GUIDELINES FOR THE DEVELOPMENT OF THE INSTITUTIONAL ANTI-MONEY LAUNDERING/COUNTERING THE FINANCING OF TERRORISM (AML/CFT) POLICY

1.0 INTRODUCTION

In keeping with international obligations and ensuring that Zambia's financial institutions and other non-financial businesses and professions are not abused by persons involved in money laundering (ML) or the financing of terrorism (TF), the Financial Intelligence Centre ('the FIC ') was established to receive suspicious transaction reports (STRs) from reporting entities, analyze and disseminate intelligence to law enforcement agencies (LEAs), pursuant to the Financial Intelligence Centre Act No. 46 of 2010 ('the Act')(as amended).

One of the cardinal responsibilities of reporting entities is to develop and implement internal programs for the prevention of ML/TF and other financial crimes. The programs include internal policies, procedures and controls to guide the reporting entity's employees in the implementation of AML/CFT obligations.

The purpose of these guidelines is to assist reporting entities in designing their AML/CFT policy. The Guidelines outline minimum requirements in respect of the institutional AML/CFT policy. These guidelines are not legal advice and should not be treated as such. The reporting entity must at all times refer directly to the relevant legislation to ascertain its statutory obligations. The guidelines have been issued in accordance with section 56 and pursuant to section 23 of the FIC Act.

2.0 THE AML/CFT POLICY

The Institutional AML/CFT policy should set the minimum and mandatory benchmarks to prevent, detect, and investigate money laundering and financing of terrorism, and to control and manage related risks. The policy should be monitored for compliance with the country AML/CFT legal and institutional framework.

The Institutional AML/CFT policy should be approved and signed off by the Board of Directors and be reviewed at such intervals as required by the Board or by changes in the regulatory environment.

3.0 DEFINITION OF KEY TERMS

The Institutional AML/CFT Policy should define and explain some of the key terms as listed below:

Attempted Transaction: Is one where a customer intended to conduct a transaction and took some form of action to do so. It is different from a simple request for information, such as an enquiry as to the price of a certain item. An attempted transaction includes entering into negotiations or discussions to conduct the transaction and involves concrete measures to be taken by either you or the customer.

Financial Action Task Force (FATF): Is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counterterrorist financing (CFT) standard.

Money Laundering: Under The Prohibition and Prevention of Money Laundering Act No 14 of 2001, as amended by Act No.44 of 2010, a money laundering offence involves various acts committed with the intention to conceal or convert property or the proceeds of property (e.g. money) knowing or believing that these were derived from the commission of a designated offence. In this context, a designated offence means a serious offence as defined in the Forfeiture of Proceeds of Crime Act, 2010. It includes among others those relating to illegal drug trafficking, corruption, bribery, fraud, forgery, murder, robbery, counterfeit money, stock manipulation. A money laundering offence may also extend to property or proceeds derived from illegal activities that took place outside Zambia.

Politically exposed Persons (PEPs): Are individuals who have or had been entrusted with prominent public functions both in Zambia and foreign countries and those associated with them. Please note the following:

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign 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.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, 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.

Persons who are or have been entrusted with a prominent function by an **international organisation** refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Proliferation Financing: means an act by any person who by any means, directly or indirectly, willfully or negligently provides funds or financial services to be used or knowing that they are to be used in whole or in part for proliferation, the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, supply, sale or use of nuclear, ballistic, chemical, radiological or biological weapons or any other weapon capable of causing mass destruction and their means of delivery and related materials including both technologies and dual-use goods used for non-legitimate purposes, including technology, goods, software, services or expertise.

Reporting Entity: An institution regulated by a Supervisory Authority and required to make a suspicious transaction report to the Centre on suspected Money Laundering, Terrorist Financing and other serious offences under the Act.

Risk Based Approach: Identification of the money laundering risks of customers and transactions which allow us to determine and implement proportionate measures and controls to mitigate these risks.

Suspicious Transaction Report: a report submitted on suspected money laundering, terrorist financing or other serious offence, or attempted

money laundering, terrorist financing or other serious offence, whether in form of a data message or otherwise.

Terrorist Financing: Terrorist financing offences extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used or in the knowledge that they are to be used in full or in part to carry out a terrorist act by a terrorist organization or an individual terrorist. Under the Anti-Terrorism Act No. 21 of 2007 (as amended), it is an offence to knowingly collect or provide property, such as funds, either directly or indirectly, to carry out terrorism or terrorist financing activities.

4.0 COMPONENTS OF THE AML/CFT POLICY

The AML/CFT policy should provide the minimum standards which must be applied throughout the reporting entity. At a minimum, the policy should cover the following areas:

- Overview of the Institution
- Institutional Commitment to fighting ML/TF and other Financial Crimes
- Policy goals and objectives
- Roles and responsibilities (Board, Management, Compliance Officer and Staff)
- Customer Due Diligence and verification processes
- Institutional Risk Assessment
- Application of enhanced or specific measures for high risk and low risk scenarios
- Sanction screening
- Transaction monitoring
- Reporting obligations
- Record keeping (including beneficial ownership information and ongoing monitoring)
- Confidentiality and tipping off
- Training
- Audit oversight
- Co-operation with competent authorities
- Penalties

4.1 POLICY OBJECTIVES

The objectives of the AML/CFT policy should be clearly outlined and may include the need to:

a) provide a framework for combatting money laundering and financing of terrorism.
b) comply with the applicable statutory and regulatory obligations
c) ensue that the risks arising from money laundering and terrorist financing are effectively mitigated and managed
d) ensure that a framework is established that will enable the recognition, investigation and reporting of suspicious and all reportable transactions.
e) optimize resources to focus on areas of high risk

4.2 ROLES AND RESPONSIBILITIES

The policy should apply to all relevant individuals in the organization in accordance with their roles and responsibilities. These should include:

- the Board – the board has the responsibility of providing oversight to senior management as well as approving the AML Policy. The board has the responsibility of ensuring that the reporting entity has the requisite ML and TF controls and procedures and processes to ensure compliance with the laws and regulations.

- Senior Management - senior management has the responsibility of ensuring that staff comply with the policy and must on a regular basis report to the board on the implementation of the policy.

- the Compliance Officer - the compliance officer should be approved by the FIC and be at management level to ensure sufficient levels of independence and access to all resources and procedures to ensure the full implementation of the policy as well as compliance to the AML/CFT regime.

- Employees – employees have the obligation to report suspicious transactions to the Compliance Officer and keep all such matters confidential.

4.3 CUSTOMER DUE DILIGENCE

Reporting entities are expected to put in place measures to identify and verify the identity of their customers (both natural and legal persons) in accordance with Section 16 of the FIC Act.

The institutional AML/CFT Policy should state the customer identification measures as well as the verification process that will be adopted by the reporting entity on both existing and potential customers.

The policy should address customer risk categorization which will help identify low, medium and high-risk customers. It should also require on-going monitoring to be conducted at appropriate times for each category of customers.

The policy should further indicate measures to be undertaken when dealing with high risk customers including politically exposed persons.

Reporting entity employees should be required to perform enhanced due diligence where the ML/TF risks are higher and simplified CDD measures where lower risks have been identified.

4.4 RISK ASSESSMENT

The Institutional AML/CFT policy should specifically indicate the requirement to evaluate the risk of money laundering and terrorist financing in order to identify areas of business, products and services where the risks are high. Further, emphasis should be made in the policy for the institutional risk assessment to be properly documented and updated periodically. Factors that may guide the frequency of the risk assessment include changes

to products, changes to market/ geographical segments, changes in delivery channels, among others.

4.5 SANCTION SCREENING

Reporting entities are required to scan all prospective and existing customers against international sanctions lists such as the Office of Foreign Assets Control OFAC, the United Nations (UN) and European Union (EU) sanctions lists as well as other watchlists. The institutional AML/CFT policy should state the screening tools used by the reporting entity and indicate the frequency for screening of customers. The policy should further outline the measures to be undertaken by employees in the event that there is a positive match, and these should include the requirement to make a report to the sector supervisor and the National Anti-Terrorism Centre.

Establishing a business relationship or making payments to entities on the sanctions lists is prohibited by the law and this should be clearly stated in the policy.

4.6 TRANSACTION MONITORING

The institutional AML/CFT policy should outline processes for monitoring transactions, whether they are automated or manual. Transaction monitoring entails that transactions undertaken by the reporting entity are scrutinized to ensure that they are consistent with the customer's business and risk profile.

4.7 OBLIGATIONS TO REPORT SUSPICIOUS TRANSACTIONS AND CURRENCY TRANSACTIONS

In accordance with Sections 29 and 30 of the FIC Act, reporting entities have the obligation to report suspicious transactions and currency threshold transactions to the FIC. The requirement that reporting entities should submit the said reports to the FIC should be set out in the institutional AML/CFT policy. The policy should

emphasize the importance of making these reports in accordance with the regulatory requirements.

4.8 RECORD KEEPING

The institutional AML/CFT policy should set out the requirement for reporting entities to maintain records on transactions and CDD information. As prescribed in the law, reporting entities are required to keep all records on domestic and international transactions, records obtained through CDD measures, account files and business correspondence relating to the customer or beneficial owner and records on filed STRs for not less than 10 years after the business relationship has ended or from the date of the transaction.

4.9 CONFIDENTIALITY AND TIPPING OFF

The importance of confidentiality should be emphasized in the AML/CFT policy. All employees of a reporting entity should be made aware that any data, information, and documents, whether in physical or electronic format, obtained during the course of suspicious activities monitoring should be protected and kept confidential in accordance with the legal framework. Further, the disclosure of the contents of the STR form is prohibited.

The institutional AML/CFT policy should clearly state that directors, employees or officers of the reporting entity are prohibited by law from disclosing the fact that an STR or related information shall be, is being or has been filed with the FIC.

4.10 TRAINING

The AML/CFT policy should define principles on training activities including minimum training requirements for different categories of employees. The type and level of training will vary depending on the employee's job functions and responsibilities. The policy may also indicate the appropriate method and frequency for delivery of training to key staff.

4.11 AUDIT OVERSIGHT

The reporting entity should ensure that regular independent reviews are conducted on the compliance function in order to ensure that AML/CFT policy requirements are properly implemented. This requirement should be set out in the institutional AML/CFT policy, which should specifically indicate that the audit function shall be independent of the compliance function and may be conducted by either internal or external auditors.

4.12 COOPERATION WITH COMPETENT AUTHORITIES

It is essential for the employees of the reporting entity to cooperate with competent authorities involved in the detection and investigation of money laundering or terrorist financing cases. This should be set out in the institutional AML/CFT policy.

4.13 PENALTIES FOR NON-COMPLIANCE

The consequences of non-compliance with requirements set out in the AML/CFT policy, which may include civil, administrative or criminal penalties, should be clearly stated to ensure that all personnel are aware and adhere to the policy.

5.0 CONCLUSION

Money laundering is a serious economic threat to the country's financial system and can have negative consequences at national, sectoral and institutional level. Non-compliance with AML/CFT regulations can expose the reporting entity to significant regulatory and reputational damage. As such, effective anti-money laundering systems need to be designed to be able to detect and prevent money laundering and the financing of terrorism in financial institutions and DNFBPs. The institutional AML/CFT policy is one of the tools intended to prevent reporting entities from being exposed to the proceeds of crime, terrorist financing and other financial crimes.

Issued by the Financial Intelligence Centre
May, 2020