GOLDENBRLDGE ASSET MANAGEMENT COMPANY LIMITED

ANTI-MONEY LAUNDERING & COUNTERING FINANCING OF TERRORISM AND PROLIFERATION MANUAL

REVISION HISTORY

Initiated By	Date	Description	Date/Initial Version	Comment	Current Version
Internal Control	October 2021	Anti-money Laundering and Countering Financing of Terrorism and Proliferation Manual	October 2021/1.0		1.0
Next Review Date: To be reviewed every two (2) years or as the business and regulatory exigencies may demand					

Table of Contents

1. INTRODUCTION

1.1 POLICY STATEMENT

Goldenbridge Asset Management Company Limited (GAMCL) is committed to:

a. Implementing sound anti-money laundering and countering financing of terrorism & proliferation policies and procedures which will ensure that it is not used as a conduit for money laundering or financing of other illicit businesses:
b. Implementing policies, procedures, guidelines and provisions of manual emanating from relevant regulatory bodies towards ensuring compliance with all domestic and international laws and regulations on money laundering and countering financing of terrorism and proliferation in order to mitigate AML/CFT risks it is exposed to;

c. Strict compliance with both the letter and the spirit of all regulatory requirements and high standard of market conduct;

d. Conducting all transaction in accordance with all regulatory policies andguidelines governing its operating environment:

e. Giving full cooperation to law enforcement authorities within the limits of the rulesgoverning confidentiality:

f. Effective communication of these policies towards raising the level of staff awareness on AML/CFT issues;
g. Retention and preservation of records of customers' transactions for a minimum of ten yearsor as may be prescribed by various regulatory bodies;

h. Exiting relationships which pose heightened money laundering risks to GAMCL and reporting same to the relevant regulatory agencies.

Drawing significantly from but not limited to recommendations of the Financial Action Task Force (FATF) 40 recommendations, provisions of the Money Laundering (Prohibition) Act 2011 (as amended), Terrorism/Prevention Act 2011 (as amended), SEC AML/CFT Compliance Manual for Capital Market Operators 2010, SEC Rules and Regulations 2013 and SEC Know Your Customer (KYC) guidelines. GAMCL has put in place the following measures in the attainment of its objective of ensuring full compliance with the letter and the spirit of all applicable laws and regulations.

GAMCL:

i. Has established sound internal policies, controls, procedures to mitigate money laundering and financing of terrorism risks.

ii. Regularly trains its staff to identify suspicious activities/transactions and to take appropriate actions.

iii. Has in place and updates the AML/CFT Employee Training Programmes for newhires and regular refresher training for existing staff.

iv. Has internal referral process and procedures for compliance matters.

v. Ensures implementation of policies and procedures and internal controls to correct/enhance and/or adapt to regulatory changes / deficiencies.

vi. Has designated a senior management staff as its Chief Compliance Officer tooversee its AML/CFT program.

vii. Regularly reviews/revises the policies to ensure that they remain relevant and current and in line with the evolving regulatory requirement and leading practices.

1.2 PURPOSE

This manual forms an integral part of GAMCL's Compliance Risk Management Framework. The essence of this AML/CFT Manual is to:

a. Document the comprehensive and constantly evolving policies, procedures and processes deployed by Goldenbridge Asset Management Company Limited to assure adherence to the provisions of AML/CFT legislations and guidelines in Nigeria and all jurisdictions where our businesses are located.

b. Create a framework for managing AML/CFT compliance risks in GAMCL.

c. Ensure that GAMCL does not fall victim of illegal activities perpetrated by its customers.

d. Specify basic expectations of all staff as regards their obligations for the management ofAML/CFT risk

1.3 ROLES AND RESPONSIBILITIES THE BOARD

The roles and responsibilities of the Board of Directors with respect to AML/CFT Compliance & Risk Management include (but shall not be limited to):

i. Assume overall accountability for Compliance performance.
ii. Ensure that appropriate AML/CFT Compliance Risk Management framework isestablished and is in operation.
iii. Approve the AML/CFT Compliance Risk Management program and policies.
iv. Provide guidelines regarding the management of AML/CFT Compliance risks.
v. Appoint and designate a Chief Compliance Officer (not less thana General Manager status) to coordinate and monitor AML/CFT Compliance by GAMCL

Chief Compliance Officer

i. Coordinate and monitor AML/CFT Compliance by GAMCL
ii. Inform Board and Management of AML/CFT Compliance efforts, compliance failures and the status of corrective actions
iii. Monitor implementation of the code of corporate governance
iv. Ensure implementation of Board decisions on compliance matters
v. Ensure that regulatory changes are effectively implemented in GAMCL
vi. Direct prompt investigation of any unusual or suspicious transaction and reports to the Regulatory body.
vii. Ensure that compliance requirements are integrated into the day-to-day activities of GAMCL and that processes are efficient and in accordance with applicable laws andpolicies.

AML/CFT Compliance Officer

i. Coordinate and monitor day to day compliance with applicable money laundering laws and regulations.
ii. Monitor transactions to detect any unusual or suspicious transactions.
iii. Conduct Preliminary investigation on any unusual or suspicious transaction.
iv. Prompt preparation and delivery of all relevant returns to the regulatory bodies in line with the MPLA 2011 and SEC AML/CFT Regulation (2013) as amended.
v. Communicate AML/CFT issues to all stakeholders.

Branch Compliance Officers

All Customer Service Managers are designated as compliance officers in their respective branches and shall perform the following functions:

i. Monitor money laundering activities in the branch.
ii. Ensure adherence to KYC principles.
iii. Coordinate submission of suspicious transactions report to the Chief Compliance Officer.
iv. Coordinate collation of documents as may be requested from time to time.

v. Ensure full implementation of GAMCL's policy and statutory regulations on compliance and money laundering activities.

vi. Ensure swift resolution of corrective action grid on all inspection reports i.e. statutory/Group reports, e.g. SEC, NSE, NFIU, Group Internal Audit Reports, Control reports, etc.

vii. Create awareness among branch staff on Compliance and anti-money laundering activities.

Group Internal Audit

i. Incorporate compliance testing in their normal audit program.
ii. Report on results of the independent testing to the Board through the MD/CEO

All Employees:

i. Be aware of and comply with GAMCL's policies and procedures.
ii. Report suspected money laundering activities to the Chief Compliance Officer
iii. Comply strictly with Know-Your-Customer directives

1.4. SCOPE

This manual is applicable to Goldenbridge Asset Management Company Limited.

2. COMPANY BACKGROUND

2.1 BRIEF HISTORY

Goldenbridge Asset Management Company Limited (GAMCL) is a licensed fund/asset and
portfolio management firm with headquarters in Abuja, Nigeria.

The firm was incorporated on 15 July 2011 and commenced operations in January 2015. GAMCL provides wealth and investment management services to individual and institutional clients, globally.

2.2 OPERATIONAL PERFORMACE

GAMCL currently operates from its corporate office at Gateway Plaza, Zakariya Maimalari Street, Central Business District, Abuja, FCT — Nigeria.

Our recent focus on institutional and high net worth clients has created a new growth trajectory making us more profitable.

2.3 OUR VISION, MISSION AND BEHAVIOURAL ATTITUDE

Vision

To distinguish GAMCL as a preferred financial principal and service provider of innovations for building, developing and protecting wealth.

Mission

Helping our clients to achieve financial solutions for better opportunities.

Values

Our track record *and* vision show that we possess world class investment management capabilities. seamless trading *and* settlement processes and an unparalleled knowledge of our chosen market. We are experts at what we do.

Value Proposition

Investment solutions driven by deep market knowledge and global standard investment management expertise.

Our Approach

Discover: Our relationship begins with a thorough understanding of you- your needs, yourlifestyles, and family, and your goals for the future.
Create: We work with you to develop a roadmap to help you pursue the outcomes you envision. Act: Next, we can help you implement investment, retirement, trust services andcash management suited to your needs.
Adjust: Achieving your goals requires vigilance and flexibility. It requires making adjustments as life evolves, markets, tax laws shift, and priorities change.

3.0 DEFINITIONS OF ACRONYMS AND TERMS

3.1 ACRONYMS

- AML - Anti Money Laundering: Refers to policies, procedures and controls which are instituted to prevent, detect and report money laundering activities.
- SEC - Securities and Exchange Commission, Nigeria: The apex regulator of the Nigerian capital market.
- CCO- Chief Compliance Officer: A senior official who is a Statutory Officer by virtue of Section 9 (1 a) of MLPA 2011, who interfaces between Management and Staff, Organizations, Regulatory and Law Enforcement Agencies on all issues pertaining to money laundering and financing of terrorism.
- CO - Compliance Officer: A statutory official of a financial institution by virtue

of Section 9 (1 a) of M L P A 2011, who interfaces with staff and Organizations, Regulators and Law Enforcement Agencies on all issues pertaining to money laundering and reports to the CCO.

- CDD - Customer Due Diligence: This means taking steps to identify your customer and checking that they are who they say they are. In practice this means obtaining the following from a customer:
  - Name
  - photograph on an official document which confirms his identity;
  - Residential address

- CTRs - Currency Transaction Reports: This is made by financial institutions and designated non-financial institutions regarding any transaction, lodgment or transfer of funds in excess of N5,000,000 or its equivalent, in the case of an individual, or N10,000,000 in the case of a corporate body pursuant to Section 10 of the ML(P)A, 2011.

- EFCC- Economic and Financial Crimes Commission: A Federal Government agency which is charged with the responsibility of coordinating the various Institutions involved in the fight against money laundering and enforcement of all laws dealing with economic and financial crimes.
- FATF — Financial Action Task Force: FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. IT was established in 1989 by the *c/-7* Summit that was held in Paris. Asa "policy making body" it works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. It is known for its 40 plus 9 recommendations which establish an AML framework for its membercountries. (See Appendix 1 for FATF 40 Recommendations).
- GAMCL- Goldenbridge Asset Management Company Limited
- KYC - Know Your Customer: Entails obtaining and verifying customer identity, Preservation of records of customers, mandatory disclosure of transactions to authorized statutory bodies.
- KYCB - Know Your Customer's Business: Another offshoot from the KYC where financial institutions are enjoined to know the line of business of their customers such that transactions by the customers are fairly predictable. This will assist in the identification of unusual transactions or activities that may appear inconsistent with the customer'sknown business.
- MLPA — Money Laundering (Prohibition) Act 2011. A Federal legislation which deals on the policies, framework and sanctions on Money laundering for both Financial Institutions and Designated Non-Financial Persons and Businesses (DNFPBs).
- NDLEA - National Drug Law Enforcement Agency.
- NFIU - Nigeria Financial Intelligence Unit: The Nigerian arm of the global

Financial Intelligence Unit (FIU). The activities of the NFIU are covered under the NFIU Act 2018 and MLPA 2011. Its core role is that it serves as the country's central agency for the intelligence information gathering, collection, analysis and dissemination of financial information regarding money laundering and the financing of terrorism.

- PEPs - Politically Exposed Persons: This involves individuals who are or have been entrusted with prominent public functions in any country, for example Heads of State or of Government, Politicians, Senior Government Official, Judicial or Military Officials, Senior Executives of State-Owned Corporations, important Political Party Officials and any "close associate" of a senior political figure (local/foreign) all fall into this category.
- STRs - Suspicious Transaction Reports: This is made by financial institutions and designated non-financial institutions or made voluntarily by any person irrespective of the amount involved pursuant to Section 6 of the MLPA, 2011. It isa transaction, which is inconsistent with a customer's known legitimate business or personal activities. The first key to the recognition of a suspicious transaction is in knowing enough about the customer's business to recognize that a transaction, or series of transactions, is unusual.

3.2 TERMS

- Management - this refers to the Managing Director and department heads.
- Executive Management — this refers to the Managing Director.
- *Stott* — This includes all employees of GAMCL.
- Shell Bank — Any financial institution or bank with no fixed (physical) andregistered address.

4.0 ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM POLICIES

4.1 MONEY LAUNDERING

Money Laundering is the process by which monies or assets derived from criminal activities are converted into funds or assets which appear to have a legitimate origin. It involves taking criminal proceeds and disguising their illegal sources in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities.

Money Laundering Predicate Offence

Money laundering predicate offence is the underlying criminal activity that generates proceeds, which when laundered, results in the offence of money laundering. These include kidnapping, illegal restraint and hostage taking, insider trading and market manipulation, embezzlement & fraud, bribery and corruption, robbery, drug trafficking, environmental crimes, terrorism, counterfeiting currency, counterfeiting and piracy of products, smuggling,

extortion, forgery, sexual exploitation, etc.

Stages of Money Laundering

Placement

The physical disposal of cash/property derived from criminal activity. The purpose of this stage is to introduce proceeds into the traditional or non —traditional financial system without attracting attention e.g., purchase of artwork, cash deposits, casinos etc.

Layering

This involves separating source of proceeds from ownership by changing the form. This is designed to hamper audit trail e.g., complex wire transfers, resell of assets/properties, opening of several accounts to disguise origin of funds etc.

Integration

Re — channeling the laundered funds back to the financial system as legitimate funds.

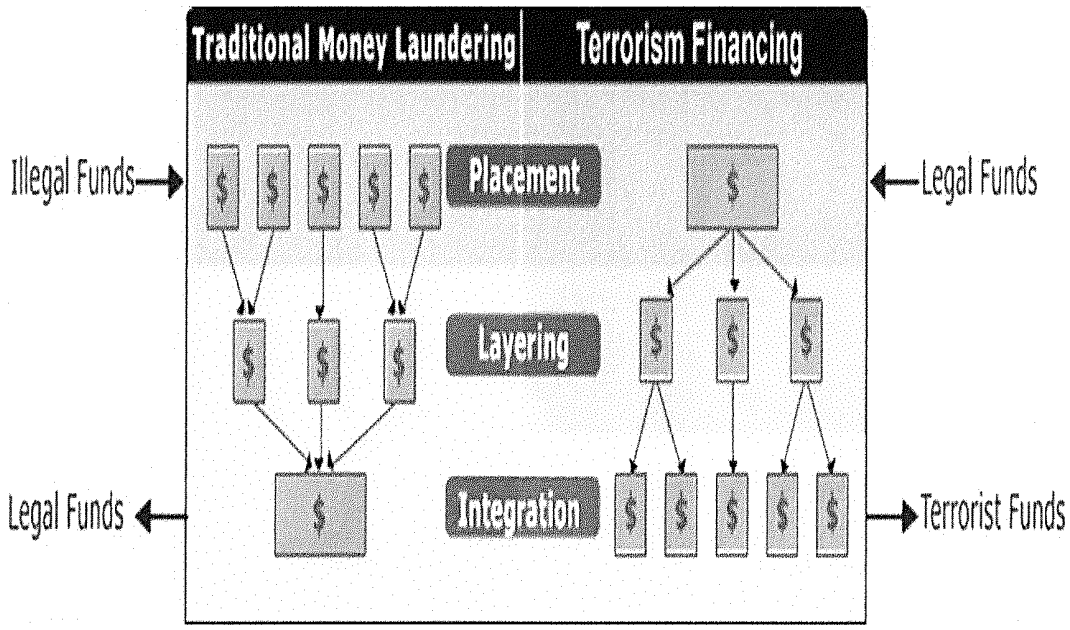
4.2. TERRORISM AND TERRORISM FINANCING

Terrorist act — any act intended to cause death or serious bodily injury to a civilian or anyother person not taking an active part in the hostilities. Usually, the purpose is to intimidate a population or to compel a government or society to do or abstain from doing any act.

Terrorism financing (TF) occurs when a person by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that such the funds will be used or in the knowledge that the funds will be used in full or in part, in order to carry out a terrorist act.

Terrorist activities are sometimes funded from the proceeds of illegal activities. Although often linked in legislation and regulation, terrorist financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorist financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.

Difference between Money Laundering and Terrorism financing



4.3. REGULATORY AND LEGAL FRAMEWORK

Nigerian financial institutions are monitored for money laundering by some organizations/agencies and under the provisions of the reputations specified below:

Institutional Framework – Local

- Economic and Financial Crimes Commission (EFCC)
- Nigeria financial intelligence Unit (NFIU)
- National Drug Law Enforcement Agency (NDLEA)
- Securities and Exchange Commission (SEC)
- Nigerian Stock Exchange (NSE)
- Federal Ministry of Trade & Investment (FMT&I)
- Independent Corrupt Practices Commission (ICPC)
- Federal Inland Revenue Services (FIRS)
- National Insurance Commission (NAICOM)
- Nigeria Custom Service (NCS)

- Nigeria Immigration Services (NIS)
- Nigeria Deposit Insurance Corporation (NDIC)
- Central Bank of Nigeria (CBN)

Institutional Framework — International

- Basel Committee on Banking Supervision
- Financial Action Task Force (FATF)
- Inter-Governmental Group Against Money Laundering (GIABA)
- Egmont Group (of Financial Intelligence Units)
- Wolfsberg Group
- United Notions Office of Drugs and Crime (UNODC)
- The World Bank
- European Union
- Interpol
- The Joint Money Laundering *Steering* Group

Legal Framework – Local

- Money Laundering (Prohibition) Act 2011
- Terrorism (Prevention) Act 2011
- CBN AML/CFT Regulation 2009
- SEC Rules and Regulations 2011
- SEC AML/CFT Regulations 2013
- Advanced Fee Fraud Act 2006
- Bank's (recovery of Debt) and financial Malpractices in Banks in Nigeria Act (as amended)
- Banks and other Financia/ Institutions Act 1991
- ICPC (Establishment) Act
- EFCC (Establishment) Act 2004
- NDLEA Act
- Dishonored Cheques *Act.* Etc,

Legal Framework – International

- Directive 2005/60/EC of the European Parliament and of the Council.
- Office of Foreign Asset Control (OFAC)
- USA PATRI0T Act: Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism.
- Sarbanes-Oxley Act
- FATF 40 Recommendation

4.4. CUSTOMER IDENTIFICATION PROGRAM (CIP)

The Customer Identification Program, also known as the Know Your Customer (KYC) process is intended to enable GAMCL form a reasonable belief that it knows the true identity of

each customer.

As a general rule, a business relationship with GAMCL will NOT be established until the identity of a potential customer is satisfactorily established. Where a potential customer declines to provide any account initiation information, the relationship will not be established. Furthermore, if follow-up information is not forthcoming, any relationship already established will be terminated.

GAMCL's account opening procedures which also specify the identification documents and information required from each customer are contained in GAMCL' Operations Policy Manual.

KNOW YOUR CUSTOMER (KYC)

KYC is the due diligence that financial institutions and other regulated companies must perform to identify their clients and ascertain relevant information before doing financial business with them.

To this end, GAMCL' KYC policies and procedures emphasize the following:

i. Obtaining the necessary documents and information from every customer asspecified in GAMCL' Operations Policy manual.
ii. Prohibition of opening numbered or anonymous accounts.
iii. Minimum acceptable identification evidence for low risk and low value accounts.
iv. Independent verification of the legal status of incorporated entities and sole proprietorships with the Corporate Affairs Commission in writing
v. screening of customer information against database of individuals and entities subject to sanction (watch-list check) at on-boarding stage and quarterly customer database scan as required by the AML/CFT regulations.
vi. Identifying the customer as well as the beneficial owners and
vii. verifying that customer's identity using reliable, independent source documents, data or information.
viii. Profiling of customers such that transactions by our customers are fairly predictable.
ix. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.
x. Customer information update whenever the need arises.
xi. Obligation to report to the regulatory authority's suspicious transactions, which may ultimately have a bearing with money laundering activities.

Prohibited Business Relationship

In line with local and international best practices, GAMCL does not open accounts orconduct transactions for customers using pseudonyms or numbers instead of actual names or maintain relationships with individuals or entities that have been sanctioned.

GAMCL as a matter of policy does not transact business with "shell corporations" as describedunder the International Conventions.

GAMCL applies each of the CDD measures under but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures to be taken shall be consistent with any guidelines issued by competent authorities. For higher risk categories including PEP, GAMCL shall perform enhanced due diligence.

Record Keeping and Retention requirements

GAMCL shall comply with the requirements of the Money Laundering (Prohibition) Act, AML/CFT Regulations and any other legislation to the effect that all records of customers' identification and transactions must be kept fora minimum of five years after the closure of the account /severance of relationship with the customer or after carrying out transactions. Records of all suspicious transactions shall be kept for the same period.

Requests for AML records by Regulatory and Law Enforcement Agencies

Upon request by a regulatory or law enforcement agency, GAMCL shall make available records related to its AML Compliance or its customers as soon as possible from the date of the request.

4.5. REPORTING SUSPICIOUS TRANSACTIONS

A. Transaction Monitoring

Transaction Monitoring occurs on a manual and automated basis. The former is performed by allmembers of Staff who are regularly provided with red flags/indicators to look out for in active transactions. The latter resides within the Compliance unit.

All Staff are aware that suspicious transactions should be immediately reported to the Compliance Unit by filing internal suspicious transactions reports. Where a report is deemed appropriate, it would be filed with the relevant authorities, (SEC, NFIU).

B. Identification of Suspicious Transactions

GAMCL shall exercise due diligence in identifying and reporting of suspicious

transaction.Suspicious transactions shall include:

1. Transaction involving a frequency which is unjustifiable or unreasonable, unusual or has unjustified complexity.
2. Transaction which appears to have no economic justification or lawful objectives.
3. Transactions which are structured to avoid reporting and record keeping requirements.
4. Transfers of foreign currency transactions which are recalled twice from the account of acustomer by correspondent bank. (Note that a first recall could be due to error.)
5. If the circumstances surrounding the first recall of a foreign currency transactions from the account of a customer by correspondence bank appeared suspicious.
6. Altered or false identification or inconsistent information or any transaction involving criminal activity in the view of GAMCL.

C. Procedures for Disclosure of Suspicious Transactions

1. Any Officer of GAMCL who suspects any transaction to be suspicious shall make in writing and signed an immediate report to the Chief Compliance Officer. If it occurred at the branches, it shall be drawn to the attention of the Head of the branch and then to the Chief Compliance Officer in the Head Office (See Appendix 2 for STR Form).

2. GAMCL has also established procedures whereby such reports are coordinated through a central point Chief Compliance Officer/Money Laundering Reporting Officer domiciled in the Head Office for onward reporting to the NFIU/EFCC.

3. In the event that urgent disclosure is required in a 'live' situation, particularly when the account concerned is part of an on-going investigation, an initial notification shall be made by telephone to the Commission.

4. Staff must not disclose to customers or anyone else that they are subject to money laundering investigation. (Tipping off).

D. Compilation of Reports and Returns to Regulatory Authorities

GAMCL shall ensure timely and accurate rendition of all AML/CFT returns as specified in the Money Laundering (Prohibition) Act 2011, the SEC Rules and Regulations as well as other relevant Regulations/Acts/Guidelines/Circulars that may be issued from time to time by various Government agencies. See GAMCL's Regulatory Returns Universe)

E. Crystallization of AML/CFT Risks

In the event that an existing or prospective client is identified as laundering money or financing terrorism, the Relationship Officer shall immediately report the finding to the ChiefCompliance Officer. Upon review of the client account transaction history, KYC documents and any other relevant available documents and the possibility of ML/FT is evident, the Chief Compliance Officer shall immediately report the case to the Managing Director for executive review before onward submission to the Securities & Exchange Commission and the National Financial Intelligence Unit. The matter shall be presented to the Commission and the NFIU with all relevant supporting documents and clearly state that GAMCL awaits further directive from the Commission and/or the NFIU while the client activity is continuously monitored. Such cases shall also be reported to the Board. The client must not be alerted to any such ongoing investigation.

4.6. Awareness and Training

The Money Laundering (Prohibition) Act 2011 requires financial institutions to ensure, first, that its employees are made aware of the provisions of the relevant legislation and the obligations i m p o s e d on staff and financial institutions. Secondly, staff shall be given training on how to recognize and deal with transactions which may be related to money laundering or terrorist financing.

GAMCL's AML/CFT training program isa mix of e-learning and instructor-led training modules. The trainings incorporate current developments and changes to the MLPA 2011 and SEC AML/CFT Regulations and other related guidelines. Changes to internal policies, procedures, processes and monitoring systems are also covered during the trainings

All staff including Senior Management are required to complete the AML/CFT training at least once in every financial year as this forms an integral part of GAMCL's employee appraisal system. Evidence of completion and records of attendance shall be kept by the Training Academy and shall be made available to Compliance unit on request.

GAMCL shall also utilize other avenues such as e-mails, compliance newsletters to disseminate compliance issues arising from new rules and regulations to all staff.

4.7. Politically Exposed Persons

"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in any country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned

corporations, important political party officials and any "close associate" of a senior political figure (local/foreign). Business relationships with family members or close associates of PEPs involve reputation risks similar to those with PEPs themselves.

A senior political figure: This includes any corporation, business, or other entity that has been formed by, or for the benefit of a senior political figure (local/foreign).

Immediate Family: The "immediate family" of a senior political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.

Close Associate: A "close associate" of a senior political figure isa person who is widely publicly known to maintain an unusually close relationship with the senior political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior political figure. Although close associates are more difficult for financial institutions to identify, they include individuals who, due to the nature of their relationship with the PEP, are in a position to conduct significant domestic and international financial transactions on behalf of the PEP.

The term PEP includes persons whose current or former position can attract publicity beyond the borders of a country and whose financial circumstances may be the subject of additional public interest.

Examples of PEPS includes, but not limited to the following:

- Heads of State or Government and Cabinet Ministers
- Governors
- Local Government Chairmen
- Senior Politicians
- Senior Government Officials
- Judicial or Military Officials
- Senior Executives of State-owned Corporations
- Important Political Party officials
- Family members or close associates of PEPS
- Members of Royal Families.

What is the risk in doing business with PEP?

Accepting and managing funds from corrupt PEPs can severely damage GAMCL's ownreputation and can undermine public confidence in the ethical standards of GAMCL, since such cases usually receive extensive media attention and stronp political reaction. Inaddition, GAMCL may be subject to costly information requests and stop debit/ seizureorders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable

to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, GAMCL and/or its officers and employees themselves can be exposed to charges of money laundering, if know or should have known that the funds stemmed from corruption or other serious crimes.

Where to begin

As with most aspects of compliance, the place to begin is with a risk assessment. GAMCL conducts a risk assessment of its products/services, customers, and geographies where business is conducted. The outcome of this assessment forms the basis of a PEP/KYC compliance program.

PEP Risk Assessment

GAMCL assesses the risks posed to its investment activities on the basis of the scope of operations and the complexity of GAMCL's customer relationships. Management establishes a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities.

The following factors are considered when identifying risk characteristics of Politically Exposed Persons:

1. Nature of the customer and the customer's business. The source of the customer's wealth, the nature of the customer's business and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing.

2. Purpose and activity. The size, purpose, types of accounts, products, and services involved in the relationship, and the anticipated activity of the account.

3. Relationship: The nature and duration of GAMCL's relationship (including relationships with affiliates) with the client.

4. Customer's corporate structure. Type of corporate structure.

5. Location and jurisdiction. The review considers the extent to which the relevant jurisdiction is internationally recognized as presenting greater risk for money laundering or, conversely, is considered to have robust AML standards.

6. Public information. Information known or reasonably available to GAMCL about the client. The scope and depth of this review depends on the nature of this relationship and the risks involved.

Risk Minimization

a. Conducting detailed enhanced due diligence at the outset of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a "politically exposed person".
b. GAMCL is more vigilant where its customers are involved in Chose businesses which appear to be most vulnerable to corruption.
c. Every effort is made to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, likewise establish that these are legitimate, both at the outset of the relationship and on an ongoing basis.
d. The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile would be regularly reviewed and updated.
e. A review at senior management or board level of the decision to commence the business relationship and regular review, on at least an annual basis of the development of the relationship.
f. Close scrutiny of any unusual lectures, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of small and unknown in secrecy jurisdictions and regular transactions involving sums just below a typicalreporting amount.
g. Full documentation of the information collected in line with the above. If the risks are understood and properly addressed, then the acceptance of such persons becomes a commercial decision as with all other types of customers.

GAMCL's obligations and position on PEP accounts

Before any account is opened for any PEP, Senior Management approval must be obtained. For this purpose, Senior Management approval must be obtained from the Managing Director and the Chief Compliance Officer. This will be done as part of account opening formalities. No account would be opened for any PEP without the approval being in place.

The customers' due diligence efforts do not end at account opening; ongoing account monitoring is expected. Activities on PEP accounts will be reviewed on a monthly basis with a view to identifying unusual and potentially suspicious transactions related to them and filing, as appropriate, STRs related to them.

Monthly returns will be sent to the SEC and NFIU on PEP transactions. This is to assist the regulators in monitoring the activities of PEPS.

GAMCL will take reasonable steps to ascertain the source of wealth and the source of funds of PEPS and report all anomalies to the SEC and other relevant authorities.

Periodic Enhanced Due Diligence and monitoring must be carried out on all PEPS by the RM and or AO concerned. On an annual basis, the relationship managers

shall certify that noneof the accounts reporting to them became PEP in the course of the year. In the event that any transaction is noted to be abnormal, such must be immediately flagged and reported to the Compliance unit immediately.

While circumstances will vary, certain transactions by PEPs are considered potentially suspicious and may be indicative of illegal activity. The following guidance provides a non-exhaustive list of red flags that includes, among other things:

- Requests to establish relationships with or route transactions through an institution that is unaccustomed to doing business with foreign persons and that has not sought out businessof that type.
- A request to associate any form of secrecy with a transaction, such as booking the transaction in the name of another person or business entity.
- The routing of a transaction through several jurisdictions without any apparent purpose other than to disguise the nature, source, or ownership of funds.
- The rapid increase or decrease in the funds or asset value in an account that is not attributable to market conditions.
- Frequent or excessive use of funds transfers or wire transfers either into or out of an account.
- Large currency or bearer instrument transactions in or out of an account.
- The frequent minimal balance or zeroing out of an account for purposes other thanmaximizing the value of the funds held in the account.
- Any situation falling into one of the above descriptions shall not automatically be treated as problematic until further investigation is done. If the facts point toa suspicious transaction, then procedures for filing a Suspicious Activity Report shall be followed and Senior Management notified of the situation.

4.8. Designated Non-Financial Businesses and Professions (DNFBPs)

Financial institutions are required, prior to establishing business relationship with designated non- financial businesses and Professions, to obtain evidence of registration (e.g., certificate of registration showing registration number) with the Special Control Unit on Money Laundering (SCUML) of Federal Ministry of Trade and Investments.

DNFBPs refer to dealers in jewelries, precious metals and precious stones, cars and luxury goods, audit firms, tax consultants, clearing and settlement companies, lawyers, notaries, other independent legal practitioners and chartered accountants, trusts and company service providers, hotels, casinos, supermarkets, real estate agents, non-governmental organizations (NGOs), religious and charitable organizations, etc.

The above DNFBPs customers include sole practitioners, partners and employed professionals within professional firms. They do not refer to "internal" professionals that are employees of other types of businesses nor to professionals working for government agencies who may already be subject to AML/CFT measures.

5.0 Audit of AML/CFT

The Internal Audit (IA) shall be responsible for review of GAMCL processes and transactions to ensure that they comply with SEC, NFIU/EFCC requirements on Anti-Money Laundering and Countering Financing of Terrorism. The purpose of the audit is to test the adequacy of the AML/CFT functions and ensure measures are effective. Internal Audit of the AML/CFT is conducted on a quarterly basis.

6.0 Review of Policy

This Policy shall be subject to review from time to time, as business exigencies require, but at least every three (3) years or less depending on changes in the Law and regulatory environment.

7.0 Data Protection

GAMCL has a duly approved Data Protection Policy which is revised on an ad-hoc basis to reflect the legal, regulatory and operating environment. GAMCL adhere strictly to both local and international data protection policies such as the National Data Protection Regulations (NDPR) 2019.

Appendix 1 : FATF Recommendations 2012 *(www.fotf-goti.org}*

A - AML/CFT POLICIES AND COORDINATION

1- Assessing risks & applying a risk-based approach
2- National cooperation and coordination

B - MONEY LAUNDERING AND CONFISCATION

3- Money laundering offence
4- Confiscation and provisional measures

C - TERRORIST FINANCING AND FINANCING OF PROLIF•ERATION

5- SRII Terrorist financing offence
6- SRIII Targeted financial sanctions related to terrorism & terrorist financing
7- Targeted financial sanctions related to proliferation
8- Non-profit organizations

D - PREVENTIVE MEASURES

9- Financial institution secrecy laws

Customer due diligence and *record keeping*

10- Customer due diligence
11- Record keeping

Additional measures for specific *customers and activities*

12- Politically exposed persons
13- Correspondent banking
14- Money or value transfer services
15- New technologies
16- Wire transfers

Reliance. Control5 Old Financial Groups

17- Reliance on third parties
18- Internal controls and foreign branches and subsidiaries
19- Higher-risk countries

Reporting *of suspicious transactions*
20- Reporting of suspicious transactions
21- Tipping-off and confidentiality

Designated non-financial Businesses and Professions (DNFBPs)

22- DNFBPs: Customer due diligence

23- DNFBPs: Other measures

E - TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL

24- Transparency and beneficial ownership of legal persons

25- Transparency and beneficial ownership of legal arrangements

F — POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES

Regulation and Supervision

26- Regulation and supervision of financial institutions

27 - Powers of supervisors

28 - Regulation and supervision of DNFBPs

Operational and *Low Enforcement*

29 - Financial intelligence units

30 - Responsibilities of law enforcement and investigative authorities

31 - Powers of law enforcement and investigative authorities

32 - Cash couriers

General *Requirements*

33 - Statistics

34 - Guidance and feedback

Sanctions

35 — Sanctions

G - INTERNATIONAL COOPERATION

36 - International instruments

37 - Mutual legal assistance

38 - Mutual legal assistance: freezing and confiscation

39 - Extradition

40 - Other forms of international cooperation

Appendix 2: Suspicious Transactions Form (STR)

NOTE: Keep Confidential. Do not alert the client of any suspicion. Ensure immediate reporting to the Chief Compliance Officer.

Confidential

Date

	Telephone No: **Mobile PhoneNo:** **E-mail Address:**
REPORTING OFFICER **Name:** **Position:**	**Tel:** **Branch/Dept:**
CUSTOMER/CLIENT DETAILS AND BACKGROUND	
Customer Name: **Customer Address:**	
ID/Passport No: **Nationality:** **Telephone No:** **E-mail Address:** **Occupation:**	
Employer's Nome: **Employer' Address:** **Employer's Tel No:**	

Type Of Alccounts	Cosh Balance	Stock Portfolio Valuation a	Portfolio Valuation Date	Date Account Opened

BRIEF DESCRIPTION OF CUSTOMER'S RELATIONSHIP WITH GAMCL

NATURE OF TRANSACTION **Reactivated dormant account Regular/unusual off-shore activity Large/unusual cash deposit/withdrawal Large/unusual inwards/outwards remittances Activity inconsistent with customer Other (Specify)**

DETAILS OF TRANSACTION AROUSING SUSPICION

Amount No(S)	Transaction Date	Details of Remitting Financial Institution (Incoming Funds) Destination (Outgoing Funds)

REASON FOR INTERNAL SUSPICION OF ML/FT	
REASONS GIVEN BY CUSTOMER FOR TRANSACTIONS/ON MAKING FURTHER ENQUIRIES	
OTHER RELEVANT INFORMATION	
IMPORTANT: Please attach copies of (1) Account opening form (2) Recent account history (3) Suspicious transaction documents AND (4) Customer identification documents	
REPORTING OFFICER'S SIGNATURE	
MANAGER'S/HEAD OF DEPARTMENT'S SIGNATURE	

Appendix 3: Money Laundering & Terrorist Financing Red Flogs/ Indicators

Potential Transactions Perceived or Identified as Suspicious

- Transactions involving high-risk countries vulnerable to money laundering, subject tothis being confirmed.
- Transactions involving shell companies.
- Transactions with correspondents that have been identified as higher risk.
- Large transaction activity involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered.
- Transaction with correspondents that have been identified as higher risk.
- Transaction activity involving amounts that are just below the stipulated reportingthreshold or enquires that appear to test an institution's own internal monitoring threshold or controls.
- Money laundering using cash transactions.
- Significant increases in cash deposits of an individual or corporate entity without apparent cause. Particularly if such deposits are subsequently transferred within short period out of the account toa destination not normally associated with the customer.
- Unusually large deposits made by individual or a corporate entity whose normalbusiness is transacted by cheques and other non-cash instruments.
- Customers who deposit cash through many deposits slips such that the amount of each
  deposit is relatively small, that overall total is quite significant.
- Customers transferring large sums of money to or from overseas locations withinstructions for payment in cash.

The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business:

- Minimal, vague or fictitious information provided by a customer that cannot be verified.
- Lack of reference or identification in support of an account opening application by a person who is unable or unwilling

to provide the required documentation.

- A prospective customer does not have a local residential or business address and there is no apparent legitimate reason for opening a brokerage account.
- Customers investing large amounts of cash with no apparent business source or in amanner inconsistent with the nature and volume of the business. Likewise, with purchase and sale of large values of shares.
- Customers making and maintaining large investment balance with no apparent rationale.
- Customers who make numerous investments into accounts and soon thereafter request for electronic transfer or cash movement from those accounts to other accounts, perhaps in other countries, leaving only small balances. Typically, these transactions are not consistent with the customer's legitimate business needs.
- Sudden and unexpected increase in account activity or balance arising from increased investment deposit. Typically, such an investment account is opened with a small amount which subsequently increases rapidly and significantly.
- Customer requests for large value sales of shares soon after the purchase, with the customer being willing to suffer loss in share price.
- Substantial increase in purchase of shares.

Persons involved in investment transactions share an address or phone number particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed)

- Financial transaction by a nonprofit or charitable organization, for which there appears to be no logical economic purpose or for which there appears to be nolink between the stated activity of the organization and other parties in the transaction.

- Funds transfer to/from high-risk countries.

Terrorist Financing Red Flogs/Indicators

- Persons involved in currency transactions share an address or phone number, particularlywhen the address is also a business location or does not seem to corresponds to the stated occupation (e.g., student, unemployed, or self-employed).

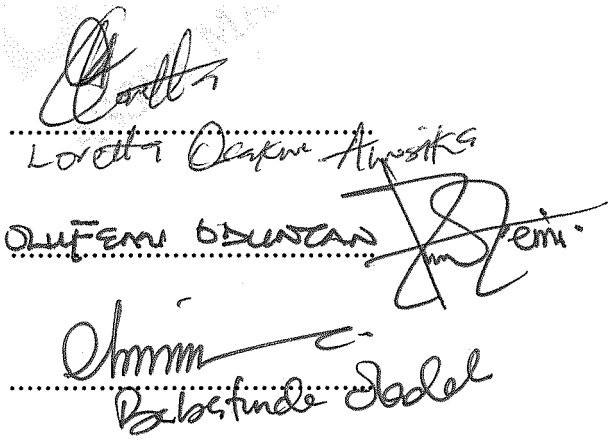
- Financial transaction by a nonprofit or charitable organization, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organization and other parties in the transaction.
- The stated occupation of the customer is inconsistent with the type and level of account activity.
- Funds transfer does not include information on the originator or the person on whose behalf the transaction is conducted the inclusion of which should ordinarily be expected.
- Funds transfer to/ from high-risk countries.

Other Unusual or Suspicious Activities for Employee Monitoring

- Employee exhibits a lavish lifestyle that cannot be justified by his/her salary
- Employee fails to comply with approved operating guidelines
- Employee is reluctant to make vacation.

Approvals:

Compliance Officer:



Chief Executive Officer:

Director:

Date: October 30, 2021