POLICY
ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT)

POLICY	ANTI-MONEY LAUNDERING & COMBATING THE FINANCING OF TERRORISM
AUTHOR (S)	HEAD, LEGAL/COMPANY SECRETARY HEAD, RISK MANAGEMENT AND COMPLIANCE
OWNER	ANTI-MONEY LAUNDERING REPORTING OFFICER
RECIPIENTS	ALL STAFF
VERSION	3.1

Connected procedures/policy	
Description	**Comments**
KYC Policy	
Detection procedure	
AML Act 2020, Act 1044	

Objectives
This policy seeks to provide the required principles and guidance regarding AML/CFT 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. POLICY STATEMENT

STARLIFE, a regulated entity operating in GHANA and regulated by the **NATIONAL INSURANCE COMMISSION** makes every effort to remain in full compliance with all applicable anti-money laundering laws, rules and standards in force in Ghana.

To facilitate compliance with anti-money laundering requirements, **STARLIFE** has appointed an **ANTI-MONEY LAUNDERING REPORTING OFFICER** to oversee its anti-money laundering program. **STARLIFE** has:

(i) Developed and implements written anti-money laundering policies, procedures, internal controls and systems, which include but are not limited to:

- Customer identification program and procedures;
- Procedures to collect and refresh, as appropriate, customer due diligence information;
- Processes to assess risk at both the program and customer level;
- Processes and systems to monitor customer transactions and activity;
- Processes and systems to identify and report suspicious activity; and
- Processes to keep required records.

(ii) Developed a program to train employees in anti-money laundering detection and prevention procedures, and also subjects its anti-money laundering policy to regular independent audit.

(iii) **STARLIFE** cooperates fully with law enforcement and regulatory investigations and inquiries, does not do business with blacklisted entities and is compliant with all legal provisions.

(iv) **STARLIFE** complies fully with AML Laws, Regulations and Circulars etc., issued by the Financial Intelligence Centre (FIC), National Insurance Commission (NIC) and other relevant authorities.

2. OBJECTIVES

In accordance with regulation with Anti-Money Laundering 2020, Act (1044) and National Insurance Commission and Financial Intelligence Center guidance on money laundering (ML) and financing terrorism (FT) 2018, this policy seeks to provide principles

and guidance regarding AML/CFT requirements and risks and to meet the following objectives :

(i) To prevent the use of StarLife products, services and channels for Money Laundering and Financing Terrorism;

(ii) Meet applicable legislation and international best standard; and,

(iii) Mitigate any reputational risks that may arise.

StarLife Assurance Company Limited ("the Company") is committed to the highest standards of Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) compliance and requires Management and employees to adhere to these standards to prevent use of its products and services for money laundering/ terrorist financing purposes.

The Company will examine its AML/CFT strategies and objectives on an ongoing basis and maintain an effective AML/CFT policy that reflects best practices. Compliance with this policy is the responsibility of all Directors, Management and employees.

The policy is formulated and directed by the Board through the Anti-Money Laundering Reporting Officer (AMLRO)."). The program includes clients screening and monitoring requirements, Know Your Customer (KYC) policies, sanctions policy, record-keeping requirements, reporting of suspicious transactions in accordance with established AML/CFT framework.

The standards set out in this policy are minimum standards based on applicable legal and regulatory requirements and applies to the entire Company. The requirements are intended to prevent the Company, its employees and clients from being used for money laundering, terrorist financing or other financial crime. Thus, the policy establishes the general framework for the fight against money laundering and financing of terrorism.

3. DEFINITION OF KEY TERMS

Money Laundering:

Money Laundering is 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.

Generally, there are three (3) stages of money laundering:

Placement: involves the introduction of illegally obtained assets/funds into the financial or non- financial institutions.

Layering: involves conducting a series of simple or complex financial transactions aimed at concealing the source or identity of the assets**.** The transactions are designed to hamper the audit trail, disguise the origin of the funds/assets and provide anonymity.

Integration: involves placing the laundered proceeds back into the economy in such a way that the funds/assets re-enter the financial system as apparently legitimate funds.

These stages are not static and overlap broadly.

4. FINANCING OF TERRORISM CRIMES

Financing of Terrorism is providing funds directly or indirectly knowing that the funds are to be used to fund terrorist acts or organizations.

“Account” means any policy or arrangement through which StarLife accepts deposits or allows withdrawals.

“Financial transactions” means:

(i) The opening, operating (depositing and withdrawing of funds) or closing of an account held with StarLife;

(ii) The telegraphic or electronic transfer of funds by StarLife on behalf of one person to another person;

(iii) The transmission of funds between the Republic of Ghana and foreign countries or between foreign countries on behalf of any person;

(iv) An application by any person for, or the receiving of, a loan from StarLife and repayment of the same;

(v) Receiving or making a monetary / financial gift; or

(vi) Selling and buying of gold, foreign currency and negotiable instruments

"Weapons of mass destructions" are used to characterize a variety of weapons, which include but not limited to nuclear weapons, chemical and biological warfare agents.

"Proceeds of crime" means any property that is derived or realized, directly or indirectly, by any person from the commission of any serious offence, 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.

5. LEGAL FRAMEWORK

The legal framework for developing the policy was based on:

(i) Anti-Money Laundering Act 2020 (1044);

(ii) Anti-Money Laundering Act, 2008 (Act 749);

(iii) Anti-Money Laundering (Amendment) Act, 2014 (Act 874);

(iv) Anti-Money Laundering Regulations, 2011 (L.I.1987);

(v) Anti-Terrorism Act, 2008 (Act 762);

(vi) Anti-Terrorism (Amendment) Act, 2012 (Act 842);

(vii) Anti-Terrorism Regulations, 2011 (L.I 2181);

(viii) The recommendations of the Financial Action Task Force on Money Laundering (FATF), February 2012;

(ix) The UN's International Money Laundering Network (IMOLIN); and,

(x) The Basel committee's instructions about customer knowledge requirement.

6. MINIMUM REQUIREMENTS

StarLife shall adopt and implement a continuous risk-based approach (RBA) to identify, assess and understand its money laundering and terrorism financing risks. It shall also ensure measures to mitigate laundering and terrorism are commensurate with the risks identified, enabling decisions on how to allocate its resources in the most effective way.

7. KNOW YOUR CUSTOMER (KYC).

There shall be implemented a KYC manual that shall provide detailed KYC requirements for various classes of clients.

7.1 Customer Identity must be ascertained:

(i) When on-boarding a new Client;

(ii) Anytime a Client transacts business on the policy;

(iii) Whenever a third party makes premium payments on behalf of a Client;

(iv) Whenever a Client makes cash premium payments of GH¢5,000 and above or its equivalent in foreign currency;

(v) When there is a change in the bio-data of the Client;

(vi) Whenever a Client requests for upward adjustments in premiums mid-term;

(vii) Two or more transactions occur on the Policy within a month;

(viii) There are doubts about the veracity or adequacy of previously obtained Client identification data; and,

(ix) There is a suspicion of money laundering or terrorist financing.

7.2 Identification of Ultimate Beneficial Owner (UBI)

When dealing with Companies, the identity of the ultimate beneficial natural person/ individual who owns, controls the client or its assets or on whose behalf the policy is held must be established and verified.

7.3 Client Identification Verification Platforms

The Company shall implement appropriate ID verification platforms for verification of Clients and third parties' identities.

7.4 Due Diligence on Contractual Parties

The Company shall implement appropriate due diligence measures on all entities and individuals it contracts with.

7.5 Client Policy Monitoring

Permanent monitoring of clients' premium payments shall be implemented to detect unusual/suspicious transactions. The Head of Premium Administration Department shall

monitor and report any unusual premium receipts to the AMLRO by way of Suspicious Transactions Reports.

7.6 Forbidden Businesses

No business shall be transacted with shell companies. No policies shall 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.

7.7 Cash Transaction Reporting (CTR)

The Company shall set up systems to enable the AMLRO 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 usual email account info@fic.gov.gh or such other address as may be notified from time to time. The report will be sent in the approved CTR format.

7.8 Suspicious Transactions Reporting (STR)

Employees are encouraged and mandated to immediately report all suspicious transactions to the AMLRO for further investigation and report to the FIC. STRs must be filed when Customer:

(i) Presents fake documentation; or

(ii) Is found to have been suspect in news publications eg. Wanted Persons etc.; or

(iii) Is involved in identity theft, that is, presents fake Identity card to impersonate someone else in order to have access to a transaction;

(iv) Fails to complete the required Customer Relationship Form within the stipulated time;

(v) Conducts transactions in a manner as to avoid a statutory reporting obligation; or

(vi) Abnormal exercise of cooling off, cancellation and surrender rights.

If an employee cannot understand or is suspicious of a customer's identity, honesty, or of the nature or purpose of the funding requested or the source of the funds, the customer should be considered high risk and the final decision should be forwarded

by AMLRO to the management.

In case of high-risk profile, strong vigilance and suspicion, the CEO should be responsible for the final decision on the business relationship for any of the clients considered as high risk

7.9 Employee Monitoring

There shall be zero tolerance for Staff who engage in fraudulent activities. Such persons shall be deemed unfit to work with the Company and their appointment terminated. Compliance Reports on Employee Policies and Conduct shall be filed with the NIC & FIC at the end of December.

7.10 Anti-Money Laundering Controls

The AMLRO shall ensure by adequate customer and business related controls that all applicable AML/CFT requirements are adhered to and properly functioning.

7.11 Anti-Money Laundering Training

All employees (temporary and permanent) and Sales Executives shall undergo periodic AML/CFT training. Initial training shall be conducted as part of orientation programme for newly employed staff and Sales Executives and subsequently every two (2) years. Training shall however be risk-based and shall focus largely on Sales Executives, Underwriters, Cashiers and Customer Service Officers. Directors shall also be trained periodically.

7.12 Anti-Money Laundering Risk Analysis

The Company shall set up systems to assess the level of client risk and implement appropriate mitigation measures. Also, the Company shall undertake comprehensive AML/CFT risk assessment prior to the launch or use of new products, services, practices and technologies and take appropriate measures to manage and mitigate the risks. This responsibility shall be exercised in conjunction with the Risk Management Unit.

The Company shall not launch any high-risk products, i.e., products that can be used to

foster money laundering/ terrorist financing.

7.13 Politically Exposed Persons (PEPS)

The AMLRO shall maintain a list of PEPs. The list must be updated monthly and sent to Underwriters, Customer Services Officers and Cashiers. PEPs are individuals who are or have been entrusted with prominent public functions both in Ghana and foreign countries and those associated with them. They include:

(i) Heads of State or government;
(ii) Ministers of State;
(iii) Politicians;
(iv) High ranking political party officials;
(v) Senior public officials;
(vi) Senior Judicial officials;
(vii) Senior military officials;
(viii) Chief executives of state owned companies/corporations;
(ix) Diplomats and reps of foreign countries and organizations;
(x) Family members or close associates of PEPs; and,
(xi) Businesses/ organizations belonging to a PEP.

The PEPs List will also contain names of High Risk and Blacklisted Persons or entities.

7.14 AML/CFT Software

The Company shall implement Anti-Money Laundering software depending on its exposure to AML/CFT risk, upon approval by the Board.

7.15 Know Your Operations

In order to avoid being used as a tool of Proceeds of Crime, StarLife monitors, for all accounts, unusual or suspicious patterns of transactions. Unusual or suspicious activities can be identified through:

(i) Monitoring of transactions, in particular using the operational software;
(ii) Client contacts (meetings, discussions, in-country visits etc.); and,
(iii) Third party information collection.

StarLife uses operations monitoring tools to:

(i) Implement key indicators in helping to isolate accounts with unusual transactions;

(ii) Ear mark higher risk accounts and performs intensified monitoring on these accounts; and,

(iii) Established limits for different categories or types of accounts or transactions. Particular attention is paid to transactions that exceed such limits.

The high-risk accounts will be subject to in-depth monitoring as defined in internal control procedures. StarLife will ensure that the information is properly transmitted to managers, so that they can analyze and monitor this type of high-risk customers with appropriate tools.

All employees involved in StarLife operations must be screened prior to employment. This will include proof of identity and reference checks, AML Checks via the sanctions list and from previous educational and professional entities

8. SCREENING OF EMPLOYEES

All employees involved in StarLife operations must be screened prior to employment. This will include proof of identity and reference checks, AML Checks via the sanctions list and from previous educational and professional entities.

9. ROLES AND RESPONSIBILITIES

9.1 Board of Directors

The Board of Directors shall:

(i) Approve the AML/CFT policy.

(ii) Be responsible for ensuring governance and oversight of the StarLife risk management framework and controls regarding money laundering and terrorism financing.

(iii) Appoint an Anti-Money Laundering Reporting Officer (AMLRO) who shall be a key management personnel and who will operationally report to the Board in

accordance with section 41(1)(b) of the Anti-Money Laundering Act, 2008 (Act 749) as amended and Regulation 5(1) of L.I. 1987.

(iv) Ensure that Management forwards all required periodic reports to the relevant regulatory authorities

(v) Review all periodic report on AML/CFT matters

(vi) Through the Board Audit & Risk Committee shall oversee compliance with this policy and all other statutory and regulatory AML/CFT obligations.

9.2 Anti-Money Laundering Reporting Officer (AMLRO)

The AMLRO shall be equipped with the relevant competence, authority and independence to implement this policy. The duties of the AMLRO include:

(i) Developing and ensuring compliance with the Company's AML/CFT policy;

(ii) Receiving and vetting Suspicious Transaction Reports (STR) from employees;

(iii) Filing and CTRS and STRs with the FIC;

(iv) Co-ordinating the training of Directors, employees and Sales Executives in AML/CFT awareness, detection methods and reporting requirements;

(v) Being a point-of-contact for employees on issues relating to money laundering and terrorist financing;

(vi) Filing appropriate returns/reports at the National Insurance Commission (NIC);

(vii) Supervising the monitoring of employee's Policies for signs of money laundering;

(viii) Oversee compliance with record keeping and independent testing;

(ix) Maintaining a Register of enquiries made by the FIC and other law enforcement agencies; and

(x) Maintaining a list of domestic PEPs, High Risk and Blacklisted Persons.

9.3 Internal Audit

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

9.4 Staff and Associated Persons:

Staff members, consultants and other associated persons shall be responsible for:

(i) Complying with this AML/CFT Policy, other standards and controls;

(ii) Familiarizing themselves with and acting in accordance with relevant processes and procedures to manage AML/CFT compliance;

(iii) Reporting to the AMLRO without undue delay any suspicions (or actual occurrences) or red flags of ML/TF activities Staff. The internal audit will perform testing of the compliance program atleast once a year to provide assurance that the regulation is being complied with; and,

(iv) The AML/CFT performance review of staff shall be part of employees' annual performance appraisals.

10. SCOPE OF UMLAWFUL ACTIVITIES

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

- Participation in an organized criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substance
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Murder, grievous bodily injury
- Kidnapping, illegal restraint and hostage-taking
- Robbery or theft
- Smuggling
- Tax Evasion
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation
- Corruption and bribery
- Fraud

- Counterfeiting currency
- Counterfeiting and piracy of products
- Environmental crime
- Any other predicate offence under the Anti-Money Laundering Act, 2008 Act 749 as amended and Anti-Terrorism Act 2008, Act 762 as amended

11. HIGHER AND LOWER LEVEL RISK CATEGORIES OF CUSTOMERS

StarLife 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 transaction.

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

Examples of higher-risk customer categories include:

- Non-resident customers;
- Private banking customers;
- Legal persons or legal arrangements ;
- Political exposed persons ;
- Designated Non-Financial Businesses and Professionals; and,
- Any other institutions deemed as high risk client.

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 istitutions – provided they are subject to requirements for the combat of money laundering and financing of terrorism & proliferation;
- Where there are low risks, StarLife Shall 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 customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in other public institutions; and,

- In circumstances of low risk, StarLife shall apply the simplified or reduced CDD procedures when identifying and verifying the identity of policy holders and the beneficial owners.

12. TRAINING

1. The training program shall encompass all Board of Directors and Employees. For newly recruited Employees, AML/CFT training shall form part of the orientation program.
2. 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 risk that the Company is exposed to. Training will be risk based with focus on the following category of persons: -

(i) **Sales Executives/ DSOs/ Corporate Relationship Managers-** KYC begins with gathering the right information about the client;

(ii) **Underwriters-** review the information above and risk rate to ensure that high risk persons are not on-boarded; and,

(iii) **Customer Service Officers/ Cashiers-** ensure that payments are made to rightful owners of the policies.

3. The Training programme shall be developed at the beginning of every year by the AMLRO in collaboration with the relevant departments.
4. Training may be conducted internally by qualified staff or by external resource persons.
5. The basic elements of the employee training program shall include:

(i) The nature of money laundering;

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

(iii) Reporting requirements;

(iv) Customer due diligence;

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

(vi) Record keeping and retention policy; and,

(vii) AML regulations and offences.

6. The Company shall submit half yearly Reports to the NIC on its level of compliance.

7. The annual AML/CFT Employee training program for the coming year shall be submitted to the NIC and FIC not later than the 31st of December every year.

13. REPORTS

11.1 Transaction and Customer Reports

If any of the cases presented here in 10.1 above occurs and if the explanations are not satisfying or not plausible, StarLife will establish a confidential written report stating the collected information, in particular:

(i) The source and recipient of funds, as well as the transaction object;

(ii) The identity of the requestor and of the beneficiary(ies) (name, address, occupation…);

(iii) The operation characteristics; and,

(iv) The conditions of account functioning, in particular opening date, name of beneficiary or other persons affiliated with the account.

If necessary, a detailed study will be carried out and in case of suspicion of an illegal transaction, StarLife shall submit a Suspicious Transaction Report (STR) to the Financial Intelligence Centre (FIC) and National Insurance Commission (NIC) within 24 hours.

11.2 Suspicion Transaction Report (STR)

If based on information supplied by the customer or from other sources, an employee has reason to believe that the customer's account is being utilized for transactions related to money laundering and/or financing terrorist activities the following should be done:

(i) He/she must immediately send a written note to the AMLRO.

The AMLRO shall within 24 hours and before any transaction, undertake the following:

(i) Reasonable measures to collect information to ascertain the purpose of the transaction, the origin and destination of funds; and,

(ii) If the suspicion is justified or not. The AMLRO shall notify CEO who shall, with the assistance of AMLRO determine report.

If suspicion remains after this investigation, AMLRO will report its suspicions to the Financial Intelligence Centre (FIC) and the National Insurance Commission and will take

measures recommended about the termination of the business relationship with this customer.

14. NEW TECHNOLOGIES

The Company shall implement controls and measures to prevent misuse of technological developments including the use of applications (Apps), and USSD platforms as a conduit to launder money. This will be done by:

(i) Assessing the KYC and money laundering risks that is posed as a result of using these technological platforms and formulating appropriate mitigations to address these risks. Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers;

(ii) Identification and verification of clients enrolled on all mobile platforms similar to the requirements of walk-in-clients in line with the respectable KYC requirement (minimum, standard and enhanced KYC); and,

(iii) Conduct due diligence on the third parties.

15. 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.

16. PROTECTION OF STAFF

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 staff 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 staff, a discussion will be held with the latter on how to proceed;

(iv) Should the staff 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; and

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

17. RECORD KEEPING

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

- All Proposal forms;
- 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.

18. SANCTIONS

The below offences shall attract sanctions/penalties from the regulators and hence StarLife shall ensure compliance to all:

(i) Failure to appoint an AMLRO at management level;

(ii) Failure to develop and implement 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 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 performance part of employee annual appraisals;

(xiii) Failure to monitor employee conduct ;

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

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

(xvi) Formal board approval of Key AML/CFT documents (AML/CFT compliance programme, policy, manual, and Risk Assessment Framework). Board shall ensure that all AML documents are approved by the Board;

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

(xviii) Submission of other Statutory Reports including mandatory Returns

Failure for;

- Non-submission.
- Incomplete submission.
- Delayed submission.
- Inaccurate submission and other reports.

19. INDEPENDENT AUDIT

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

20. REVIEW

This policy shall be reviewed periodically to reflect all new risks of money laundering identified. The revised Policy upon approval by the Board shall be submitted to the NIC & FIC. Where new areas of risk are identified, additional procedures shall be designed in the form of a Contingency Plan and submitted to the NIC & FIC.

21. 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	