

# **ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM POLICY**

The information contained herein is the property of EmpowerBank Limited and may not be copied, used or disclosed in whole or in part, stored in a retrieval system or transmitted in any form or by any means without the express authority in writing from the Chief Executive Officer.

## Summary of Changes

- Replacement of Heads of Departments with Department Managers
- Replacement of Deloitte with Axcentium Ethics Line.

## REVIEW AND ADOPTION CERTIFICATE

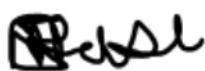
### REVIEWED



11/09/2025

.....  
Operations

.....  
Date



11/9/2025

.....  
Compliance Manager

.....  
Date

### APPROVED



25/09/2025

.....  
Acting Chief Executive Officer

.....  
Date

### RATIFIED



26/09/2025

.....  
Board Chairman

.....  
Date

## TABLE OF CONTENTS

<b>REVIEW AND ADOPTION CERTIFICATE</b> .....	<b>2</b>
<b>LIST OF ACRONYMS</b> .....	<b>4</b>
<b>1. OVERVIEW</b> .....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
1.1. <b>POLICY STATEMENT</b> .....	<b>5</b>
1.2. <b>PURPOSE</b> .....	<b>5</b>
1.3. <b>SCOPE</b> .....	<b>6</b>
<b>2. TERMS AND DEFINITIONS</b> .....	<b>7</b>
<b>3. GOVERNANCE FRAMEWORK</b> .....	<b>9</b>
3.1 <b>BOARD OF DIRECTORS</b> .....	<b>9</b>
3.2 <b>SENIOR MANAGEMENT</b> .....	<b>10</b>
3.3 <b>MONEY LAUNDERING REPORTING OFFICER</b> .....	<b>10</b>
3.4 <b>LINE MANAGERS</b> .....	<b>10</b>
3.5 <b>INTERNAL AUDIT</b> .....	<b>10</b>
3.6 <b>ALL INTERNAL STAKEHOLDERS</b> .....	<b>10</b>
<b>4. AML/CFT MITIGATION MEASURES</b> .....	<b>11</b>
4.1 <b>AML/CFT RISK ASSESSMENT</b> .....	<b>11</b>
4.1.1. <b>RISK-BASED APPROACH</b> .....	<b>11</b>
4.1.2. <b>INSTITUTIONAL ML/TF RISK ASSESSMENT</b> .....	<b>11</b>
4.1.2.1. <b>GEOGRAPHY</b> .....	<b>11</b>
4.1.2.2. <b>CUSTOMER RISK</b> .....	<b>12</b>
4.1.2.3. <b>PRODUCTS, SERVICES AND TRANSACTIONS</b> .....	<b>12</b>
4.1.2.4. <b>DELIVERY CHANNELS</b> .....	<b>13</b>
4.1.2.5. <b>OTHER QUALITATIVE RISK FACTORS</b> .....	<b>13</b>
4.2. <b>KNOW YOUR CUSTOMER</b> .....	<b>13</b>
4.3. <b>CUSTOMER IDENTIFICATION AND VERIFICATION</b> .....	<b>14</b>
4.4. <b>HIGH RISK CUSTOMERS AND PEPS</b> .....	<b>14</b>
4.5. <b>TRANSACTIONS MONITORING</b> .....	<b>15</b>
4.6. <b>SANCTIONS RISK MANAGEMENT</b> .....	<b>15</b>
4.7. <b>REPORTING OF STR</b> .....	<b>15</b>
4.7.1 <b>PROTECTION OF PERSON AND INFORMATION RELATING TO STRS</b> .....	<b>15</b>
4.7.2 <b>TIPPING OFF</b> .....	<b>16</b>
4.8 <b>REPORTING OF CTR AND EFT</b> .....	<b>16</b>
4.9. <b>RECORD-KEEPING</b> .....	<b>16</b>
4.10. <b>CORRESPONDING BANKING RELATIONSHIPS</b> .....	<b>16</b>
4.11. <b>ANTI-BRIBERY AND ANTI-CORRUPTION</b> .....	<b>16</b>
4.12. <b>STAFF TRAINING</b> .....	<b>17</b>
<b>5. COMPLIANCE AND MONITORING</b> .....	<b>17</b>
<b>6. BREACH OF POLICY</b> .....	<b>18</b>
<b>7. POLICY REVIEW</b> .....	<b>18</b>
<b>APPENDIX A: POLICY RETURN FORM</b> .....	<b>19</b>

## LIST OF ACRONYMS

AML/CFT	Anti-Money Laundering/ Counter Financing of Terrorism
CDD	Customer Due Diligence
CTR	Cash Transactions Report
EDD	Enhanced Due Diligence
EFT	Electronic Fund Transfer
FIU	Financial Intelligence Unit
IRA	Institutional ML/TF Risk Assessment
KYC	Know Your Customer
ML/FT	Money Laundering/ Financing of Terrorism
MLRO	Money Laundering Reporting Officer
PEPs	Politically Exposed Persons
PF	Proliferation of financing
RBA	Risk Based Approach
STR	Suspicious Transactions Report
SAR	Suspicious Activity Report

## **1. Overview**

### **Policy Statement**

EmpowerBank is dedicated to taking all sound measures to prevent money laundering and combat the financing of terrorism and sanctions risks. The entity is committed to actively participate in local, regional and international undertakings and initiatives to prevent and combat money laundering (ML) and the financing of terrorism (FT).

The basis of this anti-money laundering and counter financing of terrorism (AML/CFT) policy is the principal obligations contained in the following statutes and their corresponding regulations, exemptions and guidelines:

- a) Money Laundering and Proceeds of Crime (MLPC) Act [Chapter 9: 24] herein “the Act”
- b) Bank Use Promotion Act [Chapter 24:24] herein “BUP Act”
- c) Suppression of Foreign and International Terrorism Act [Chapter 11:21]

In addition, the international standards and recommendations from inter-governmental bodies such as the Financial Action Task Force (FATF) also form the basis of this policy.

### **1.2 Purpose**

This policy document forms an integral part of the EmpowerBank’s Compliance Risk Management Framework. It provides guidance to employees to how there are to fight against financial crimes i.e money laundering, proliferation financing, terrorist financing, anti-bribery and anti-corruption. It also formalizes EmpowerBank’s strategies against money laundering, proliferation financing, and financing terrorism.

The policy also seeks to:

- a) Create a framework for the identification and management of ML/TF risks to protect the entity against being used as a channel for the flow of illicit funds.

- b) Specify basic expectations of all employees in regard to their statutory obligations for the detection and prevention ML and TF.
- c) Set out EmpowerBank's minimum standards regarding the prohibition of financial crimes.

#### **d.3 Scope**

The Policy applies to;

- Shareholders
- Board of Directors
- Employees
- Agencies
- Customers
- Service Providers/Suppliers
- Consultants
- Other Stakeholders

This policy should be effectively applied in both the letter and spirit. The aim is to comply with relevant regulatory requirements and to mitigate and reduce the potential risk of the entity's services and delivery channels being used to launder the proceeds of illegal activity, fund terrorist activities, perform transactions in breach of financial sanctions or for any other financial crime.

## 2. Terms and Definitions

Term	Meaning
Money Laundering	Any activity that has, or is likely to have, the effect of concealing or disguising the nature, source, location, disposition, or movement of the proceeds of unlawful activities or interest anyone has in such proceeds.
Reverse Money Laundering	A process that disguises a legitimate source of funds that are to be used for illegal purposes.
Financing of terrorism	Directly or indirectly, providing or collecting funds, or attempts to do so, with the intention that they should be used or in the knowledge that they are being used in whole or in part in order to carry out a terrorist act; or by a terrorist; or by a terrorist organisation.
Proliferation financing	The act of providing funds or financial services which are used in, 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 used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.



Beneficial Owner	<p>A natural person who ultimately owns or controls the rights to or benefits from property, including the person on whose behalf a transaction is conducted; or a person who exercises ultimate effective control over a legal person or legal arrangement. More specifically, it refers to a natural person who—</p> <ul style="list-style-type: none"> <li>a) directly or indirectly holds more than twenty <i>per centum</i> of the company's shares; or</li> <li>b) directly or indirectly holds more than twenty <i>per centum</i> of the company's voting rights; or</li> <li>c) directly or indirectly holds the right to appoint or remove a majority.</li> </ul>
Customer	<p>The person for whom a transaction or account is arranged, opened, or undertaken; a signatory to a transaction or account; any person to whom an account or rights or obligations under a transaction have been assigned or transferred; as well as any person who is authorised to conduct a transaction or control an account.</p>
Employee	<p>Any individual working at any of the levels and grades within the Microfinance Bank including executives, senior managers, officers, and other employees (whether permanent, fixed term or temporary).</p>
Politically exposed person (PEP)	<ul style="list-style-type: none"> <li>a) Any person who is or has been entrusted with prominent public functions in any jurisdiction, including but not limited to, a Head of State or of government, a senior government, judicial or military official, a senior executive of a state-owned corporation, or a senior official of a political party; or</li> <li>b) any person who is or has held a position as a member of senior management of an international organisation, including the position of director, deputy director, member of the board or equivalent functions; or</li> <li>c) any close associate, spouse or family member of a person referred to in paragraphs (a) or (b) above.</li> </ul>

Shell Bank	A bank without physical presence in any country.
Customer Due Diligence (CDD)	It is an investigation, audit, or review performed to confirm the facts of a matter under consideration. It includes: <ul style="list-style-type: none"> <li>• client identification, verification and profiling (Know Your Client-KYC);</li> <li>• record-keeping; and</li> <li>• account/transaction monitoring and reporting</li> </ul>
Enhanced due diligence (EDD)	Additional examination and caution measures taken on perceived higher risk customers. It is aimed at identifying clients and confirming that their activities and funds are legitimate, e.g. document and verify sources of wealth and funds.
Know your client (KYC)	Anti-money laundering policies, processes, practices, and procedures used to: <ul style="list-style-type: none"> <li>• determine the true identity of a client and the type of activity that is ‘normal and expected’;</li> <li>• detect activity that is ‘unusual’ for a client.</li> </ul>
Reportable/Suspicious transaction	A transaction or series of transactions that must be reported to the Financial Intelligence Unit (FIU) in terms of applicable local legislation, this includes transactions resulting in suspicions of possible money laundering or the financing of terrorism.
Large cash transactions report	Threshold-based transactions reports covered by section 30 (6) of the Money Laundering and Proceeds of Crime Act [Chapter 9:24] as accordance to FIU directives issued from time to time.
Electronic Fund Transfer	RTGS Transfer as accordance to the RBZ Directives. An electronic funds transfer is the electronic transfer over an online network.

Account	Any facility or arrangement by which the microfinance bank does any of the following—  a) accepts deposits of funds or other assets; or b) allows withdrawals or transfers of funds or other assets; or c) pays negotiable or transferable instruments or payment orders on behalf of any other person.
---------	---

### 3. GOVERNANCE FRAMEWORK

#### 3.1 Board of Directors

The Board of Directors shall be fully committed to an effective AML/CFT program through the adoption of appropriate policies and procedures including the appointment of an appropriately qualified manager as Compliance Officer/Money Laundering Reporting Officer (MLRO) to coordinate and monitor AML/CFT Compliance by the bank.

#### 3.2 Senior Management

Senior management shall:

- a) Provide direction to, and oversight of the entity's AML/CFT strategy and policy implementation.
- b) Provide adequate resources to the Compliance function including appropriate staff and technology to combat ML/TF.
- c) Support and participating in AML/CFT initiatives.

#### 3.3 Money Laundering Reporting Officer

The Compliance Manager shall be the microbank's MLRO who shall be mandated to direct the implementation of this policy and to prescribe minimum standards for associated processes, methodologies and tools.

In that regard, the MLRO shall:

- a) Have full responsibility for overseeing, developing, updating and enforcing the AML/CFT programs for the bank;
- b) Be competent and knowledgeable regarding AML/CFT issues;
- c) Develop policies and procedures designed to deter and detect ML and TF

activities;

- d) Coordinate submission of suspicious transaction reports (STRs) to the FIU;
- e) Respond promptly to information request by the FIU and other competent authorities; and
- f) Communicate all relevant AML/CFT issues throughout the entity.

### **3.4 Line Managers**

Line managers shall ensure that adequate controls are implemented and maintained within areas of their control to prevent ML/TF.

### **3.5 Internal audit**

The Internal Audit function shall independently review the adequacy and effectiveness of the entity's AML/CFT compliance programs.

### **3.6 All Internal Stakeholders**

Every employee and Director of EmpowerBank shall be individually responsible i.e bear a personal obligation for observing and complying with applicable AML/CFT laws, regulations, policies and procedures.

## **4. AML/CFT MITIGATION MEASURES**

### **4.1 AML/CFT RISK ASSESSMENT**

The entity shall implement AML/CFT measures outlined below;

#### **4.1.1 Risk-Based Approach**

The risk-based approach shall be adopted in:

- a) Identification and assessment of money laundering and terrorist financing risks within all business activities.
- b) Designing and implementing controls to manage and mitigate the recognized risks.
- c) Continuously review and monitoring of the effectiveness of the controls in place through keeping customer identification and beneficial ownership information up to date and ongoing monitoring of financial transactions that pose higher risks.

#### **4.1.2 Institutional ML/TF Risk Assessment**

EmpowerBank Limited shall annually, conduct an institutional ML/TF risk assessment to evaluate the money laundering and terrorist financing risks to which it is exposed. Based on the risk assessment results, enhanced measures shall be applied for high-risk areas while simplified measures will be permitted where the risks are lower.

Before launching any new product, service or business practice and before the use of any new technological innovation, for both new and existing products, EmpowerBank Limited shall assess and document the money laundering and terrorist financing risk posed by such products, services, business practices or technology and put in place adequate measures to mitigate the risk.

The areas of focus in the ML/TF risk assessment shall be:

##### **4.1.2.1 Geography**

The EmpowerBank Limited shall assess origin and destination countries' area's ML/TF risk. Factors that may result in determining that a customer from, in or connected to a particular country poses a higher risk include;

- a) Countries subject to sanctions, embargoes or similar measures.
- b) Countries identified by credible sources (such as FATF, national authorities or other recognized evaluation bodies) as lacking adequate AML/CFT laws, regulations and or controls.
- c) Countries identified as providing funding or support for terrorist activities or having significant levels of corruption, or other criminal activities.

Geography extends to the local areas and stratifying the risk in terms of the towns i.e border towns, main cities, other cities.

##### **4.1.2.2 Customer Risk**

The bank shall conduct profiling to enable identification of high-risk customers and implement appropriate controls to combat money laundering and financing of terrorism. In this regard, customers shall be profiled based on factors that include;

- a) Geographical location.
- b) Customer type (Politically Exposed Persons, High Net worth or Ordinary).
- c) Nationality.

d) Nature of business conducted by the customer.

#### **4.1.2.3 Products, Services and Transactions**

The bank shall assess its products, services and transactions then apply mitigations corresponding with the identified risk. The bank's product offering in the following categories shall be assessed regularly to ascertain vulnerability to money laundering and financing of terrorism:

- Cash based products
- Savings Products
- Electronic products
- Money Transfer Agencies
- Lending products
- Insurance and licensing products.

#### **4.1.2.4 Delivery Channels**

The microfinance shall assess the extent to which its delivery channels pose ML/TF risks. The delivery channels are face to face channels i.e when customers physically use the banking facilities in banking halls and the non-face to face channels. The bank shall formulate appropriate mitigating strategies.

#### **4.1.2.5 Other Qualitative Risk Factors**

Other qualitative risk factors shall also be assessed. These are those factors that can have an impact on operational risks and contribute to an increased or decreased likelihood of breakdowns in key AML/CFT controls.

Other Qualitative Risk Factors include:

- Client base stability
- Integration of IT systems
- Recent AML Compliance employee turnover
- Reliance on third party providers
- Recent/planned acquisitions
- Recent projects and initiatives related to AML Compliance matters (e.g. remediation, elimination of backlogs)
- Recent relevant enforcement actions
- National Risk Assessments

- Initiatives by the Governance departments.

#### **4.2 Know Your Customer**

The bank shall undertake measures to know the customers that they do business with.

The KYC process shall comprise of:

- a) Identification and verification of the identity of the customer. Under no circumstances may be transactions be carried out or relationships established for anonymous customers, or customers not physically present for the customer identification purposes.
- b) Establishment of, whether the customer is acting for another person or entity and to identify the beneficial owner.
- c) Acquiring additional and appropriate KYC information. KYC information shall include, but not limited to, appropriate personal, business and financial details regarding the customer as well as details of the anticipated transactional activity and source of funds/wealth taking into account all the data privacy and protection laws of Zimbabwe.
- d) EmpowerBank Limited shall take steps to ensure that it holds appropriate up-to-date information on its customers.
- e) Acceptable proof of identification shall be a national identification card, a valid passport or a valid driver's license a copy of which shall be kept together with the transaction details as required.

#### **4.3 Customer Identification and Verification**

At EmpowerBank Limited, identification and verification of the identity of each customer shall take place before the establishment of the business relationship or before the carrying on of further business. Customer identification by means of an identification document shall also be done when there is suspicion of money laundering or financing of terrorism involving the customer.

#### **4.4 High Risk Customers and PEPs**

Politically Exposed Persons (PEPs) shall be regarded as high-risk, hence needing Enhanced Customer Due Diligence. EmpowerBank Limited shall:

- Obtain relevant Senior Management approval for establishing business relationship with PEPs.

- Establish beneficial owners for all Company and other Business Entities.
- Take reasonable measures to establish the source of funds for PEPs.
- Conduct enhanced ongoing monitoring of the business relationship.

#### **4.4.1 Establishing beneficial owners for all corporate clients**

Before opening an account with EmpowerBank Limited, the bank shall ensure that the corporate client provides the following documents:

- Proof of Residence (not more than 3 months old).
- Copy of IDs or Valid Passport & Passport sized Photos.
- Directors valid ID & Passport sized Photos.
- Registration Documents (Articles and Memos, CR5, CR6, CR2, and CR16 Certificate of Incorporation/Constitution, Deed of Partnership, Trust Deed).
- Directors valid ID & Passport sized Photos.
- Tax clearance certificate.
- Group Constitution (Signed by Board Members)

EmpowerBank Limited shall establish the shareholding structure of the company as well as the person who exercises ultimate effective control over a legal person or legal arrangement. More specifically, a natural person and EmpowerBank Limited shall assess the risk poses by the beneficial owner.

#### **4.5 Transactions Monitoring**

The bank shall appropriately scrutinize and monitor transactions that pass through its delivery systems in order to identify unusual or suspicious activities. Enhanced monitoring shall be applied on transactions involving customers regarded as high risk.

#### **4.6 Sanctions Risk Management**

Sanctions risk management forms an essential part of EmpowerBank' s fight against financial crime, as such it shall not accept any instructions or otherwise deal with any payments to or from sanctioned countries or sanctioned nationals. The institution shall conduct real-time transactions screening on all transactions in relation to UN sanctions list as well as any other relevant lists of designated persons, groups and entities subject to financial sanctions. EmpowerBank Limited shall implement FIU Directives issued from time to time on updates on the UN ISIL (Da'esh) and UN Al-Qaeda Sanctions Lists.



#### **4.7 Reporting of STRs**

EmpowerBank Limited shall have a reporting procedure for all suspicious transactions which shall be adhered to by all business units. All suspicious transactions shall be verified by the MLRO before being escalated to the Financial Intelligence Unit (FIU) for further investigations.

All suspicious transactions shall be reported to the MLRO within 24 hours of identification and to the FIU within 72 hours using the GOAML Platform.

##### **4.7.1 Protection of Persons and Information Relating to STRs**

As provided for by the MLPC Act (9:24), no civil, criminal, administrative or disciplinary proceedings for breach of professional secrecy or contract shall be taken against any person for submitting a STR in compliance with the provisions of the Act.

##### **4.7.2 Tipping Off**

Complete confidentiality must be maintained regarding any suspicions formed and regarding the consideration of a transaction for a report. Employees are prohibited from disclosing to any of their customers or any other third party excluded from the reporting process, that a report or any other information concerning suspected money or financing of terrorism will be, is being or has been submitted to the FIU or that a money laundering or financing of terrorism investigation is being or has been carried out, except in the circumstances where required to do so by law.

#### **4.8 Reporting of CTR and EFT**

The bank shall report CTR and EFT using the FIU Platform (GOAML) through the Money Laundering Reporting Officer as stipulated by the FIU Directives with the threshold for the transaction amount to be reported on.

#### **4.9 Record-keeping**

EmpowerBank Limited shall maintain all client identification, verification, and transaction records for not less than five years after the business relationship has ended or after date of transaction. All copies of suspicious transaction reports made shall also be maintained for at least five years from the date the report was made. These record

and all the underlying information shall be timely made available on request by the FIU or such other competent authorities.

#### **4.10 Corresponding Banking Relationships**

The bank shall identify and verify the identity and nature of business of the correspondent financial institution with which it intends to do business. It shall also assess the corresponding bank's compliance to AML/CFT systems and controls.

#### **4.11 Anti-Bribery and Anti-Corruption**

EmpowerBank Limited is committed to applying high standards of integrity and has a zero-tolerance policy towards bribery and corruption as these are often associated ML/TF. In this regard, employees shall not;

- a) Offer, promise or pay bribe of any kind to customers, business partners, suppliers
- b) Make facilitation payments i.e payments to secure or speed up a service to which the payer is entitled.

Customers and employees are encouraged to immediately report all bribery, fraud and corruption incidences through established reporting means such as whistleblowing hotline, website or email for formal investigation to Axcentium EthicsLine.

#### **4.12 Staff training.**

All new staff and agencies shall be provided with suitable and timely training on bank's approach to AML/CFT. EmpowerBank shall also ensure that all employees dealing with customers, customers' transactions or matters involving money laundering and or terrorist financing are provided with regular training about the nature of the money laundering and terrorist financing risks, as well as any new trends within the field. The Compliance department shall be responsible for providing refresher training at least once annually, to all members of bank's staff to keep them alert to the risks of ML/TF. Additional training shall be provided whenever there are material changes in AML/CFT laws, regulations, policies or procedures.

### **5. Compliance and Monitoring**

This policy shall be monitored through periodic reviews.



## **6. Breach of Policy**

The bank does not tolerate any breach of the requirements set forth in this policy as that could jeopardize the soundness and integrity of the microfinance.

Disciplinary action following the bank's code of conduct shall be taken against staff members who fail to comply with the provisions of this policy.

All staff members shall sign the policy return form in **appendix A** of this policy as evidence of have read and understood the bank's policy on AML/CFT.

## **7. Policy Review**

The policy shall be reviewed on an annual basis or whenever there are material changes relating to money laundering and financing of terrorism. The policy review shall be done to ensure that it remains relevant to the prevailing circumstances.

# APPENDIX A: POLICY RETURN FORM

1. All Departmental Managers, Branch Managers, Head of Sections and supervisors should thoroughly go through the policy on AML/CFT to ensure that all employees under their jurisdiction/supervision have read and that they are conversant with information contained therein.
2. All members of staff shall sign the Policy Return Form below and it is the Responsibility of the Departments Managers and Sections to return the completed forms to the bank's Money Laundering Compliance Officer.

NAME	SIGNATURE	DATE
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

Department: .....

SIGNED ..... DATE .....

DEPARTMENT MANAGER/ SECTION / BRANCH