Policy and Procedure Manual for the Prevention of Money Laundering and Terrorism Financing

June 2019

Table of Contents

1. Introduction

TY Danjuma Foundation (TYDF) is an independent grant making organisation established in 2009 and dedicated to contributing to improving the quality of life of Nigerians, notably in the area of health and education. The Foundation was established by General Theophilus Yakubu Danjuma GCON (RTD) to advance his firm belief in and commitment to philanthropy. The Foundation has its headquarters in Abuja with field offices in Jalingo, Taraba State and Benin City, Edo State. However, the work of the Foundation spread across Nigeria.

The Board of Trustees and management of T.Y Danjuma Foundation acknowledge good corporate citizenship as a means of creating enduring corporate value by upholding strict ethical standards, which meet the expectations of stakeholders, constituted authorities and the society at large. Consequently, the Board considers the organisation as a veritable partner with relevant authorities as the first line of defense against exploitation of its resources, brand, and goodwill and those of its grantees and beneficiaries, as a conduit for money laundering and financing of terrorism. The Board's commitment to this noble cause is reaffirmed in this manual which provides guidance for compliance with the Anti-Money Laundering and Counter Financing of Terrorism regime in Nigeria, as set out in the Money Laundering Prohibition Act, 2011 (as amended) and the Special Control Unit against Money Laundering (SCUML), 2013.

Compliance with the contents of this manual is mandatory for all employees of T.Y Danjuma Foundation; therefore, its effective application requires that staff and senior management be familiar with its contents and the laws and regulations under which they were written. The Foundation will provide all employees with a copy of the manual to serve as operational guide in protecting the Foundation against fraud, reputational and other forms of risks.

Vision

A Nigeria where all people have access to affordable quality health care, education, and opportunities to realize their potential.

Mission

The TY Danjuma Foundation is committed to enhancing the quality of life of Nigerian by supporting initiatives that improve access to health and educational opportunities.

Values

The Foundation will operate with the following core values:

- Proudly Nigerian
- Integrity and accountability
- Responsiveness and sensibility
- Learning and innovation
- Community involvement
- Government engagement

2.0 Definition of Terms

2.0.1 Money Laundering

The offence of money laundering is described as concealment; disguise of origin; converting or transferring; remove from jurisdiction or acquire, use, or take possession or control of any fund or property, knowingly or when one reasonably ought to have known that such funds or property is, or form part of the proceed of an unlawful act.

2.0.2 Terrorist Financing

Terrorism Financing occurs when one knowingly, in any manner, directly or indirectly, solicits, acquires, provides, collects, receives, possesses or makes available funds, property or other services by any means to terrorists, or terrorist groups, or possesses funds intending that it be used or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act by terrorists or terrorist groups.

2.0.3 Special Control Unit against Money Laundering

The Special Control Unit against Money Laundering is a specialized unit of the Federal Ministry of Industry, Trade and Investment, which is operationally domiciled within the Economic and Financial Crime Commission. Its acronyms is SCUML (pronounced as "school mule").

2.0.4 Nigerian Financial Intelligence Unit (NFIU)

Nigerian Financial intelligence Unit is an operationally independent unit of the Economic and Financial Crime Commission, which serves as the National repository of financial information in Nigeria. Basically, the unit provides support to investigation on request from law enforcement agencies.

2.0.5 Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is an inter-governmental body established to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. Nigeria is a member of FATF and FATF monitors the progress of its member in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measure globally. In collaboration with other international stakeholders, the FATF works to identify national- level vulnerabilities with the aim of protecting the international financial system from misuse.

2.0.6 Predicate Offences to Money Laundering

A predicate offence is an action that provides the underlying resources for another criminal act. Predicate offences to money laundering are such offences from which the illicit proceeds that are laundered are derived. In Nigeria, predicate offences to money laundering include all unlawful acts and terrorism financing activities.

2.0.7 Politically Exposed Persons (PEP) or Public Officers

Politically Exposed Persons or Public Officers means individuals who are or have been entrusted with prominent public function, both within and outside Nigeria and those associated with them. This classification includes all public office holders, Head of Ministries, Department and Agencies, Nigerian and Foreign Diplomats etc.

2.0.8 Beneficial Ownership

Beneficial owner refers to natural persons who ultimately own or control resources such as a grantee 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.

2.0.8 Legal Arrangements

Refers to express trust or similar legal arrangements.

2.0.9 Legal Person(s)

Legal person(s) refers to Businesses, Organizations, Foundations, Partnerships or Association, or any similar bodies that is incorporated under the Companies and Allied Matters Act, 2004 or under similar legislation in other countries and as such are capable of establishing a long-term or short-term financial relationship with T.Y Danjuma Foundation or otherwise own property.

2.0.10 Know Your Employee (KYE)

The Foundation has adopted Anti-money Laundering policies and procedures for acquiring a better knowledge and understanding of the employees of the Foundation for the purpose of detecting conflicts of interests, money laundering, past criminal activity and suspicious activity. KYE is a key tool in detecting suspicious activity because employees may be accomplices of money launderers.

2.0.11 Cross Border Transaction

This involves any wire transfer by TY Danjuma Foundation in which the originator and beneficiary institutions are located in different jurisdictions. A cross-border transfer also refers to any chain of wire transfers involving TY Danjuma Foundation that has at least one cross-border element.

2.0.12 Grantees' Confidentiality

Grantees' Confidentiality means keeping certain facts, data and information relating to the grantees out of public or unauthorized view. The Money Laundering (Prohibition) Act 2011 (as amended) prohibits failure to disclose information requested within the scope of the law on the ground of confidentiality. Consequently, all confidential information relating to grantees must be released to competent authorities upon request within the scope of the Money Laundering (Prohibition) Act 2011.

3.0 Anti-Money Laundering and Terrorist Financing Risk Management Policy

T.Y Danjuma Foundation shall apply the following processes in managing the risk of exposure to money laundering and terrorist financing:

3.0.1 Risk Identification

Every transactions receipt of income, disbursement of grants to grantees or payment to service providers shall be assessed to identify any associated elements of money laundering or terrorism financing risk. This process shall asses the line of implementation, legal status, ownership structure and geographic location.

3.0.2 Risk Measurement

Having identified the risk in the transaction, the Foundation will assess the likely impact of the risk based on the following:

- Amount involved or likely to be involved in the transaction;
- Number of years of relationship with the grantee or service provider; and
- Availability of reliable third party guarantee.

3.0.3 Risk Monitoring

Throughout grant implementation, in the case of a grantee, service delivery, in the case of service providers, the profile of the grantee, partner or service provider will be reviewed to ensure that they are into legitimate activities.

3.0.4 Risk Control

This process involves verifying the status of grantees or service providers to ensure that funds are used as agreed with the Foundation. It also involves conducting enhanced due diligence or requesting for third party assurances or guarantees. Where there is a breach of the anti-money laundering and terrorism financing manual the Foundation shall discontinue funding and report the situation to the appropriate authorities.

3.1 Risk-Based Approach (RBA)

This involves the assessment of the varying risks associated with awarding grants and engagement of service providers or employee in order to maximize the effectiveness of an anti-money laundering policy. Taking a grant disbursement or payment of service providers through these four processes will inform the Anti-Money Laundering Compliance Officer to classify the risk involved and actions to be taken as follows:

Table 1 Risk Level and Recommended Actions

Level of Risk	**Action**
Extreme Risk Transaction	• Refusal
High Risk Transaction	• Obtain Board or Management approval, Do not conduct until the risk is reduced
Medium Risk Transaction	• • Conduct Enhanced Due Diligence, Demand for reliable third party assurances or guarantee
Low Risk Transaction	• Conduct standard verification and control procedures

4.0 Obligations under the Money Laundering Prohibition Act, 2011 (as amended)

4. 0.1 Limitation to Make or Accept Cash Payments

Subject to Section 1 of the Money Laundering Prohibition Act, 2011 (as amended), the Foundation will ensure that all cash transactions above the sum of Five Million Naira (N5,000,000) or its **equivalent and Ten Million (10,000,000) or its equivalent for individuals and corporate bodies respectively**, shall be made, received or accepted through a designated bank or banks.

4.0.2 Partners Due Diligence (PDD)

The term due diligence describes a general duty to exercise care in any transaction. As such, it entails investigation into all relevant aspects of the past, present, and predictable future of our partners (grantees, consultants and other service providers). Partners Due Diligence means:

1. Identifying partners (grantees, consultants and other service providers) on the basis of documents, data or information obtained from a reliable and independent source;
2. Identifying, where applicable, the beneficial owner and taking risk- based and adequate measures to understand the ownership and control structure of the partner (grantees,

consultants and other service providers);

3. Obtaining information on the purpose and intended nature of the transaction;
4. Conducting ongoing monitoring of the activities of the partners (grantees, consultants, and other service providers) which is not limited to ensure the activities being carried out by the partners are consistent with the operation of the Foundation. The Foundation will also ensure that the risk profile which includes the source of funds, profile, data or information held about them is updated where necessary.

4.1 Who is a Partner

A partnership is an arrangement where parties, known as partners agree to cooperate to advance their mutual interest. The partners in a partnership may be individuals, businesses, interest-based organizations, schools, governments or combinations. Grantees, consultants and other service providers are regarded as partners to the Foundation.

4.1.1 Types of Partners

4.1.2 Habitual/Frequent or Regular Partners: Partners with existing and ongoing relationship with the Foundation

4.1.3 Causal Partners: Partners (grantees, consultants and other service providers) with relationships established between six months to one year and the transactions are expected to be completed within the same period or less.

4.1.4 Walk-In / One-Off Partners: Partners (grantees, consultants and other service providers) who transacts for once and the first time. The relationship is not assumed to be on a continuous basis.

4.1.5 Anonymous and Fictitious Partner: means any person whether natural or legal seeking to establish a relationship with the Foundation but whose identity and legal status cannot be ascertained. A person can also deemed to be anonymous or fictitious where the person or persons that exercise control or ultimately benefit or own the outcome of the transaction cannot be verified.

4.2 Requirements for conducting Partners Due Diligence

Section 5(b) of the Money Laundering (Prohibition) Act 2011 (as amended) stipulates that prior to any transaction involving a sum exceeding $1,000 or its equivalent in any currency, the Foundation shall identify the Partner (grantees, consultants and other service providers) by requiring him/her to fill a standard data form and present his international passport, driver's license, national identity card or such other document bearing his photograph as may be prescribed by the ministry.

For emphasis valid means of customer's identification include:

4.2.1 For Individuals

1. International passport
2. Driver license
3. National ID
4. Permanent Voters registration Card or any such documents that may be prescribe by the honorable minister in charge of commerce.

4.2.2 For Corporate bodies

All documents relating to their incorporation either within or outside Nigeria, or both as the case may apply. Section 3(a)(b)&(c) of the Money Laundering (Prohibition) Act (as amended) 2011 and

section 10(2a &b) of SCUML regulation requires the Foundation to identify and verify potential and existing partners identity using reliable and independent source documents, data and information before engaging them to carry out any activity.

4.3 When to Conduct Partners Due Diligence

4.3.1 Before the initiation of a business relationship

At the initiation of business, the Foundation shall consider the following in assessing the risk involved in the business transaction and consequently inform the level of Know Your Partner (KYP) to be conducted:

1. What type of services or project is the prospective partner seeking to deliver?
2. What is the value of the grant or service?
3. Is the person initiating the transaction or proposal acting for himself or on behalf of another person(s)? In this respect, TYDF must be mindful of professionals and professional firms such as lawyers and law firms, accountants and accounting firms, trust and company service providers, etc., who may be acting on behalf of their client under a client –professional confidential arrangement.
4. Who is/are the beneficiary (ies) of the project or transaction?
5. Is the identity of the prospective grantee or beneficiaries of the project obtainable and verifiable?
6. Is the project location or transaction face to face or remote-such as hard-to- reach terrain, volatile area.
7. Does the transaction fit the regular or normal activity of the Foundation?
8. What will be the mode of payment?

Note: the Foundation is obliged to make report of suspicious transactions if there are reasonable grounds to suppose an impending illegality at the time of initiating the transaction and also undertake the required steps, where possible subject to section 6(2) of the Money Laundering (Prohibition) Act 2011 as amended.

4.3.2 During the Period of the Implementation of Grants or Rendering of Service (On-Going Due Diligence)

The Foundation shall continually review and demand for complementary information during the implementation of project by grantees or rendering of service by service providers. There shall be an on-going review of partners' profile and transaction patterns to ensure consistency. Additional information may be required as the transaction pattern or partner's profile changes.

Where the partners (grantee, consultant or other service provider) is changing his activities, service, location, engaging an intermediary, changing mode of transaction, currency of transaction etc., additional due diligence shall be conducted.

4.4 Procedures for Conducting Partners Due Diligence (PDD)

PDD must be conducted on a continuous basis. In addition to obtaining valid means of identity, staff conducting PDD should know that:

1. Conducting PDD is mandatory;
2. Some level of confidentiality should be applied to information collected on partner during and after the conduct of PDD. Such information should be treated on a "need to know" basis. Every transaction has its inherent risk, every transaction should have its PDD priorities. Staff should have recourse to their experience and knowledge of the industry and the peculiarities of the transaction or project to guide PDD priorities specific to each transaction or project;

3. If the staff has good reason to suspect the transaction or the proposal is for money laundering or terror financing, efforts should be made to enhance the due diligence by requiring for additional information, preferably documented evidences;
4. Other relevant information which may not documentary may be obtained for enhanced assurance;
5. PDD should also be conducted on agents, representatives and other relevant parties in the project implementation;
6. For Politically Exposed Persons, the Foundation should conduct PDD that targets separation of official transactions from personal transactions. Authorization and approvals should be verified that it is commensurate with the nature, volume, location and geographical scope, currency type etc of the activity or transaction;
7. All PDD information obtained should be filed in a chronological order; and
8. File should be open for each grantee to enable continuous update of PDD information and preservation of records.

4.5 Risk Based Approached to Conducting PDD

Risk means the likelihood or chances that:

1. The grant is intended as a channel to finance terrorism;
2. The grant is intended to be used to offer support to commission of an act of terrorism;
3. The grantee founder of the organization is listed as wanted for terrorism, a proscribed person, member of a terrorist organization or such similar person(s) or described in the Terrorist Prevention Act 2011.
4. The grantee is linked with criminal activities and predicate offences to money laundering.
5. The organization's ownership is in complexity or arrangements in which the identity of the ultimate beneficiary of the transaction and other relevant parties in the implementation cannot reasonably be ascertained by any means possible
6. The grant facility would be used for a criminal act or support part of on-going criminal activity(s)
7. The grant disbursement is not processed through the bank.

Staff should be aware that determinants of riskiness of a transaction are not limited to the above mentioned scenarios.

Conducting PDD on a risk based approach demands that every transaction and customer is assessed in light of the following:

- **Materiality** – Conducting PDD on a risk based approach requires that consideration be given to the financial significance of grant amount or contract sum in terms of size, frequency and currency type, vis-à-vis what would be its consequence for money laundering or terrorist financing. For example lower level of PDD may be conducted for beneficiaries of a capacity building training, vendors supplying basic office stationeries of low transaction volume etc. ***Staff should be aware that although individual transactions related to a particular partner may not be material in amount, however, situation may demand that these transactions are aggregated to determine if an enhanced PDD should be conducted, especially for an existing grantee, consultant or service provider.***

- **Fundamentality-** Fundamentality suggests that an immaterial amount may still warrant enhanced PDD even, if the circumstances surrounding the transaction or additional information obtained from the customer give good reason not to suggest that the grant proposal or contract is suspicious, i.e, will facilitate a crime, is part of an on-going

criminal activity or most importantly, will facilitate commission of an act of terrorism. In conducting a risk based PDD, the compliance officer should endeavor to balance materiality of the amount involved in the transaction with its fundamentality as the circumstance suggests.

In consideration of fundamentality of a transaction, staff should exercise sound professional judgment and act reasonably in the circumstance.

- **Substance Over Form** – Staff should give priority to the overall financial reality of the transaction (its economic substance) rather than its legal form. Notably, Staff should be particular about who will be in control of the funds and who the ultimate beneficiary of the transaction would be.

4.6 Types of Partners Due Diligence

The adoption of a risk based approach will actually determine what level of PDD to be conducted in the transaction. Basically PDD is classified into;

4.5.1 Simplified Due Diligence

Simplified due diligence is the lowest level of due diligence that can be completed on a grantee or service provider. This basically suggests that;

- the minimum means of identity verification is obtained;
- a reliable third party provides assurance;
- The Foundation is providing assurance.

The Foundation shall not go below fulfilling at least two of the above mentioned conditions when applying Simplified Due Diligence to transactions.

This is appropriate where there is little opportunity or risk of your service providers or grantee becoming involved in money laundering or terrorist financing. However, if at any point during the execution with your grantee or service provided additional intelligence becomes available which suggests that the grantee or service provider may pose a higher risk than originally thought, an enhanced level of due diligence should be conducted.

4.5.2 Standard Due diligence

Standard due diligence requires you to identify the grantees and service providers as well as verify their identity. In addition, there is a requirement to gather information to enable you to understand the nature of their activities. This due diligence should provide you with confidence that you know who your grantee or service provider is and that your fund is not being used as a tool to launder money support to terrorist groups or any other criminal activity.

Standard Due Diligence should be conducted in situations where there are potential risks but a low likelihood that the risks will be realized.

4.5.3 Enhanced Due Diligence (EDD)

This goes beyond obtaining the minimum means of identification to acquiring *additional* ***DOCUMENTARY*** *evidences* to provide assurance on the various components of a grant, the beneficiaries, agent/representatives and other relevant parties in a transaction. Enhance Due Diligence suggests that;

- Approvals and Authorizations are obtained and verified to commensurate the volume, location and powers of the parties involve;

- Additional assurances are provided by reliable and regulated third parties like banks, embassies, agency of foreign and domestic government etc.,
- Additional documentary evidences such as board resolutions, minutes of meetings, approvals etc., are obtained, and
- Additional examination and cautionary measures aimed at identifying customers and confirming that their activities and funds are legitimate.

EDD should be conducted when transacting with the following classes of people:

- **Politically Exposed Persons (PEPs)**
  Bearing in mind the definition of Politically Exposed Persons in section 4.9 of this manual, Politically Exposed Persons acting in their official capacity should be required to provide documentary authorization to do so.

- **Non-Residents**
  Nonresident customers should be required to present their international passport only as a means of identification.

- **Unincorporated Non-Governmental Organizations**
  At least five individuals who are responsible for promoting and managing the NGO should be identified with valid official documents and third party referrals such as banks, employers etc., should be obtained.

- **Cash Based Transaction Reporting (CBTR)**
  The Foundation should ensure that all **cash inflow** above **One Thousand Dollars ($1,000)** or its equivalent in other currencies must be reported in the prescribed format to the Special Control Unit against Money Laundering within seven (7) days of completion of such transaction. Such transaction will be recorded in a chronological order.

5.0 Suspicious Transaction Reporting (STR)

5.0.1 Definition of Suspicious Transaction

The Money Laundering Prohibition Act, 2011 as (amended) describes suspicious transaction as such transaction that;

1. involves an unjustifiable or unreasonable frequency;
2. is surrounded by conditions of unusual or unjustified complexity;
3. appears to have no economic justification or lawful objective;
4. in the opinion of the Foundation, involves terrorist financing or is inconsistent with the known transaction or activities of the grantee, consultant or service provider.

5.0.2 Anti-Money Laundering/Countering Financing of Terrorism Red Flags

1. Using corporate vehicles or legal arrangement to hide the beneficial owner(s) of the construction project.
2. The ownership structure of the grantee appears unusual or excessively complex given the nature of the business
3. Customers associated with known criminal entities or terrorist group.
4. Non-resident partner from countries or geographic areas identified as providing funding or support for terrorist activities or that have designated terrorist organization(s) operating within their territory
5. High value project proposals from potential grantee, especially unincorporated ones with

links to politically exposed persons.

6. High value project proposals from politically exposed persons; and
7. Given account details to make payments through unknown or un-associated third parties.

The list above is not exhaustive. The Foundation's compliance officer should update the list from time to time. Consequently, staff must pay attention to red flags that may come up during all transactions. All staff must be alert to detect and report any unusual activity that may arise, while on their duty post.

5.0.3 Reporting Suspicious Activity

- **Internal**

  Any staff that encounters a suspicious transaction or project activity should report same directly to his unit or departmental head. Where the suspicious transaction or project implementation activities occur at a state office, the members of staff who encounter such suspicious transaction or activity should report it directly to the State Coordinator. Irrespective of the perceived veracity of the report, the unit or departmental head should file an "Internal Operation Report" to the compliance officer immediately.

- **External**

  The Compliance Officer shall review the Internal Operation Report filed from the unit or State Office reporting the suspicious transaction. He or she will evaluate it and prepare a Suspicious Transaction Report, to be submitted to the Nigerian Financial Intelligence Unit, not later than twenty four hour (24 hours) of receipt of the Internal Operation Report on the suspicious transaction or project implementation activities.

5.0.4 Placing Transaction on Hold

If acknowledgement of receipt of the Suspicious Transaction Report (STR) submitted to the Nigerian Financial Intelligence Unit (NFIU) is accompanied by a stop notice, the transaction shall be put on hold for not later than 72 hours after which the transaction may be conducted.

6.0 Record Keeping

As part of its obligation to provide audit trail for all transactions conducted by the Foundation , it shall be mandatory for all responsible persons to ensure that records of transaction which shall include but not limited to the following;

- Signed grant Agreements;
- Sales and purchase receipts;
- Invoices;
- Means of Identification obtained from grantees, consultants or service providers;
- Cash and cheque registers,
- Contract agreements and bidding documents;
- Bank statement;
- Payment Advisories;

Grantees, consultant or service providers' files, etc shall be preserved for a minimum of five (5) years. During this period the Foundation is obliged under the law to make these records available to authorized government agencies on request. It shall be the duty of every employee of the Foundation to preserve the confidentiality of these records as information can only be shared by a duly authorized officer.

7.0 AML Internal Control Measure

7.0.1 Appointment of a Compliance Officer

At every given time, the Foundation shall have an **Anti-Money Laundering Compliance Officer, who shall always be a senior management staff of the Foundation.** The role of the Compliance Officer shall be as follows;

1. It shall be the duty of the Compliance Officer to file all statutory reports under the Money Laundering (Prohibition) Act 2011 (as amended) and other supplementary regulations issued by SCUML or other competent authorities, for the purpose of Anti-Money Laundering and Combating the Financing of Terrorism;
2. It shall be the duty of the Compliance Officer to conduct review of the Foundation operations and identify areas which the Foundation may be exposed to the risk of money laundering or terrorist financing and advise the Board of Trustees through the Chief Executive Officer (CEO) on remedial actions without delay;
3. It shall be the duty of the Compliance Officer to conduct or facilitate periodic training on Anti-Money Laundering and Combating the Financing of Terrorism for all relevant staff and agents of the Foundation ;
4. The Compliance Officer shall be the interface between SCUML and
5. The Foundation
6. The Compliance Officer shall undertake all other duties that may arise from or incidental to the compliance of the Foundation with the Money Laundering and Combating Financing of Terrorism laws and regulations in Nigeria.

7.0.2 Reporting Line of the Compliance Officer

The Compliance Officer shall report to the Board of Trustees through the Chief Executive Officer.

7.1.0 Training

- **Periodic Trainings**

  Anti-Money laundering and combating the Financing of Terrorism trainings shall be conducted at least twice in a year for all relevant staff of the Foundation.

- **Induction Trainings**

  Every newly recruited staff of the Foundation, who will have a role in the flow of financial and operational activities in the Foundation, must be trained on Anti-Money Laundering and Combating Financing of Terrorism as part of his or her induction program. Other trainings organized by third parties shall also count as part of the Foundation's compliance effort in this respect.

7.1.1 Centralization of Information Collected

For the purpose of complying with the Money Laundering (Prohibition) Act 2011 and supplementary regulations from SCUML, all transaction reports shall be collated and reported from the Head Office of the Foundation.

7.1.2 Responsibilities of Internal Audit Unit

Internal Audit Unit shall ensure that the Compliance Officer does his/her duties to ensure complete compliance of the Foundation at any given time. The Internal Audit shall conduct a periodic assessment of the compliance unit in terms of its prompt rendition of statutory reports and its general compliance with the requirements of the Money Laundering (Prohibition) Act 2011(as amended) and SCUML regulations.

8.0 Currency Transaction Reports

All transaction inflow of Ten Million Naira (N10, 000,000) and above shall be reported within seven (7) days of completion of such transactions as Currency Transaction Reports to SCUML by the Foundation.

9.0 Nil Reporting

In accordance with the Special Control Unit against Money Laundering (SCUML) regulation for Designated Non-Financial Institutions, 2013, the Foundation shall within 30 days, during which there was no transaction that meet any of the reporting threshold, make a "Nil Report" declaration on its letter head.

10.0 State of Commitment

On behalf of the Board of Trustees and Management of T.Y Danjuma Foundation, we hereby affirm the commitment of T.Y Danjuma Foundation to the adoption and implementation of this manual as our Anti-Money Laundering and Countering Financing of Terrorism policy document.

Chairman
Board of Trustees