GUARANTY TRUST BANK (KENYA) LIMITED

COMPLIANCE POLICY

(Version 7.0)

Approved by the Board of Directors 29.06.2022

Head of Risk & Compliance

NOTICE AND WARNING

This Compliance Policy is the property of Guaranty Trust Bank Kenya ("the Bank" or "GTBank"), Plot 1870 Woodvale Close, Westlands and is for the sole use of individuals working for the Bank or on its behalf. The policy aims to provide guidance at ensuring that only legitimate transactions and relationships are maintained by the Bank.

The information and guidance contained in this Compliance Policy is confidential and may not be disclosed to any third party unless the prior consent of the Compliance Group has been obtained.

The information and guidance given in this Compliance Policy is subject to change and will be revised from time to time. If a hard copy is taken, it shall remain the responsibility of users of that copy to keep it up to date at all times.

Employees are reminded that compliance with this Policy forms an essential part of their contracts of employment. While most issues can be addressed, one-off scenarios may arise and such cases should be referred to the Compliance Unit at riskandcomplianceke@gtbank.com

Document History

Version	Date	Purpose	Reviewers
2.0	4-July-2016	Annual review	James Mutegi David Kilonzi Dipan Shah Victor Ezaga
3.0	23-July-2018	Annual review	Festus Rotich Ruth Muiruri Dipan Shah Victor Ezaga
4.0	28-June-2019	Annual review	Festus Rotich Dipan Shah Victor Ezaga Olabayo Veracruz
5.0	June 2020	Annual review	Flora Njau Virginia Angwenyi Victor Ezaga Olabayo Veracruz
6.0	May 2021	Annual review	Caroline Macharia Virginia Angwenyi Ayodele Popoola Olabayo Veracruz
7.0	***March 2022***	***Annual Review***	***Vivian Oluoch*** ***Virginia Angwenyi*** ***Ayodele Popoola*** ***Olabayo Veracruz***

Summary of Changes

Page	*Description of Change*
10	***The company shareholders***
42	*Appendix j: Approaches to compliance monitoring*
44	*Appendix k: Miscellaneous*

Table of Contents

1. OVERVIEW

1.1 Introduction

Guaranty Trust Bank (Kenya) Limited ("GTBank" or "the Bank") remains committed to the strict adherence and conformance to internal, regulatory and statutory rules and procedures applicable to the business of banking. The Bank recognizes that compliance with regulatory requirements at all times constitute global best practice and ensures accountability to all stakeholders of the Bank, including regulators and customers.

This Compliance Policy outlines the measures and systems put in place by the Bank to ensure that the Bank and its staff conduct business activities in an ethical manner, consistent with fiduciary and legal/regulatory obligations and with the Bank's business principles and code of conduct.

1.2 Definition of Compliance and Compliance Risks

Compliance refers to the system or procedures and controls required to ensure conformance with established internal, statutory and regulatory guidelines and rules.

Compliance Risk is defined as the current and prospective risk to earnings or capital arising from violations of or non-conformance with laws, rules, regulations, prescribed practices, internal policies, and procedures or ethical standards. Compliance risk also arises in situations where the laws or rules governing products or activities of the Bank's clients may be ambiguous or untested.

At GTBank, the principles of good corporate governance practices and compliance remain part of our core values. We ensure that our behavior is Ethical, Transparent and Legal at all times. We recognize that non-compliance exposes the Bank to monetary fines and penalties, payment of damages arising from litigation, poor rating by rating agencies or regulatory authorities and the voiding of relationships. Compliance risk can also lead to reputational damage, loss in franchise value, limited business opportunities, reduced expansion potential and law suits by customers

1.3 Purpose

The objective of the Compliance function at GTBank is to ensure that a clear- cut approach is in place for ensuring that only legitimate transactions and relationships are maintained by the Bank. It's standards would be backed by relevant global and local regulatory guidelines in line with the rules of Governance, Risk Management and Compliance.

1.4 Scope of Policy

This Policy outlines the scope of the Bank's Compliance Policy, the strategies for ensuring compliance and managing the compliance risk, stakeholders' roles and responsibilities, the application of the Policy and the required reporting lines and reports. It would stipulate guidelines for the compliance function of the Bank, which include the following:

- Promoting a culture of zero tolerance for regulatory breaches/sanctions;
- Anti-Money Laundering /Combating Financing of Terrorism (AML/CFT) transactions monitoring, reporting and training;
- Politically Exposed Persons (PEPs) (classification, monitoring and reporting);
- Regulatory and law enforcement agencies' enquiries and management;
- Implementation of "Know Your Customer" principles;
- Internal, Independent (non-regulatory) and Regulatory Audit;
- Sanctions Compliance Management;
- Timely rendition of returns and reports;
- Communicating the impact of current and newly released policies and regulatory guidelines to all staff;
- Ensuring adherence to internal and regulatory policies and guidelines, including the Code of Corporate Governance of the Bank;
- Expected guidelines for core stakeholders within the Bank (Funds Transfer, Cash and Monetary Instrument, Foreign Correspondent financial institutions and Product Policies);
- Setting acceptable turnaround time for activities and ensuring escalation, where necessary.

1.5 Stakeholders

The stakeholders comprise of:

a. The Bank's Customers

This refers to any person or group of people who are using any or all of the services offered by GTBank. Our customers expect compliance with the laws, rules and regulations applicable in banking locally and in line with global best practices. They expect compliance and strict adherence with the various applicable laws and regulations in all dealings and interactions with the Bank.

b. The Board of Directors

The Board of Directors has oversight function over all compliance functions in

the Bank. The Board shall receive Compliance reports at its quarterly Board meetings and review the reports to ensure that the Bank is in strict compliance with all regulatory and internal procedures. The Board shall also ensure that the provisions of this Policy are strictly adhered to. The Board has delegated this oversight function to the Board Risk Management Committee.

c. Executive Management

Executive Management is responsible for the implementation and adherence to the Compliance Policy and to ensure that its minimum standards are enforced. It ensures a centrally controlled Compliance Programme, implemented bank wide by the Compliance Unit, which is headed by the Head of Risk and Compliance (HoRC) who is a Management Staff. In addition, it would ensure that all branches have designated a Compliance Officer who is the Branch Operations Head of the branch.

Executive Management provides sufficient resources and support to the HoRC to ensure that compliance functions are properly carried out. Through the HoRC, it would ensure that regular training programmes are organized for all employees on their compliance roles and responsibilities.

Management also ensures that the Internal Audit Unit of the Bank carries out periodic audit on the compliance function of the Bank.

d. The Bank's Staff

Members of staff are duly trained to understand their role in ensuring that all transactions in which the Bank is involved complies with regulatory, statutory and internal guidance and procedures.

Staff shall inform the Compliance Unit of all compliance related issues. All staff are to read and fully understand the requirement of the Bank's Compliance Policy.

All staff are also to attend training programmes on Compliance.

e. Regulatory Bodies

Regulatory bodies ensure that the Bank:

- Is transparent in all its dealings with its customers and regulators;
- Complies with all regulatory principles and guidelines applicable to its business;
- Put in place guidelines to ensure that the culture of compliance flows from

the Board of Directors through Management to the entire staff;

- Has a robust system of senior management controls and responsibility to effectively carry out the Bank's compliance responsibilities;
- Has effective system(s) in place to prevent money laundering and the financing of terrorism.

f. Compliance Officers

Compliance officers' roles and responsibilities include:

- Ensuring a culture of compliance in the Bank;
- Recommending for approval and implementing the approved policies and procedures relating to the compliance obligations of the Bank;
- Ensuring that all staff of the Bank are appropriately trained on the Bank's compliance obligations in conjunction with the Human Resources Group of the Bank;
- Advising and monitoring compliance with all legal, statutory, regulatory and internal rules, guidelines and regulations affecting the Bank;
- Liaising with external regulators and law enforcement agencies on the compliance responsibilities of the Bank and maintaining open, honest and transparent relationship with these stakeholders;
- Providing advice, guidance and support on regulatory issues affecting the business and interpreting relevant rules and regulations.
- Collaborating with internal stakeholders in the Bank, including members of control function groups and divisions to ensure compliance is maintained bank wide.
- In liaison with human resource department, persons are screened before being hired as employees.

g. The Company's Shareholders

This refers to a person or group of individuals who hold shares in a company. Our shareholders expect compliance with the laws, rules and regulations applicable to the company and in line with the global best practices in order to ensure that the company is a good "corporate citizen".

2. COMPLIANCE STRUCTURE: APPROACH TO MANAGING COMPLIANCE RISK

This Policy will be centered on ensuring that GTBank is in full compliance with regulatory guidelines that promote ethical banking practices, including the Bank's Code of Corporate Governance and that the relationship between the Bank and its customers is not jeopardized.

The Policy will be maintained and continually reviewed to ensure compliance with relevant provisions of the AML/CFT regulations, and in line with global best practices promoted by bodies such as Financial Action Task Force (FATF), The Basel Committee on Banking supervision, European Union directive on Money Laundering, Wolfsburg Group and any other regulatory body.

The Compliance function handles:

- Legal and Regulatory compliance.
- AML/CFT compliance.

This Policy should be read in conjunction with the Bank's AML/CFT Policy and the KYC Policy.

2.1 Legal and Regulatory Compliance

I. **Internal Policies**

The Bank ensures that all staff comply with its internal rules and regulations governing the Bank's business as well as corporate ethical standards, including the Code of Corporate Governance and the Code of Professional Conduct for the Bank's employees.

The Corporate Governance Compliance status report shall be included in the audited financial statements of the Bank.

The Bank has established 'whistle blowing' procedures that encourage, (under assurance of confidentiality), all stakeholders (staff, customers, shareholders, suppliers, applicants and the general public etc.) to report any unethical activity/ breach of the Corporate Governance Code using, amongst others, a special email or hotline.

The CCO shall be responsible for monitoring the whistle blowing channels to review reported cases and initiate appropriate action, if necessary, at the level of the Board or the Managing Director to redress the situation.

All staff of the Bank are expected to comply with all policies and ethical

standards stipulated in the Bank's Code of Professional Conduct. Where full compliance with the Bank's Standards and Code of Ethics is not achieved and where this impacts on the overall scope of operation of internal audit activity, this will be disclosed to the Board Audit Committee.

Employees of the Bank shall subscribe to the Code of Professional Conduct of the Bank upon resumption of office, and subsequently on an annual basis.

II. Laws and Regulatory Guidelines

The Compliance Unit advises and monitors compliance with all legal, statutory, regulatory guidelines affecting the Bank, particularly as it relates to compliance. GTBank ensures that all its regulatory obligations are addressed by employing and upholding transparent practices fashioned along local/international regulatory standards as well as global best control practices.

The Bank accordingly ensures compliance with the Corporate Governance guidelines as set out in the CBK Prudential Guidelines.
The Compliance Unit ensures that all staff are aware and adhere to local and international regulatory requirements. This is achieved by maintaining a Compliance Grid that contains all the regulatory guidelines and policies that all Departments, Groups and Divisions, are to abide by. It would also ensure that timely rendition of regulatory returns is put in place.

GTBank's Compliance function ensures that the Bank's operations are tailored in line with the stipulations of relevant regulators including the following:

- Central Bank of Kenya (CBK)
- Financial Reporting Centre (FRC)
- Deposit Protection Fund Board

The Compliance unit in conjunction with the Legal Group periodically reviews and updates all laws, policies and regulations affecting the Bank, monitor the compliance levels, and ensure that staff are notified and informed of new and revised policies and rules.

III. Rendition of Reports and Returns

The Bank ensures that all regulatory and statutory returns and reports are provided to regulators and law enforcement agencies as at when due, including the provision of certain information on the Bank that are required to be displayed at the business premises of the Bank.

To promote a culture of timely rendition of returns, the Compliance Unit would

send reminders on the first working day of the reporting period and two days to the lapse of the deadline to the relevant business areas to ensure timely and accurate returns rendition. The Compliance unit also maintains a tracking system that would log attestations for timely and correct rendition of returns. Defaulting business areas are reported to the Internal Control Group of the Bank on a monthly basis for appropriate sanctioning.

IV. Responses to Enquiries from Regulators and Law Enforcement Agencies

The Compliance unit ensures timely and satisfactory responses to regulatory enquiries in compliance with the laws and regulatory requirements.

The Bank liaises with external regulators and law enforcement agencies on its compliance responsibilities and maintains an open, honest and transparent relationship with them.

2.2 AML/CFT Compliance

AML/CFT compliance refers to the adherence to all regulatory directives, statutory rules and global best practices put in place to ensure that the Bank is not used as a conduit for illegal/suspicious transactions relating to money laundering and financing of terrorism. This is in recognition of the global threats which money laundering and terrorism pose to international peace and security and which is capable of undermining Kenya's development and progress.

AML/CFT compliance requires a risk-based approach to customer due diligence by applying "know-your-customer" principles to transactions, customer account reviews, monitoring and reporting.

i. Transaction Monitoring

Transaction monitoring is the act of screening daily transactions of all types that occur in any account managed by GTBank. The main objective of this procedure is for the timely identification of significant changes in patterns or unusual account behavior. This would also enable further investigation that would ascertain whether or not such accounts can be classified as 'suspicious' and disclosed to the relevant authorities.

This outlook is in line with the Basel Committee Guideline on Banking Supervision which stipulates that, banks should not only establish the identity of their customers but must also monitor account activity to identify those transactions that do not conform to the normal or expected transactions for that customer or type of account.

One of the ways the Bank ensures that only credible customers are maintained on the Bank's books is by regularly monitoring and carrying out thorough review of customers' transactions towards identifying those that have elements of suspicion, transactional complexity or irregularity. This is carried out by all relevant business units processing customers' transactions. Upon identification of these transactions, the business unit is required to deliver schedules containing the data of these customers to the Compliance unit for further review and due diligence.

For purposes of transaction monitoring at branches, all Branch Operation Heads are assigned the role of Branch Compliance Officer. They ensure that suspicious transactions carried out at the branch level are promptly identified and reported to the Compliance unit for further investigation.

Generally, Compliance Officers in the Bank are responsible for monitoring the plethora of transactions that are reported via mails from relevant business units and those captured by the K-printer AML Software and SAS platform, the application used for AML/CFT monitoring purposes in GTBank.

K-Printer AML software is an outsourced monitoring tool while SAS is managed by GTBank Nigeria. AML/CFT Scenarios defined for monitoring purposes shall be subject to business experience, changes in regulatory thresholds and as may be occasioned by trends in the country or globally.

This holistic procedure is premised on the need to ensure that no loopholes exist within the system from account opening (KYC) as well as throughout the life of the account (transaction monitoring).

ii. Transaction Reporting

International best practice and regulatory requirements stipulates those certain reports and returns are made to regulatory bodies. In Kenya, the FRC is the regulatory agency responsible for receipt of the following core transaction-based reports:

- Cash Transaction Reports (CTR)
- Suspicious Transaction Reports (STR)
- Suspicious Activity Reports (SAR)

Among the numerous transactions carried out on any business day within the Bank, all transactions within the regulatory thresholds are captured in the CTR reports and submitted to the FRC as stipulated in the reporting requirements. The CTR report contains all cash transactions in excess of USD 10,000 (or its equivalent

in any other currency).

In order to comply with CBK Circular dated 05 January 2016 on Additional Guidelines on Large cash transactions, Large Cash Transaction questionnaire must be filled by all customers cash transactions in excess of USD 10,000 (or its equivalent in any other currency). (Appendix I).
All transactions identified as suspicious with no economic justification are promptly reported to the FRC in the accepted STR reporting format. Appendix "H" Transactions are considered suspicious for the following reasons:

(a) Involve frequencies which are unjustifiable or unreasonable;
(b) Are surrounded by conditions of unusual or unjustified complexity;
(c) Appear to have no economic justification or lawful objective;
(d) Involve inconsistency with the known transaction pattern of the account or business relationship.

iii. Politically Exposed Persons (PEPs)

A PEP is an individual who has been entrusted with prominent public functions in the country, such as a Head of State, senior politician, senior government official, judicial or military official, senior executive of a state-owned corporation or important political party official, as well as their families and close associates.

Enhanced measures of due diligence would be applied to ensure that the Bank is not unknowingly supporting fraudulent activities such as money laundering and/or the financing of terrorism.

In line with FATF's recommendation, GTBank would employ the use of appropriate discretionary risk-based systems based on the definition of a PEP which includes all persons that might have some form of relationship with an actual current political office holder or all persons who have been political office holders at one time or another. This would be achieved through the thorough review of details provided by the customer and transaction trends to help in determining which customers should be classified as PEPs.

Establishment of new accounts for PEPs as well as continuity of such accounts (for those already existing in the system) is subject to Chief Operating Officer's approval. The provision of supporting documents establishing the source(s) of funds must be ensured whilst continued monitoring of the account is carried out.

Regular update of internal PEP list is done once a PEP has been identified.

iv. Regulatory Enquiries

The power to demand and obtain records is a major highlight of regulatory AML/CFT monitoring. To demonstrate compliance with this requirement, the Bank's Compliance Officers are to ensure that prompt responses are delivered to authorized officers of relevant regulatory authorities {such as the CBK, Kenya Revenue Authority (KRA) and FRC} upon receipt of requests demanding for any information or record on any customer of the Bank.

Insistence on proper and adequate KYC documentation from the point of account-opening and throughout the duration of the banking relationship would ensure that records submitted to regulators are complete and accurate.

All information sharing with the various law enforcement agencies, whether by form of routine renditions (such as the CTR and STR/SAR reports to the FRC) or on demand, are properly reviewed for completeness and accuracy and must also be delivered in good time as the Bank is obligated to accede to all regulatory enquiries in addition to ensuring compliance with all AML/CFT regulations and laws.

Branch Operation Heads would also ensure that account opening documentation is properly stored and easily accessible on demand to minimize the risk of delayed responses to the authorities.

v. KYC Implementation

In alignment with the Bank's KYC Policy, proper identification by means of a valid identity card as well as evidence of residential/employment addresses are obtained from customers prior to commencement of the banking relationship.

GTBank ensures proper customer verification, record keeping, Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), customer sanctions screening, and appropriate classification of customers, as part of its strategies for entrenching a superior Customer Information culture in the Bank.

The Bank would request for customers' sources of funds in conformity with the regulatory requirements of proper identification, verification and documented validation for all account holders and their transactions.

vi. Sanctions Compliance Management

Safeguard against maintaining relationships with blacklisted persons or entities are assured by employing the use of aggregate blacklists of the United States of America Office of Foreign Assets Control (OFAC) and Her Majesty's Treasury of the United Kingdom. The Bank subscribes to the Sanctions list of the United

Nations, European Union, and other relevant international regulatory bodies it decides to comply with from time to time.

Updates on guidelines would be obtained by subscribing to the publications / information centers of these bodies. Strict compliance with sanctions of persons or entities blacklisted by these organizations would be ensured.

Regular updates are received from the Group Compliance for screening against the Bank's database for positive matches and for updating the Bank's internal watchlist.

Screening would be carried out from the account opening process through the life of the relationship with the customer. Screening would also be required before applicants are invited for job interviews, before a new contractor or supplier is signed on, and periodically through the life of such relationships.

Relevant processes that require interface with external parties (customers, contractors, suppliers and applicants) would carry out screening against the Bank's Sanctions Blacklist. The Bank's Sanction compliance programme is managed by the Compliance Unit.

Real Time Monitoring for RTGS and telegraphic transfers for both incoming and outgoing Swift Messages are scanned by the K-printer system for possible name match in the sanctions list, if any name is a match, an alert is generated and sent to Risk and Compliance for further investigation.

vii. Compliance Audit

The Internal Audit Group of the Bank would conduct comprehensive audits of the activities of Compliance unit periodically. A risk-based audit approach that would identify high, medium and low risk practices of Compliance would be employed.

The Bank's External Auditors would also be required to ensure the Bank adheres to the Banking Act, the attendant regulations and the prudential guidelines issued by the Central Bank of Kenya. Appendix "A" contains details of the Compliance Audit Policy.

viii. Ensuring adherence to regulatory guidelines with respect to new products and services

An objective review/appraisal of new products and services would be undertaken by the Compliance unit with a view to ensuring that the conditions for usage and modality of operations will neither circumvent nor

infringe AML/CFT regulatory guidelines.

Where any such infraction is observed, this would be promptly communicated to the unit in charge of the product for appropriate redress such as would ensure that the product dynamics conforms to relevant regulatory guidelines. Appendix "F" contains details of the AML/CFT policy for new products.

ix. AML/CFT Training

In alignment with the AML/CFT Training Policy of the Bank, a wide range of job-specific AML/CFT courses would be provided by the Human Resources Group of the Bank. This training covers all staff and members of the Board. All options for training including in-classroom and e-learning would be explored for this purpose. Training would also include AML/CFT training for new staff and Board members as part of their induction/orientation programme.

All staff shall be trained annually. Records would be maintained by the Human Resources Group for monitoring and tracking of training coverage. Appendix "C" contains details of the AML/CFT Training policy

x. Other AML/CFT Policies of the Groups and Units in the Bank

Funds Transfer, Cash and Monetary Instrument, Foreign Correspondents (Financial institutions) and Product policies would all be predicated on the need to combat AML/CFT activities as a result of the many AML/CFT risks associated with such transactions.

Handling of all FX instruments, requests and correspondences shall be carried out with utmost care and thoroughness while adhering to reasonably set criteria that do not conflict with the policies, processes and procedures requirements of regulatory bodies.
Criteria for opening and terminating relationships as well as review of unusual or suspicious transactions must be strictly adhered to in addition to ensuring that details of acceptable and unacceptable transactions are not compromised.

All products including but not limited to electronic cash, Automated Clearing house transactions, electronic banking, Funds transfers, third party/non-customer electronic payment, Trade financing must also be evaluated based on the possible risk exposure to the Bank that may arise as a result of these products.

Related policies have been included as Appendixes to this document.

3. TURNAROUND TIME AND ESCALATION

All transactions communicated to Compliance unit are expected to be addressed as per the Bank's internal Service Level Agreement (SLA). Transactions that are not resolved as per SLA would be escalated to the HoRC and relevant Head of Division at the earliest possible time for timely redress.

All transactions elicited by the alerts from K Printer or SAS AML software are also treated in like manner. Regulatory enquiries are responded to within a maximum of three (3) working days or on or before the due dates specified in the letters.

4. RISK BASED APPROACH

In line with the Wolfsburg AML Principles, GTBank is adopting a risk-based approach in the management of its compliance risks. To ensure proper assessment of related risks, risk rating templates would be maintained for evaluating the risk profiles of all customers and products managed by the Bank. All customers and products shall be evaluated periodically with the aim of determining the proportion of customers and products that fall into these three risk categories:

- High Risk
- Medium Risk
- Low Risk

Periodic risk assessments shall be carried out to ensure that the Bank's exposures to compliance risks are identified promptly. Appropriate mitigants for addressing risks identified in the medium and high categories would be recommended and responsibilities for implementation and timely close-out, and controls on high-risk customers like PEPs and correspondent banking relationship would also be defined.

This risk-based approach would ensure the application of appropriate due diligence in line with regulatory requirements throughout the life of all banking relationships.

Criteria for measuring the potential money laundering risks are carefully set by the creation of various scenarios on the SAS AML software which captures transactions set within the defined parameters for further investigation by the Compliance unit.

Existing customers would not be exempted from on-going risk assessments as

part of measures to ensure that due diligence and KYC principles are adhered to as strictly as possible.

The variables of the risk-based approach methodology may increase or decrease over time depending on the perceived risk that is posed by a particular customer or transaction. This may be in terms of a number of factors such as the transaction volume, transaction pattern or the duration of the relationship. Hence, the trend of customers'/products transaction dynamics based on observation of past and present activities, would enable appropriate classification of a transaction as suspicious or unusual.

5. REPORTING LINES

The Compliance function is the collective responsibility of all members of staff. All Branch Operations Heads would also act as Compliance Officers at respective branches and report all suspicious accounts and transactions to the Compliance unit.

The HoRC of the Bank shall report to the Board of Directors through the Board Risk Management Committee and administratively to the Managing Director. Periodic reports on current trends and risks identified shall be reported to Management and the Board.

- Monthly reports on Compliance activities shall be submitted to the COO/Managing Director;
- Compliance unit shall submit comprehensive Compliance Report to the Board Risk Management Committee from time to time;
- A summary of the Compliance Policy of the Bank should be included in the audited Financial Statements of the Bank to shareholders.

6. SUBSIDIARIES

All subsidiaries would be required to adopt this framework and customize to suit local regulatory requirements. Where Kenyan regulations are stricter, subsidiaries would be expected to adopt the Kenya principles.
The HoRC would ensure that all subsidiaries abide by relevant local regulatory guidelines.

7. APPENDICES

APPENDIX A: AML/CFT AUDIT POLICY

1. OVERVIEW

1.1 Definition

The Bank's AML/CFT Compliance Program consists of structures, policies and procedures established by the Bank to ensure compliance with current and emerging AML/CFT regulatory requirements.

Independent testing (audit) refers to the routine assessment of the AML/CFT Compliance Program to determine whether the Program is being adhered to and if it is in conformance with current AML/CFT regulations and global best practice.

1.2 Purpose

The Internal Audit Group shall carry out the independent testing of the AML/CFT Compliance Program with the following objectives:

- To evaluate the overall adequacy and effectiveness of the Bank's AML/CFT Compliance Program, in view of all AML/CFT regulations of the CBK, FRC and other regulatory bodies;
- To determine whether the AML/CFT Compliance Program is in conformance with global best practice;
- To assess the Bank's compliance with its AML/CFT Compliance Program and all applicable regulations;
- To identify areas of improvement in the overall quality of the Bank's AML/CFT Compliance Program, in order to remain in compliance with all relevant regulations;
- To collaborate with relevant units and persons to address areas of improvement identified from audit exercises, in order to remain in compliance with all relevant regulations;
- To generate and present reports on audit findings to Management and the Board of Directors.

1.3 Frequency

The independent testing shall be conducted on an annual basis. Some aspects of the AML/CFT Compliance Program may however be assessed more than once in the year under review based on the outcome of the risk assessment of each activity.

1.4 Scope of Audit

Every aspect of the Bank's AML/CFT Compliance Program shall be audited in order to evaluate the overall adequacy and effectiveness of the Program.

1.5 Approach

In conducting the assessment, the Internal Audit Group shall adopt a risk-based audit approach.

The frequency and depth of the exercise shall be determined after giving strong consideration to the risk assessment of the respective business units/branches and activities being audited within the year under review.

1.6 Stakeholders

In carrying out the assessment of the Bank's AML/CFT Compliance Program, the Internal Audit Group shall interface with the following key stakeholders, amongst others:

- Regulatory bodies
- The Bank's Management
- All relevant departments of the Bank

1.7 Reporting Line

The Internal Audit Officers responsible for carrying out the independent testing exercise shall report directly to the Bank's Head of the Internal Audit Group, who in turn renders reports to the Board of Directors through the Audit Committee.

2. REGULATORY REQUIREMENTS

The exercise shall be guided by the independent testing (audit) guidelines in the Compliance Manual.

The assessment will consider the Bank's compliance with all applicable regulations as stipulated in the AML/CFT Compliance Program and other relevant regulatory requirements.

3. DEPENDENT TESTING PROCEDURES

3.1 Access to Information

In carrying out its assignment, the Internal Audit Group shall have unfettered access to all records, systems, people and data in the Bank that is required for the audit.

3.2 Audit Procedures

The Audit procedures to be followed in carrying out the independent testing are elaborated in the AML/CFT Audit Programme.

4. REPORTING

4.1 Resolution of Non-Conformances and Escalation Procedure

Any violations, exceptions or other lapses noted during the audit shall be included in the audit report and presented to Management and the Board through its Audit Committee.
The audit report shall specify time-lines within which the violations, exceptions or lapses noted during the audit must be addressed. The Internal Audit Officers will be responsible for tracking the exceptions and documenting the corrective actions taken.

The Head of the Unit audited has the responsibility of notifying the Internal Audit team when the exceptions noted in the audit have been closed out. The Internal Audit Officers may request the Unit Head to provide documentary evidence to assure that the exceptions have been duly closed out.

In a case where certain identified lapses cannot be regularized by the Unit Head; the Unit Head must quickly notify the Internal Audit Officers of the challenges. The Auditors shall then investigate the matter further and refer it to appropriate quarters.

4.2 Circulation of Audit Reports

The report of the AML/CFT assessment shall be presented to the Bank's Board of Directors through the Audit Committee. The report shall also be circulated to the under listed persons:

- Managing Director/ Chief Operating Officer
- Chief Compliance Officer
- Head, Systems and Control Division
- Unit Head of Unit audited

APPENDIX B: E-BUSINESS & CARD SERVICES AML/CFT PRODUCT POLICY

1. OVERVIEW

1.1 Definition

This AML/CFT Product Policy refers to Card and E-Channel products which

have been created to support the migration of customers to alternative banking channels and also to enhance profitability.

1.2 Purpose

The purpose of this Policy is to highlight relevant AML/CFT dynamics as it relates to the E-Business and Card Services Group

1.3 Stakeholders

The stakeholders are existing and potential GTBank customers, GTBank Staff and Internal Business Groups

1.4 Approach

- Marketing and managing the portfolio of International and Domestic card products (MasterCard)
- Identify and develop new card products to suit the needs of different customer segments
- Create awareness for all card products among customers (internal & external)
- Drive/increase acquisition and usage of card products
- Monitor industry trends and competitor activity to ensure all AML/CFT guidelines are upheld in the course of our business activities

1.5 Scope of Policy

Developing, marketing and supporting world-class card solutions, tailored to enhance the banking transactions of our customers without increased exposure to AML/CFT infractions.

1.6 Monitoring Strategy

Close monitoring of industry trends and competitor activity, and local / international regulatory guidelines.

1.7 Regulatory Strategy

The Domiciliary accounts in respect of United States Dollars-denominated cards would be funded in line with relevant Anti-Money laundering regulation on foreign currency (as applicable)

1.8 Business Functions Affected

The withdrawal of funds via ATM through transaction set limits (Daily and transaction limits) would be closely monitored by setting the Bank's system to ensure that limits are not breached. Monitoring will also be done by the relevant Transaction processing and Internal Control teams in the Bank.

Deposits into card accounts (daily deposit of limits into account), as well as transactions done off shore would be closely monitored

1.9 Reporting Line

The Head of E-Business would report directly to the Managing Director and would also report all AML/CFT issues to the Chief Compliance Officer of the Bank

2. REGULATORY REQUIREMENTS

The Group shall abide by all local and international regulatory guidelines adopted by the Bank

3. APPLICATION OF POLICY

This policy shall apply to all cardholders of the following card products:

- World Mastercard Credit (Kenya Shilling)
- Platinum Mastercard Credit (Kenya Shilling)
- General Mastercard Debit (Kenya Shilling)
- Gold Debit Mastercard (Dollar and Kenya Shilling)
- General Prepaid Spend Mastercard (Kenya Shilling)
- Any other products that may be added from time to time.

APPENDIX C: AML/CFT COMPLIANCE TRAINING POLICY

1. OVERVIEW

1.1 Definition

The Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Compliance Training Policy specifies the framework through which GTBank would ensure that it complies with the relevant regulatory provisions relating to awareness among staff on anti-money laundering and combating the financing of terrorism

1.2 Purpose

To stipulate guidelines for implementing AML/CFT training

1.3 Approach

- In line with local and global regulatory requirements, adequate provision shall be made in the annual training plan in terms of budget and curriculum for all aspects of Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) training.
- The curriculum shall cover all known and emerging AML/CFT issues.
- Responsibility for developing and implementing these training programmes shall jointly fall on the Compliance Unit and on the Human Resources Group of the Bank.
- All new staff shall undergo the AML/CFT training as part of their induction/orientation.
- All new Directors shall be taken through the AML/CFT training as part of their induction/orientation. In addition, AML/CFT awareness fliers shall be included in their retreat packs from time to time.
- This provision shall cover all core staff without exception and non-core staff involved in operations, funds transfer and marketing.
- Every staff member shall, without excuse, take the AML/CFT course every year and pass the associated end-of-course test. The training sessions may be instructor-led or in the e-learning mode

1.3. Monitoring Strategy

- Job-Specific AML/CFT training curricula shall be designed for Central Operations, Transaction Services Division, Marketing Groups and Treasury.
- The Human Resources Group shall be responsible for compiling attendance records.

APPENDIX D: CORRESPONDENT BANKING POLICY

1. OVERVIEW

1.1 Definition

A correspondent banking relationship involves the provision of banking services by one financial institution (the correspondent bank) to another financial institution (Respondent Bank), where the financial institutions carry on activities or business at or through permanent establishments in different countries.

The banking services provided by the Correspondent Bank involves the provision of cash management services, international funds transfer, cheque clearing, foreign exchange services, loans and trade finance services.

1.2 Purpose

This Policy enunciates guidelines for identifying and managing Money Laundering/Financing of Terrorism risks in relation to Correspondent Banking, and for establishing and maintaining due diligence policies, procedures, systems and controls particularly when the Correspondent banks are located in jurisdictions presenting high risks of money laundering or terrorist financing.

1.3 Approach

The Correspondent Bank will typically have no direct relationship with the underlying parties to the transactions and therefore needs to take appropriate steps to verify the identity of the underlying parties to the transactions and determine the nature and purpose of those transactions. These steps shall include, but not be limited to having appropriate risk assessment and due diligence, as well as ongoing assessments of countries that carry the highest risk of money laundering or terrorists financing.

1.4 Stakeholders

The stakeholders shall include:

- The Bank's customers
- Respondent banks /Other Financial Institutions
- Regulatory agencies
- Treasury

1.5 Scope of Policy

The scope of this policy shall cover:

- Due diligence on the Correspondent Bank, to determine its ownership, nature of business, products and customer base
- Adequacy of the Correspondent Bank's AML/CFT controls and internal compliance practices

- Stipulations on documentation and recording, suspicious activity reporting and international resources for screening and monitoring of transactions and suspects
- Requirement for Board approval to commence correspondent banking relationships

1.6 Monitoring Strategy

The Bank shall employ an annual and on-going review of its correspondent banking relationships to access the nature and adequacy of the AML/CFT controls and practices. Review will include:

1. Risk Assessment & Due Diligence

When establishing and managing Correspondent Banking relationships, the Bank shall consider assessing the following matters in conducting due diligence:

A. Correspondent Banking Identity

- The ownership, control and management structures of the Correspondent Bank and any parent company, including whether a Politically Exposed Person has ownership or control of the Correspondent Banking or any parent company;
- The beneficial owners who have a controlling interest in the Correspondent Bank;
- Whether the Correspondent Bank is duly organized, registered, licensed and/or authorized.

B. Correspondent Banking Risk

- The nature of the Correspondent Bank's business, including its product and customer base;
- The country of residence of the Correspondent Bank;
- The country of residence of any parent company of the Correspondent Bank;
- Intended purpose of the Correspondent Account of transaction;
- The adequacy of the Correspondent Bank's AML/CFT controls and internal compliance practices;
- Whether the Correspondent Bank maintains correspondent accounts, the details of such accounts maintained and the adequacy of the Correspondent Bank's internal anti-money laundering controls;
- The Correspondent Bank's financial position;
- The reputation and history of the Correspondent Bank, including its business history and compliance history;
- The reputation and history of any parent company of the Correspondent Bank;
- Whether the Correspondent Bank has been the subject of an investigation or any criminal or civil proceedings relating to money laundering or terrorism financing;

- The senior management/Board of the Correspondent Bank and whether there have been any recent changes in ownership or senior management.

C. Jurisdiction Risk

- The primary regulatory body overseeing the Correspondent Bank and the existence and quality of any AML/CFT regulation in the Correspondent Bank's country of residence;
- The primary regulatory body overseeing the parent Company of the Correspondent Bank, the existence and quality of any AML/CFT regulation in the Correspondent Bank's parent company's country of residence, where the parent company has Group-wide control within which the Correspondent Bank's client operates;
- The overall AML/CFT strategies of the Correspondent Bank's country of residence;
- Whether the Correspondent Bank's home jurisdiction (including government, regulators and other relevant authorities) sufficiently apply the FATF recommendations;
- Whether the Correspondent Bank's home jurisdiction is known to be drug producing or drug transit country;
- Whether the Correspondent Bank's home jurisdiction has been classified as having inadequacies in their AML/CFT regulations;
- Whether the Correspondent Bank's home jurisdiction has any secrecy or data protection laws that would prevent access by the bank to relevant data;
- Whether the Correspondent Bank is involved with a Politically Exposed Person, or with the family members or close associates of a Politically Exposed Person.

D. Further Due Diligence Steps

In assessing the money laundering/terrorist financing risks posed by a Correspondent Bank, particularly one that is high risk or from a high risk jurisdiction, the Bank would take the following steps (where applicable):

- Obtain the Correspondent Bank's annual report and financial statements (audited if available);
- Review the applicable laws and regulations regarding the prevention of Money Laundering /Terrorist Financing in the Correspondent Bank's home jurisdiction;
- Meet with senior management of the Correspondent Bank (where applicable);
- Document the respective AML/CFT responsibilities of the Correspondent Bank;
- Review reports by bank rating agencies where available regarding the Correspondent Bank's client;
- Determine the expected level of activity of the Correspondent Bank through the Correspondent Account;
- Request general information on the respondent Bank's categories of

customers.

For privately owned Correspondent Banks, the Bank will ascertain the identity of each of the owners of the respondent Bank and perform an appropriate level of due diligence with regards to such owners. The Bank will review publicly available information to determine whether the Correspondent Bank has been subject to money laundering or other criminal investigation, criminal indictment or conviction, any civil enforcement action based on violations of anti-money laundering laws or regulations or any investigation, indictment, conviction or civil enforcement action relating to financing of terrorists; and

The Bank shall also undertake ongoing assessments of countries that carry the highest risk of money laundering or terrorists financing.

2. REGULATORY REQUIREMENTS
The Bank shall abide by all applicable local and international regulatory guidelines.

3. RISK BASED APPROACH
The Bank shall adopt a risk-based approach when assessing any business relationship or transaction with respect to its specific Money Laundering risk and the information and evidence that might be required or validated for this purpose.
GTBank shall take specific and adequate measures to address the higher risk of Money Laundering which might arise from correspondent banking relationships.
The Bank shall establish even more stringent due diligence measures in relation to Correspondent Banks that are high risk or are from high risk jurisdictions.

Before entering into a correspondent banking relationship with another bank, ensure that the bank does not permit their accounts to be used by shell banks.

APPLICATION OF POLICY
This Policy shall apply to all correspondent banking relationships.

APPENDIX E: FUNDS TRANSFER AML/CFT POLICY

1. OVERVIEW

1.1 Definition

Funds Transfer Unit is responsible for international funds transfer transaction processing and domiciliary account transactions. The Processing of foreign currency transfers and settlement and management of foreign currency cash and monetary instruments also falls under this unit.

1.2 Purpose

This document outlines strategies for timely and effective processing of customer transactions in line with established best practices and strict adherence to customer mandates, whilst also ensuring compliance with AML/CFT regulatory guidelines.

1.3 Stakeholders

- The Bank's customers
- The Bank's staff
- Correspondent banks
- Beneficiary banks
- Government regulatory agencies (local and international)

1.4 Approach

The Bank shall leverage on its correspondent banking relationships in ensuring a continual and efficient handling of customer transactions. A deliberate strategy shall be employed for addressing glitches encountered on processed customers' transactions with a view to restoring customer satisfaction and ensuring the retention of their patronage while complying with all relevant AML/CFT regulations.

The Bank shall also employ effective and innovative use of technology to enhance its transactional processing, monitoring and associated business activities whilst ensuring a continuous improvement in service delivery.

1.5 Scope of Policy

The Policy covers the Unit's functions and processes amongst which are:

- Foreign Currency Inward Transfer (FX Inflow)
- Foreign Currency Outward Transfer (FX Outflows)
- Foreign Currency Clearing / Collection: Foreign currency instruments that GTBank sends for clearing/collection on behalf of our customers include: cheques, and drafts.
- Foreign Currency Draft Issuance

- Foreign Currency Forwards and Swaps

1.6 Monitoring Strategy

- Continuous review and update of this policy manual as and when necessary.
- Update process strategies in line with developments in local and international business process requirements as and when necessary.

1.7 Regulatory Strategy

The Bank shall strictly adhere to the directives and provisions of the CBK Prudential Guidelines, Proceeds of Crime and Anti-Money Laundering Act, 2009, Prevention of Terrorism Act 2012 and Proceeds of Crime and Anti-Money Laundering Act, 2013 (subsidiary legislation); and Monetary guidelines and policies as well as the Standard Operating Procedure (SOP).

The Bank shall pursue an approach of continuous application of industry best practices on processes whilst ensuring adequate updates with changes in regulatory guidelines and procedures. This will be managed on both the local and international fronts.

1.8 Business Functions Affected

- Marketing Teams
- Technology Team
- Control Teams

1.9 Reporting Line

The Team Leader, Funds Transfer (which is part of the Settlement Group of the Bank) has oversight functions over the Unit. The Team Leader reports to the Head of Settlements and manages the daily activities of the desks and human resource of the unit. Team Leaders review and verify the transactional output of Processing Officers who initiate the processing of customer transactions, and report all AML/CFT related issues to the Compliance team.

2. REGULATORY REQUIREMENTS

The Bank's processes are subject to the provisions governing financial transactions locally and internationally. The unit shall ensure timely and adequate rendition of prescribed returns to relevant agencies of government as and when due, and shall also adhere strictly to regulatory directives.

2.1 Local Regulators

- Central Bank of Kenya
- Kenya Revenue Authority
- Financial Reporting Centre

2.2 International Regulators

APPENDIX F: NEW PRODUCTS AML/CFT POLICY

1. OVERVIEW

1.1 Definition

The term "Product" or "Products" may be used to refer to all or any of Products, Services and Initiatives. A Product can be a current account, savings account or loan account and any variant of these. A product can also be a transaction based electronic delivery channel; or other services that offer some form of custody or value to customers.

1.2 Purpose

This manual document the AML/CFT issues relating to product development, process improvement and business development policies and procedures to be employed for the development of new products in order to:

- Ensure uniformity, completeness and consistency in the performance of tasks related to product development, product/service enhancement and business development;
- Provide clarity and accountability for all job responsibilities in the unit;
- Prevent and minimize information gap on the Bank' product development/ enhancement and business development policies and procedures in the event of staff turnover; and
- Ensure that feasible and viable support and control processes are in place to support the new and amended products/services.

1.3 Stakeholders

This refer to all functions that are required to provide input with respect to the risks that new and amended products give rise to within their areas. These may include but are not limited to:

- Legal Group
- Compliance Unit
- E-Business and Card Operations Unit
- Human Resources Unit
- Treasury Group
- Financial Control
- Internal Control Group
- Risk Management Group
- Bank's Management Credit Committee (MCC)

1.4 Scope of Policy

The scope of the Policy shall cover AML/CFT risks associated with new products development, and the mechanisms by which these risks would be managed. The Bank shall ensure that a money laundering and terrorism financing risk assessment is conducted prior to the introduction of a new product, new business practice or new technology for both new and pre-existing products.

1.5 Approach

- Identify emerging financial needs of consumers in the society through surveys (field and desk), interviews and literature reviews as well as conduct market sizing for the industry/market in question;
- Analyze the competitive landscape for new products proposed through espionage and thorough product reviews;
- Develop product paper(s) (liability and Asset) containing product features based on the findings of research conducted earlier and obtain necessary approvals (Internal and External) for new products;
- Conduct periodic product and process reviews/analysis, thereby enhancing such products and processes, and ensuring compliance with AML/CFT regulations;
- Initiate periodic product knowledge trainings/test to intimate staff of new/enhanced products/processes and controls;
- Continuous review of products to prevent loopholes being exploited for money laundering activities.

1.6 Reporting Line

The Head of the Unit developing the new product would report all AML/CFT issues to the Chief Compliance Officer of the Bank.

2. REGULATORY REQUIREMENTS

The Unit developing the product and the Compliance Unit shall abide by all local and international regulatory guidelines adopted by the Bank.

3. RISK BASED APPROACH

The key risk associated with the AML/CFT New Products Development Policy is the Compliance Risk. The Bank shall ensure adherence to all relevant laws and regulations which may be applicable to its products.

The Head of the Unit developing the new product shall work with other stakeholders to identify all risks and obtain reasonable assurance that all risks and areas of concern are appropriately addressed.

4. APPLICATION OF THE POLICY

This policy is applicable to all new products, and underscores the Bank's readiness to have all its products comply with relevant regulations.

Product Development Process Outline

Idea generation – The basic idea is created and described (Entry level idea hunt, Feedbacks from sales force, customer service units etc.)

↓

Idea screening – The costs, profits and potential sales of the offering are calculated at different price level, how the offering fits in with its competitive strategy (Stakeholders' meeting to critique idea and make constructive recommendations)

↓

Feature specification and CBK Notification/ Approval – Detailed Specifications for the product are developed, features and pricing are established. When seeking to introduce a new products / business, the Bank shall prior to charging, levying or imposing any rate or charge on the new product, notify CBK in writing of the rate or charge to the new product.

↓

Development – The actual offering is designed (Unit developing new product, Technology, FINCON, Internal Control Unit, Treasury, Corporate Communication and Legal)

↓

Implementation – The offering is tested, to ensure that product features work as approved in the product paper (Unit developing new product, Technology, Internal Control, TSG)

↓

Launch/Commercialization – The offering is made available to Customers (Unit developing new product, Corporate Communication, Technology, and General Administration Unit)

↓

Evaluation- The offering is evaluated as to whether it is delivering the appropriate value to customers, as well as meeting the Bank's business goals (Unit developing new product, Research team)

APPENDIX G: CUSTOMER INFORMATION POLICY
(This policy shall be read in conjunction with the Bank's KYC Policy and Data Protection and Retention Policy)

1. OVERVIEW

1.1 Definition

The Customer Information Policy sets out the policies and guidelines to be employed by the Bank in determining the adequacy of customer information and fulfilling the requirements of Know Your Customer (KYC) and due diligence.

1.2 Purpose

The policies and controls documented herein are designed to mitigate potential risks impacting each process in the Standard Operating Procedure manual for TSG Unit of the Bank, especially as it relates to customer information and KYC. It is designed to be used in two principal ways:

- As a reference manual for persons already familiar with the TSG Unit of the Bank
- As a guide for interested persons with no prior exposure to the TSG Unit of the Bank

1.3 Scope of Policy

This Policy shall cover the Bank's AML/CFT procedures as it relates to the Customer Information functions.

1.4 Approach

The strategy for ensuring compliance with AML requirements shall include the following:

Customer Identification

The TSG Officer/RM shall obtain a minimum of the following identification information from the customer before opening the account:

- Name
- Date of birth for individuals
- Address
- Identification number such as Personal Identification Number (PIN), National Identity Card Number (NIN), birth certificate, International Passport Number, Certificate of Incorporation
- The detailed due diligence requirements are set out in the AML policy

Know Your Customer (KYC)

I. For Individual or Joint Account

The TSG Officer/RM shall undertake all "Know Your Customer" procedures specified in the CBK AML/CFT Regulation and other applicable laws, regulations or Bank policies.

II. For Corporate Account

The Legal Unit shall conduct a search to ascertain the authenticity of the information provided by the customer

Customer Verification

Specifically, the TSG Officer/RM shall ensure that:

i. Customer identification using documentary methods must provide evidence of customers nationality or residence and bear a photograph or similar safeguard (e.g., International Passport and National Identity card);

ii. For a person other than an individual (such as a corporation, partnership or trust), the institution shall obtain documents showing the legal existence of the entity. Such documents include certified Memorandum and Articles of Association of the incorporation, Certificate of Incorporation or an unexpired government- issued business license, a partnership agreement or trust instrument.

iii. For non-individual accounts, the officer shall obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity.

iv. For a current account, the identity and accuracy of the information supplied are verified by contacting customers' referees (current account holder within/outside GTBank) for confirmation.

v. Where a customer requires utilization of funds before an independent verification of identification document (i.e., search from Company registry or address verification) is concluded, the approval of the Head of Transaction Services or Chief Operating Officer shall be sought.

Record-keeping and Retention Requirements

- The identification information of a customer shall be retained for a period of 7 years after the account is closed
- The credit card information shall be retained for a period of 7 years after the account is closed or becomes dormant
- The bank shall also keep a description of the following for 7 years after the record was made:

i. any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance and the date of issuance and expiration date (if any)

ii. the method and the results of any measures undertaken to verify identity

iii. the results of any substantive discrepancy discovered when verifying the identity