ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM & THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (AML/CFT&P) POLICY

POLICY	ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM & THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION
AUTHOR (S)	HEAD, LEGAL/COMPANY SECRETARY HEAD, RISK MANAGEMENT AND COMPLIANCE
OWNER	ANTI-MONEY LAUNDERING REPORTING OFFICER
RECIPIENTS	ALL STAFF
VERSION	3.2

Connected procedures/policy
Description
KYC Policy
Detection procedure
AML Act 2020, Act 1044
FIC AML/CFT &P Guideline
Risk Rating Guideline
NIC AML Guideline

Objectives
This policy is designed to provide clear principles and guidance for meeting AML/CFT &P requirements, highlight its associated risks and to prevent the use of StarLife products, services and channels for Money Laundering and Financing Terrorism, thereby meeting applicable legislation and international standard and mitigate any reputational risks that may arise.

CONTENT

1. INTRODUCTION

StarLife Assurance Limited Company ("The Company") is a member of the Star Assurance Group and a leading life insurance Company in Ghana. The Company offers a comprehensive range of need-based life insurance products designed to meet the financial security needs of the insuring public.

As a regulated entity operating in Ghana, the Company complies fully with applicable Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT), and Proliferation Financing (PF) laws, rules, and standards enforced by the National Insurance Commission (NIC).

Insurance companies, by their nature, are exposed to varying ML/TF&P risks and potential financial and reputational damage if they fail to manage these risks adequately. Recognizing these risks, the Company has adopted a risk-based approach to identifying and managing ML/TF&P risks effectively. In accordance with applicable AML/CFT&P laws and regulatory requirements, the Company has developed the AML/CFT&P policy to minimize the risk of being used to launder the proceeds of crime, protect the Company against economic and organized crime, reputational and financial risks and to ensure compliance with all relevant laws, standards and best practices in the insurance industry.

The Company is committed to ongoing evaluation and improvement of its AML/CFT&P strategies and objectives. It will maintain an effective AML/CFT&P policy that reflects global best practices and evolving regulatory requirements.

Compliance with this policy is the responsibility of all Directors, Management, and employees. The policy is formulated and directed by the Board of Directors, with oversight provided through the Anti-Money Laundering Reporting Officer (AMLRO).

2. DEFINITIONS

For the purpose of this policy, the following definitions apply:

a. **Money Laundering (ML)"** refers to the process in which the proceeds of crime are transformed into ostensibly legitimate money or assets. It involves the introduction of assets derived from illegal and criminal activities (predicate offences) into the legal financial system and business cycle. These predicate offences include drug

trade, child trafficking, forgery of money, organized crime etc.

b. **Terrorism Financing (TF)"** refers to providing funds directly or indirectly knowing that the funds are to be used to fund terrorist acts or organizations.
c. **"Proliferation Financing (PF)"** is defined by FATF as "the act of providing funds or financial services which are used, in whole or part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations."
d. **"Account"** refers to any policy or arrangement through which the Company accepts deposits or allows withdrawals.
e. **"Proceeds of crime"** refers to any property that is derived or realized, directly or indirectly, by any person from the commission of any serious offense, such as trafficking in illegal drugs, people smuggling or arms smuggling, political or other corruption, financing of terrorist or other criminal acts by either legitimate or illegitimate funds.
f. **Weapons of mass destruction"** refers to a variety of weapons, which include but are not limited to nuclear weapons, and chemical and biological warfare agents.
g. **"The Company"** refers to StarLife Assurance Limited Company.
h. **"AML"** refers to Anti-Money Laundering.
i. **"AMLRO"** refers to Anti-Money Laundering Reporting Officer.
j. **AML/CFT&P"** refers to Anti-Money Laundering, Combating the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction.
k. **"AML/CFT&CPF"** refers to Anti-Money Laundering, Combating the Financing of Terrorism, and Countering the Proliferation of Financing.
l. **"ML/FT&PF"** refers to Money Laundering, Financing of Terrorism, and the Proliferation of Financing.
m. **"Board"** refers Board of Directors.
n. **"CDD"** refers to Customer Due Diligence.
o. **"CFT"** refers to Combating the Financing of Terrorism.
p. **"CTR"** refers to Cash Transaction Report.
q. **"EDD"** refers to Enhanced Due Diligence.
r. **"FIC"** refers to the Financial Intelligence Centre.

s. **"KYC"** refers to Know Your Customer.
t. **"KYE(S)"** refers to Know Your Employee/Staff.
u. **"NIA"** refers to the National Identity Authority.
v. **"NIC"** refers to the National Insurance Commission.
w. **"OFAC"** refers to the Office of Foreign Assets Control.
x. **"PEP"** refers to a Politically Exposed Person.
y. **"STR"** refers to Suspicious Transaction Report.
z. **"The Policy"** refers to Anti-Money Laundering, Combating the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction.

3. POLICY STATEMENT

StarLife Assurance Company Limited ("the Company") is committed to upholding the highest standards of AML/CFT&P compliance. The Company requires the Board, Management and employees to strictly adhere to these standards to prevent the misuse of its products and services for ML/FT&P purposes.

To facilitate compliance with AML/CFT&P requirements, the Company has appointed an AMLRO to oversee its AML/CFT&P program.

The key components of the policy are:
Development and Implementation of AML/CFT&P Policies, Procedures, and Controls
The Company has developed and implemented written AML/CFT&P policies, procedures, internal controls, and systems that include, but are not limited to:
i. Customer Identification Program (CIP): Procedures to identify and verify the identity of customers.
ii. Customer Due Diligence (CDD): Processes to collect, verify, and periodically update customer information to ensure compliance with regulatory requirements.
iii. Risk Assessment: Processes to assess risk at both the program and customer levels to identify potential ML/FT&P threats.
iv. Transaction Monitoring: Systems to monitor customer transactions and activities to detect unusual or suspicious behavior.
v. Suspicious Activity Reporting (SAR): Processes to identify and report suspicious activities in line with regulatory guidelines.
vi. Record Keeping: Systems to maintain and safeguard required records for compliance and audit purposes.

b. AML/CFT&P Employee Training

The Company has developed a comprehensive training program to educate employees on AML/CFT&P detection and prevention procedures. This program ensures that employees are equipped with the knowledge and tools to comply with regulatory requirements. The Company also subjects its AML/CFT&P policies and procedures to regular independent audits to ensure their effectiveness.

c. Cooperation with Authorities

The Company fully cooperates with law enforcement and regulatory investigations and inquiries. It strictly avoids business relationships with blacklisted entities and ensures compliance with legal provisions, including those relating to sanctions and blacklists.

d. Compliance with Regulatory Requirements

The Company adheres fully to AML/CFT&P laws, regulations, circulars, and directives issued by the Financial Intelligence Centre (FIC), the National Insurance Commission (NIC), and other relevant regulatory authorities.

4. PURPOSE

The purpose of this policy is to protect the Company, its employees, and its clients from being exploited for money laundering (ML), terrorism financing (TF), and proliferation financing (PF) activities. The policy provides a general framework for combating ML/FT&P and ensures that the Company operates in full compliance with applicable laws, regulations, and international standards.

This policy aims to:

a. Ensure Regulatory Compliance

Enable the Company to understand and comply with AML/CFT&P laws, regulations, and requirements while mitigating the implications of non-compliance.

b. Establish Consistent Guidelines

Provide uniform guidelines and procedures to ensure adherence to AML/CFT&P requirements across all functions, products, and services.

c. Clarify Roles and Accountability

Clearly define roles, responsibilities, and expectations for the Board, Management, and employees to ensure compliance with AML/CFT&P laws and regulatory obligations.

d. Implement an Effective Risk-Based Approach

Develop and maintain effective risk-based AML/CFT&P compliance programs that support the identification, monitoring, and reporting of suspicious activities.

e. Facilitate Training and Development

Serve as a resource for educating employees, including new hires, on AML/CFT&P policies, compliance requirements, and their responsibilities in detecting and preventing illicit activities.

f. Provide a Reference Guide

Act as a critical reference tool, ensuring employees have quick and easy access to information and procedures necessary for compliance with AML/CFT&P requirements.

By establishing this policy, StarLife Assurance Company Limited reaffirms its commitment to ethical business practices, safeguarding its operations, and contributing to the global effort to combat financial crimes.

5. APPLICATION AND SCOPE

The policy is based on applicable legal and regulatory requirements and applies to the all Board, Management, Employees and vendors of the Company.

The scope of the policy includes the following, but not limited to:

a. Cooperation with Competent Authorities.
b. AML/CFT&P Governance Framework.
c. Scope of Unlawful Activities.
d. Stages of ML/FT&P.
e. Financing of Terrorism Crimes.
f. Legal Framework.
g. Know Your Client (KYC).
h. Know Your Employee (KYE).
i. Employee Reporting.
j. Regulatory Reporting.

k. AML/FT&P Risk Management Framework and Risk-Based Approach
l. Monitoring of Transactions.
m. Politically Exposed Persons.
n. Higher and Lower Level Risk Categories of Clients.
o. Training.
p. AML/CFT&P Software.
q. Whistleblowing.
r. Protection of Employee.
s. Record Keeping.
t. Independent Audit.
u. Sanctions.

6. CO-OPERATION WITH RELEVANT AUTHORITIES

The Company is committed to fully cooperating with competent authorities to ensure compliance with all applicable laws, regulations, and requests for information. The Company will collaborate with the NIC, FIC, and other relevant authorities to fulfill its obligations in combating ML / TF & PF.

The Company in responding to authorized requests for information related to ML/TF&PF will:

a. Conduct Immediate Record Searches: Promptly search its records to identify relevant information in response to authorized requests.

b. Ensure Timely Reporting: Report the outcome of the search promptly and accurately to the requesting authority in compliance with legal and regulatory requirements.

c. Maintain Security and Confidentiality: Protect the security and confidentiality of all requests and ensure that sensitive information is handled with the highest level of discretion and in compliance with applicable laws.

7. AML/CFT&P GOVERNANCE FRAMEWORK

7.1 Culture of Compliance

The Company is committed to fostering a strong culture of compliance as a cornerstone of its AML/CFT&P Governance Framework. To achieve this, the Company will maintain a comprehensive AML/CFT&P policy and an accompanying compliance

program to guide its efforts and ensure the diligent implementation of its guidelines.

By embedding a culture of compliance, the Company seeks to:

- Minimize Risks: Reduce the likelihood of the Company being exploited for money laundering (ML), terrorism financing (TF), and proliferation financing (PF) activities.
- Protect Against Unlawful Activities: Safeguard the Company from involvement in illegal activities that could jeopardize its operations and integrity.
- Mitigate Reputational and Financial Risks: Enhance the Company's reputation as a responsible corporate entity and prevent financial losses associated with regulatory non-compliance or criminal activities.

7.2 The Company's Commitment
The Company's commitment to compliance will be supported by:

- Clear Policies and Procedures: Ensuring all employees and stakeholders understand and adhere to the AML/CFT&P policy.
- Leadership Oversight: Promoting compliance as a priority at all levels of the organization, starting with the Board of Directors and Executive Management.
- Training and Awareness: Providing employees with the necessary training and tools to fulfill their compliance responsibilities effectively.
- Ongoing Monitoring: Continuously reviewing and improving compliance efforts to adapt to evolving risks, laws, and regulations.

By entrenching this culture of compliance, the Company demonstrates its unwavering commitment to ethical business practices, regulatory adherence, and the protection of its stakeholders.

7.3 Roles and Responsibilities
7.3.1 Role of the Board
The Board has ultimate responsibility for ensuring the effectiveness of the AML/CFT&P compliance programme. In this regard, the Board's oversight in respect of AML/CFT&P will align with international best practices, including the NIC Risk Management and Governance Framework Directive. The Board will ensure that there is documented evidence of its oversight function, for example, in minutes of meetings

of the Board through the Board Risk Management, Audit & Compliance Committee.

The following are the key responsibilities of the Board but not limited to:

a. Approving the appointment of the AMLRO.
b. Approving AML/CFT&P policy/manual.
c. Approving the AML/CFT&P compliance programme, training programme, compliance reports.
d. Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT&P policies and procedures to ensure their continued relevance in line changes in the AI's products and services and to address new and emerging ML/TF&PF risks.
e. Ensuring that the Board receives the requisite training on AML/CFT&P generally as well as on the Company's specific AML/CFT &P risks and controls at least once a year.
f. Ensuring receipt of regular and comprehensive reports on the Company's AML/CFT&P function from the AMLRO for its information and necessary action including but not limited to:
    i. Remedial action plans if any, to address the results of independent audits (either internal or external).
    ii. Regulatory reports received from NIC or other regulators on its assessment of the Company's AML/CFT&P programme.
    iii. Results of compliance testing and self-identified instances of non-compliance with AML/CFT&P requirements.
    iv. Recent developments in AML/CFT&P laws and regulations and their implications to the Company.
    v. Details of recent significant risk events and potential impact on the Company.
    vi. Statutory report to the FIC and NIC.
g. Ensuring that AMLRO forwards all required periodic statutory reports to the relevant regulatory authorities.
h. Ensuring that copies of the approved AML/CFT&P policy are submitted to NIC and FIC.

7.3.2 Role of Executive Management

Executive Management is responsible for the day-to-day implementation, monitoring

and management of the Company's AML/CFT&P compliance programme, including ensuring adherence to established AML/CFT&P policies and procedures.

The key responsibilities of the Executive Management are to ensure the following but not limited to:

a. All significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT&P programme are addressed in a timely manner.
b. Relevant, adequate and timely information regarding AML/CFT&P matters is provided to the Board.
c. The AMLRO receives appropriate training on an ongoing basis to effectively perform his duties.
d. There is an ongoing employee training programme (at once a year) which enables employees to have adequate and relevant knowledge to understand and discharge their AML/CFT&P responsibilities.
e. The Compliance Officer / AMLRO and Internal Audit functions are resourced adequately in terms of personnel, IT systems and budget to implement, administer and monitor the AML/CFT&P programme requirements effectively.

7.3.3 Role of Anti-Money Laundering Reporting Officer (AMLRO)

The AMLRO will implement the policy and report to the Board or a Sub-Committee of the Board to ensure operational independence.

The following are the key responsibilities of the AMLRO but not limited to:

a. Develop written AML/CFT&P policies and procedures that are kept up to date and approved by the Board.
b. Have oversight of the AML/CFT&P control activity in all relevant business areas for the purposes of establishing a reasonable risk level consistent across the Company.
c. Keep the AML/CFT&P programme current relative to the Company's identified inherent risks and give consideration to local and international developments in ML/TF&PF.
d. Receive and vet suspicious (unusual) transaction/activity reports from the employees,
e. Conduct regular risk assessments of the inherent ML/TF&PF risks including timely assessments of new products, services and business acquisition initiatives to

identify potential ML/TF&PF risks and develop appropriate control mechanisms.

f. File suspicious, Politically Exposed Persons, Cash Transaction Reports and other relevant regulatory reports with the NIC and FIC (where applicable).
g. Conduct periodic assessments of AML/CFT&P control mechanisms to ensure their continued relevance and effectiveness in addressing changing ML/TF&PF risks, assess operational changes, including the introduction of new technology and processes to ensure that ML/TF&PF risks are addressed.
h. Ensure systems, resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the Company.
i. Ensure that ongoing training programmes on ML/TF&PF are current and relevant and are carried out for all employees, senior management and the Board.
j. Ensure that systems and other processes that generate information used in reports to Senior Management and the Board are adequate and appropriate, use reasonably consistent reporting criteria, and generate accurate information.
k. Report pertinent information to the Board and Executive Management regarding the adequacy of the AML/CFT&P framework or any associated issues.
l. Serve both as a liaison officer with the NIC and the FIC and a point-of-contact for all employees on issues relating to ML/TF&PF.

7.3.4 Role of Internal Audit

The internal audit will perform independent testing of the compliance program at least once a year to assure that the regulation is being complied with.

7.3.5 Role of Employees and Associated Persons

Employees, consultants and other associated persons will be responsible for but not limited to:

a. Complying with this AML/CFT&P policy, other standards and controls.
b. Familiarizing themselves with and acting in accordance with relevant processes and procedures to manage AML/CFT&P compliance.
c. Reporting to the AMLRO without undue delay any suspicions (or actual occurrences) or red flags of ML/TF&P activities.
d. Attending all ML/TF&P trainings.

8. SCOPE OF UNLAWFUL ACTIVITIES

The Company will identify and report to the NIC and the FIC, the proceeds of crime derived from unlawful activities including, but not limited, to the following:

a. Participation in an organized criminal group and racketeering
b. Terrorism, including terrorist financing.
c. Trafficking in human beings and migrant smuggling.
d. Sexual exploitation, including sexual exploitation of children.
e. Illicit trafficking in narcotic drugs and psychotropic substance.
f. Illicit arms trafficking.
g. Illicit trafficking in stolen and other goods.
h. Murder, grievous bodily injury.
i. Kidnapping, illegal restraint and hostage-taking.
j. Robbery or theft.
k. Smuggling.
l. Tax Evasion.
m. Extortion.
n. Forgery.
o. Piracy.
p. Insider trading and market manipulation.
q. Corruption and bribery.
r. Fraud.
s. Counterfeiting currency.
t. Counterfeiting and piracy of products.
u. Environmental crime.
v. Any other predicate offence under the Anti-Money Laundering Act.

9. STAGES OF ML

Generally, all employees will be aware of the three (3) stages of money laundering which criminals may use to disguise the origins of illegally obtained funds or assets. Understanding these stages is critical to identifying suspicious activities and ensuring compliance with AML/CFT&P guidelines.

a. Placement: This stage involves the introduction of illegally obtained funds or assets into the financial system or non-financial institutions. Common methods of placement include:

- Depositing cash into bank accounts.
- Purchasing financial instruments or assets.
- Using cash to buy goods or services that are difficult to trace.

b. Layering: This stage consists of conducting a series of financial transactions—ranging from simple to highly complex—that are designed to obscure the origin or identity of the funds or assets. These transactions aim to:

- Disguise the audit trail.
- Conceal the source of the funds or assets.
- Provide anonymity to the criminals involved.

Layering often includes:

- Moving funds between multiple accounts or jurisdictions.
- Using shell companies or intermediaries.
- Engaging in high-volume or rapid trades to mask activity.

c. Integration: In the final stage, the laundered proceeds are reintroduced into the legitimate economy, appearing to originate from lawful sources. This stage is often characterized by:

- Investing in legal businesses.
- Purchasing high-value assets, such as real estate or luxury goods.
- Using funds for legitimate financial transactions to complete the cycle.

These stages are not static and overlap broadly.

10. FINANCING OF TERRORISM CRIMES

The financing of terrorism poses significant risks to its operations, reputation, and the broader financial system. The financing of terrorism crimes can occur through various transactions facilitated by the Company, including but not limited to:

a. Account Transactions: The opening, operation (depositing and withdrawing of funds), or closing of an account held with the Company.

b. Funds Transfers: The telegraphic or electronic transfer of funds by the Company on behalf of one person to another person.

c. Cross-Border Transfers: The transmission of funds between the Republic of

Ghana and foreign countries, or between foreign countries, on behalf of any person.

d. Loans and Repayments: Applications for loans by any person, the disbursement of such loans, and their subsequent repayment.

e. Monetary or Financial Gifts: The receipt or provision of monetary or financial gifts that may be used to fund terrorism-related activities.

f. Trading in Assets: The buying and selling of gold, foreign currency, or negotiable instruments, which may be exploited to transfer or conceal funds used for financing terrorism.

11. LEGAL FRAMEWORK

The legal framework for developing the policy was based on:

a. Anti-Money Laundering Act 2020 (1044).
b. Anti-Money Laundering Act, 2008 (Act 749).
c. Anti-Money Laundering (Amendment) Act, 2014 (Act 874).
d. Anti-Money Laundering Regulations, 2011 (L.I.1987).
e. Anti-Terrorism Act, 2008 (Act 762).
f. Anti-Terrorism (Amendment) Act, 2012 (Act 842).
g. Anti-Terrorism Regulations, 2011 (L.I 2181).
h. The recommendations of the Financial Action Task Force on Money Laundering (FATF), February 2012.
i. The UN's International Money Laundering Network (IMOLIN).
j. NIC FIC AML/CFT Guideline.
k. The Basel AML Index.

12. KNOW YOUR CLIENT (KYC)

The Company will develop a KYC policy guideline that will provide detailed KYC requirements for various classes of clients.

12.1 Client Identity will be ascertained:

a. When onboarding a new Client.
b. Anytime a client transacts business on the policy.
c. Whenever a third party makes premium payments on behalf of a Client.
d. Whenever a Client makes cash premium payments of GH¢5,000 and above or its equivalent in foreign currency.

e. When there is a change in the bio-data of the client.

f. Whenever a Client requests for upward adjustments in premiums mid-term.

g. Two or more transactions occur on the account within a month.

h. There are doubts about the veracity or adequacy of previously obtained Client identification data.

i. There is a suspicion of money laundering or terrorist financing.

12.2 Identification of Ultimate Beneficial Owner (UBI):
When dealing with Companies, the identity of the ultimate beneficial natural person/ individual who owns, and controls the client or its assets or on whose behalf the account is held will be established and verified wherever possible.

12.3 Client Identification Verification Platforms:
The Company will liaise with NIA and other approved regulatory bodies to implement appropriate ID verification platforms for the verification of clients' and third parties' identities.

12.4 Due Diligence on Contractual Parties:
The Company will implement appropriate due diligence measures on all entities and individuals it contracts with.

12.5 Forbidden Businesses:
No business will be transacted with shell companies. No accounts will be issued to anonymous clients or in fictitious names. Shell Companies are companies incorporated in jurisdictions in which it has no physical presence and in which it is unaffiliated with a regulated financial group.

13. KNOW YOUR EMPLOYEE/STAFF (KYE/S)

In addition to maintaining robust Know Your Customer (KYC) procedures, the Company is committed to implementing strong Know Your Employee (KYE) measures to ensure the integrity and competence of its workforce. The Company recognizes that the ability to implement an effective AML/CFT&P program relies, in part, on the quality and integrity of its employees.

13.1 Recruitment and Pre-Employment Due Diligence
The Company will have a comprehensive recruitment policy to attract and retain employees with the highest levels of integrity and competence. As part of this

policy, the Company will conduct due diligence on prospective employees. At a minimum, the Company will:

a. Verify Applicant Information: Confirm the applicant's identity and personal information, including employment history, using a risk-based approach.

b. Risk-Based Background Screening: Develop a risk-based approach to determine when pre-employment background screening is required or when enhanced screening is necessary. It is also important to consider the sensitivity of the position, responsibilities, or access level associated with the role. Enhanced screening will include verification of references, professional qualifications, education, and experience.

c. Ongoing Employee Screening: Conduct periodic screenings for specific positions as circumstances change or as part of a comprehensive review of employees over time. Establish internal policies and procedures, including codes of conduct, ethics, and conflict of interest guidelines, to evaluate employees' integrity and compliance with Company standards.

d. Use of AML Screening Tools: Screen employees using AML Disclaimer Database Checker Software to identify any potential risks related to money laundering or financing of terrorism.

13.2 Monitoring of Employee Lifestyle

The Company will actively monitor employee lifestyle for signs of money laundering (ML), terrorism financing (TF), or proliferation financing (PF). This monitoring will include:

- Paying particular attention to employees whose lifestyles appear inconsistent with their salary or known financial circumstances.
- Supervisors and managers are encouraged to remain vigilant, know the employees in their department, and investigate any significant lifestyle changes that may indicate financial inconsistencies or potential misconduct.

13.3 Performance Review and Training

The AML/CFT&P performance review of employees will form part of their annual performance appraisal. This ensures that compliance with AML/CFT&P

responsibilities is ingrained in the overall evaluation of employee performance and accountability.

14. EMPLOYEE REPORTING

The Company is committed to maintaining robust systems and processes for identifying and reporting cash transactions, suspicious activities, and politically exposed persons (PEPs) to ensure compliance with AML/CFT&P regulatory requirements.

14.1 Cash Transactions Report (CTR):
The Company shall establish systems to ensure the cashiers report daily, all cash premiums of GH¢5,000 and above or its equivalent in foreign currency to the AMLRO. The report will be sent in the approved CTR format.

14.2 Suspicious Transactions Reporting (STR):
The Company requires employees to immediately report any suspicious activity or transactions that may be related to money laundering (ML), terrorism financing (TF), or proliferation financing (PF).

a. Reporting Suspicious Transactions:

If an employee has reason to believe that a client's account or transaction is being used for ML/TF&P activities, they must:

- Submit a written report to the AMLRO.
- Follow the STR procedure for further investigation and submission to the Financial Intelligence Centre (FIC).

b. Triggers for Filing STRs: Suspicious Transaction Reports (STRs) must be filed under the following circumstances:

- When the client presents fake documentation.
- When the client fails to complete the required client relationship form within the stipulated time.
- When the client is identified as a suspect in news publications (e.g., Wanted Persons).
- When transactions are conducted in a way that appears to evade statutory reporting obligations.

- When there is abnormal exercise of cooling-off, cancellation, or surrender rights.
- When the client is involved in identity theft, such as using fake identification to impersonate someone else.

c. High-Risk Client Profiles:

- If an employee has doubts or suspicions regarding a client's identity, honesty, the nature or purpose of the transactions, or the source of funds, the client should be considered high-risk.
- Such cases must be immediately forwarded to the AMLRO for further action.

d. Final Decision on High-Risk Profiles:

- For clients considered high-risk, the CEO will be responsible for making the final decision on whether to continue or terminate the business relationship.

14.3 Politically Exposed Persons (PEPs):
Employees must exercise enhanced due diligence for clients who are identified as Politically Exposed Persons (PEPs).

- Reporting PEPs: If an employee believes, based on client information or other sources, that a client is politically exposed, they must submit a report to the AMLRO detailing the circumstances and relevant details about the PEP.
- Enhanced Monitoring: All PEP-related accounts or transactions must be subject to heightened scrutiny to mitigate risks associated with PEPs.

15. REGULATORY REPORTING

To ensure compliance with applicable AML/CFT&P regulations the Company will establish systems and processes to facilitate timely and accurate reporting to the Financial Intelligence Centre (FIC) and the National Insurance Commission (NIC).

15.1 Cash Transaction Reporting (CTR):
The Company will set up systems to enable the AMLRO to report daily, all cash premiums of GH¢5,000 and above or its equivalent in foreign currency to the

Financial Intelligence Centre (FIC). The Report will be sent via the FIC's GoAML portal or such other address as may be notified from time to time.

15.2 Suspicious Transactions Reporting (STR):

In the event of suspicious activities or transactions, the AMLRO will conduct a detailed review and investigation.

a. Suspicious Transaction Investigation:
    - If suspicion of illegal transactions persists after investigation, the AMLRO will:
        - File a Suspicious Transaction Report (STR) with the FIC and the NIC within 24 hours of determining that a transaction or activity is suspicious.
    - The CEO, in collaboration with the AMLRO, will review the findings and determine the STR submission, ensuring compliance with STR procedures.
b. Next Steps:
    - The FIC and NIC will provide guidance to the Company on the appropriate next steps regarding the business relationship with the client.
c. Reporting Mechanism:

STRs will be submitted through the GoAML portal or other approved communication channels as directed by the FIC

15.3 Other regulatory reports

The AMLRO will submit the following reports to NIC and FIC as per the AML/CFT&P regulatory guidelines and timelines. These include, but not limited to:

a. Quarter AML/CFT returns.
b. Half-Year Self-Assessment questionnaire.
c. AML/CFT Annual Compliance Programme.
d. Employee Training & Employee Conduct Monitoring report
e. Other regulatory reports as requested.

16. AML/FT&P RISK MANAGEMENT FRAMEWORK AND RISK-BASED APPROACH

The Company AML/CFT&P policy shall be aligned with and integrated into the overall Enterprise Risk Management Framework (ERMF). The Company is committed to adopting and implementing a continuous risk-based approach (RBA) to identify, assess, and understand its ML/FT&P risks. This approach will be applied to clients' countries or geographical areas, products and services, transactions or delivery channels in the form of an AML/CFT&P risk rating guideline.

Through this risk-based approach, the Company will assess the level of client risk and ensure that measures to mitigate ML / FT are proportionate to the risks identified. The Company will also allocate its resources effectively to focus on areas of highest risk, ensuring efficient and effect risk management.

16.1 AML/CFT&P Risk Assessment for New Products & Technologies

The Company is committed to proactively identifying and managing AML/CFT&P risks associated with new products, services, practices, and technologies. To achieve this, the Company will:

a. Comprehensive Risk Assessment:
   - Conduct a thorough AML/CFT&P risk assessment prior to launching or adopting any new products, services, or technologies.
   - Review, identify, and document potential ML/TF&P risks associated with new products or technologies in collaboration with the Risk Management and Compliance Department.

b. Prohibition of High-Risk Products:
   - Refrain from launching any high-risk products or services that could be exploited for money laundering or terrorist financing purposes.

c. Technological Controls and Safeguards:
   - Implement robust controls and measures to prevent the misuse of technological developments (e.g., applications, USSD platforms) as conduits for laundering money or financing terrorism.

d. Risk Mitigation Measures for Technological Platforms:
   - KYC and Risk Assessment:

- Assess the specific KYC and money laundering risks posed by technological platforms and formulate appropriate mitigation strategies;
- Implement effective Customer Due Diligence (CDD) procedures for non-face-to-face clients, ensuring robust verification mechanisms.

- Client Identification and Verification:
  - Ensure that clients enrolled via mobile or digital platforms are identified and verified using standards similar to those applied to walk-in clients. This will adhere to KYC requirements (minimum, standard, and enhanced KYC levels).
- Due Diligence on Third Parties:
  - Conduct comprehensive due diligence on all third-party providers associated with technological platforms to ensure they meet regulatory and compliance standards.

17. MONITORING OF TRANSACTIONS

To prevent the Company from being used as a conduit for laundering the proceeds of crime, the Company will develop tools to monitor, for all client accounts, unusual or suspicious patterns of transactions.

17.1 Identification of Unusual or Suspicious Activities

Unusual or suspicious activities can be identified through the following mechanisms:

a. Transaction Monitoring:

Using operational software and systems to identify irregular or suspicious patterns in transactions.

b. Client Interactions:

Through direct client contact, including meetings, discussions, or in-country visits, which may reveal unusual activity.

c. Third-Party Information Collection:

Leveraging information from third parties to identify and validate suspicious behavior or patterns.

17.2 Monitoring Tools and Measures

The Company will use operational monitoring tools to:

a. Key Indicators:

Implement key indicators to isolate accounts that exhibit unusual transaction patterns.

b. High-Risk Accounts:

Identify and earmark higher-risk accounts, subjecting them to intensified monitoring.

c. Transaction Limits:

Establish transaction limits for different categories or types of accounts. Particular attention will be given to transactions that exceed such limits, with enhanced scrutiny applied.

17.3 Monitoring Premium Payments

To ensure early detection of unusual or suspicious activities, the Company will implement permanent monitoring of client premium payments.

a. Reporting of Unusual Premium Receipts:

The Technical Operations Department and the Collections and Data Analysis Department will monitor premium payments and report any unusual or suspicious receipts to the AMLRO by filing a Suspicious Transaction Report (STR).

b. In-Depth Monitoring of High-Risk Accounts:

Accounts identified as high-risk will be subject to in-depth monitoring as outlined in the Company's internal control procedures.

17.4 Monitoring by Risk Management and Compliance

The Risk Management and Compliance Department will be responsible for:

- Monitoring patterns in client account transactions to detect suspicious activity.
- Ensuring that any suspicious transactions are promptly reported to the AMLRO for further action.

18. POLITICALLY EXPOSED PERSONS (PEPs)

The AMLRO shall maintain a list of PEPs. PEPs are high-risk individuals who are or have been entrusted with prominent public functions both in Ghana and foreign countries and those associated with them. They include:

a. Heads of State or government.
b. Ministers of State.
c. Politicians.
d. High-ranking political party officials.
e. Senior public officials.
f. Senior Judicial officials.
g. Senior military officials.
h. Chief executives of state-owned companies/corporations.
i. Diplomats and reps of foreign countries and organizations.
j. Family members or close associates of PEPs.
k. Businesses/ organizations belonging to a PEP.

The AMLRO will monitor the accounts of PEPs and report any suspicious transactions as per the STR procedure.

19. HIGHER AND LOWER LEVEL RISK CATEGORIES OF CLIENTS

The Company shall determine in each case whether the risks are lower or not, having regard to the type of customer, policy, transaction or the location of the customer and perform enhanced due diligence for higher-risk categories of customers, business relationship or transactions.

Where there is doubt, the Company will seek clearance from the National Insurance Commission.

Examples of higher-risk clients' categories include:

- Non-resident clients.
- Private/Prestige banking clients.
- Legal persons or legal arrangements such as trusts, client accounts, personal assets, and holding vehicles.
- Companies that have nominee-shareholders or shares in bearer form.
- Politically Exposed Persons (PEPs).
- Ministries, Departments, and Agencies (MDAs).

- Metropolitans, Municipals and District Assemblies (MMDAs), and other public institutions.
- High Net Worth individuals.
- Religious Leaders.
- Chief Executives and Board Members of private-owned companies/corporations
- Natural or legal persons who do business in precious metals/minerals, petroleum.
- Designated Non-Financial Businesses and Professions.

Lower Risk Customers, Transactions or Products: these include:

- Public companies or listered companies, pension firms, and all institutions subjected to the same due diligence requirements as financial institutions – provided they are subject to requirements for the combat of ML/FT&P;
- Where there are low risks, the Company will apply reduced or simplified measures. There are low risks in circumstances where the risk of money laundering or terrorist financing is lower, where information on the identity of the client and the beneficial owner of a client is publicly available or where adequate checks and controls exist elsewhere in other public institutions; and,
- In circumstances of low risk, the Company will apply the simplified or reduced CDD procedures when identifying and verifying the identity of policyholders and the beneficial owners.

20. TRAINING

The AMLRO will develop an annual training program approved by the Board.

The following will apply to the training program, but not limited to:

1. The training program shall encompass all Board of Directors, Management and Employees.
2. Onboarding for newly recruited employees, AML/CFT training shall form part of the onboarding program.
3. Annual refresher training for all Board of Directors, Management and Employees.
4. The timing, coverage and content of the employee training program must meet the Company's perceived needs. And must be commensurate with the

established level of AML/CFT&CP risk that the Company is exposed to. Training will be risk-based with a focus on roles and responsibilities of employees.

5. The Training programme will be developed at the beginning of every year by the AMLRO in collaboration with the relevant departments.
6. Training may be conducted internally by qualified staff or by external resource persons.
7. Employees will complete the AML/CFT&CP Knowledge testing exercise after the training.
8. The basic elements of the employee training program will include:

(i) The nature of money laundering;

(ii) Money laundering 'red flags' and suspicious transactions;

(iii) Reporting requirements;

(iv) Client due diligence;

(v) Risk-based approach to AML/CFT&P;

(vi) Record keeping and retention policy; and,

(vii) AML regulations and offences.

21. AML/CFT&P SOFTWARE

The Company will implement ML/FT&P checker software which will contain the database of PEP, Disclaimers, OFAC, UK sanction list and other sanction list as directed by the regulator. The database will be updated regularly and as and when the various sanction lists are updated.

22. WHISTLE BLOWING

Employees must co-operate fully with the NIC and other enforcement agencies to ensure compliance with the AML/CFT laws. Employees must report all violations of this policy to the AMLRO. Such reports shall be confidential and the whistle blower shall be protected from victimization. Any violations by the AMLRO must be reported to the Chief Executive Officer.

23. PROTECTION OF EMPLOYEE

In order not to discourage staff from reporting AML/CFT activities, StarLife shall protect to the extent possible the staff identity and person:

(i) Any direct or indirect pressure or retaliation towards the staff (if its identity was to be revealed) will be severely punished by Management.

(ii) The identity of the employee and the content of the reporting form will be kept confidential.

(iii) If, for the needs of the investigation, it is required to disclose the identity of the employee, a discussion will be held with the latter on how to proceed.

(iv) Should the employee be pressured by his team following his declaration, Management will ensure a transfer in another team so that it does not affect his/her professional career.

(v) The employee will be kept informed of the developments of the investigation.

24. RECORD KEEPING

The Company through the ICT Department (Records) shall keep records of the following:

- All proposal forms (digital or paper);
- Surrender, Loan, Partial Withdrawal, Cash back and Maturity Application Forms;
- Types and details of ID cards used by Clients for each transaction; and,
- All CTR and STR made to the AMLRO & FIC.

Notwithstanding that the AML (Amendment) Act, 2014 (Act 874) has reduced the statutory record retention period to 5 years, the Company shall maintain the 6 years duration in conformity with the Limitations Act, 1972 (NRCD 54) which allows persons to take legal action on simple contracts within 6 years after the cause of action has accrued.

25. SANCTIONS

The offences outlined below will attract sanctions/penalties from the regulators:

(i) Failure to appoint an AMLRO at the management level.

(ii) Failure to develop and implement the Internal Risk Assessment Framework.

(iii) Failure to give access to information to NIC and FIC or any competent authority.

(iv) Failure to conduct effective Customer Due Diligence (CDD).

(v) Failure to develop and implement risk assessment for new technologies and Non-Face-to-Face products and distribution channels.

(vi) Failure to maintain records.

(vii) Failure to report Unusual and Complex Large / Suspicious Transactions.

(viii) Failure to develop and implement internal rules and policies.

(ix) Conducting Business with Shell Banks.

(x) Failure to ensure foreign branches and subsidiaries comply with AML/CFT&P provisions.

(xi) Failure to submit and implement employee education and training Programme.

(xii) Failure to screen when hiring new employees and not making AML/CFT&P performance part of employee annual appraisals.

(xiii) Failure to monitor employee conduct.

(xiv) Failure to undertake an Independent Audit of the AML/CFT&P Compliance Programme.

(xv) StarLife shall make it a policy commitment to subject its AML/CFT&P compliance program to independent testing or require its internal auditor to determine its efficiency.

(xvi) Formal board approval of Key AML/CFT&P documents (AML/CFT&P compliance programme, policy, manual, and Risk Assessment Framework).

(xvii) Failure to attend training or workshop organized by NIC/FIC.

(xviii) Failure for;

- Non-submission of statutory reports.
- Incomplete submission of statutory reports.
- Delayed submission of statutory reports.
- Inaccurate submission of statutory reports.

26. INDEPENDENT AUDIT

Independent internal audit of the AML/CFT&P policy and its implementation shall be conducted by the Internal Audit Department annually and a written Report of Compliance made available to the Board Risk Management, Audit & Compliance Committee. The Report of Compliance will be submitted to the NIC & FIC.

27. REVISION

The AML/CFT&P policy will be subject to regular reviews to ensure its relevance, currency, and alignment with evolving regulatory requirements and best practices.

The policy will be reviewed at least once every year to ascertain its applicability and effectiveness. Additional reviews and revisions will be conducted as needed, particularly in response to:

- Changes in laws, regulations, or guidelines issued by regulatory authorities (e.g., FIC, NIC).
- Updates to global standards on AML/CFT&P compliance.
- Significant changes in the Company's operations, risk profile, or governance framework.

By maintaining a rigorous review and revision process, the Company demonstrates its dedication to:

- Ensuring Compliance: Keeping the policy updated to meet all applicable legal and regulatory requirements.
- Enhancing Governance: Upholding high standards of governance and operational excellence.
- Mitigating Risks: Proactively addressing new and emerging risks related to money laundering, terrorism financing, and proliferation financing.

The review and revision process will involve input from the Board of Directors, Risk Management and Compliance Department, and the AMLRO, ensuring a comprehensive approach to maintaining the policy's effectiveness and relevance.

28. DOCUMENT HISTORY

Document Name	Anti-Money Laundering (AML) Policy	Date
Version	1.0	
Prepared by	Name: Legal and Compliance Department	
Reviewed by	Name: Executive management	
Approved by	Name: Board audit & risk committee	
Approved by	Name: Board of Directors	

Document Name	Anti-Money Laundering (AML) Policy	Date
Version	2.0	
Prepared by	Name: Legal and Compliance Department	
Reviewed by	Name: Executive management	
Approved by	Name: Board audit & risk committee	
Approved by	Name: Board of Directors	

Document Name	Anti-Money Laundering (AML) Policy	Date
Version	3.0	
Prepared by	Name: Legal and Compliance Department	
Reviewed by	Name: Executive management	31 October 2019
Approved by	Name: Board audit & risk committee	6 November 2019
Approved by	Name: Board of Directors	18 December 2019

Document Name	Anti-Money Laundering (AML) & Combating The Financing of Terrorism Policy	Date
Version	3.1	
Prepared by	Name: Risk Management and Compliance	3 August 2022
Reviewed by	Name: Executive management	10th August 2022
Approved by	Name: Board audit & risk committee	24th August, 2022
Approved by	Name: Board of Directors	14 September, 2022
Description of change	To comply with the AML Act 2020 , Act 1044 Section 1: AMLCO changed to AMLRO Section 2: Addition of objectives Section 3: Addition of key definition terms Section 4: Addition of Financing of Terrorism Section 5: Addition of the new regulatory Act Section 6: New Section 6.0 added Section 7.8: New addition Section: New Section 7.15 added Section 8: New addition Section 9.1: New addition Section 9.3: New addition Section 9.4: New addition Section 10: New addition Section 11: New addition Section 13: New addition Section 14: New addition Section 16: New addition Section 18: New addition	

Document Name	Anti-Money Laundering /Combating the Financing of Terrorism and Proliferation of Weapons of Mass Destruction Policy.	Date
Version	3.2	
Prepared by	Name: Head, Risk Management and Compliance	30th December 2024
Reviewed by	Name: Head, Legal	20th January 2025
Approved by	Name: Executive management	30th January 2025
Approved by	Name: Board Risk Management, Audit and Compliance committee.	16th April 2025
Approved by	Name: Board of Directors	16th December 2025
Description of change	1. Addition of Proliferation of Weapons of Mass Destruction to the name of the policy as per FIC guidelines. 2. Section 1 Introduction: Added 3. Section 2 Definition: Revised to include other definitions. 4. Section 4 Purpose: Added 5. Section 5 Application and Scope: Added 6. Section 6 Co-operation with Relevant Authorities: Added 7. Section 7 AML/CFT&P Governance Framework: Added 8. Section 13 Know your employee: Added 9. Section 14: Employee reporting added 10. Section 27 Revision: Revised.	