بسم الله الرحمن الرحيم

Alnile Bank for Commerce & Development

بنك النيل

Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy

Documentation and Approval

Prepared by:

Compliance Manager

Signature: 

Reviewed by:

Compliance Committee

Head of the Compliance Committee

Signature: 

Approved by:

Board of Directors

Chairman of the Board of Directors

Signature: 

2026

بنك النيل

Table of Contents

بنك النيل

This document is referred to as the

Anti-Money Laundering and Counter-Financing of Terrorism

(AML/CFT) Policy of Alnile Bank for Commerce and Development

It reflects the bank's commitment to compliance with global best practices in combating illicit activities and implements the standards issued by local, regional and international regulatory authorities.

بنك النيل

1-Policy Objective

This policy aims to prevent the misuse of Alnile Bank for Commerce and Development in financial crimes by ensuring:

1. Compliance with all applicable legal and regulatory requirements.
2. Taking appropriate measures to reduce risks related to financial crimes.
3. Establishing a framework for Anti-Money Laundering, Counter - Terrorist Financing (AML/CTF) and financial sanctions.

The Bank's objective is not limited to legal compliance only, but also includes mitigating potential risks arising from customers using products, services and delivery channels for laundering proceeds of illegal activities and financing terrorist activities or engaging in activities related to prohibited financial sanctions which may expose the Bank to sanctions and reputational risks.

2-Requirements

* The bank shall adhere to all requirements set forth under applicable local laws.

* The bank shall comply with all directives issued by regulatory authorities concerning the prevention of the financial system's misuse for money laundering, terrorist financing, and financial sanctions.

*The bank shall comply with all relevant regional laws and regulations.

* The bank shall follow applicable regulations of international organizations and multinational bodies relating to financial sanctions & the prevention of the financial system's misuse for money laundering or terrorist financing.

* The bank may exceed the requirements stipulated in such laws and regulations to ensure that its services and products are not exploited for financial crimes.

Compliance with the above requirements is mandatory , and the Board of Directors must be informed of any material breach .

بنك النيل

3-Definitions

Anti-Money Laundering and Counter-Terrorist Financing

The terms " Anti-Money Laundering " and " Counter-Terrorism Financing" are generally used to refer to predicate financial crimes.

Money Laundering

Money laundering is defined as the conversion or transfer of property knowing that it is derived from criminal activities, in accordance with each country's legislative framework and according to the recommendations issued by the Financial Action Task Force (FATF) for the purpose of concealing or disguising the illicit origin of the property, assisting a person involved in committing the predicate offence, evading legal consequences and concealing the true nature, source, location, disposition, movement, ownership, or rights related to such property.

Terrorist Financing

Terrorist financing is defined as the act of a person, group, institution, or any other entity directly or indirectly and intentionally providing or collecting funds or other assets with the Intention that they be used wholly or partially to facilitate terrorist acts, support terrorists and support terrorist organizations or entities.

Financial Sanctions

Financial sanctions are measures imposed by governments, regulatory bodies, or multinational organizations to influence the behavior and decisions of governmental or non-governmental entities that may:

* Threaten international security .

* Violate international standards such as human rights.

According to regulatory directives, Alnile Bank must comply with:

- Local sanctions lists .
- United Nations Security Council sanctions (UN) .
- U.S.Treasury Office of Foreign Assets Control (OFAC) sanctions lists.
- Any future regulatory directives.

4-Risk

The Bank operates in several sectors and provides integrated banking services to different customer segments. Therefore, the Bank must establish an effective AML/CFT system including:

a - Risk Assessment : establishing a comprehensive framework for the assessment and management of financial crime risks.

b - Risk Classification: in accordance with the Bank's financial crime risk assessment framework.

c - Risk-Based Approach (RBA) : Appropriate risk assessment methodology .

d - Customer Profiling .

e - Risk Tolerance .

a - Risk Assessment

In order for the institution to effectively understand, identify and evaluate potential financial crime risks, it is necessary to establish a structured framework for identifying relevant risk factors, which include :

* Customer risks .

*Product, service and delivery channel risks .

*Geographic risks .

Accordingly, the suitable control mechanism for monitoring each risk shall be developed and applied through the following:

- Employing regulatory controls to mitigate risks.
- Prior to launching new products, the firm must verify its ability to mitigate potential AML/CFT risks .
- Conducting ongoing risk assessments of banking products and services post-launch.
- Conducting periodic risk reassessments for all categories.

b - Risk Classification

Risks are categorized according to three levels:

* Low Risk .

*Medium Risk .

* High Risk .

Based on the accurate classification of risks arising from the various categories, appropriate due diligence measures shall be applied in accordance with the level of risk, as follows:"

* Simplified Due Diligence (SDD) shall be applied to low-risk categories.
* Standard Due Diligence (CDD) shall be applied to low and medium-risk categories.
* Enhanced Due Diligence (EDD) shall be applied to high-risk categories, and to medium-risk categories where deemed necessary.

c - Risk-Based Approach(RBA)

The Risk-Based Approach is a methodology that entails understanding, identifying and assessing the risks associated with money laundering and terrorist financing . It involves determining the level of exposure arising from clients, transactions, products, services, delivery channels and geographical locations . Based on this assessment , proportionate measures and controls are established to effectively mitigate risks commensurate with their potential level.

The Risk-Based Approach reflects the potential likelihood that a client may use any banking services or products for financial crime purposes. For this reason, Alnile Bank has adopted the Risk-Based Approach, given its flexibility and emphasis on areas demanding the highest effectiveness in mitigating internal and external risks related to natural persons and legal entities.

* The Bank undertakes a number of initiatives to enhance its ability to ensure compliance with the aforementioned requirements.
* The Bank continuously makes the necessary adjustments to achieve maximum effectiveness in line with updates related to the Risk-Based Approach.

d) Customer Profile

Our policy mandates the completion of comprehensive identification files for all natural and legal persons, including the verification of beneficial ownership structures. We maintain rigorous transaction monitoring protocols.

Utilizing a defined Risk-Based framework, we classify relationships as low, medium, or high risk to determine the appropriate level of due diligence, or to prohibit the relationship entirely. We reserve the right to terminate any business relationship predicated on financial crime concerns.

This policy explicitly prohibits dealings with sanctioned products or geographic regions, whether conducted directly or through commercial partners.

e - Risk Tolerance

Risk tolerance refers to the level and type of risk that the Bank is willing to accept or tolerate in pursuit of its business objectives. This includes risks arising from customers, transactions, products and services, delivery channels, and the geographic locations in which the Bank operates or to which it is exposed.

Onboarding and Ongoing Relationship Management

The bank prohibits:

* Numbered accounts.
* Anonymous or fictitious name accounts.
* Correspondent banking with shell or paper banks.
* Relationships with sanctioned persons or jurisdictions.

Additionally, the bank may suspend services or products where a suspicion exists that a customer intends to use them for an unlawful purpose.

Third Party:

The Bank shall not engage third parties or outsource any functions unless it has conducted appropriate due diligence to ensure that the third party has the capability, competence, and effective internal controls to implement adequate Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) measures.

Such engagement shall be subject to prior approval by the Board of Directors or its duly authorized committee. The Bank shall remain fully responsible for ensuring that outsourced activities comply with all applicable regulatory requirements and internal policies.

5.Suspicious Cases:

* Transaction Monitoring

Transaction monitoring aims to assess the extent to which a client's activities including their use of products and services, as well as their overall behavior align with the declared nature and purpose of the business relationship.

As part of this process, the bank conducts additional inquiries into activities deemed "unusual" and evaluates their consistency with the information provided by the client at the outset of the relationship.

A thorough understanding of suspicious transaction patterns and the nature of clients' businesses enables staff to detect any potentially suspicious elements in client transactions.

This assessment is further strengthened by reviewing key banking transaction statements and comparing them with the client's transactional history.

In-depth knowledge of the client, along with access to relevant information and details regarding their business, activity volume, income sources, transaction records and any other available data, is the only means to either substantiate or dispel any suspicions.

Reporting to Relevant Authorities

A mechanism must be established to enable branch & departments staff to submit "Unusual Activity Reports" to the Compliance Manager. The Compliance team is then responsible for evaluating whether the activities described in the report are indeed suspicious and warrant the filing of a Suspicious Activity Report (SAR) to the Financial Information Unit (FIU), or retainted .

If an employee has any doubts that are not based on clear evidence, they may discuss the matter with the compliance team .

It is possible that a client may occasionally conduct unusual but legitimate transactions.

6. Data Protection & Confidentiality

The Bank shall comply with all applicable data protection and privacy laws and regulations by:

* Ensuring adherence to legal and regulatory requirements governing the protection, confidentiality, and proper handling of data.

* Maintaining strict confidentiality of all customer information and transaction data, and implementing appropriate safeguards to prevent unauthorized access, disclosure, or misuse.

* In the Context of Reporting Suspicious Activities to the Financial Information Unit (FIU):

- The Bank shall enforce strict confidentiality obligations and impose disciplinary measures on any employee who breaches confidentiality or discloses, directly or indirectly, any information related to a suspicious activity report or investigation to the subject of the report or any unauthorized party ("tipping-off").

- The Bank shall ensure that employees who report suspicious activities in good faith are fully protected from any form of retaliation, liability, or adverse consequences, in accordance with applicable laws and internal policies.

7. Cooperation with Judicial and Law Enforcement Authorities

The Bank shall:

* Provide full cooperation with the Financial Information Unit (FIU) in investigations related to money laundering and terrorist financing.
* Cooperate fully with the competent authorities in investigations concerning money laundering and terrorist financing.
* Submit all required information and documents to the relevant authorities in a timely manner .

8. Record Keeping

* All records and documents shall be properly maintained and archived to ensure their accessibility throughout the duration of the customer relationship with the Bank, and for a minimum period of five (5) years following the termination of the business relationship for bank customers.
* For occasional or walk-in vcustomers, records shall be retained for at least five (5) years from the date of completion of the transaction.

* Notwithstanding the above, in cases involving ongoing legal proceedings or litigation, all relevant records and documents shall be retained until the final resolution of the case, even if this exceeds the five-year retention period.

9. Training and Awareness:

The Bank shall provide ongoing training programs for all employees on Anti-financial Crime (including AML and CTF) through the following measures:

* Implement targeted awareness programs at the level of the Board of Directors, senior management, and key leadership positions.

* Ensure continuous employee awareness of the importance of compliance with applicable laws, regulations, and internal policies.

* Provide appropriate training and awareness materials to employees across all organizational levels.

* Deliver annual, role-based training programs to ensure that all employees are adequately equipped to identify and respond to financial crime risks relevant to their functions.

* Support employees in obtaining relevant professional certifications and provide specialized training for staff occupying critical or sensitive positions.

10 - Auditing

* This policy shall be reviewed and updated regularly to reflect changes in applicable laws, regulations, and emerging risks.

* The effectiveness of this policy shall be periodically assessed to ensure its adequacy and proper implementation.

* This policy, as well as any subsequent amendments, shall be subject to approval by the Board of Directors.

* Any material breaches or significant deviations from this policy shall be promptly reported to the Board of Directors.

Implementation

This Anti-Money Laundering and Counter-Terrorist Financing Policy was approved by the Board of Directors on February 17, 2025. All employees of Alnile Bank for Commerce and Development are required to comply with and adhere to the provisions set forth therein, effective as of the above date.

بنك النيل
NAILE BANK

2026