

Greenwich Capital Markets Limited (GCML)

AML/CFT/CPF Policy

Version: 1.0

VERSION CONTROL

Revision of this document is the principal way of implementing and communicating changes that may arise in response to the changing needs and requirements of the Bank overtime. The Compliance Unit shall formally review this document at least every three years.

DOCUMENT HISTORY

Version	Purpose	Date	Reviewers
1.	This Policy was drafted to maintain high standard of Compliance in line with AML, CFT & CPF Regulations.	February 2026	1. Compliance Unit 2. Executive Management Committee 3. Board Risk Management Committee 4. Board of Directors

Approvals

This Policy was reviewed and approved by:

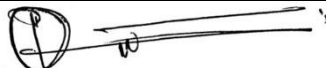
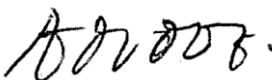
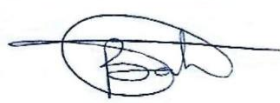
Name	Representing	Signature	Date
Chairman	Board of Directors		February 27, 2026
Chairman	Board Audit & Risk Management Committee		February 27, 2026
Managing Director	Executive Management		February 27, 2026
Compliance Officer	Compliance Department		February 27, 2026

Table of Contents

DOCUMENT HISTORY.....	2
1. INTRODUCTION	4
2. CUSTOMER ACCEPTANCE POLICY	5
3. RISK PROFILING	5
4. CUSTOMER DUE DILIGENCE (CDD)	5
5. RECORD-KEEPING.....	10
6. ONGOING MONITORING	11
7. MANAGEMENT INFORMATION SYSTEM.....	11
8. SPECIAL ATTENTION	11
9. SUSPICIOUS TRANSACTION REPORTING	12
10. REPORTING MECHANISMS	12
11. OTHER ISSUES	13
12. COMBATING THE FINANCING OF TERRORISM.....	13
13. POLICIES, PROCEDURES AND CONTROLS	13
14. STAFF INTEGRITY	14
15. COMPLIANCE OFFICER.....	15
16. STAFF TRAINING AND AWARENESS PROGRAMMES	16
17. INDEPENDENT AUDIT	17
18. APPENDIX: DEFINITION OF TERMS	17

1. INTRODUCTION

Here we present the Anti-money laundering, Counter Terrorism Financing, and Counter Proliferating Financing Policy for GREENWICH CAPITAL MARKETS LIMITED (hereinafter referred to as "GCML" or "the firm").

1.1. Money Laundering

1.1.1. In general terms, money laundering is defined as the process of converting money/property, which is derived from illegal activities to give it a legitimate appearance. There are 3 stages in money laundering, namely:

1.1.1.1. Placement: The physical disposal of proceeds derived from illegal activities;

1.1.1.2. Layering: Separating the illicit proceeds from their sources through transactions that disguise the audit trail and provide anonymity

1.1.1.3. Integration: Integrating the laundered proceeds into the economy as normal funds.

1.1.2. Money laundering has been further defined as the act of a person who: engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity: acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Nigeria proceeds of any unlawful activity; or conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of rights with respect to, or ownership of, proceeds of any unlawful activity; where, as may be inferred from objective factual circumstances, the person knows or has the reason to believe, that the property is proceeds from any unlawful activity; or in respect of the conduct of a natural person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property proceeds from any unlawful activity.

1.2. Financing Of Terrorism

1.2.1. Financing of terrorism generally refers to carrying out transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism.

1.2.2. Essentially, financing of terrorism includes: providing or collecting property for carrying out an act of terrorism; providing services for terrorism purposes; arranging for retention or control of terrorist property; or dealing with terrorist property.

1.2.3. In the financing of terrorism, the focus is on the determination or use of funds, which may have been derived from legitimate sources.

1.3. Proliferation Financing

Proliferation Financing of Weapons of Mass Destruction is the act of providing funds or financial services which are used in whole or in 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 for non-legitimate purposes) in contravention of national laws or, where applicable, international obligations.

1.4. Statutory and Regulatory Requirements for AML/CFT/CPF

1.4.1. The following laws and regulations regulate the AML, CFT & CPF regime in Nigeria:

1.4.1.1. The Securities and Exchange Commission AML/CFT/CPF 2022

1.4.1.2. The Money Laundering (Prevention and Prohibition) Act 2022

1.4.2. By way of adopting and implementing international best practices in AML, CFT & CPF, the Firm shall strive to adopt and implement the requirements of the following standard setters:

1.4.2.1. The Financial Action Task Force (FATF) 40 regulations and other guidelines and

1.4.2.2. standards issued by the body.

1.4.2.3. The Office of Foreign Asset Control (OFAC) sanctions requirements.

1.4.2.4. The United Nations Security Council sanctions requirements.

1.4.2.5. The European Union (EU) sanctions requirements.

1.4.2.6. Her Majesty Treasury (I-IMT) sanctions requirement.

1.4.2.7. Other AML, CFT & CPF laws, regulations, principles, guidelines or standards that the Firm may be required to comply with.

2. CUSTOMER ACCEPTANCE POLICY

2.1. The firm has developed the customer acceptance policy and procedures to address the establishment of business relationship with the customer. For that purpose, the firm identifies and assesses the risks of customers, that is, risk profiling, especially in identifying the type of customers associated with high risk of money laundering, financing of terrorism and proliferation financing.

2.2. Reflective of the risk profiling conducted; the firm has reasonable measures in its internal policies and procedures, including customer due diligence, to address the different risks posed by each type of customer.

3. RISK PROFILING

3.1. In creating the risk profile of a particular customer or type of customer, the firm takes into consideration the following factors;

3.1.1. The origin of the customer and location of business;

3.1.2. Background or profile of the customer;

3.1.3. Nature of the customer's business;

3.1.4. Structure of ownership for a corporate customer; and

3.1.5. Any other information suggesting that the customer is of higher risk.

3.2. Following the initial acceptance of the customer, the firm continuously monitors each customer's transaction activity pattern to ensure it is in line with the customer's profile. Unreasonable differences prompt the firm to reassess the customer's risk profile.

4. CUSTOMER DUE DILIGENCE (CDD)

4.1. The firm's staff is expected to conduct customer due diligence and obtain satisfactory evidence and properly establish the identity and legal existence of any person applying to do business with it. Such evidence must be substantiated by reliable and independent source documents.

4.1.1. The firm must conduct customer due diligence, when:

- 4.1.1.1. establishing business relationship with any customer;
 - 4.1.1.2. carrying out cash or occasional transaction that involves a sum in excess of the amount specified by the regulators
 - 4.1.1.3. it has any suspicion of money laundering or financing of terrorism; or
 - 4.1.1.4. it has any doubt about the veracity or adequacy of previously obtained information.
- 4.1.2. The customer due diligence undertaken by the firm shall at least comprise the following:
- 4.1.2.1. identify and verify the customer;
 - 4.1.2.2. identify and verify beneficial ownership and control of such transaction;
 - 4.1.2.3. obtain information on the purpose and intended nature of the business relationship/transaction; and
 - 4.1.2.4. conduct on-going due diligence and scrutiny, to ensure the information provided is updated and relevant.
- 4.1.3. Unwillingness of the customer to provide the information requested and to cooperate with the firm's customer due diligence process may itself be a factor of suspicion.
- 4.1.4. The firm does not commence business relation or perform any transaction, or in the case of existing business relation, it should terminate such business relation if the customer fails to comply with the customer due diligence requirements and consider lodging a suspicious transaction report with the Economic and Financial Crimes Commission (EFCC) and Nigerian Financial Intelligence Unit (NFIU).
- 4.1.5. In certain special circumstances where the risks of money laundering, financing of terrorism and proliferation financing are low or where measures are already in place to effectively manage such risk, the firm shall, not later than 14 days after the business relationship has been establishment, furnish the relevant documents.
- 4.2. Individual Customers
- 4.2.1. In conducting customer due diligence on an individual customer, the firm obtains from the individual customer at least the following information:
- 4.2.1.1. Full name
 - 4.2.1.2. Drivers license/international passport number/National ID (issued by NIMC) or Permanent Voters card;
 - 4.2.1.3. Permanent and mailing address;
 - 4.2.1.4. Date of birth;
 - 4.2.1.5. BVN and
 - 4.2.1.6. Nationality.
- 4.2.2. The firm substantiates the above required information by requiring the individual to furnish the original and make a copy of the relevant documents.
- 4.2.3. Where there is any doubt, the firm requests the customer to produce other supporting identification documents, preferably bearing a photograph of the customer, issued by an official authority, to enable the customer's identify to be ascertained.
- 4.3. Corporate Customers
- 4.3.1. In conducting customer due diligence on a corporate customer, the firm requires

the company/business to furnish the original and make a copy each of the following documents:

- 4.3.1.1. Memorandum/Article/Certificate of incorporation/Partnership;
- 4.3.1.2. Identification document of Directors/Shareholders/Partners;
- 4.3.1.3. Authorization for any person to represent the company/business; and
- 4.3.1.4. Identification document of the person authorized to represent the company/business in its dealing with the firm.

4.3.2. Where there is any doubt, the firm conducts a basic search or enquiry on the background of such company/business to ensure that it has not been, or is not in the process of being, dissolved or liquidated; and verify the authenticity of the information provided by the company/business with the Corporate Affairs Commission (CAC).

4.3.3. The staff of the firm is expected to know the beneficial owners and controls structure of the corporate customers and determine the source(s) of funds of the company/business in order to ascertain any suspicion concerning the changes to the company/business structure or ownership or the payment profile of its account.

4.3.4. In the event, the firm's corporate customer is a public company which is subjected to regulatory disclosure, it would not be necessary for the firm to identify or verify the identity of any shareholder.

4.4. Clubs, Societies and Charities

In conducting customer due diligence on a club, society or charity, the firm requires the club, society or charity to furnish the relevant constituent documents (or other similar documents) including certificate of registration and the identification of the office bearer and authorization for any person to represent the club, society or charity.

4.5. Legal Arrangements

4.5.1. Legal arrangements can be used to avoid customer due diligence on the beneficiary of such transactions and disguise the source of funds involved. The firm needs to establish whether the customer is acting on behalf of another person as a party to a legal arrangement, for example, a trustee or nominee.

4.5.2. The firm is expected to take reasonable measures to understand the relationship among the relevant parties in handling a trustee or nominee business and obtain satisfactory evidence of its legal status, the identity of the said trustee, settler or nominee, authorized signatories, beneficiaries and the nature of their capacity and duties as trustee or nominee.

4.5.3. It shall be reasonable for the firm to rely on the trustee or nominee to verify or confirm the identity of the beneficial owners. For this purpose, the firm should require a written undertaking from the trustee or nominee that identification documents of the beneficiaries have been obtained, recorded and retained. In addition, such documentation needs to be made available promptly to the firm upon request.

4.6. Beneficial Ownership and Control

- 4.6.1. The firm should conduct customer due diligence on any natural person who ultimately owns or controls the customer's transaction if it suspects a transaction is conducted on behalf of a beneficial owner and not the customer who is conducting such transactions.
- 4.6.2. The customer due diligence conducted should be as stringent as that for individual customer. In the event, the beneficial owner is identified as a politically exposed person (PEP) based on the firm's risk management framework, the requirement under for PEP would apply.
- 4.6.3. When the firm uses the services of intermediaries, such as licensed sub broker, to introduce business it relies on the customer due diligence conducted by such intermediaries. However, the ultimate responsibility for customer's due diligence remains with the firm.
- 4.6.4. In facilitating effective oversight, the relationship between the firm and its intermediaries is governed by an arrangement/agreement that clearly specifies the rights, responsibilities and expectations of all parties. At the minimum, the firm must be satisfied that the intermediary:
 - 4.6.4.1. has an adequate customer due diligence process;
 - 4.6.4.2. has a reliable mechanism to verify customer identity;
 - 4.6.4.3. can provide the customer due diligence information and make copies of the relevant documentation available immediately upon request; and
 - 4.6.4.4. where appropriate, is properly regulated and supervised by the respective authorities.
- 4.6.5. In addition, customer due diligence procedures should be performed, either on the firm's own records or via copy of records obtained from the introducing entity.
- 4.6.6. The firm pays special attention in establishing and conducting business relationship via information communication technology, for example, the internet, post, fax or telephone. The firm believes that any business relationship/transaction that avoids face-to-face contact without proper customer identification and verification may be subject to abuse by money laundering and financiers of terrorism in gaining access to the economic system.
- 4.6.7. The firm should only establish business relationship upon completion of the customer due diligence process conducted through face-to-face interaction.
- 4.6.8. The firm is also required to establish appropriate measures for customer's verification that should be as stringent as that for face-to-face customers and implement monitoring and reporting mechanisms to identify potential money laundering, financing of terrorism and proliferation financing activities. Where there is contract to outsource CDD, the requirement does not apply because the "outsource" or agent is regarded as synonymous with the firm that is, the processes and documentation are those of the firm itself.

4.7. Politically Exposed Persons (PEPS)

- 4.7.1. PEPs individuals being, or who have been, entrusted with prominent public functions, such as heads of state or government, senior politicians, senior government officials, judicial or military officials and senior executives of public organizations.
- 4.7.2. The concern placed in dealing with PEPS lies with the possibility of such PEPs abusing their public powers for their own illicit enrichment, especially in countries where corruption is widespread.
- 4.7.3. Hence, the firm has, in addition to their respective customer due diligence process, a risk management framework to determine whether current or new customers are PEPs. In establishing whether or not the customer is a PEP, the firm should at least gather sufficient and appropriate information from the customer and through publicly available information.
- 4.7.4. Once a PEP is identified, the firm takes reasonable and appropriate measures to establish the source of wealth and funds of such person.
- 4.7.5. The decision to enter into or continue business relationships with PEPs should be made by the Senior Management of the firm at the head office.
- 4.7.6. In addition, the firm should conduct enhanced ongoing due diligence on PEPs throughout its business relationships with such PEPs. For such purpose, the firm should note that business relationships with family members or close associates of PEPs involve similar reputational risks to those with PEPs themselves.

4.8. Higher Risk Customers

- 4.8.1. For higher risk customers, the firm shall conduct enhanced customer due diligence. Enhanced due diligence should include at least:
 - 4.8.1.1. Obtaining more detailed information from the customer and through publicly available information, in particular, on the purpose of transaction and source of funds; and
 - 4.8.1.2. Obtaining approval from the Senior Management of the firm before establishing the business relationship with the customer.
- 4.8.2. Senior Management refers to any person(s) responsible for the management and administration of the firm.
- 4.8.3. Examples of higher customers are:
 - 4.8.3.1. High net worth individuals;
 - 4.8.3.2. Non-resident customers;
 - 4.8.3.3. From locations known for their high rates of crime (for example, drug producing, trafficking, smuggling);
 - 4.8.3.4. Countries or jurisdictions with inadequate AML/CFT/CPF laws and regulations such as the Non-Cooperative Countries and Territories (NCCT)
 - 4.8.3.5. PEPs;
 - 4.8.3.6. Legal arrangements that are complex – (for example, trust,

- nominee);
- 4.8.3.7. Cash based businesses; and
- 4.8.3.8. Unregulated industries.

4.9. Existing Customers

- 4.9.1. The firm should take the necessary measures to ensure that the record of existing customers, including its customer's profile, remains updated and relevant. In addition, further evidence in identifying the existing customers should be obtained to ensure compliance with the firm's current customer due diligence standards.
- 4.9.2. The firm should conduct regular reviews on existing records of customers, especially when;
 - 4.9.2.1. A significant transaction is to take place;
 - 4.9.2.2. There is a material change in the way the account is operated;
 - 4.9.2.3. The customer's documentation standards change substantially; or
 - 4.9.2.4. It discovers that the information held on the customer is insufficient.
- 4.9.3. The firm, based on risk assessment, may require additional information consistent with its current Customer Due Diligence standards from those existing customers that are considered to be of higher risk.

5. RECORD-KEEPING

5.1. Retention Period:

- 5.1.1. The firm should keep all records and documents of transactions, in particular; those obtained during customer due diligence procedures, for at least six years after the transaction has been completed or after the business relations with the customer have ended.
- 5.1.2. In situations where the records are subject to ongoing investigations or prosecution in court, they shall be retained beyond the stipulated retention period until it is confirmed that such records are no longer needed.

5.2. Audit Trail

- 5.2.1. The firm must ensure that the retained documents and records are able to create an audit trail on individual transactions that are traceable by the relevant regulatory, supervisory and law enforcement agencies.
- 5.2.2. In addition, the records kept must enable the firm to establish the history, circumstances and reconstruction of each transaction. The records shall include at least:
 - 5.2.2.1. The identity of the customer;
 - 5.2.2.2. The identity of the beneficiary;
 - 5.2.2.3. The type of transaction (for example, deposit or withdrawal);
 - 5.2.2.4. The form of transaction (for example, by cash or by cheque);
 - 5.2.2.5. The instruction and the origin and destination of fund transfers; and
 - 5.2.2.6. The amount and type of currency.

5.3. Format

- 5.3.1. The firm should retain the relevant document in the form that is acceptable and retrievable, upon request, in a timely manner.

6. ONGOING MONITORING

- 6.1. The firm shall conduct ongoing customer due diligence to examine and clarify the economic background and purpose of any transaction or business relationship that appears unusual, does not have any apparent economic purpose or the legality of such transaction is not clear especially with regards to complex and large transactions or higher risk customers. All findings must be documented and made available to the relevant supervisory authority upon request.
- 6.2. An effective customer due diligence process would enable the firm to detect related money laundering, financing of terrorism and proliferation financing transactions at the point of customer contact (based on the front-line staff's ad hoc report). Generally, most detection would be made through analyzing patterns or activities of the customer.

7. MANAGEMENT INFORMATION SYSTEM

- 7.1. The firm shall have in place an adequate management information system to complement its customer due diligence. The management information system should provide the firm with timely information on a regular basis to enable it to detect any suspicious activity. Such information would include multiple transactions over a certain period, large transactions, anomaly in transactions pattern and transactions exceeding any internally specified threshold.
- 7.2. The management information system should be part of the firm's information system that contains its customer's normal transaction/business profile, which is accurate and updated.

8. SPECIAL ATTENTION

- 8.1. The firm should establish internal criteria ("red flags") to detect suspicious transactions and may be guided by examples of suspicious transactions provided by Central Bank of Nigeria (CBN) or sourced from other corresponding competent authorities as well as international organizations, for example, Bank of International Settlements (BIS), International Association of Insurance Supervisors (IAIS) or International Organisation of Securities Commission (IOSCO). The firm should be prompted to conduct enhanced due diligence if any transaction matched the "red flags" list. Transactions that matched the "red flags" should be subjected to ongoing monitoring.
- 8.2. The firm should also conduct due diligence or monitoring of transactions with regards to business relationships and transactions with individuals, businesses, companies, and financial institutions from countries which have insufficiently implemented the internationally accepted AML/CFT/CPF measures, such as the Non-Cooperative Countries and territories (NCCT). Such business relationships and transactions would require the firm to make further enquiries, as detailed as possible, about their background and purpose and to document the findings in writing. These findings should be made available to the relevant supervisory authority.

9. SUSPICIOUS TRANSACTION REPORTING

- 9.1. The firm is required to promptly submit a suspicious transaction report to the EFCC when any of its employees suspect or have reason to suspect that the transaction or attempted transaction involves proceeds from an unlawful activity, or the customer is involved in money laundering or financing of terrorism. For this purpose, the firm must establish a reporting system for the submission of suspicious transaction reports to the NFIU.

10. REPORTING MECHANISMS

- 10.1. The firm should appoint one officer (or more) at the Senior Management level to be the Compliance officer responsible for the submission of suspicious transaction reports to the NFIU.
- 10.2. In addition, the firm should appoint at each branch a Compliance officer. The branch Compliance officer is responsible, amongst others, for channeling all internal suspicious transaction reports received from the employees of the respective branch to the Chief Compliance Officer at the head office. For employees at the head office, such internal suspicious transaction reports would be channeled directly to the Compliance officer.
- 10.3. Upon receiving any internal suspicious transaction report, whether from the head office, branch or subsidiary, the compliance officer should evaluate the grounds for suspicion, and if suspicion is confirmed, promptly submit the suspicious transaction report to the EFCC and NFIU. In the case where the compliance officer decides that there are no reasonable grounds for suspicion, he should document his decision, ensure it is supported by the relevant documents and file the report.
- 10.4. The compliance officer should submit to the Financial Intelligence Unit all the suspicious transactions report in the specified suspicious transaction report form.
- 10.5. Where applicable and upon the advice of the Financial Intelligence Unit, the compliance officer of the firm should submit its suspicious transaction reports on-line.
- 10.6. The compliance officer should ensure that the suspicious transaction report is submitted within the next working day, from the date the compliance officer establishes the suspicion.
- 10.7. In the course of submitting the suspicion transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. Hence, the compliance officer must be given the independence to report suspicious transactions without the need to go through any elaborate approval process.
- 10.8. The firm's compliance officer is authorized to cooperate with the NFIU/EFCC in providing such additional information and documentation as it may request and to respond promptly to any further enquiries with regards to any suspicious transaction report.
- 10.9. The firm should ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preservation of secrecy.
- 10.10. The firm shall consider submitting a suspicious transaction report when it is unable to complete the customer due diligence process on any new or existence customer that is

unreasonably evasive or uncooperative. The firm would base such a decision on normal commercial criteria and its internal policy.

- 10.11. The firm should also consider submitting a suspicious transaction report when any of its customer's transaction or attempted transaction fits the firm's list of "red flags".

11. OTHER ISSUES

- 11.1. The firm must ensure that the compliance officer maintains a complete file on all internally generated suspicious transaction reports and any supporting documentary evidence regardless that such reports have been submitted to the EFCC.
- 11.2. The firm must undertake reasonable measures to ensure that all its employees involved in conducting or facilitating the customer's transaction are aware of these reporting procedures and that failure to report suspicious transaction when they have reasonable grounds to believe that the transaction is "suspicious" is an offence.

12. COMBATING THE FINANCING OF TERRORISM

- 12.1. The firm should ensure that the existing suspicious transaction reporting system and mechanism for the identification of suspicious transactions are extended to cover financing of terrorism.
- 12.2. In ensuring efficient detection of suspected financing of terrorism, the firm should maintain a database of names and particulars of terrorist in the UN Consolidated List and such orders as may be issued by the National Security Adviser (NSA). In addition, the firm should consolidate its database with the other recognized lists of designated person/entities.
- 12.3. The firm shall ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary for the purpose of identifying suspicious transactions.
- 12.4. The firm shall conduct regular checks on the names of new and existing customers against the names in the database, the firm shall immediately:
- 12.4.1. Inform the EFCC
 - 12.4.2. Reject the customer if the transaction has not commenced; and
 - 12.4.3. Freeze the customer's transaction if it is an ongoing customer.
- 12.5. Where the firm suspects that a transaction is terrorist-related, it should make a suspicious transaction report to the relevant authority(ies).

13. POLICIES, PROCEDURES AND CONTROLS

- 13.1. The firm's Board of Directors and Senior Management should be aware of the money laundering, financing of terrorism and proliferation financing risks associated with all its business products and services and understand the AML/CFT/CPF measures required by law, regulations, guidelines and the industries standards are the best practices as well as the importance of implementing AML/CFT/CPF measures to prevent it from being abused by money launderers and financial terrorist. It is the duty of the Board of Directors to maintain adequate oversight of the overall AML/CFT/CPF measures undertaken by the firm

and the duty of the Senior Management to ensure that the Board of Directors is updated with timely information.

- 13.2. The Board of Directors should be fully committed in establishing an effective internal control are in place and implemented effectively, including the mechanism to monitor and detect complex and unusual transaction.
- 13.3. The Board of Directors should be fully committed in establishing an effective internal control system for AML/CFT/CPF. It is the responsibility of the Senior Management to ensure such internal controls are in place and implemented effectively, including the mechanism to monitor and detect complex and unusual transactions.
- 13.4. The Board of Directors shall ensure that the firm has, at the minimum, policies on AML/CFT/CPF procedures and controls. For this purpose, the Senior Management will assist the firm in formulating the policies and ensure that the policies are in line with the risks associated, nature of business, complexity and the volume of the transactions undertaken by the firm.
- 13.5. The Board of Directors shall set minimum standards and approve the policies regarding AML/CFT/CPF measures within the firm, including those required for customer acceptance suspicious transactions and combating the financing of terrorism. The Senior Management in relation to this must ensure that such procedures are formulated and effectively implemented. For this purpose, the Board of Directors shall assess the implementation of the approved AML/CFT/CPF policies through regular updates by the Senior Management and audits.
- 13.6. To ensure effective implementation, the Board of Directors should define the lines of authority and responsibilities for implementing the AML/CFT/CPF measures and ensuring that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls. In line with this, the Board of Directors should ensure the:
 - 13.6.1. Compliance Officer at the Head Office is appointed; and
 - 13.6.2. Effectiveness of internal audit in assessing and evaluating the controls to prevent money laundering and the financing of terrorism.
- 13.7. The Board of Directors shall review and assess the AML/CFT/CPF policies and procedures in line with changes and developments in the firm's products and service, technology as well as trends in money laundering and the financing of terrorism. The Senior Management is responsible for implementing the necessary changes to the AML/CFT/CPF policies and procedures with the approval of the Board of Directors to ensure that the current policies are sound and appropriate.
- 13.8. The Board of Directors and the Senior Management should ensure that there is adequate AML/CFT/CPF training provided for the firm's employees, including promoting employees' awareness of their AML/CFT/CPF obligations.

14. STAFF INTEGRITY

- 14.1. The Senior Management must ensure the integrity of the firm's employees at all times by establishing an appropriate employee assessment system (commensurate with the size of

operations and risk exposure of the firm to money laundering, financing of terrorism and proliferation financing), that is approved by the Board of Directors to adequately screen its employees.

- 14.2. The employee assessment system shall include evaluation of an employee's personal information, including criminal records, employment and financial history as part of the recruitment process.

15. COMPLIANCE OFFICER

- 15.1. The firm's Senior Management is responsible for appointing the Compliance officer at Senior Management level who is "fit and proper" to carry out his AML/CFT/CPF responsibilities and can effectively discharge it. In general, the compliance officer acts as the reference point for the AML/CFT/CPF matters, including employee training and reporting of suspicious transactions.
- 15.2. The firm should inform, in writing, the supervisory regulatory bodies i.e. SEC on the appointment or change in the appointment of the compliance officer, including details as his name, designation, office address, office telephone number, e-mail address and such information as may be required.
- 15.3. The firm shall ensure that the role and responsibilities of the compliance officer are clearly defined and documented. The compliance officer should ensure the following.
 - 15.3.1. The firm's compliance with the AML/CFT/CPF requirements;
 - 15.3.2. Implementation of the AML/CFT/CPF procedures, including customer acceptance policy, customer due diligence, record-keeping, ongoing monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
 - 15.3.3. The AML/CFT/CPF mechanism is regularly assessed to ensure that it effective and sufficient to address any change in money laundering and financing terrorism trends;
 - 15.3.4. The channel of communication from the respective employees to the compliance officer is secured and that information is kept confidential;
 - 15.3.5. All employees are aware of the firms AML/CFT/CPF measures, including policies control mechanism and the channel of reporting;
 - 15.3.6. Internally generated suspicious transaction reports by the compliance officers are appropriately evaluated before submission to the EFCC; and
 - 15.3.7. The identification of money laundering and financing terrorism risks associated with new products or services or arising from the firm's operational changes, including the introduction of new technology and processes.
 - 15.3.8. It is important and imperative that the compliance officer appointed by the firm has the necessary knowledge, experience and required authority to effectively discharge his responsibilities, including knowledge on AML/CFT/CPF obligations

required under the relevant laws and regulations, the latest developments in money laundering and financial terrorism techniques, the AML/CFT/CPF measures undertaken by the industry and timely access to customer due diligence documentation and other relevant information.

16. STAFF TRAINING AND AWARENESS PROGRAMMES

- 16.1. The firm must conduct awareness and training programs on AML/CFT/CPF practices and measures for its employees, in particular, 'front-line' staff and officers in charge of processing and accepting new customers as well as staff responsible to monitor transactions.
- 16.2. The Senior Management must ensure that a proper channel of communication is in place to effectively communicate to all levels of employees, the AML/CFT/CPF policies and procedures. The employees should be aware that they may be held personally liable for any failure to observe the internal AML/CFT/CPF requirements. In this regard, the firm should make available its AML/CFT/CPF measures should at least contain the following:
 - 16.2.1. The relevant guidelines on AML/CFT/CPF; and
 - 16.2.2. The firm's internal AML/CFT/CPF policies and procedures.
- 16.3. The training conducted for employees shall be appropriate to their level of responsibility in detecting money laundering, financing of terrorism and proliferation financing faced by the firm. The firm shall at least adapt its training needs to the following levels of employees:
- 16.4. New Employees: provide a general background on money laundering and financial terrorism, the requirement and obligation to monitor and report suspicious transactions to the compliance officer and the importance of the "Know Your Customer" policy.
- 16.5. "Front-Line" Employees: Employees who deal directly with the customers are the first point of contact with potential money launderers and financiers of terrorism. Hence they must be trained to conduct effective ongoing customer due diligence, detects suspicious transaction and the measures that need to be taken upon determining a transaction as suspicious. Training should also be provided on factors that may give rise to suspicion. Training should also be provided on factors that may give rise to suspicion, such as dealing with non-regular customers transacting in large, PEPs, higher risk customers and the circumstances where enhanced customer due diligence is required.
- 16.6. Employees Establishing Business Relationship (Marketing Personnel);
- 16.7. Employees who are responsible for acceptance of new customers, must receive the adequate training given to "front-line" employees. The training should be focused on customer identification, verification and customer due diligence procedures, including when to conduct enhanced due diligence, including with new customers until customer due diligence procedures, including when to conduct enhanced due diligence, including circumstances where there is a need to defer establishing business relationship with new customers until customer due diligence is completed and obligations to report suspicious transaction to the EFCC.
- 16.8. Supervisors and Managers: include a higher level of instructions covering all aspects of AML/CFT/CPF procedures, in particular, the risk-based approach to customer acceptance,

customer due diligence and risk profiling of customers. The other areas include the penalties for non-compliance to the AML/CFT/CPF requirements, procedures in addressing the financing of terrorism issues such as the Consolidated List, list of terrorist under the AMLA, internal suspicious transaction reporting procedures and the requirement for customer due diligence and recordkeeping.

- 16.9. These training and awareness programmes should be conducted regularly and supplemented with refresher courses for employees, with special emphasis for those employees who are exposed to higher risk of potential money laundering, financing of terrorism and proliferation financing activities, for example, the 'front-line' employees. These programs shall update staff on the latest AML/CFT/CPF developments such as products or transaction modes, which are susceptible to the risk of money laundering, financing of terrorism and proliferation financing and remind them of their responsibilities under the AML/CFT/CPF program.

17. INDEPENDENT AUDIT

- 17.1. The Board of Directors is responsible for ensuring regular independent audit of the internal AML/CFT/CPF measures to determine their effectiveness and compliance with the law and other regulatory requirements.
- 17.2. The Board of Directors shall ensure that the roles and responsibilities of the auditors are clearly defined and documented. The roles and responsibilities of the auditors shall at least include:
- 17.3. Checking and testing the compliance, and effectiveness of, the AML/CFT/CPF policies, procedures and controls; and
- 17.4. Assessing whether current measures are in line with the latest development and changes of the relevant AML/CFT/CPF requirements.
- 17.5. The auditor must submit a written report on the audit findings to the Board of Directors, which should be used to highlight inadequacies of any internal AML/CFT/CPF measures and controls and the Board of Directors should ensure that necessary steps are taken to rectify the inadequacies, if any.

18. APPENDIX: DEFINITION OF TERMS

Beneficial Owner

refers to any natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

For companies – the person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted includes the natural person with a controlling interest and the natural persons who comprise the mind and

	management of company.
Constituent document	in relation to a firm, means the statute, charter, memorandum of association and articles of association, rules and by-laws, partnership agreement, or other instrument, under, or by, which the firm is established and its governing and administrative structures and the scope of its functions and business are set out, whether contained in one or more documents.
Intermediaries	generally refer to third parties, namely persons or businesses who are relied upon by the firm to conduct the customer due diligence process.
Person	includes a body of person, corporate or unincorporated.
Property Means:	a.) Assets of every kind, whether corporate or incorporated, moveable or immovable, tangible or intangible, however acquired; or b.) Legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in such assets, including bank credits, traveler's cheques, money orders, shares, securities, bonds drafts and letters of credit.
Territory Property	means: a.) Proceeds from the commission of a terrorist act; b.) Property that has been, is being, or is likely to be used to commit a terrorist act; c.) Property that has been, is being, or is likely to be used by a terrorist, terrorist entity or terrorist group; d.) Property owned or controlled by or on behalf of a terrorist, terrorist entity or terrorist group, including funds derived or generated from such property; or e.) Property that has been collected for the purpose of providing support to a terrorist, terrorist entity or terrorist group or funding a

terrorist act.

Terrorist act:

an act or threat of action within or beyond
Nigeria that:

a.) Involves serious bodily injury to a person;

b.) Involves serious damage to property;

c.) Endangers a person's life;

d.) Creates a serious risk to the health or the
safety of the public or a section of the public;

e.) involves the use of firearms, explosives or
other lethal devices;

f.) Involves releasing the public or any part of
the public to any dangerous, hazardous,
radioactive or harmful substance; Any toxic
chemical; or Any microbial or other biological
agent or toxin;

g.) is designed or intended to disrupt or
seriously interfere with, any computer system
or the provision of any services directly related
to communications infrastructure, banking or
financial services, utilities, transportation or
other essential infrastructure;

h.) Is designed or intended to disrupt, or
seriously interfere with, the provision of
essential emergency services such as police,
civil defense or medical services;

i.) Involves prejudice to national security or
public safety; or

j.) involves any combination of any of the acts
specified in paragraphs (a) to (i), where the act
or threat is intended or may reasonably be
regarded as being intended to;

(aa) intimidate the public or a section of the
public; or

(bb) influence or compel the Government of
Nigeria or the Government of any State in
Nigeria, any other government, or any
international organization to do or refrain from

doing any act, and includes any act or omission constituting an offence under the Aviation Offences Act.