Anti-Money Laundering Policy
HNB Assurance PLC Group

(HNB Assurance PLC and HNB General Insurance Limited)

Version Control status of the Anti-Money Laundering Policy

Version Number	Dates produced and approved (Include committee)	Reason for Production / Areas of revision)	Author / Reviewer (Designation)	Ownership
V 1.0	2006	In compliance with the Prevention of Money Laundering Act No 5 of 2006 and Financial Transaction Reporting Act No 6 of 2006	Senior Manager Risk and Compliance	Risk and Compliance Department
V 2.0	21st October 2016 (Risk Committee meeting) November 2016 (Board Meeting)	Annual Review Process	Senior Manager Risk and Compliance	Risk and Compliance Department
V 3.0	February 2019	• Include the guidelines for identifying Politically Exposed Persons (PEPs) in terms of AML as an Annexure • Instructions on the Risk Rating of customers when creating new customers in the system	Author: Assistant Manager Risk and Compliance Reviewer: Head of Risk and Compliance	Risk and Compliance Department
V 4.0	21st August 2019 (Risk Committee meeting)	• In compliance with Rules cited as the Insurers (Customer Due Diligence) Rules, No.1 of 2019 under Section 2 of the Financial Transaction Reporting Act, No.6 of 2006	Author: Manager Risk and Compliance Reviewer: Manager Legal & Chief Legal Officer	Risk and Compliance Department
V 4.1	19th August 2021 (Risk Committee meeting)	• Policy amended as per new requirements stated in FIU guidelines on Non face to face Customer identification and verification Using electronic interface provided by the Department for Registration of Persons (DRP) and recommendations and comments given by the Compliance Department of HNB	Author: Manager Risk and Compliance Reviewer: Senior Manager Legal	Risk and Compliance Department

V 5.0	17th February 2022 (Risk Committee meeting) 18th February 2022 (Board Meeting)	Policy amended based on the recommendations given by the IRCSL through its Remote onsite examination report examination was conducted by IRCSL jointly with FIU in August 2021.	Author: Manager Risk and Compliance Reviewer: Senior Manager Legal	Risk and Compliance Department
V 6.0	05th February 2025 (Risk Committee meeting) 17th February 2025 (Board Meeting)	Policy amended based on FIU Circular 01/2024 on 'Compliance with the Reporting Requirements under the Financial Transactions Reporting Act, No. 6 of 2006' for GoAML reporting, Red Flag Indicators No.3 of 2023- Identification of reporting Suspicious Transactions relating to the Insurance Sector	Author: Manager Compliance Reviewer: Compliance Officer of HNBA & HNBGI	Legal and Compliance Department

Table of Contents

1. Introduction

1.1 Policy Statement and Principles

In compliance with the Prevention of Money Laundering Act No 5 of 2006 and subsequent amendments thereto , Financial Transaction Reporting Act No 6 of 2006 and Convention on Suppression of Terrorist Financing Act No 25 of 2005 and subsequent amendments thereto strengthening the relevant authorities to administer the above Acts by providing appropriate tools required to intercept, prevent and obstruct money laundering and financing to terrorism, HNB Assurance PLC ("HNBA") and HNB General Insurance Limited ("HNBGI") have adopted an Anti-Money Laundering (AML) Policy ("Policy").

2. Scope

2.1 Scope of Policy

This Policy applies to HNB Assurance PLC Group ("the Group"), (which includes HNB Assurance PLC ("HNBA") who carries out Life Insurance business and its fully owned subsidiary HNB General Insurance Limited ("HNBGI") who carries out General Insurance business) its officers, employees, appointed agents and products and services offered by the Group. All business units and Branches within the Group will cooperate to create a cohesive effort in the fight against money laundering and terrorist financing. Each business unit and Branch will implement risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions required under Financial Transaction Reporting Act No 6 of 2006.

2.2 Policy

It is the policy of the Group to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Group is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed agents to adhere to these standards in preventing the use of its products and services for money laundering purposes. Also, to bring to the attention of relevant authorities, transactions those are of a nature defined as money laundering as per the relevant Acts.

3. Definition of the Term Money Laundering

For the purposes of the Policy, money laundering is generally defined as the process of transforming the proceeds derived from illegal and or criminal activities into some form of legitimate asset.
Or
Money laundering is generally defined as the Processing of criminal proceeds (Profits or other benefits) in order to disguise their illegal origin (The Financial Action Task Force -FATF)

Generally, money laundering occurs in three stages.

Proceeds first enters the financial system at the "***placement***" stage, where the Proceeds generated from unlawful activities is converted into monetary instruments,such as money orders or traveler's cheques, or deposited into accounts at financial institutions.

At the "***layering***" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its unlawful origin.

At the "***integration***" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other lawful activities or legitimate businesses.

4. Money Laundering (ML) & Terrorist Financing (TF) Risk exposure in relation to HNBA Group issued products and related other activities

HNBA Group issue Life Insurance Products through the HNBA and General Insurance Products through the HNBGI, further Group has performed required other related financial activities such as Reinsurance transactions, sale of salvage items etc. based on the features of issued Insurance Products (Product related ML & TF risk), customer related factors, Delivery channel related factors, Geographic related factors effect to Group exposed to Money Laundering and Terrorist Financing risk on various levels. Therefore, the Group has developed appropriate level of control environment to fight against ML & TF risks. Below section provides brief details regarding the ML & TF exposure level of Group issued Products and other related activities.

4.1 HNB Assurance PLC (HNBA) issued Products and related other activities

Life Insurance product related risk refers to the vulnerability of a product to ML/TF based on its design. HNBA has issued some products which has the attribution of increasing the ML/TF risk profile such as acceptance of very high value or unlimited value payments or large volumes of lower value payments, acceptance of non-traceable payments such as cash, Mobile cash payments, money orders, cashier cheques, acceptance of frequent payments outside a normal premium or payment schedule, allowance of withdrawals at any time or early surrender with limited charges or fees, products that allow for high cash values, Products that accept high amount lump sum payments, Products with provisions that allow a policy to be cancelled within a stipulated time frame and the premiums paid to be refunded and products that allow for assignment without the Company being aware that the beneficiary of the contract has been changed, Products with features that allow loans to be taken against the Policy etc. HNBA has designed and issued various kinds of products which include above features on different levels, therefore the Company is Conducting ML/TF risk assessment prior to the launch of new products and new business practices. Accordingly, HNBA has developed required control mechanisms to mitigate the ML/TF risk exposure of its Products. The features of the several products issued by the Company and features of other activities involved with the Company (e.g. Reinsurance Transactions) are stated below.

1. Universal Life insurance Products which offer a low cost protection of term insurance as well as a savings element which is invested to provide cash value buildup.

2. Single premium products-where the money is invested in lump sum and surrendered at earliest opportunity.

Investment Policy
This is a single premium investment policy which has fixed term. At maturity, Life assured will entitle to get the amount agreed in the policy. In the event of the death during the policy term beneficiary will be entitled to amount agreed in the policy.

Mortgage Reducing Policy
Outstanding loan capital is payable in the event of death or permanent total disability to lending institution.

Single premium Endowment Policy
Accidental death benefit and total permanent disability can be taken as riders in addition to life cover.

Micro Insurance Policy for HNB
Outstanding loan capital is payable in the event of death or permanent total disability to lending institution and basic sum assured is payable to the nominee in case of the death of the life assured.

3. Term Life Insurance contracts, in view of the absence of cash surrender value and stricter underwriting norms for term policies. (especially those with large face amounts)
   Term assurance product offered by HNBA includes TPD and PPD due to accident as riders in addition to life cover.

4. Group term Life Assurance Schemes offered by HNBA covers Life, Accidental death, Total Permanent Disability, Partial Permanent disability and Critical illness, Group Personal Accident, Group WCI, Group Medical Expenses and Fidelity Guarantee, etc.

5. Unit linked products which provide for withdrawal and unlimited top up premiums
   (Currently these kinds of Products not offered by HNBA).

6. Reinsurance contracts where treaties are between insurance companies and do not involve transactions with customers. Further, when Company dealing with Reinsurance Companies ensure to comply with guidelines requirements issued by IRCSL regarding reinsurance placement therefore possibility to expose in Money laundering risk and terrorist Financing risk is minimal.

4.2 HNB General Insurance Limited (HNBGI) issued Products and related other activities.

Owing to some features, General Insurance Products are less vulnerable to ML/TF risk when compared to Life Insurance Products. However, HNBGI also has created an adequate control environment within the Company to fight against ML & TF risk. Further, HNBGI has performed threshold reporting requirements as prescribed by the regulatory authority on a continuous basis. HNBGI issued products features and features of other activities involved by the Company (e.g. Reinsurance Transactions, Salvage Transactions etc.) also include in below section.

1. Policies issued by HNBGI are less vulnerable to money laundering as it covers the risk of an Asset where the Asset value is significantly higher than the insurance premium. If a Financial Institute

has a financial interest over the assets that were insured those policies will be considered as Low Risk exposure in terms of ML/TF.

2. HNBGI policies issued to individuals where there is no financial interest by a Financial Institute over the assets insured are considered as appropriate risk exposure in terms of ML/TF, All transactions are report to Required regulatory authorities subject to the annual premium of the policy being over Rs. 1,000,000/-.

3. Group Insurance Business, which are typically issued to a company, financial institution, or association and generally restrict the ability of an individual insured or participant to manipulate its investment. However, all transactions are subject to the requirement of reporting same to required regulatory authorities under the threshold reporting requirements.

4. Reinsurance contracts where treaties are between insurance companies and do not involve transactions with customers. Further, when Company dealing with Reinsurance Companies ensure to comply with guidelines requirements issued by IRCSL regarding reinsurance placement therefore possibility to expose in Money laundering risk and terrorist Financing risk is minimal.

5. Sale of salvage in HNBGI is exposed to a greater risk of Money Laundering and therefore proper screening of buyers is required. HNBGI is required to follow the customer identification programme applicable to 'Insurance contracts with individuals' as stated in this policy when registering and selecting the salvage buyers.

5. Customer Identification Programme

The Group will adopt a Customer Identification Programme (CIP). The Group will collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare customer identification information with the sanctioned lists provided by the Central Banks of Sri Lanka and other relevant authorities with known criminal background or with banned entities and those reported to have linked with terrorist organizations. Further, in this process HNBA will adopt with all required requirements stated in the Insurers (Customer Due Diligence) Rules, No.1 of 2019.

5.1 Required Customer Information

5.1.1 Insurance contracts with individuals

The Group will obtain the following information reasonably required to identify all new customers:

- Full Name as appearing in the Identification Document
- Permanent Address as appearing on the identification Document.
- National Identification Number
- In the absence of NIC the Passport number and Country and place of issuance
- Profession/Occupation
- Nationality

For photo identification, Group may endeavor to obtain copies/peruse any one of the following documents to verify the identity of all customers:

- National Identity Card
- Valid Passport
- Valid Driving Licence

If necessary, the Group will also endeavor to obtain copies of any one of the following documents as proof of residence of all new customers:

- Telephone Bill (Fixed line)
- Bank Account statement
- Electricity bill
- Water bill

The Group shall also obtain further information/Documentation when and where required for the purpose of identifying and initial risk profiling of customers.

Refer instructions in relation to the above laid down under AML Procedure.

5.1.2 Insurance Contracts with Companies

The Group will obtain the following information reasonably required to identify all new customers:

- Name of Company appearing in the business registration document
- Nature of Business
- Registered address of Principal place of Business
- Mailing address of the Company
- Telephone /Fax Number/E-Mail
- Income Tax File Number
- Bank references
- Identification of all Directors as in the case of individual customers
- List of Major shareholders with equity interest of more than ten percent
- List of subsidiaries and affiliates
- Details of names of signatories

The Group may also endeavor to obtain any one of the following documents to verify the identity of all new customers:

- Certificate of Incorporation and Memorandum & Articles of Association
- Board Resolution authorizing to obtain the insurance Policy.
- Power of Attorney granted to its managers, officers or employees to transact business on its behalf

The Group shall also obtain further information/Documentation when and where required for the purpose of identifying and initial risk profiling of customers.

Refer AML procedure given instructions regarding the above for more details.

5.1.3 Insurance Contracts with partnership firms

The Group will obtain the following information reasonably required to identify all new insurance customers:

- Legal name
- Nature of the business
- Registered Address

- Names of all the partners and their addresses.
- Telephone numbers of the firm and partners

The Group may endeavor to obtain any one of the following documents to verify the identity of all new customers:

- Registration certificate, if registered
- Partnership deed
- Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf
- Any officially valid document to identifying the partners and the persons holding the Power of Attorney and their addresses

The Group shall also obtain further information/Documentation when and where required for the purpose of identifying and initial risk profiling of customers.

Refer AML procedure given instructions regarding the above for more details.

5.1.4 Insurance Contracts with trusts, foundations, Clubs, Societies, Charities, Associations and Non-Governmental Organizations.

The Group will obtain the following information reasonably required to identify all new insurance customers:

- Name of trustees, settlers beneficiaries and signatories
- Names and addresses of the founder, the managers/directors and beneficiaries
- Telephone / fax numbers

The Group may endeavor to obtain any one of the following documents to verify the identity of all new customers:

- Certificate of Registration, if registered
- Power of Attorney granted to transact business on its behalf
- Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders /managers/directors and their addresses
- Resolution of the managing body of the foundation/association

The Group shall also obtain further information/Documentation when and where required for the purpose of identifying and initial risk profiling of customers.

Refer instructions laid down under AML Procedure for further details.

5.2 Prohibit to issue Numbered Insurance Policy

The Group shall not open, operate or maintain any anonymous insurance policy, any insurance policy in a false name or in the name of a fictitious person, or any insurance policy that is identified by a number only. (Prohibit to issue “Numbered Insurance Policy”)

(Note: Numbered Insurance Policy includes an insurance policy that the ownership is transferrable without knowledge of the Insurer and an insurance policy that is operated and maintained with the insurance policy holder’s name omitted)

6. Risk Profile of Customers and Due Diligence

Upon the initial acceptance of a customer, the Group shall categorize its customers into low risk, medium risk and high risk Customers (Create Customer's risk Profile) based on his or her level of money laundering and terrorist financing risk, in the event of risk profiling on its customers, Group is required to consider following factors and make the judgment accordingly.

- Risk level according to customer category (e.g. different types of customers such as resident or non-resident, occasional or one-off, legal persons, politically exposed persons (PEPs) and customers engaged in different types of occupations)
- Geographical location of business or country of origin of the customer
- Products, services, transactions or delivery channels of the customer (e.g. cash based, face to face or non-face-to -face, cross-border)
- Any other information regarding the customer.

The group categorizes its customers in to low, medium and high risk customers and relevant staff members update the core system accordingly. following section give required directions and recommendations to create Customer risk profile, however, relevant staff members who are engaged with customer on boarding activities must consider Customer's identification, transaction and other relevant details appropriately and make this judgment accordingly. Further Customer risk profile details must be updated based on customer's updated information.

6.1 Low risk customers are considered as individuals (other than high net worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile.

6.2 Medium risk customers are likely to pose a higher than average risk to the Company depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc., such as

a) Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.

b) Where the client profile of the person/(s) opening the account, according to the perception of the Company is uncertain and/or doubtful/dubious.

6.3 High risk customers are considered to be customers vulnerable to money laundering and terrorist financing such as non-residents, high net worth individuals, trusts, charities, NGO's, People who are live in High Risk Countries 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. Refer Anti-Money Laundering procedure regarding the details of High Risk Countries. Note that all customers who are categorize as PEPs need not rate as High Risk customer in terms of ML, company is required to consider his or her profession and features of obtaining policies and volume of premium amount, source of funds and source of wealth etc. to make the judgment regarding his or her appropriate risk category.

6.4 Due Diligence Tests

6.4.1 Low and Medium Risk Customers

The Group will obtain basic minimum information and documents in order to confirm its identity and location.

6.4.2 High Risk Customers

Apart from basic information obtained for low and medium risk customers the information as to sources of funds will be obtained for high risk customers.

The Group shall apply enhanced Customer Due Diligence (CDD) measures and shall apply appropriate counter measures when entering into Business relationships and transactions with customers who have been rated as High Risk.

Refer further instructions on enhanced Customer Due Diligence (Enhanced CDD) measures laid down under AML Procedure.

6.4.3 Sources of Funds

The Group will, where necessary, request its new customers to provide information as to source of income and availability of a tax file.

The Group will make every effort reasonably possible to obtain Standard Income Proof as given below with regard to high risk customers:

In the case of individuals

- Income tax assessment orders/Income Tax Returns
- Employee Certificates

In the case of Company's

- Audited Company Accounts
- Income Tax Returns

In the case of Partnerships

- Audited firm accounts and Partnership Deed
- Income Tax Returns filed by partners individually.

In the absence of Standard Income Proofs the Group will resort to obtain Non – Standard Income Proof of income as given below:

- Chartered Accountant's Certificate
- Bank Cash flow statements
- Pass-Book

In the absence of above information, the customer could suggest any other form of proof of income, which would be decided by the Compliance Officer whether it is adequate to serve the purpose for which it is required.

6.4.4 Non face to face business /Products issuing through new Technologies

In case of non-face to face business, which includes Tele calling, internet marketing, logging in of business or payment of premium / lump sums at business units documents in order to confirm identity, proof of income and residency to be obtained by the Group within such number of days as required by each product and in respect of premiums exceeding by such amount as described in each

product. Further, in these arrangements the Group adopts Premium accepting process through the banking channel such as Fund transfers, debit card or credit card payments and Group ensures that the required details are received from the Customers.

Under this HNBA should follow the Guidelines on Non face to face Customer identification and Verification Using Electronic Interface provided by the Department of Registration of persons, (DRP). No.3 of 2020 appropriately.
Refer AML procedure given instructions regarding the above for more details.

6.4.5 Verifying Information
Based on the risk, and to the extent reasonable and practicable, the Group will ensure that it has a reasonable belief of the true identity of its customers.

Refer instructions laid down under AML procedure in relation to the Non Face to Face Customer Identification and verification using Electronic Interface provided by the Department for Registration of Persons (DRP)

6.4.6 Customers Who Unreasonably Refuse to Provide Information
If a customer unreasonably refuses to provide the information described above when requested or appears to have intentionally provided misleading information the business unit (direct acceptance of application) or the appointed agent shall notify the relevant Head of the Department. The Head of the Department will decline the application and notify the Compliance Officer for further required actions.

6.4.7 Identification of Ultimate Beneficial Owner:
Whenever the Company is required to identify a customer, it must establish and verify the identity of the ultimate natural person,
- who owns or
- controls the customer or its assets or
- on whose behalf the transaction is carried out or the business relationship is established

(Note: The Group will obtain basic minimum information and documents in order to identify Beneficial Owner of the Transaction)

6.4.8 Screening of policyholders against sanctions list:
It is a directive of CBSL that all Financial Institutions of the country to strictly comply with sanctions screening in AML/CFT Compliance.

The Group shall exercise care in determining with whom the Company should do business.
The Group shall comply with the sanction rules of Anti money laundering (AML) and Countering the Financing of Terrorism (CFT) by complying with sanction lists imposed by the United Nations (UN) Security Council and other similar institutions. Sanctions data shall be updated and maintained on a regular basis. Updated Sanctions lists details are included in both companies' intranet and relevant sanction lists are as follows. Refer Anti-Money Laundering procedure regarding the full details of screening process, frequency etc.

- United Nations Regulation, No.1 of 2012 (for UNSCR 1373 regime on Local terrorists List) – 1373 Regulations
- United Nations Regulation, No. 2 of 2012 (for UNSCR 1267,1988,1989,2253 regimes on Al-Qaida, Taliban and ISIL List) – 1267 Regulations

- United Nations (Sanctions in relation to Democratic People's Republic of Korea) Regulations of 2017 (for UNSCR 1718 regime on North Korea) – DPRK Regulations
- United Nations (Sanctions in relation to Iran) Regulations No.1 of 2018 – Iran Regulations (This List is no longer in effect from 23rd October 2023).

A periodic review of the customer base is needed to ensure the Company is not doing business with sanctioned individuals and entities to avoid and mitigate the severe penalties for noncompliance with regulations. Accordingly, Group will perform the Customer screening activities at the time of new customer onboarding stage and at the time of sanctioned lists are updated by the relevant authorities.

As stated above, Sale of salvage in HNBGI is exposed to a greater risk of Money Laundering and therefore proper screening of Salvage buyers is required. Accordingly, HNBGI will collect certain minimum identification information from each salvage buyer, record such information and the verification methods and results; and compare identification information with the sanctioned lists and other relevant authorities with known criminal background or with banned entities and those reported to have linked with terrorist organizations.

Furthermore, the Group shall not provide any financial services I.e. Agency code issuing & commission payments, Providing Employment opportunities & any other transactions e.g. supplier payments, Salvage transactions, Investigation fee payment, any other payments. Additionally, the Group will not make funds available for the usage or benefit of designated persons and their associates mentioned in the aforesaid designated lists published by the Central Bank of Sri Lanka time to time.

6.4.9 Politically Exposed Person (PEP)

A PEP is a term which describes individual who is entrusted with a prominent public functions either domestically or by a foreign country, or in an international organization and includes a head of a state or a Government, a politician, a senior government officer, judicial officer or military officer, a senior executive of a state owned Corporation, Government or autonomous body but does not include middle rank or junior rank individuals , a relative or known associate of that person. A PEP is one of the categories of people who may be subject to 'enhanced due diligence'. In essence, this means they will be subject to more rigorous checks when entering into a business relationship with the Company than other categories of customers.

HNBA will follow below steps at the time of Customer onboarding stage applicable to politically exposed person or an immediate family member and a close associate of a politically exposed person is a customer or beneficial owner.

- Obtain approval from the senior management (e.g. Head of Life Operations/CTO/CEO) to enter or continue business relationship with PEPs.
- Identify, by appropriate means, the source of funds and the source of wealth.
- Conduct enhanced CDD and ongoing monitoring of their business relationship with the Company.

HNBA will follow the above steps at the time of existing customer become a PEP customer.

Refer further instructions on identification of Politically Exposed Person (PEP) laid down under AML Procedure.

6.4.10 Insurance Agents required to perform CDD

Insurance Agents are required to perform the required level of Customer Due Diligence (CDD) measures and the Company takes appropriate enforceable action against the Agent in the event of non-compliance of required level of CDD performance by the Agent stipulated in the Agency agreement signed with the Company.

Refer instructions on the CDD measures laid down under AML procedure.

6.4.11 Safeguards

The Group will issue the following instructions to its employees as a safeguard against money laundering:

- To endeavor to accept premiums beyond Rs.500,000/= through cheques, demand drafts, credit card or any other banking channel.
- For integrally related transactions, premium amount greater than Rs.500,000/= in a calendar year should be examined more closely for possible angles of money laundering. This limit will apply at an aggregate level considering all the roles of a single person as a proposer or life assured or assignee.

- With regard to life insurance, no payments should be made to third parties except in cases like superannuation/gratuity accumulations and payments to legal heirs in case of death benefits. All payments will be made after due verification of the bona fide beneficiary, through account payee cheques.

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

- To obtain wherever possible the details of the Bank Accounts of customers to ensure that they have gone through a more rigorous screening on Anti-Money Laundering through another Financial Institute.

6.4.12 Conducting On-Going Customer Due Diligence

The Group shall conduct on-going Customer Due Diligence and on-going transactions scrutiny in terms of the provisions of section 5 of Financial Transactions Reporting Act, No.06 of 2006 on continuing business relationship with the customer. Accordingly Group scrutinizing transactions undertaken throughout the course of relationship to ensure that the transactions being conducted are consistent with the knowledge of the Company in respect of the Customer and its business and risk profile including the source of funds, Further, ensuring that documents, data or information collected under the CDD process are kept up to date and relevant. The Group is taking into consideration the economic background and purpose of transaction or business relationship with customer. Accordingly, Group will monitor and report Customer's renewal premiums under its threshold reporting process.

Refer further instructions regarding On-going customer due diligence laid down under AML Procedure.

6.4.13 Reliance on Third-Parties when conducting CDD in certain situations

The Group may rely on a third party financial institution or designated non-financial business to conduct CDD measures, when it is not practical to do it by the company itself.

The Group, when relies on a third party as stated above shall obtain necessary information/ Copies of identification data/relevant documentation if required.

7 Monitoring and Reporting

Systems will be adapted for transaction based monitoring which will occur within the appropriate business units of the Group. Monitoring of specific transactions will include, but is not limited to transactions aggregating Rs.500,000 /= or more and those with respect to which HNBA and HNBGI has a reason to suspect suspicious activity. Systems would be adapted to document and retain reports in accordance with the Act.

HNBA and HNBGI will immediately (within 2 working days) upon identification of suspicious transactions, will submit the STR to FIU in accordance with the guidance given by FIU. Respective Business units heads or relevant branch officials should immediately report such suspicious transactions with relevant details (e.g. KYC details and ground of suspicion) to Compliance Officer (CO), accordingly, CO responsible to perform further verification of reported suspicious transaction details and will submit the STR to FIU within the given deadline.

With the implementation of new Reporting Requirements, goAML reporting requirements, as a Financial Institute (FI), HNBA group needs to comply with the Financial Transactions Reporting Act (FTRA), No.06 of 2006 & relevant subsequent amendments and as per the matters stated in Circular 1 of 2024 issued by the FIU dated 01st April 2024, Suspicious or information about transactions relating to unlawful activities or other offences (as per Section 7 of the FTRA) to the FIU exclusively through the goAML system.

Further in compliance with the new Reporting Requirements, goAML reporting system under Section 6 of the FTRA No.06 of 2006 and as per the matters addressed pertaining to aforesaid area under Circular 1of 2024 dated 01st April 2024 issued by FIU, details of transactions in cash and electronic fund transfers ("threshold transactions") exceeding Rupees one million or its equivalent in any foreign currency, shall be submitted exclusively through the goAML system.

As stated in the above legislations, FIs are required to use one of the following methods for submission of threshold transactions and suspicious transactions to the goAML system.

i. Manually input transaction details into the goAML web forms and submit the reports, or

ii. Create XML (Extensible Markup Language) reports containing transaction details and upload the XML reports to the goAML system

As stipulated by Section 6 of the FTRA, HNBA Group shall ensure that all threshold transactions are 'Reported' to the goAML system within 31 calendar days of the transaction's occurrence.

Further, for suspicious transactions, as stipulated in Section 7 of the FTRA, the reporting timelines specified therein shall apply, regardless of the number of returns and subsequent re-submissions made by Reporting Institutes due to any issues or errors in the submitted data.

7.1 Suspicious Activity

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the Compliance Officer.
Examples of red flags are:

- The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.

- Policy from a place where he does not reside or is employed.

- Frequent request for change in address.

- Borrowing the maximum amount against a policy soon after buying it.

- Inflated or totally fraudulent claims e.g. by arson or other means causing a fraudulent claim to be made to recover part of the invested illegitimate funds.

- Overpayment of premiums with a request for a refund of the amount overpaid.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs 1,000,000/= reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

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

- In case of policy being assigned to a third party not related to him. (except where third party is to banks/financial institutions/capital market intermediaries regulated by CBSL/IRCSL/SEC)

Further, the FIU regularly issues red flag indicators to the financial sector from 2020 to guide them in identifying possible money laundering/terrorism financing (ML/TF) and other criminal activities and to report suspicious transaction by identifying any transaction patterns, activity or consumer behavior.
Accordingly, FIU has developed and issued Red Flag Indicators No.03 of 2023 – Identification of Suspicious Transactions relating to the Insurance Sector, to increase the awareness of the Insurance sector in identifying such suspicious transactions & activities and the same has been enclosed in AML Procedure.

Any suspicious transaction relating to any of the unlawful activities and offences should be report immediately to the Compliance Officer as per the instructions given in AML procedure.

7.2 Investigation

Upon notification to the Compliance Officer of a match to the list of high risk persons which will be provided by IRCSL or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies (FIU). The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a STR will be filed with the appropriate law enforcement or regulatory agency (FIU). The Compliance Officer is responsible for notifying the law enforcement or regulatory agency (FIU).

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know.

7.3 Record-keeping

The Compliance officer will be responsible to ensure that AML records are maintained properly and that STRs, CTRs and EFTs are filed as required. HNBA and HNBGI will maintain copies of STRs, CTRs and EFTs submitted to FIU as well as records of identity verification in relation to same for at least six years. The Six-year retention period will be applied for six years from the date of the transaction, correspondence or furnishing of the report as the case may be.

Such documents will be filed in a manner that would enable to provide to FIU at any time the

information requested by them. The copies of STRs, CTRs and EFTs will be kept in the safe custody of Compliance Officer.

7.4 Recruitment

The Group shall implement a comprehensive Employees / Agents due diligence and screening procedure to be carried out at the time of appointing or hiring of all employees/Agents irrespective whether they are permanent, contractual or outsourced.

7.5 Training

The Group will provide in house training on AML/CFT to its officers, employees and appointed agents if required to ensure awareness of requirements under the Act. The training will include, how to identify red flags and signs of money laundering; what roles the officers, employees and appointed agents have in the Group's compliance efforts and how to perform such duties and responsibilities; what to do once a red flag or suspicious activity is detected; The Group's record retention policy; and the disciplinary consequences for non-compliance with the Act and this Policy.

Training will be conducted on a periodic basis. The Compliance Officer will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training.

7.6 Conducting entity wide Money Laundering & Terrorist Financing risk Assessment

HNBA will provide a report of its risk assessment, regarding money laundering and terrorist financing risk profile and the effectiveness of risk control and mitigation measures to the Board of Directors annually (during the second Quarter of each year). Its reporting frequency shall commensurate with the level of risks involved and will decide accordingly. This risk assessment covers the ML/TF risk control and mitigation measures applicable in the areas such as Customers, Products, delivery channels, Agents, Employees etc.

7.7 Reporting to the Board and Board Risk Management Committee

The Compliance Officer will submit report to the Board on Bi-annual basis its money laundering and terrorist financing risk profile and the effectiveness of risk control and mitigation measures adopted by the HNBA. It consists of result of monitoring activities carried out by the HNBA for combating money laundering and terrorist financing risks, details of recent significant risks involved in internally or externally and its impact or potential impact on HNBA, recent developments in written laws on anti-money laundering and suppression of terrorist financing and its implications etc. Further, Group will report threshold reporting submission status to the Board on monthly basis through the Compliance check lists.

8 Roles and Responsibilities

8.1 Compliance Officer

Head of Legal and Compliance & Board Secretary of both HNBA and HNBGI shall hold the title Compliance Officer under the AML Rules and shall have the authority to sign as such. The duties of the Compliance Officer with respect to the Policy shall include, but are not limited to, the design and implementation as well as updating the Policy as required; dissemination of information to officers,

employees and appointed agents of the Group; monitoring the compliance of the Group operating units and appointed agents, maintaining necessary and appropriate records, filing of STR's when warranted; filing of CTR's and EFT's.

All efforts exerted will be documented and retained in accordance with the Act. The Compliance Officer is responsible for reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the Compliance Officer.

Further at the time of new product development stage Compliance Officer approve the product when reviewing the ML/TF risk aspect also in addition to other Legal requirements of same with the assistance of Compliance department and approve the product accordingly.

8.2 Compliance Assistant

The second highest Official in the Compliance function of both HNBA and HNBGI shall hold the Compliance Assistant position of each Company. The duties of the Compliance Assistant with respect to the Policy shall include assisting the Compliance Officer to perform the AML/CFT function of the group.

8.3 Internal Auditors

The internal auditors will be advised to device an audit programme that would be carried out on a regular basis in order to

- ensure that procedures implemented with regard to AML are strictly followed,
- the Policy to be tested and report there on of any findings to the Audit Committee, Risk Management Committee for appropriate action.

9 Review of the Policy

The Compliance Officer is responsible for the administration, revision, interpretation, and application of this Policy. The Policy will be reviewed annually and revised as needed.