRDAI/RBI/ SEBI)

Notwithstanding the above, the Company 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, necessary due diligence will have to be carried out on such assignments and STR should be filed with FIU-IND, if necessary.

h. Sharing KYC information with the Central KYC Registry (CKYCR)

Below are the norms with respect to sharing KYC information with CKYCR:

Basis the adequacy of the data previously obtained, CDD and KYC shall be done for the existing customers from time to time.

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 high-risk customers).

For the continued operation of accounts of existing customers having an insurance policy of not more than an 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.

6.2. Risk Assessment /Categorization

The Company shall carry out a risk assessment to identify, assess, document, and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions, or delivery channels that are consistent with any national risk assessment conducted by a body or authority duly notified by the Central Government. The risk assessment shall:

a. be documented.

b. Consider all the relevant risk factors before determining the level of overall risk and the appropriate levelland type of mitigation to be applied.

c. be kept up to date; and

d. be available to competent authorities and self-regulating bodies.

Risk categorization shall be undertaken based on parameters such as the customer's identity, social/financial status, nature of the business activity, information about the client's business and location, etc. While considering the customer's identity, the ability to confirm identity documents online or other services offered by issuing authorities may also be factored in.

The Guidelines require the Company to classify the customer into high risk and low risk based on the individual's profile and product profile. The IRDAI master AML guidelines further require identifying, assessing, documenting, and taking effective measures to mitigate Money Laundering and Terrorist Financing risks for customers or geographic areas, products, services, nature, and volume of transactions or delivery channels.

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

Therefore, the susceptibility of the health insurance business to money laundering is minimal. Keeping in view the above, health insurance business can be classified as low risk from an AML point of view and therefore it will be appropriate to undertake risk categorization on the basis of the underlying asset, amount of premium, the quantum of sum insured, and mode of premium payment apart from specified category of customers which may pose a higher risk.

All customers would be covered under this policy. The Company customers will be categorized based on twocategories — A & B. Category B customers include low risk while Category A is high-risk customers.

a) **High risk – (Category A):** High-risk customers typically include,

i. firms with sleeping partners

ii. politically exposed persons (PEPs)

iii. non-face-to-face customers and

iv. persons with dubious reputations as per public information available

v. non-resident customers

vi. high net worth individuals

vii. trust, charitable organizations, non-govt organizations (NGO), organizations receiving donations

viii. companies having close family shareholding or beneficial ownership

Sales team to ensure that the Source of Funds declaration or Income Proof is taken for all such customers. In addition to the income proof, if required, there will be independent

inquiries on the details provided by the customerand credible databases shall be consulted. KYC and underwriting procedures should ensure higher verification and counter checks.

b) **Low risk – (Category B):** Low-risk individuals (other than high net worth) and entities are those whose identities and sources of wealth can be easily identified and all other persons are not covered under the above category. Illustrative examples of low-risk customers could be
   i. salaried employees,
   ii. people belonging to lower economic strata of the society,
   iii. government departments and government-owned companies,
   iv. regulators and statutory bodies.

In the above cases, the basic requirements shall be to verify the identity and location of the customer.

On the basis of the risk specific to the health insurance business, the risk categorization will be done as per thetable below:

Basis of categorization:

Particulars	Low Risk (Category B)	High Risk (Category A)
How to Identify the Risk	• All risks other than those defined as High risk, • In case of individual policies, where the aggregate insurance premium is not more than Rs 10,000/ - per annum.	**I. Mode of Payment is Cash, DD or Bearer Cheque** • Where the premium is received in cash or through bearer cheque and the premium is Rs 50,000 or above but not beyond Rs 2 lakhs in the following situations: a. for a single transaction in a single day. ii. for a single insurance policy even if payment is done through multiple transactions *Clarification: Transaction in cash or through bearer cheque for an amount of Rs 2 Lakhs or above for a single transaction in a single day or for a single insurance policy even if the payment is done through multiple transactions, is not permissible as per the section 269 ST of Income Tax.* Act **II. Type of Customer**

		• **HNI customer -** Individual customer paying a premium of Rs. 5 lakhs. • **PEP** and customers who are family members, close relative / associates of PEPs (as declared by the customer). These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner(s). ***"Politically Exposed Persons"*** (PEPs) are individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. • **Non-residents,** including such individuals/entities connected with countries identified by FATF as having deficiencies in their AML/CFT regime. • **Trusts, charities, NGO's, Societies and organizations receiving donations.** • **Partnership Firms (other than LLPs)**
KYC and Due Diligence requirement	**Simplified Due Diligence as required in the document**	**Enhanced Due Diligence:** Apart from the basic requirements of verifying theidentity and location of the customer background, in case of high-risk customer, the following enhanced due diligence needs to be done: • Verify the identity of the customer using Aadhar subject to the

		consent of the customer, or verify the customer using other modes / methods of KYC, • Verify insurable interest, • Examine the purpose of the transaction especially for such customers which do not have apparent economic or visible lawful purpose, • Examine the ownership and financial position, including client's source of funds commensurate with the assessed risk of customer and product profile.

6.3. Due Diligence, Monitoring and Reporting of Transactions:

The transaction includes a proposal for an insurance policy, claims under a policy, transactions with intermediaries, etc.

Monitoring of transactions will be done taking into consideration the risk profile of the Customer. The Company shall make endeavors to understand the normal and reasonable activity of the customer so that the transactions that fall outside the regular / pattern of activity can be identified. Special attention will be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose.

It is imperative to ensure that the customer's source of funds, country of origin, estimated net worth, etc., could be documented where considered necessary. The Company shall take appropriate measures, commensurate with the assessed risk of customer and product profile as part of their due diligence measures including conducting independent inquiries on the details collected on /provided by the customer where required, and consulting a credible database public or others, etc..,

a. Simplified Due Diligence

SDD is to be carried out by collecting the KYC documents as specified in Annexure III for the below-mentioned instances,

- In the case of individual policies, where the aggregate insurance premium is not more than Rs10,000/ - per annum.
- the customers are classified under low risk.

The above-mentioned will not apply in the case of;
- suspicion of money laundering

- terrorist financing
- high risk scenarios

b. Enhanced Due Diligence (EDD)

EDD is to be carried out for customers who fall under high-risk categories as mentioned in Section 12AA of the PML Act. Below are the steps to be ensured in the case of EDD.

- Verify the identity of the clients preferably using Aadhaar subject to the consent of the customer or throughother modes/ methods of KYC as specified in the policy.
- Examine the ownership and financial position, including the client's source of funds commensurate with theassessed risk of the customer and product profile.
- Record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties

c. Monitoring & Reporting of Transaction

In terms of Rule 3 of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, and in terms of Rule 7 thereof, the following reports shall be furnished to Financial Intelligence Unit-India as per guidelines prescribed by FIU as applicable and within the timelines specified.

The Company have a process in place to monitor & report suspicious transactions within the below prescribed timelines.

Sr. No	Report	Due Date	Description
1.	CTR	Not later than the 15th day of the succeeding month	As stipulated in Red Flag Indicator (RFI)
2.	CCR	Not later than the 15th day of the succeeding month	All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgeryof a valuable security or a document has taken place facilitating the transactions.
3.	STR	On being satisfied that the transaction is suspicious	All suspicious transactions whether or not made in cash and as stipulated in Red Flag Indicator (RFI).
4.	NTR	Not later than 15th day of the succeeding month	All transactions involving receipts by non-profit organisations valued at more than Rs.10 lakhs or its equivalent in foreign currency in amonth.

e. Suspicious Transaction Report (STR)

The Company shall explore the possibility of validating the fresh transactions with various watch lists available inthe public domain. After due diligence, the transactions of a suspicious nature – **(Suspicious Transactions Report- STR)** will be electronically reported by the Principal Officer to the Director, Financial Intelligence Unit — India (FIU-IND) on being satisfied that the transaction is suspicious. Illustrative cases of STR are mentioned below in this policy.

A Suspicious Transaction is one that is inconsistent with a customer's known, legitimate activities or with the normal business for that type of policy account. A transaction may also be suspicious in the following scenarios:

1. If it gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or

2. If it appears to be made in circumstances of unusual or unjustified complexity; or

3. If it appears to have no economic rationale or bonafide purpose.

At any stage of the insurance transaction, if any employee/intermediary of the Company feels that the true identity of the insured could not be established or is not satisfied with the identity of the customer, intimation needs to be provided to the Compliance team. The Compliance team will further analyze the same and will assist the Principal Officer in filing a STR with all particulars with FIU — IND

All documents/ office records/ memorandums/ clarifications sought in relation to suspicious transactions and the purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records, and related documents shall be made available to auditors and also to IRDAI/ FIU- IND/ other relevant Authorities, during audit, inspection, or as and when required. These records are required to be maintained and preserved for a period as per the record-keeping policy.

While furnishing information to the Director, FIU-IND, a delay of each day in not reporting a transaction or a delay of each day in rectifying a mis- represented transaction beyond the time limit shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is *no tipping* off to the customer at any level.

The Principal Officer shall monitor and ensure that suspicious transactions shall be regularly reported to the Director, FIU-IND

Transactions, where the attempt is made to circumvent the requirement of submission of PAN, will be considered as suspicious activity requiring reporting to FIU-IND. Concerned employee/intermediary to intimate Compliance team within 1 day of

identifying such incident. The Compliance team would further analyze the same and assistthe Principal Officer in reporting it to FIU-IND

No employee or Director of the Company shall provide any information to any policyholder on the status of said policyholder's name(s) being reported to FIU-IND.

f. Cash Transaction Report (CTR)

Premium deposits beyond Rs. 50,000 will be accepted preferably through cheques, demand drafts, credit card or any other banking channel. Premium /proposal deposits remittances in cash beyond Rs. 50000/- up to Rs. 1,99,999/- per transaction shall be accepted subject to the customer quoting PAN. The Company shall verify the authenticity of the details of PAN so obtained. In case of customers not required to have PAN or with only agricultural income, Form 60/61 prescribed under the provisions of Income Tax Rules shall be obtained. The Integrally connected transactions exceeding Rs 50,000/- in cash in a month will be closely monitored and examined for possible angles of money laundering by the Compliance team. Premium /proposal deposits remittances in cash for an amount involving Rs. 2 Lakhs and above per transaction cannot be accepted.

CTR analysis shall be carried out by compliance function as stipulated in Red Flag Indicator and report if any within the prescribed timeline. This shall however exclude premium collected from various Customers and remitted to the Company by agents/intermediaries.

g. No claim payment will be made in cash.

The Company under no circumstances shall make payment of claims either in cash or any other form or denomination equivalent to cash.

h. Reporting of receipts from Non-Profit making Organizations

All transactions, involving receipts from non-profit organizations (either in the form of assignments and/or in the form of top-up remittances) of value more than Rs 10 lacs or its equivalent in foreign currency will be reported to FIU-IND within the above prescribed timeline. PAN/Form 16 to be collected or less than Rs. 50,000.

Procedure for reporting:
Operations team to provide confirmation immediately, on such transactions, to the Compliance team. The compliance team will further compile all the details and assist the Principal Officer in filing it further with FIU-IND.All such transactions will be reported to FIU within the above-prescribed timeline.

i. Counterfeit Currency/Forged Bank notes (CCR)

As per Rule 3 of PML Rules, the Company will report to FIU-IND on identification, all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine, and where any forgery of a valuable security or a document has taken place facilitating the transactions. The reporting of the counterfeit notes shall be done within the above-prescribed timeline.

The Company will stamp each such note as "COUNTERFEIT NOTE" and impound the same. Each such impounded note shall be recorded under authentication, in a separate register and file CCR simultaneously.

Apart from the above report submissions, information collected from the Customer shall be treated as confidential and such information will not be divulged or used for cross selling or any other like purposes. The Company shall ensure that information sought from the Customer is relevant to the perceived risk, is not intrusive and is in conformity with the guidelines issued by IRDAI in this regard.

Procedure for reporting:
In case any Counterfeit Currency / Forged Bank Notes / Fake KYC Documents are identified, Accounts / Operations team needs to intimate the Compliance team immediately. Compliance team will compile all the details and assist the Principal Officer to further file it with FIU-IND

7. Contracts with Politically Exposed Persons (PEPs)

All proposals of PEPs shall be examined by senior management of the Company. Further, appropriate on-going risk management procedures needs to be implemented by the Risk & Operation's Function for conducting due diligence on on-going basis to PEPs (individually as well as being the beneficial owner) and customers who are family members, close relatives/associates of PEPs.

Keeping in view the fact that the information relating to PEPs is neither available in public domain nor any data base is in existence, the Company may take necessary declarations from the customers besides trying to procure information from other available resources.

8. New Business Practices/Developments

AML risk should be considered for new products, new business practices and use of new technology for both new/ pre-existing products to source non-face-to-face business. Risk Function 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.

Because of ease of access to digital facility and speed of electronic transactions the Company should lay down systems to prevent the misuse of money laundering framework e.g., system should be able to detect the multiple fictitious applications. In case of non-face-to-face customers the extent of verification shall depend on the risk profile of the product and that of the customer e.g., verification of details of customer through on-site visits, etc.

9. Contracts emanating from Countries identified as deficient in AML/CFT regime

The Company is required to:

9.1. Specifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

9.2. Pay Special attention to business relationships and transactions, especially those that do not have an apparent economic or visible lawful purpose. In all such cases, the background and purpose of such transactions will as far as possible, have to be examined, and written findings have to be maintained to assist competent authorities.

9.3. Agents/intermediaries/ employees to be appropriately informed to ensure compliance with this stipulation.

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

9.5. 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).

9.6. The principles above shall be applied with respect to all product offerings of the Company including Health and Travel Insurance.

9.7. The Compliance function of the Company will on a continuous basis monitor the FATF status of different countries and keep the underwriting and other relevant functions of the Company updated about the same for the purpose of complying to the same.

10. Collection of Aadhaar & PAN as KYC documents

The company shall not seek Aadhaar from the proposer/policyholder as mandatory documents. However, if the proposer/policyholder voluntarily offers Aadhaar as one of the documents for KYC purposes, the company may accept Aadhaar. However, any acceptance of Aadhaar shall be subject to the masking facility available with the company.

11. Termination of Business Relationship

Following KYC norms will be mandatory for all the employees/ agents/intermediaries.

11.1. The services of the defaulting employees/intermediaries who expose the Company to AML / CFTrisks on more than 2 occasions would be terminated.

11.2. The decision of Termination would be taken by the Principal Officer.

11.3. Head of HR to intimate the same to the concerned employee and Head of Sales channel to the concerned intermediary/agent.

12. Illustrative list for identifying suspicious transactions

The proposals/policies are to be analyzed on a regular basis to identify any suspicious transactions. Below is the illustrative list for identifying suspicious transactions.

12.1. Customer (including assignees, where applicable)/ beneficiaries/ legal heirs/ nominee/ Insured/ Beneficial Owner (wherever applicable) whose identity matches with any person whose name figures in the list of designated individuals and entities.

12.2. If the aggregate number of cash or DD receipts exceeds 3 or Rs. 5 Lakhs in a calendar month from a single person towards payment of any nature under all the insurance policies or proposals under which such person is the Policy Owner or Proposer or Assignee.

12.3. If the aggregate number of cash or DD receipts exceeds 21 or Rs. 75 Lakhs in a financial year from a single person towards payment of any nature under all the insurance policies or proposals under which such person is the Policy Owner or Proposer or Assignee.

12.4. Where 3 or more free look cancellation requests are received from a single policyholder in a calendar month, under which the amount refunded under all the 3 policies put together exceeds Rs.1 lakh.

12.5. Receipt of request for cancellation of policies beyond the free look period from a Single policyholder where the aggregate refundable amount is in excess of Rs. 2 lakhs in a calendar month and where the Proposal deposit was paid by cash or demand draft(s) of under Rs.50,000/- or a combination thereof, other than cancellations initiated by the Company. Also, PAN/Form 16 should be collected for the same.

12.6. Inflated or totally fraudulent claims.

12.7. Receipt of request for change of addresses 3 or more times from the same policyholder in a financial year.

12.8. Refund of premiums or proposal deposits, other than on account of declinature or postponement of insurance cover, under which the total amount refunded is Rs.5 lakhs or above in a calendar month or Rs 25 lakhs or above in a financial year.

12.9. A common address or (up to two) PAN email IDs or contact phone numbers are found between 2 or more customers.

12.10. Adverse media report appears in a Newspaper, Television, Radio, or any other media about an existing Policyholder.

12.11. Receipt of any notice of inquiry from any Law Enforcement Authority or Financial Sector Regulators, calling for information about any Policyholder of an insurance company

12.12. A suspicious profile of the customer is observed.

12.13. Premium payment or attempts for payment made by an unrelated third party {irrespective of the mode) with no economic rationale or any justified reasons.

12.14. Any entities/persons of entities who are barred/disqualified by Financial Sector Regulators/MCA

13. Sharing of the customer Information / Data

The Company can share the information on customers with different organizations such as Income tax authorities, local government authorities, etc. as per the statutory requirements.

14. Responsibility on behalf of the Agents and Intermediaries

It is necessary that steps are taken to strengthen the level of control of the agents and intermediaries engaged by the company.

a. KYC norms compliance will be mandatory for all agents and intermediaries.

b. Services of defaulting agents/intermediaries who expose the Company to AML/CFT-related risks willbe terminated as mentioned in the "termination of business relationship" part of the policy.

When faced with a non-compliant agent(s)/intermediary the Company will take necessary actions to secure compliance including, when appropriate, terminating its business relationship with such an agent/intermediary.

15. Maintenance & Retention of Information / Records:

The Company is required to maintain (either in electronic or physical form) the information/records of types of all transactions [as mentioned under Rules 3 and 4 of PML Rules 2005] as well as those relating to the verification of identity of clients for a period of five years. The records referred to in the said Rule 3 shall be maintained for a period of five years from the date of transaction, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit the construction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for the prosecution of criminal activity.

The obligation of the Company with respect to retaining the records under the following circumstances.

a. The contracts which have been settled by claim or canceled retain records for a period of at least 5years after that settlement.

b. On-going investigations, or transactions that have been the subject of a disclosure, should be retained until it is confirmed that the case has been closed where practicable. The Company will retainrelevant identification documents for all such transactions and report the offer of suspicious funds.

c. All other transactions, (for which the Company is obliged to maintain records under other applicable Legislations/Regulations/Rules) to retain records as provided in the said Legislation/Regulations/Rules but not less than for a period of five years from the date of end of the business relationship with the customer.

d. In the case of customer identification data obtained through the CDD process, account files

and business correspondence should be retained for at least five years after the business relationships ended.

e. The PO shall review all reports required to be submitted to regulatory/law enforcement authorities priorto submission from time to time.

16. Appointment of a Designated Director and a Principal Officer

16.1. Appointment:

The Company will designate 'Designated Director' and 'Principal Officer' and intimate the names of the 'Designated Director' and 'Principal Officer' to IRDAI and FIU-IND. Any change in incumbency will be intimated to IRDAI and FIU-IND within 7 days of its effect.

The 'Designated Director' will be a Managing Director or a whole-time Director duly authorized by the Board of Directors and the "Principal Officer" will be at a senior level.

16.2. Responsibilities:

The Designated Director & Principal Officer (PO) shall ensure,

a. Overall compliance with the obligations imposed under Chapter IV of the PML Act and the PML Rules.

b. Additionally, PO to monitor and ensure that Suspicious transactions are regularly reported to the Director, FIU- IND.

16.3. Recruitment and training of Agents / Intermediaries/ Employees

The Company shall have an ongoing employee training program so that the Team members are adequately trained in AML/CFT policy. To communicate policies related to AML / KYC to all levels of management & staff handling policyholder information. Training requirements shall have different focuses for frontline staff, compliance staff, and staff dealing with new customers and claims. It is crucial that all those concerned fully understand the rationale behind the AML policies and implement them.

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

a. *New employees:* A general appreciation of the background to money laundering and any other criminal history, and the subsequent need for identification and reporting of any suspicious transactions to the appropriate designated point will be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority.

b. *Sales/Advisory staff*: Members of staff who are dealing 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. The "front-line" staff will be made aware of the Company's

AML/CFT policy for dealing with non-regular customers particularly where large transactions are involved, and the need for extra vigilance in these cases and shall need to carry out necessary KYC.

c. *Processing Staff*: Those members of staff who receive completed proposals and premiums will receive appropriate training in the processing and verification procedures as laid down in this policy.

d. Administration / Operations supervisors and managers shall cover all the aspects of money laundering procedures laid down in this policy.

As most part of the insurance business is through agents /intermediaries which brings in non-face business relationships with the policyholders, the selection process of agents/intermediaries will be monitored carefully. The monitoring of the agents/intermediaries will include monitoring sales practices followed by agents/intermediaries 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 the company's strict adherence to laid down process and strong ethical and control environment.

a) The HR Department shall maintain records of AML training imparted to staff in LMS. Respective Heads of Department to ensure that all the employees of their team are aware of the AML policy
b) Compliance Team with the help of the HR Department using Learning Management Software (LMS) to provide refresher training to all their existing employees on a yearly basis.
c) The HR Department should put in place an adequate screening mechanism as an integral part of their personnelrecruitment/hiring process.

16.4. Internal Control / Audit

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.

Role of Internal Audit:

Below is the list of functions to be carried out by the Internal Audit department;

a. To periodically verify compliance with the extant policies, procedures, and controls related to money laundering activities based on overall risk assessment.

b. To upgrade its questionnaire and system periodically from time to time to be in sync with applicable norms

c. To ensure compliance with the policies, procedures, and controls relating to the prevention of ML and TF

d. To carry out 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 has to be monitored on a regular basis.

e. To ensure that the reports include the robustness of the internal policies and make constructive.

f. To submit the audit notes and compliance to the Audit Committee.

17. Implementation of section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)

The Company will comply with the applicable order issued by the Government of India. As required by the order, the Company will match the particulars of the customers with the consolidated list of individuals or entities suspected to be engaged with terrorism which is received from the UAPA nodal officer, and the list will be circulated by the Nodal officer designated by the IRDAI for this purpose.

The Company shall not enter into any transaction with a Customer whose identity matches with any person with a known criminal background or with banned entities and those reported to have links with terrorists or terrorist organizations identified by the Ministry of Home Affairs (MHA) and as intimated to the Company by IRDAI (hereinafter designated individuals/entities).

The Company shall 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 policy with the Company.

The list available in the above-mentioned link needs to be updated by the Compliance team in the GC system. The compliance team shall get automated mails for matching records found. Further analysis needs to be done by the Compliance team to ascertain the authenticity of the matches found.

In case matching records about designated individuals/entities are identified, the following procedure shall be adopted:

a. To maintain updated designated lists in electronic form and run a check on the given parameters on a daily basis to verify whether individuals or entities listed in the Schedule to the Order, hereinafter, referred to as designated individuals/entities are holding any funds, financial assets or economic resources or related services held in the form of insurance policies with them.

b. Compliance team to inform the Principal Officer about matching records identified within 12 hours of identifying the match.

c. The Principal Officer shall within a maximum of 24 hours from identifying a match, inform full particulars of all insurance policies held by such Customer to the Central (designated) Nodal Officer for the UAPA, at Telephone Number: 011- 23314458, 011- 23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].

d. In case, the match of any of the customers with the particulars of designated

individuals/entities is beyond doubt, the Company shall prevent such designated individuals/entities from conducting any transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Telephone Number: 011- 23314458, 011-23314435, 011-23314459 (FAX), email address: dir@fiuindia.gov.in].

e. Also send a copy of the communication, to the State Nodal Officer, where the account/transaction is held, and to IRDAI as the case may be, without delay.

f. In all such matched cases STR shall also be filed with FIU-IND by the Principal Officer.

g. On receipt of the particulars (held in the form of Insurance Policies) of suspected designated individuals/entities the Central [designated] Nodal Officer for the UAPA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the Company are the ones listed as designated individuals/entities and the insurance policies, reported by Company are held by the designated individuals/entities.

h. In case, the results of the verification indicate that the insurance policies are owned by or are held for the benefit of the designated individuals/entities, an order to freeze these insurance policies under section 51A of the UAPA would be issued without delay, and conveyed electronically by the Central [designated] Nodal Officer for the UAPA to the concerned office of Company under intimation to

i. Upon receipt of the order for freezing insurance policies from IRDAI in respect of matched cases, the Company shall immediately implement the order without any intimation to such designated individuals/ entities.

j. The Company shall also freeze such on the same business day but not later than 24 hours, in any case, the funds or other assets, as per the abovementioned procedure, of persons who commit or attempt to commit terrorist acts; of entities owned or controlled by such persons; and entities acting on behalf, or at the direction of such persons, including property owned, directly or indirectly, by such persons, upon receipt of any such request by the UAPA nodal officer.

18. Procedure for unfreezing of insurance policies of individuals/entities inadvertently affected by the freezing mechanism, upon verification that the individual/ entity is not a designated individual/entity.

18.1. Any individual or entity, if they have evidence to prove that the insurance policies, owned/held by them have been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned Company.

18.2. Company shall inform and forward a copy of the application together with full details of the insurance policies inadvertently frozen as given by any individual or entity, to the Central [designated] Nodal Officer of MHA withintwo working days.

18.3. The Central [designated] Nodal Officer for the UAPA shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, without delay, unfreezing the insurance policies

owned/held by such applicant, under intimation to the concerned Company. However, if it is not possible for any reason to pass an Order unfreezing the assets within 5 working days, the Nodal Officer shall inform the applicant. The insurer shall act basis of the feedback received from the Nodal Officer and proceed for unfreezing of the insurance policy.

19. Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001

19.1. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or otherassets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets, derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

19.2. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the Central [designated] Nodal Officer for freezing of funds or other assets.

19.3. The Central [designated] Nodal Officer of MHA, shall cause the request to be examined without delay, so as to satisfy that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, the request would be electronically forwarded to the Nodal Officer in IRDAI. The proposed designee, as mentioned above, would be treated as a designated individual/entity.

19.4. Upon receipt of the request by the Nodal Officer in IRDAI from the Central [designated] Nodal Officer, the request will be forwarded to the Company and the procedure as enumerated in paragraphs (i) above on freezing of insurance policies shall be followed.

19.5. The freezing orders shall take place without prior notice to the designated persons involved.

20. Updation of Policy

The Principal Officer will be authorized to amend / modify the KYC Policy or other related guidance notes of the company, to be in line with IRDAI or such other statutory authority's requirements/updates from time to time.

21. IRDAI Reporting obligation:

The Company shall file the annual compliance certificate as provided in **Annexure I** within 45 days of the end of the Financial Year.

Annexure I

Certificate of Compliance (Master Guidelines AML/CFT)

Name of Insurer:

Financial Year:

We do hereby submit that our company ..... (name) has fully complied with all the norms laid down under Master AML / CFT guidelines 2022, and the company has set up a robust mechanism to comply with the extant PML Rules / Acts.

Principal Officer/Chief Compliance Officer (Name and Signature)

Chief Executive Officer (Name and Signature)

Annexure II- List of Officially valid Documents

Individual	
Proof of Identity	Any of the below '*Officially valid document'* namely; i. Passport ii. Permanent Account Number (PAN) Card iii. Proof of possession of Aadhaar number iv. Driving license v. Voter's Identity Card issued by Election Commission of India vi. Job card issued by NREGA duly signed by an officer of the State Government vii. Letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator viii. such documents as are required to generate CKYC An individual can also submit the following: • Aadhaar number where, (i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or (ii) he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the Act; or • Proof of possession of Aadhaar number where offline verification can be carried out;or • the proof of possession of an Aadhaar number where offline verification cannot be carried out or any officially valid document the equivalent e-document thereof containing the details of his identity and address; and • the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and • such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the reporting entity. Provided that if the client does not submit the Permanent Account Number, he shall submit one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph, and such other documents including in respect of the nature or business and financialstatus of the client as may be required by the reporting entity. [Explanation. - Obtaining a certified copy by reporting entity shall mean comparing the copy of an officially valid document so produced by the client with the original and recording the same on the copy by the authorized

Proof of Address	officer of the reporting entity in a manner prescribed by the regulator.] **Provided that where simplified measures are applied for verifying the identity of the clients the following documents shall [also] be deemed tobe *'officially valid documents'*:** (a) identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; (b) letter issued by a gazetted officer, with a duly attested photograph of the person;] In case of officially valid document furnished by the client does not contain updated address, the following documents [or their equivalent e-documents thereof] shall be deemed to be officially valid documents for the limited purpose of proof of address:- (a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill); (b) property or Municipal tax receipt; (c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings,if they contain the address; (d) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and license agreements with suchemployers allotting official accommodation: Provided that the client shall submit updated officially valid document [ortheir equivalent e-documents thereof] with current address within a period of three months of submitting the above documents. **Provided further that where simplified measures are applied for verifying the limited purpose of proof of address of the clients, where a prospective customer is unable to produce any proof of address, the following documents shall [also] be deemed to be *'officially valid document'*:** (a) bank account or Post Office savings bank account statement [or if the reporting entity is located in an International Financial Services Centre, statement of foreign bank]; Provided also that in case the officially valid document presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

	Provided also that in an International Financial Services Centre, the national identity card and voter identification card, by whatever name called, issued by the Government of foreign jurisdictions or agencies authorized by them capturing the photograph, name, date of birth, and address of a foreign national shall alsobe considered as an officially valid document: Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India; [Explanation. - For the purpose of this clause, a document shall be deemed to an "*officially valid document*" even if there is a change in the name subsequentto its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.] e) such documents as are required to generate CKYC
Companies • **The name, legal form, proof of existence** • **Powers that regulate and bind the juridical persons,** • **Address of the registered office/main place of business** • **Authorized individual person(s), who is/are purporting toact on behalf ofsuch client, and** • **Ascertaining Beneficial Ownership**	The certified copies of the following documents [or the equivalent e-documents thereof], namely; *(i)* Certificate of incorporation; *(ii)* Memorandum and Articles of Association; *(iii)* Permanent Account Number of the company; *(iv)* Resolution from the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf *(v)* such documents as are required for an individual relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf *(vi)* the names of the relevant persons holding senior management position, and *(vii)* the registered office and the principal place of its business, if it is different.
Partnership Firms • **The name, legal form, proof of**	The certified copies of the following documents [or the equivalent e-documents thereof], namely: - (i) registration certificate; (ii) partnership deed;

existence • **Powers that regulate and bind the\juridical persons, Address of the registered office/ main place of business,** • **Authorized individual person(s), who is/ are purporting to act on behalf of such client, and** • **Ascertaining Beneficial Ownership**	(iii) PAN of the partnership firm; (iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as thecase may be, holding an attorney to transact on its behalf the names of all the partners and address of the registered office, and the principal place of its business, if it is different
Trusts and Foundations	The certified copies of the following documents [or the equivalent e-documents thereof], namely:- (i) registration certificate; (ii) trust deed; (iii) Permanent Account Number or Form No.60 of the trust; and (iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees,as the case may be, of the person holding an attorney to transact on its behalf (v) the names of the beneficiaries, trustees, settlor "protector if any" and authors of the trust and the address of the registered office of the trust; and vi) list of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust.
Unincorporated association or abody of individuals	The certified copies of the following documents [or the equivalent e-documents thereof], namely:- (i) resolution of the managing body of such association or body of individuals; (ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals; (iii) power of attorney granted to him to transact on its behalf; [and] (iv) such documents as are required for an individual under sub-rule

	(4) relating to beneficial owner, managers, officers or employees as the case may be, holding an attorney to transact on its behalf; (v) such information as may be required by the reporting entity to collectively establish the existence of such association or body of individuals. vi) such documents as are required to generate CKYC

Note-:

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

(ii) Where a customer submits an 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.

(iii) 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

(iv) In case of low-risk customers and cases where the aggregate premium per annum is less than or equal to Rs. 10,000/-, simplified due diligence needs to be undertaken. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.

(v) In the case of high-risk customers, KYC and underwriting procedures should ensure higher verification and counter checks. An enhanced due diligence in the form of 'Customer evaluation sheet' capturing the customer profiling details needs to be undertaken by the sales staff/agent/intermediary at the point of sale.

(vi) To register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and insurer has ended or the account has been closed, whichever is later.

(vii) To collect the updated the documents as and when informed by the customer, within 30 days of such updation.

Annexure III
Identification and KYC of the beneficial owner

S. No	Applicable for	Beneficial owner		KYC Documents required for
I	Where the client is acompany	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means	a) Ownership of more than 10 % of shares or capital or profits of company b) Control shall include the right to appoint majority of the directors or to control	KYC to be taken for beneficial owners if they fall in the category as defined under the Guidelines.
Ii	Where the client is apartnership firm	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person	Ownership of/entitlement to morethan 10% of the capital or profits of thepartnership	KYC to be taken for beneficial persons ifthey fall in the category as defined under the Guidelines.
iii	Where the 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	Ownership of/entitlement to morethan15% of the property or capital or profits of such association or body of individuals	KYC to be done for beneficial owners.
iv	Where no natural person is identified under (i), (ii) or (iii) above	The beneficial owner is the relevant natural person who holds the position of senior managing official		KYC to be done for the specified natural person.

V	Where the client is atrust	The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% percent 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	KYC for the settler of the trust, the trustee, the protector and the beneficiaries with 10% or more interest needs to be conducted.
vi	Where the client or the owner of the controlling interest is a company listed onastock exchange, or is a subsidiary of such a company	Not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.	

*****