Anti-Money Laundering (AML) Policy Summary

HNB Life PLC

Anti-Money Laundering (AML), Countering Financing Terrorism (CFT) & Countering Proliferation Financing (CPF) Policy Summary

1. Purpose and Legal Framework

The AML, CFT & CPF Policy of HNB Life PLC establishes the framework to prevent, detect, and mitigate risks related to Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF).

The Policy is aligned with:

- Prevention of Money Laundering Act No. 5 of 2006
- Financial Transactions Reporting Act (FTRA) No. 6 of 2006
- Convention on Suppression of Terrorist Financing Act No. 25 of 2005
- Insurers (Customer Due Diligence) Rules No. 1 of 2019

2. Scope

The Policy applies to:

- All Directors, officers, and employees
- Appointed agents and intermediaries
- All branches and business units
- All insurance products and related services (including reinsurance)

The Company adopts a risk-based approach to prevent misuse of its products and services for ML/TF/PF purposes.

3. Key Risk Areas

a) Product Risk

Certain life insurance products may present higher ML/TF risks, particularly those with:

- High-value lump sum premiums
- Early surrender features
- Refund/cancellation options
- Cash value accumulation
- Policy loans or assignment flexibility

ML/TF risk assessments are conducted before launching new products, practices, technologies, or branches to identify the possible ML/TF Risks.

b) Customer Risk

Upon the initial acceptance of a customer, the company shall categorize customers into low, medium, or high risk (Create Customer's risk Profile) based on their potential exposure to money laundering and terrorist financing risk, based on predetermined criteria.

- **Low Risk** – Standard individuals/entities with transparent profiles
- **Medium Risk** – Customers with uncertain or moderately elevated risk factors
- **High Risk** – Non-residents, high-net-worth individuals, trusts, NGOs, PEPs, high-risk jurisdictions, etc.

Enhanced Due Diligence (EDD) is conducted for high-risk customers. The customer risk profile is determined based on the established risk scoring system.

4. Customer Identification Program (CIP)

The Company collects and verifies:

- Identity information
- Proof of address
- Business registration documents (for entities)
- Beneficial ownership details
- Source of funds (for high-risk customers)

Anonymous or numbered insurance policies are strictly prohibited.

5. Beneficial Owner

The company also identifies and verifies the ultimate beneficial owners of every corporate customer before onboarding and conducts sanction screening for ultimate beneficial owners upon identification.

6. Politically Exposed Persons (PEP)

The identification of Politically Exposed Persons (PEPs) is carried out through customer self-declaration and other identification methods in accordance with regulatory requirements at the onboarding stage as well as in during periodic customer due

diligence reviews. Where a customer is identified as a PEP, the prescribed onboarding procedures are followed, including obtaining approval from Senior Management.

7. Sanctions Screening

Sanctions screening is conducted:

- Onboarding
- prior to the processing of transactions
- Periodically
- Upon sanctions list updates

For all,

- Policyholders and Beneficiaries
- Employees and Sales Advisors/Agents
- Suppliers and any other counterparty

Screening is performed using the KTMS system and against:

- UN Security Council sanctions
- Local terrorist lists
- Other applicable regulatory sanctions

Dealings with designated people are strictly prohibited.

8. Transaction Monitoring & Reporting

The Company monitors transactions using automated AML systems aligned with regulatory expectations.

Reporting Obligations:

- **Suspicious Transaction Reports (STRs)** – Submitted via goAML within regulatory timelines.
- **Threshold Transactions (Cash/EFT above LKR 1 million)** – Reported within 31 days via goAML.
- Attempted suspicious transactions must also be reported.

Strict prohibition of tipping-off applies.

9. Red Flag Indicators

Examples include:

- Large unexplained premiums
- Frequent early surrenders
- Overpayments and refund requests
- Use of cash or third-party payments
- Suspicious source of funds
- Adverse media reports
- Transactions structured below reporting thresholds

FIU Red Flag Indicators No. 03 of 2023 (Insurance Sector) are incorporated into procedures.

10. Governance & Oversight

Compliance Officer

Responsible for:

- Policy implementation and updates
- STR/CTR/EFT filing
- Regulatory liaison
- Sanctions escalation
- Board reporting

AML Reporting Officer / Compliance Assistant

Supports AML monitoring and regulatory compliance.

Internal Audit

Conducts independent testing and reports findings to the Audit and Risk Committees.

11. Training & Recruitment

- AML/CFT/CPF training provided to Directors, employees, and agents in accordance with the annual compliance plan.

- Screening and due diligence conducted before recruitment/appointment of employees and agents.

12. Record Keeping

- STRs, CTRs, EFTs, and CDD documents remained for a minimum of six (6) years.
- Records maintained to ensure prompt access for regulatory authorities.

13. Risk Assessment & Board Reporting

- Annual entity-wide ML/TF/PF risk assessment conducted.
- Bi-annual AML report submitted to the Board.
- Monthly and quarterly threshold reporting updates provided.
- New product/branch ML/TF risk assessments submitted to the Board Risk Management Committee.

14. Internal Auditors

The Internal Audit Department shall include AML/CFT/CPF compliance within its annual audit plan.