The New India Assurance Company Limited, Mumbai

INTIMATION OF DECISIONS TAKEN AT THE 1599 BOARD MEETING HELD ON MONDAY 13TH FEBRUARY,2023 AT THE REGISTERED OFFICE OF THE COMPANY AT MUMBAI

From - CMD_Board Secretariat

To - Ms. Rekha Gopalkrishnan, General Manager& CFO
Ms. Prabha Vijaykumar, Chief Manager

Date of the Meeting: Monday, 13th February, 2023

Item No.	Description of Item
44	Implementation Plan of IRDAI Master Guidelines dated 1st August 2022 and NIA's Anti-Money Laundering / Counter Financing of Terrorism (AML/CFT) Policy 2022

Decision of the Board:

Board considered the note dated 03rd February, 2023, placed before it in respect of the above.

After discussion, Board approved the proposal and passed the following resolution unanimously:

"**RESOLVED THAT** the Implementation Plan of IRDAI Master Guidelines dated 1st August 2022 and NIA's Anti-Money Laundering / Counter Financing of Terrorism (AML /CFT) Policy 2022 as proposed is hereby approved".

Jayashree Nair
Company Secretary
13th February, 2023

Implementation plan based on IRDAI guidelines

Sr. no.	Activity	Details
1	Insurers shall take steps to implement provisions of PML Act and the PML Rules, as amended from time to time	Draft of Company's Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) Policy 2022 is presented before Board for approval
2	Appointment of a Designated Director and a Principal Officer	Appointment has been made. Mr. Y K Shimray, Director & GM has been appointed as Designated Director and Mrs. Prabha Vijaykumar, Chief Manager has been appointed as Principal Officer.
3	Insurers shall submit annual compliance certificate as provided in Annexure I within 45 days of end of Financial Year.	Report will be prepared in the given format as per timeline.
4	Training of employees and intermediaries.	Training will be imparted on regular basis.
5	Internal Control/Audit	All Audit Teams at HO / RO have been advised for observation of AML / CFT compliance in respective Auditee Office and to report accordingly.
6	Know Your Customer (KYC) Norms	eKYC [Electronic Know Your Customer] is being done for new and renewed policies and CKYC [Central Know Your Customer] is being done with CKYCR [Central KYC Registry].
7	Risk Assessment/ Categorization	Classification of customer into high risk and low risk based on the individual's profile and product profile, to decide upon the extent of due diligence is under process.
8	Simplified Due Diligence [SDD]	Currently this is done by ckyc/ekyc for all policies.
9	Enhanced Due Diligence [EDD]	It is to be done for High Risk Clients, Politically Exposed Persons(PEP) etc. after categorization as per point 7.
10	Reliance on third party KYC	At present NIA is doing kyc of all clients directly.
11	Contracts with Politically Exposed Persons (PEPs)	All ROs are advised to be vigilant on this exposure and keep on record.
12	New Business Practices/Developments	This aspect will be considered while filing/reviewing products.

13	Implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA)	As per the Master Guidelines, a list of individuals and entities subject to UN sanction measures under UNSC Resolutions would be circulated to the insurers through General Insurance Council, on receipt of the same from the Ministry of External Affairs (MEA) and will be informed for necessary action to all concerned.
14	Contracts emanating from countries identified as deficient in AML/CFT regime	As per guidelines FATF public statements will be circulated through General Insurance Council. All concerned dept./offices will be informed.
15	Reporting obligations	We have noted the reporting formats and comprehensive reporting format guide, prescribed/released by FIU-IND and Report Generation Utility and Report Validation Utility. Suitable technological tools for extracting CTR/STR from live transaction data, is being explored.
16	Record keeping	Records of 5 years will be stored either digitally or in physical form.
17	Monitoring transactions	Company will specify internal threshold limits for each class of client accounts and monitor the transaction which will exceed the threshold given.

New India Assurance Anti-Money Laundering / Counter Financing of Terrorism (AML/CFT) Policy, 2022

1. Introduction

1.1. In terms of the provisions of Prevention of Money Laundering Act, 2002 (PML Act) and the Prevention of Money- Laundering (Maintenance of records) Rules, 2005 (PML Rules) (as amended from time to time), Company is required to follow Customer Identification Procedures while undertaking a transaction at the time of establishing an account based relationship/ client based relationship and monitor their transactions on-going basis.

1.2. Company shall take steps to implement provisions of PML Act and the PML Rules, as amended from time to time, including operational instructions issued in pursuance of such amendment(s).

1.3. The obligation to establish an anti-money laundering program applies to Company as per provisions of clause (ii) and (iii) sub rule (14) of Rule 9 of the PML Rules. Company has responsibility for guarding against insurance products and services being used to launder unlawfully derived funds or to finance terrorist acts.

1.4. Money Laundering is a process or activity of moving illegally acquired money through financial systems so that it appears to be legally acquired. Section 3 of PMLA specifies the Offence of Money Laundering.

2. Short Title, Applicability and Commencement

2.1. This policy shall be called as "New India Assurance Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) Policy 2022".

2.2. This policy would be applicable for all businesses carried out by the Company including the business carried out at International Financial Services Centre Insurance Office [IFSC Insurance Office] at GIFT City, Gandhinagar. This policy shall also fulfill the requirement as narrated in the notification dated October 28th, 2022 issued by International Financial Services Centre Authority, Gandhinagar. Foreign Offices of the Company, in line with the master guidelines and this policy shall formulate their Anti Money Laundering / Counter Terrorism Financing procedures incorporating the local requirements and guidelines in this regard in the respective jurisdiction of their operation and ensure strict compliance thereof. The foreign offices should also ensure that the same is updated on regular basis and all the officials working in the foreign offices are provided periodic training.

1.3. This policy would come into force from 1st January 2023 and replace the AML/Counter Financing of Terrorism (CFT)Policy 2013.

3. Definitions

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

3.1. "**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".

3.2. **"Authentication**", means the process as defined under clause (c) of section 2 of the Aadhaar Act as amended from time to time.

3.3. "**Beneficial owner"** shall have the meaning assigned to it under sub clause (fa) of clause (1) of Section 2 of the PML Act.

3.4. **"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.

3.5. "**Client"** shall have the meaning assigned to it under sub clause (ha) of clause (1) of Section 2 of the PML Act.

Explanation: For the purpose of this policy, the term client includes a customer/ person (Natural or Juridical) who may be a proposer or policyholder or master policyholder or beneficiaries or assignees, as the case may be.

3.6. **"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.

3.7**. "Designated Director"** shall have the meaning assigned to it under sub clause (ba) of clause (1) of Rule 2 of the PML Rules.

3.8. **"Digital KYC**" shall have the meaning assigned to it under sub clause (bba) of clause (1) of Rule 2 of the PML Rules.

3.9. **"KYC Templates**" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

3.10. **"KYC Records"** shall have the meaning assigned to it under sub clause (cd) of clause (1) of Rule 2 of the PML Rules.

3.11. **"Offline verification**" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar Act.

3.12. **"On-going Due Diligence**" means regular monitoring of transactions to ensure that they are consistent with the customers' profile and source of funds.

3.13. **"Officially valid document**" shall have the meaning assigned to it under sub clause (d) of clause (1) of Rule 2 of the PML Rules.

3.14. **"Politically Exposed Persons (PEPs**)" shall have the meaning assigned to it under sub clause (xii) of 3(b) of Chapter I of Master Direction – Know Your Customer (KYC) Direction, 2016 issued by Reserve Bank of India (RBI), as amended from time to time.

3.15**. "Principal Officer"** shall have the meaning assigned to it under sub clause (f) of clause (1) of Rule 2 of the PML Rules.

3.16. **"Suspicious Transaction"** shall have the meaning assigned to it under sub clause (g) of clause (1) of Rule 2 of the PML Rules.

3.17. **"Video Based Identification Process (VBIP)"** means an alternative (optional)electronic process of Identification/ KYC in paperless form, carried out by the Company/authorised person (person authorised by the Company and specifically trained for face-to-face VBIP) by undertaking seamless, secure, realtime, 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.

3.18 **"Company**" shall mean "The New India Assurance Company Limited".

3.19 **"Standard Operating Procedure [SOP]"** shall mean the procedure adopted by the Company under this policy

3.20. **Words and expressions** used and not defined in this policy but defined in the Insurance Act, 1938 (4 of 1938), Insurance Regulatory and Development Authority Act, 1999 (41 of 1999),the PML Act, the PML Rules, the Aadhaar Act, Unlawful Activities (Prevention) Act, 1967 shall have the meanings respectively assigned to them in those Acts, Rules, Regulations, Guidelines issued under those Acts, as the case may be.

4. Internal policies, procedures, controls and compliance arrangement

4.1. This policy is to establish and implement policies, procedures and internal controls that effectively serve to prevent and impede Money Laundering (ML) and Terrorist Financing (TF).

4.2. To be in compliance with these obligations, the policy is fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The policy will:

4.2.1. Develop a Standard Operating Procedure for dealing with ML and TF reflecting the current statutory and regulatory requirements.

4.2.2. Ensure that the content of the Standard Operating Procedure is understood by all staff members/agents. Develop awareness among staff members /agents and make them vigilant to guard against ML and TF.

4.2.3. Periodical review to be done on the basis of risk exposure and suitable changes (if any) be effected based on experience and to comply with the extant Act / Rules / Regulations and other applicable norms.

4.2.4. Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF.

4.2.5. Undertake CDD measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction.

4.2.6. Strengthen the system for identifying, monitoring and reporting suspected ML or TF transactions to FIU-IND and the law enforcement authorities (if so required).

4.3**. Standard Operating Procedure** set under the AML/CFT policy will ensure :

4.3.1. Communication of information relating to prevention of ML and TF to all level of management and relevant staff that handle policy holders' information in all the offices of the Company;

4.3.2. Client Due Diligence Program including policies, controls and procedures approved by the senior management, which will enable the Company to manage and mitigate the risk that have been identified either by the Company or through national risk assessment.

4.3.3. Maintenance of records;

4.3.4. Compliance with relevant statutory and regulatory requirements;

4.3.5. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information;

4.3.6. Role of internal audit/compliance function to 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 will be independent, adequately resourced and commensurate with the size of the business and operations, organization structure, number of clients and other such factors.

4.4. Responsibility:

The Standard Operating Procedure will ensure that the following steps are taken to strengthen the level of control on the intermediaries/representative engaged by the Company:

4.4.1. The list of rules and regulations covering performance of intermediaries/representative of insurer must be put in place. A clause will be added making KYC norms mandatory and specific process document can be included as part of the contracts.

4.4.2. Appropriate action shall be initiated against defaulting intermediaries /representative of Company who expose the Company to AML/CFT related risks on multiple occasions.

4.4.3. The selection process of intermediaries /representative of the Company shall be monitored scrupulously in view of set AML/CFT measures.

4.5. **Compliance Certificate**:

Company will submit annual compliance certificate as provided in **Annexure I** within 45 days of end of Financial Year.

5. Appointment of a Designated Director and a Principal Officer

5.1. A "Designated Director", who has to ensure overall compliance with the obligations imposed under chapter IV of the PML Act and the PML Rules, will be appointed or designated.

5.2. A Principal Officer (PO) at a senior level will be appointed to ensure compliance with the obligations imposed under chapter IV of the Act and the Rules.

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

5.4. In terms of Section 13 of the PMLA, the Director, FIU-IND can take appropriate action, including imposing a monetary penalty on Company or its Designated Director or any of its employees for failure to comply with any of its AML/CFT obligations.

6. Recruitment and Training

6.1. Adequate screening mechanism as an integral part of personnel recruitment/hiring process will be put in place.

6.2. On-going training programme will be put in place so that the members of staff are adequately trained in AML/CFT policy. The focus of the training will be different for frontline staff, compliance staff, staff dealing with new customers and claims. The front line staff will be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT Act/ Policies / Rules, guideline and related issues shall be ensured.

7. Internal Control/Audit

Internal audit/inspection department of Company will periodically verify compliance with the extant procedures and controls related to money laundering activities on the basis of overall risk assessment.

The audit reports will specifically render constructive suggestions where necessary, to strengthen the policy and implementation aspects. Audit notes and compliance will be submitted to the Audit Committee.

8. Know Your Customer (KYC) Norms

8.1. What are KYC Norms?

8.1.1. Considering the potential threat of usage of the insurance services by a money launderers, best efforts should be made to determine the true identity of customer(s).

8.1.2. Effective procedures 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/ insurance policies are not under anonymous or fictitious names.

8.1.3. Where a client is a juridical person, steps shall be taken to identify the client and its beneficial owner(s) and all reasonable measures be taken 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 sub rule (3) of Rule 9 of PML Rules.

8.1.4. While implementing the KYC norms on juridical persons, verification of identify and their legal status is to be done through various documents (indicated, but not limited to, at sub-rule (6) to (9) of rule 9 of the PML Rules), collected in support of

8.1.4.1. The name, legal form, proof of existence,

8.1.4.2. Powers that regulate and bind the juridical persons,

8.1.4.3. Address of the registered office/ main place of business,

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

8.1.4.5. Ascertaining Beneficial Owner(s)**.**

No opening of or keeping any anonymous account or accounts in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified, be allowed.

8.1.5. While implementing the KYC norms on juridical person other than those mentioned in sub-rule (6) to (9) of rule 9 of the PML Rules, it is to be verified that any person purporting to act on behalf of such client is so authorized and verification of the identity of that person is to be done.

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

A list of documents to be verified and collected under KYC norms for individuals is given in sub-rule (4) and (18) of rule 9 of the PML rules.

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

Under Individual Insurance 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.

8.1.7. KYC process may be performed by any of the following methods:

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

8.1.7.2. Aadhaar based KYC through offline verification Or

8.1.7.3. Digital KYC as per PML Rules Or

8.1.7.4. Video Based Identification Process (VBIP) as consent based alternate method of establishing the customer's identity, for customer. The process of VBIP has been specified in **Annexure II** Or

8.1.7.5. By using 'KYC identifier' allotted to the client by the CKYCR Or

8.1.7.6. By using Officially Valid documents

AND

8.1.7.7. PAN/Form 60 (wherever applicable) and any other documents as may be required by the Company

8.1.8. Under all kinds of Group Insurance Policies(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.

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

8.1.10 Care has to be exercised to avoid unwitting involvement in insuring assets bought out of illegal funds.

8.1.11 It is imperative to ensure that the insurance premium should not be disproportionate to income/ asset.

8.1.12 At any point of time, where Company is 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.

8.2. Client Due Diligence (CDD)

Company shall undertake CDD as per the provisions of Rule 9 of PML Rules. Accordingly, the Company shall undertake CDD as follows:

8.2.1. 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.

8.2.2. Knowing Existing Customer/Client

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 from time to time basis the adequacy of the data previously obtained.

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 continued operation of accounts of existing customers having insurance policy in a financial year, PAN/Form 60 may be obtained by such date as may be notified by the Central Government.

8.2.3. Ongoing Due Diligence

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

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

8.2.4. Verification at the time of payout/claim stage/refunds/reimbursement etc.

8.2.4.1. 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 .

8.2.4.2. Necessary due diligence should be carried out of the policyholders / beneficiaries/ legal heirs/ assignees before making the pay-outs.

8.2.4.3. Free look cancellations need particular attention of the Company especially in cases of client indulging in free look cancellation on more than one occasion at short intervals frequently.

8.2.5. 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, it 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.

9. Risk Assessment/ Categorization

9.1. Company has to carry out ML and TF Risk Assessment exercise as provided in sub rule (13) of Rule 9 of PML Rules periodically based on risk exposure to identify, assess, document and take effective measures to mitigate its ML and TF risk for clients/customers or geographic areas, products, services, nature and volume of transactions or delivery channels etc. While assessing the ML/TF risk, the Company is required to take cognizance of the overall sector specific and country specific vulnerabilities, if any, that the Government of India / IRDAI may share with Company from time to time. Further, the internal risk assessment carried out by Company should be commensurate to its size, geographical presence, complexity or activities/ structure etc.

9.2. In the context of the very large base of insurance customers and the significant differences in the extent of risk posed by them, as part of the risk assessment, the Company shall classify the customer into high risk and low risk, based on the individual's profile and product profile, to decide upon the extent of due diligence.

9.3. The documented risk assessment shall be updated from time to time. The Company shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. It shall be made available to competent authorities and law- enforcement agencies, as and when required.

9.4**. Risk Categorization**:

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

9.4.2. For the purpose of risk categorization, individuals (other than High Net Worth) and entities whose identities and source of wealth can be easily identified and transactions, which, by and large conform to the known profile may be categorized as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society, government departments and government

owned companies, regulators and statutory bodies. In such cases, it is required that only the basic requirements of verifying the identity and location of the customer are to be met. Notwithstanding the above, in case of continuing insurance policies, if the situation warrants, as for examples if the customer profile is inconsistent with this investment through top-ups, a re-look on customer profile is to be carried out.

9.4.3. The profiles, like for customers who are non - residents, high net worth individuals, trusts, charities, NGOs and organizations receiving donations, companies having close family shareholding or beneficial ownership, firms with sleeping partners, politically exposed persons (PEPs), and those with dubious reputation as per available public information who need higher due diligence, will be monitored for categorization for low / high risk.

10. Simplified Due Diligence (SDD)

10.1. 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 all insurance policies.

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'.

10.2. The list of simplified due diligence documents are specified in sub clause (d) of clause (1) of Rule 2 of the PML Rules.

11. Enhanced Due Diligence (EDD)

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

11.2. 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.

11.3. Company shall

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

11.3.2. Verify the client through other modes/ methods of KYC as specified in this policy.

11.4. Company shall examine the ownership and financial position, including client's source of funds commensurate with the assessed risk of customer and product profile.

12. Sharing KYC information with Central KYC Registry (CKYCR)

12.1. 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. 3183(E) dated November 26, 2015.

12.2. 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.

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

12.4. 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.

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

12.6. 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.

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

12.7.1. For online Authentication,

a) The redacted Aadhar Number (Last four digits)
b) Demographic details

c) The fact that Authentication was done

12.7.2. For offline Verification

a) KYC data

b) Redacted Aadhaar number (Last four digits)

12.8. 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 inforce /paid-up insurance policies against which "KYC identifier" are yet to be allotted/generated by the CKYCR.

12.9. 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).

13. Reliance on third party KYC

For the purposes of KYC norms under clause 8, while Company is 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.

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

14. Contracts with Politically Exposed Persons (PEPs)

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

14.2. 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 close relatives of PEPs are enumerated in Standard Operating Procedure. These measures are also to be applied to insurance contracts of which a PEP is the ultimate beneficial owner (s).

14.3. 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.

15. New Business Practices/Developments

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

15.1.1. Development of new products

15.1.2. New business practices including new delivery mechanisms

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

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

15.3. Standard Operating Procedure lays 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:

15.3.1. Ease of access to the facility;

15.3.2. Speed of electronic transactions;

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

15.4. 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.

15.5. Standard Operating Procedures lays down the procedure to manage specific increased risks associated with such relationships e.g. verification of details of the customer through on-site visits.

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

16.1. Section 51A of the Unlawful Activities (Prevention) Act, 1967(UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated 2nd February 2021 detailing the procedure for the implementation of Section 51A of the UAPA.

16.2. The Company should not enter into a contract with a customer whose identity matches with any person in the UN sanction list or with banned entities and those reported to have links with terrorists or terrorist organizations.

16.3. Company shall periodically check MHA [Ministry of Home Affairs] website for updated list of banned entities.

16.4. A list of individuals and entities subject to UN sanction measures under UNSC Resolutions (hereinafter referred to as "designated individuals/ entities") would be circulated to the Company 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 Ministry of Home Affairs (MHA) that have been circulated to the Company till date.

16.5. 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 policies with the Company. An updated list of individuals and entities which are subject to various sanction measures as approved by Security Council Committee established pursuant to UNSC 1267 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list and UNSC 1988 can be accessed regularly from the United Nations website at https://www.un.org/securitycouncil/sanctions/1988/materials.

16.6. By virtue of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), the Central Government is empowered to freeze, seize or attach funds of and/or prevent entry into or transit through India any individual or entities that are suspected to be engaged in terrorism. [The list is accessible at website http://www.mha.gov.in]. To implement the said section an order reference F. No. 14014/01/2019/CFT dated 2nd February, 2021 has been issued by the Government of India. The salient aspects of the order with particular reference to insurance sector are provided at **Annexure III**.

16.7. The list of Nodal Officers for UAPA is available on the website of Ministry of Home Affairs.

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

Company is required to:

17.1. 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.

17.2. Pay Special attention to business relationships and transactions, especially those which do not have 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 for assisting competent authorities.

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

17.4. 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.

17.5. 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).

18. Reporting Obligations

18.1. 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.

Explanation: In terms of Third Amendment Rules notified in September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU- IND shall have powers to issue guidelines to the Company for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

18.2. The reporting formats and comprehensive reporting format guide, prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist Company in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of until Company installs/adopt suitable technological tools for extracting CTR/STR from their live transaction data. The Principal Officers of the Company(nodal officer in all operating offices) shall have suitable arrangement to cull out the transaction details from Operating Offices to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

18.3. Illustrative list of Suspicious Transactions is shared by IRDAI through General Insurance Council. Further, Red Flag Indicators issued by FIU-IND also be taken in account for Suspicious Transaction, wherever necessary.

18.4. While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a mis- represented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. Company shall not put any restriction on operations in the accounts where an STR has been filed. 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.

18.5. Robust software, throwing alerts when the transactions are inconsistent with risk] categorization and updated profile of the customers is put in to use as a part of effective identification and reporting of suspicious transactions.

18.6. Company will leverage the broadest number of data points / records available with it in implementing alert generation systems to assist in identifying and reporting suspicious activities.

18.7. Company will not enter into arrangement with any unregulated entity which may have the effect of directly or indirectly impairing any reporting obligations of the Company.

19. Record Keeping

19.1. In view of Rule 5 of the PML rules, the Company, its Designated Director, Principal Officer, employees are required to maintain 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. Records pertaining to all other transactions, (for which Company is obliged to maintain records under other applicable Legislations / Regulations / Rules) Company will 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.

19.2. Records will be maintained in electronic form and/or physical form. In cases where services offered by a third party service providers are utilized,

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

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

19.2.3 The service provider has established standard transmission and encryption formats and non-repudiation safeguards for electronic communication of data.

19.2.4 It should also be ensured that the provisions under the relevant and extant data protection statutes are duly complied with.

19.3. Company has implemented specific procedures for retaining internal records of transactions both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved (if any) so as to provide, if necessary, evidence for prosecution of criminal activity. Company will retain the records of those contracts, which have been settled by claim or cancelled, for a period of at least five years after that settlement.

19.4. In situations, where the records relate to ongoing investigations, or transactions which have been the subject of a disclosure, they should be retained until it is confirmed that the case has been closed. Wherever practicable, Company is required to seek and retain relevant identification documents for all such transactions and report such transactions of suspicious funds.

19.5. In case of customer identification data obtained through the customer due diligence process, account files and business correspondence will be retained (physically or electronically) for at least five years after the business relationship is ended.

20. Monitoring of Transactions

20.1. Regular monitoring of transactions is vital for ensuring effectiveness of the AML/CFT procedures. This is possible only if an understanding of the normal activity of the client is there so that it can identify deviations in transactions/ activities.

20.2. Company will pay special attention to all complex large transactions/ patterns which appear to have no economic purpose. The Company has specified internal threshold limits for each class of client accounts and pay special attention to transactions which exceeds these limits. The background including all documents/ office records/ memorandums/ clarifications sought pertaining to such transactions and 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 of five years from the date of transaction between the client and Company.

20.3. The Principal Officer of the Company shall monitor and ensure that Suspicious transactions shall be regularly reported to the Director, FIU- IND.

20.4. Further, the compliance cell of Company shall randomly examine a sample of transactions undertaken by clients to comment on their nature i.e. whether they are in nature of suspicious transactions or not.

21. Repeal Provisions

From the date of coming into force of this policy, the instructions / guidelines contained in the New India Assurance Anti-Money Laundering / Counter Financing of Terrorism [AML / CFT] Policy 2013 shall stand repealed.

22. Notwithstanding anything contained in this policy, in case of any issue with respect to interpretation of any provision of this policy, the provisions/ directives of the FIU-India, the PML Act/ Aadhaar Act / Income Tax Act and their rules as amended from time to time, will prevail.

-Sd/-
(Neerja Kapur)
Chairman-cum-Managing Director

Annexure I

Certificate of Compliance

Name of Company: ***The New India Assurance Company Limited***

Financial Year:

We do hereby submit that our company ***The New India Assurance Company Limited*** 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)

Chairman Cum Managing Director (Name and Signature)

(* to be submitted within 45 days of end of FY)

Annexure II

Video Based Identification Process(VBIP)

Company may undertake live VBIP by developing an application which facilitates KYC process either online or face-to-face in-person verification through video. This may be used for establishment/continuation/ verification of an account based relationship or for any other services with an individual customer/beneficiary, as the case may be, after obtaining his/her informed consent and shall adhere to the following stipulations:

a) The Company/authorised person while performing the VBIP for KYC shall record clear live video of the customer/beneficiary present for identification and obtain the identification information in the form as below:

   i) Aadhaar Authentication if voluntarily submitted by the Customer/ beneficiary, subject to notification by the government under Section 11 A of PMLA or

   ii) Offline Verification of Aadhaar for identification, if voluntarily submitted by the Customer/beneficiary or iii) Officially Valid Documents (As defined in rule 2(d) under PML Rules 2005) provided in the following manner –

      1) As digitally signed document of the Officially Valid Documents, issued to the DigiLocker by the issuing authority or
      2) As a clear photograph or scanned copy of the original Officially Valid Documents, through the eSign mechanism.

b) The Company may also utilize this facility to verify PAN (wherever applicable). The Company/authorised person shall capture a clear image of PAN card to be displayed by the customer during the process, except in cases where e-PAN is provided by the customer. The PAN details shall be verified from the database of the issuing authority including through Digilocker. Use of printed copy of e-PAN is not valid for VBIP.

c) The Company/authorised person shall ensure that the online video is clear and the customer/beneficiary along with the authorised person in the video shall be easily recognisable and shall not be covering their face in any manner.

d) Live location of the customer/beneficiary (Geotagging) shall be captured (both for online/ face-to-face VBIP) to ensure that customer/beneficiary is physically present in India.

e) The authorised person/ Company shall ensure that the photograph and other necessary details of the customer/beneficiary in the Aadhaar/ Officially Valid Documents/ PAN matches with the customer/beneficiary present for the VBIP.

f) The authorised person/ Company shall ensure that the sequence and/or type of questions during video interactions are varied in order to establish that the interactions are real-time and not pre-recorded.

g) In case of offline verification of Aadhaar using XML file or Aadhaar Secure QR Code, if voluntarily submitted by the Customer/ beneficiary, it shall be ensured that the generation of XML file or QR code is recent and not older than 3 days from the date of carrying out VBIP.

h) All accounts opened or any service provided based on VBIP shall be activated only after being subject to proper verification by the Company to ensure that the integrity of process is maintained and is beyond doubt.

i) Company shall ensure that the process is a seamless, real-time, secured, end- to-end encrypted audio-visual interaction with the customer/beneficiary and the quality of the communication is adequate to allow identification of the customer/ beneficiary beyond doubt. Company shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations.

j) To ensure security, robustness and end to end encryption, the Company shall carry out software and security audit and validation of the VBIP application as per extant norms before rolling it out and thereafter from time to time.

k) The audio-visual interaction shall be triggered from the domain of the Company itself, and not from third party service provider. The VBIP process shall be operated by the Company/authorized persons. The activity log along with the credentials of the official performing the VBIP shall be preserved.

l) Company shall ensure that the video recording bears the GPS coordinates, date (DD:MM:YY) and time stamp (HH:MM:SS) along with other necessary details, which shall be stored in a safe and secure manner as per PML Rules.

While exercising Online VBIP, the Company shall exercise extra caution and the additional necessary details viz. IP address etc. shall be preserved by the Company to substantiate the evidence at the time of need.

m) Company are encouraged to take assistance of the latest available technology (including Artificial Intelligence (AI) and face matching technologies etc.) to strengthen and ensure the integrity of the process as well as the confidentiality of the information furnished by the customer/beneficiary. However, the responsibility of identification shall rest with the Company.

n) Authorized person of the Company shall facilitate face to face VBIP process only at the customer/beneficiary end.

However, the ultimate responsibility for client due diligence will be with the Company.

o) Company shall maintain the details of the concerned Authorised person, who is facilitating the VBIP.

p) Company shall ensure to redact or blackout the Aadhaar number as per extant PML Rules.

q) Company will adhere to the IRDAI Cyber security guidelines as amended from time-to-time along with the necessary security features and standard as mentioned below:

- The Video KYC application and related APIs/Web Services shall undergo application security testing (both gray box and white box) through an CERT-In empanelled vendor and all reported vulnerabilities shall be mitigated before moving into production.

- The infrastructure components used for hosting Video KYC application shall undergo vulnerability assessment and secure configuration review through an CERT-In empanelled vendor and all reported vulnerabilities shall be mitigated before moving into production.

- There shall be an end-to-end encryption from the customer/beneficiary to the hosting point of the Video KYC application. The minimum encryption standards and key lengths like AES 256 for encryption should be used.

- If the Video KYC application and video recordings are located at a third party location and/or in Cloud then the third party location and/or cloud hosting location shall be in India.

Annexure III

Implementation of Section 51A of UAPA

To implement the said section an order reference F. No. 14014/01/2019/CFT dated 2nd February, 2021, has been issued by the Government of India. The salient aspects of the order with particular reference to insurance sector are detailed in the following paras:

i. Procedure for reporting/freezing of insurance policies of 'designated individuals/entities'

In case any matching records are identified, the procedure required to be adopted is as follows:

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) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the Company shall immediately inform full particulars of the funds, financial assets or economic resources or related services in the form of insurance policies, held by such a customer on their books to the Central [designated] Nodal Officer for the UAPA, at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: jsctcr-mha@gov.in.

c) The Company shall also send a copy of the communication mentioned in 1(b) above to the UAPA Nodal Officer of the State/UT (where the account is held) and to IRDAI and FIU-IND without delay.

d) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, Company shall prevent such designated individuals/entities from conducting any transactions, under intimation to the Central [designated] Nodal Officer for the UAPA at Fax No. 011-23092551 and also convey over telephone No. 011-23092548. The particulars apart from being sent by post should necessarily be conveyed on e-mail id: jsctcrmha@gov.in, without delay.

e) Company shall file a Suspicious Transaction Report (STR) with FIU-IND in respect of the insurance policies covered by paragraph (1) (a) above, carried through or attempted, in the prescribed format.

f) On receipt of the particulars (held in the form of Insurance Policies) of suspected designated individual/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.

g) 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 IRDAI and FIU-IND.

h) The said order shall take place without prior notice to the designated individuals/entities.

'Freezing of insurance contracts' would require not-permitting any transaction (financial or otherwise), against the specific contract in question.

ii. 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

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

b) 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 within two working days.

c) 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.

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

a) U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets 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.

b) 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.

c) 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, request would be electronically forwarded to the Nodal Officer in IRDAI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

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

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

iv. Communication of orders under section 51A of UAPA

IRDAI would communicate all Orders under section 51A of UAPA relating to insurance policies, to all the Company after receipt of the same from MHA.

v. Exemption in accordance with UNSCR 1452

The above provisions of freezing shall not apply to funds and other financial assets or economic resources that are necessary for paying insurance premiums or exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services or fees or service charges for routine holding or maintenance of frozen funds or other financial assets or economic resources, after notification by the MEA of the intention to authorize, where appropriate, access to such funds, assets or resources and in the absence of a negative decision within 48 hours of such notification.