Anti-Money Laundering and Combating Financing of Terrorism policies and procedures

2026

Concise Version

Table of Contents

1. INTRODUCTION

This document sets out the **National Islamic Bank (NIB)** ("the Bank's") policies and procedures for combating money laundering and financing of terrorism. It covers the policies required to conduct the Bank's business in compliance with guidelines provided by the regulators (Know Your Customer (KYC), customer due diligence, internal and external Suspicious Transaction Reporting (STR), staff training and record keeping).

The Bank's Board of Directors has approved the AML/CFT policies and procedures, a compliance department shall review the mentioned policies and procedures periodically to ensure that it is in line with the changes in the Bank's product, operational procedures, and/or any other changes introduced by the Central Bank of Syria or Combating Money Laundering & Terrorism Financing Commission and other regulatory authorities that may have an impact on the processes described in this document.

The Bank takes the appropriate steps to identify and assess the money laundering and terrorist financing risks (for customers, countries/geographic areas, products, services, transactions and delivery channels). And these assessments must be documented in order to be able to demonstrate the basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the relevant regulatory authorities. The nature and extent of any assessment of money laundering and terrorist financing risks must be appropriate to the nature and size of the business.

2. LAWS AND DEFINITIONS

– The laws and legislations related to combating money laundering and financing of terrorism:
  - Legislative Decree No. 33 dated 05/01/2005 on combating money laundering and financing of terrorism and its amendments.
  - System of supervision of banking and financial transactions, Resolution No. (19) of the Combating Money Laundering and Financing of Terrorism Commission of 2019, and its amendments.
  - Law No. 28 of 2001 on the establishment of private banks in Syria, as amended by Law No. 3 of 2010.
  - Legislative Decree No. 35 of 2005 on the establishment of Islamic banks
  - Basic Monetary Order (Law No. 23 of 2002), as amended by Legislative Decree No. 21 of 2011.
  - Legislative Decree No. 30 of 2010 on the banking secrecy.
  - Resolution of the Credit and Monetary Council No. 534 of 16/07/2009 containing the establishment of the "Compliance Department".
  - Resolution of the Credit and Monetary Council No. 57 of 01/07/2019 containing the compliance department work system in the banks.

  In addition to the recommendations issued by the Global Financial Action Task Force (FATF) to Combat Money Laundering and Terrorist Financing (Known as the '40+9 recommendations') &Wolfs berg Group standards and principles.

– **Money-laundering:**

Money Laundering is the process by which the direct or indirect benefit of crime is channeled through financial institutions to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the money can lose its criminal identity and appear legitimate. Generally, the process of money laundering comprises three stages, during which there may be numerous transactions that could alert a bank to the money laundering activity:

- **Placement:** the physical placement of illegally derived funds into the financial system, usually through a financial institution.
- **Layering:** the separation of the benefits of criminal activity from their source by creating layers of financial transactions designed to disguise the audit trail and provide anonymity.
- **Integration:** the placement of funds back into the economy to give the appearance of a legitimate source.

Any act having any of the following aims shall be deemed a money-laundering offence:

- The concealment or masking of the true nature, source, place, method of disposal, movement, ownership of illegal funds or the related rights in the knowledge that they are illegal funds;

- The transfer or substitution of funds in the knowledge that they are illegal funds, for the purpose of concealing or masking the source or helping a person involved in the commission of an offence to evade responsibility;
- The acquisition, possession, management, investment or use of illegal funds to purchase movable or immovable properties or to carry out financial transactions in the knowledge that they are illegal funds.

– **Terrorist Financing:**

Any act aimed at providing or collecting funds by any means, whether directly or indirectly, from lawful or unlawful sources, for the purpose of their being used, totally or partially in a terrorist act, or to finance a terrorist organization or person.

– **The Commission for Combating Money Laundering and Financing of Terrorism:**

It is an independent commission (established within the Central Bank of Syria) with judicial status and a legal personality. It is responsible for all matters related to money laundering and terrorist financing and may instigate legal actions. The competent courts shall have the authority to examine the merits of the case.

– **Compliance Department:**

It is an independent Department subordinated directly to the Bank's Board of Directors and responsible for the compliance with the applicable laws and regulations

– **Money Laundering Reporting Officer (MLRO)**

The MLRO is responsible for overseeing all AML/CFT activity within the Bank and must be approved by the Central Bank of Syria and Combating Money Laundering & Terrorism Financing Commission.

The Bank will appoint an MLRO and a Deputy MLRO, who will act in the absence of the MLRO, The MLRO will have unrestricted access to all transaction information relating to financial services provided by the Bank to customers.

The MLRO is responsible for:

- Establishing and maintaining the AML/CFT policies and procedures.
- Ensuring that the Bank complies with the applicable AML/CFT laws and related decisions and circulars.
- Ensuring the day-to-day compliance with the Bank's own internal AML/CFT policies and procedures.
- Acting as the Bank's main point of contact in respect of handling internal suspicious transaction reports from the Bank's staff and as the main contact for the Central Bank of Syria and Combating Money Laundering & Terrorism Financing Commission and other concerned bodies regarding AML/CFT.
- Making external suspicious transactions reports to the Combating Money Laundering & Terrorism Financing Commission.

- Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters.
- Producing reports (periodically) on the effectiveness of the Bank's AML/CFT controls for consideration by Board of directors and senior management.
- On-going monitoring of customers' accounts and transactions.
- Maintaining all necessary records for the required periods.
- Making the required external reports to the Central Bank of Syria and Combating Money Laundering & Terrorism Financing Commission.

– **The customer:**

- Permanent customers: customers who have a relationship with the bank which is expected to be long lasting.
- Transient customers: customers who do not have any relationship with the bank that is expected to be long lasting.

– **The holder of the economic right:**

The natural person who has the original will or real interest in the relationship existing between the bank and the Customer. This includes the natural persons to whom the ownership of the legal entity reverts and who exercise the actual control over the said entity.

3. DUE DILIGENCE TOWARDS CUSTOMERS

– It is the policy of the Bank to maintain effective and systematic internal guidelines for establishing and verifying the identity of its customers, the "Know Your Customer" policy is considered a fundamental pillar of our activity in order to protect the bank from the risks of entering into banking transactions with undesirable customers. The implementation of this policy will help managing the risks, in particular those related to transactions and the bank's reputation, and others.

– It is the Bank's policy to;

- Collect certain minimum customer identification information from each customer.
- Verify the identity of each customer.
- Record customer identification information and the verification methods and results.
- Understand and obtain information on the purpose and intended nature of the business relationship.
- Conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the bank's knowledge of the Customer, their business and risk profile, including, where necessary, the source of funds.

- World-Check to ensure that customers do not appear on the black lists.
- Respond to requests for information from the Bank's regulators and counterparties in a complete and timely manner, in accordance with local regulations.

I. CUSTOMERS ACCEPTANCE POLICY

- The Bank shall not accept to deal with any permanent or transient customer, by opening an account, granting any banking facilities or offering any banking services, without identifying the customer, and determining the holder of the economic right.
- The customer identification shall be through the official identity documents, (Identification card for Syrian residing in Syria, passport for foreigners and the residency permit duly issued by the Immigration Service for residents, passport and examination of the exit and entry visas for non-residents,…..).
- If the customer is a legal entity, a recent Commercial Registration shall be requested, including the identity of the legal entity, its legal form, the authorized signatories and the official identity cards of the partners and the management in control of the legal entity, in addition to the act of incorporation or by-laws.
- The Bank shall keep a copy of the identity document, signed by the Bank employee, stating that it is a true copy of original.
- The Bank does not accept to deal with customer whose involvement in illegal matters is evidenced.
- The bank screens all its potential and existing customers before on-boarding and on an on-going basis from a sanctions perspective and is committed to ensuring that there is no dealing with any individual/entity that appears on local and international sanctions lists (such as OFAC, EU, UN, etc[1]).
- The Bank classifies the customers according to the relationship banking risks associated with them, such as doubts about the validity of the provided information, customer's concealment of identity-related information, investigating the customer's activity is required by the commission, customers subject to political risks, customers whose income derives from high-risk activities (such as weapons, leisure and entertainment activities, etc.), customers holder of the nationality of a high-risk country, the customer's reputation and history. All the mentioned cases constitute high-risk customer accounts.
- If the customer or the holder of the economic right is a person with a high relationship banking risk, the approval of the general management on the banking relationship with him should be obtained, all reasonable measures for determining the source of funds must be taken in addition to the continuous monitoring of this relationship.
- The Bank must verify the information provided by the Customer In case it is unable to check the said information, it shall not accept to deal with the Customer.

[1] The bank uses a monitoring system integrated with Dow Jones for this purpose.

– The acceptance policy applicable to customers who are natural persons shall also be applied to their proxies and representatives.

II. CUSTOMERS' IDENTIFICATION AND VERIFICATION

The Bank must verify the customers' identity and the validity of the information provided at the beginning of the banking relationship, i.e. when opening a debit or credit account or drafting bank guarantees or contracts that fall within the Bank's activity, by adopting the following procedures:

– **Natural person**

- Keeping a true copy of the customer's identity card, bearing the signature of the Bank's employee.
- The Customer's signature on the acknowledgment of the holder of the economic right of the account, and a declaration identifying the economic right holder of the transactions executed on behalf of third parties if he executes transactions on behalf of a third party.
- Applying due diligence procedures to know the Customer, by collecting reliable data included in the account opening agreement.
- Collecting information from neutral credible sources, which may help verifying the accuracy of the information provided by the Customer.
- The purpose and the nature of the working relationship.
- Banking queries through neutral credible sources by telephone or field visits to verify the validity of the information provided by the Customer.
- Monitoring the transactions executed by the Customer and their consistency with the information provided.

– **Legal entity (profit or nonprofit organizations)**

- Keeping a true copy of the originals of the legal documents to determine the identity of the legal entity, its legal form and the date of registration (exp: a recent commercial register).
- Collecting all of the identification data included in the legal entity identification form.
- Collecting data about the partners as required by the bank KYC.
- Collecting data regarding the Customer's representatives authorized to carry out transactions on the account, and verifying their personal identities.
- Monitoring the executed transactions and checking their consistency with the submitted data and with the purpose and nature of the business relationship.

– **Incapacitated person**

Documents relating to the persons who are duly authorized to represent the incapacitated persons in the management and movement of the accounts must be obtained, and all of the procedures of investigation of their identities must be taken as stated in the preceding paragraphs.

- **The identification and verification by correspondence**

  If the account was opened by correspondence, the validity of the signatures must be authenticated, and the Bank must identify and verify the identity of the dealing party through the correspondent bank, after verifying the correspondent bank's compliance with the anti-money laundering and terrorist financing procedures and the Customer identification and investigation procedures.

- **Transient Customers**

  The Bank must identify and verify the identity of Transient Customers as well as the identity of Permanent Customers, The Bank must execute the identification and investigation procedures, and check if there is any doubt that the transient transaction is related to money laundering or financing of terrorism transaction.

III. COMPLETION OF THE VERIFICATION PROCEDURES

Completion of the verification procedures may be postponed as the following**:**

- The postponement of the verification procedures can be necessary in order not to interrupt the natural conduct of the economic activity if it does not involve money laundering or terrorism financing risks.
- The verification procedures should be completed as early as possible.
- For any transactions exceeding a defined amount, the identification and investigation procedures must be completed.
- If it is impossible to execute all of the Customer identification and investigation procedures, the Bank must put an end to the relationship with the Customer.
- In the event of discrepancies between the information provided by the Customer and the banking queries about the latter, the Commission must be notified if this discrepancy raises any doubt about the concealment of suspicious transactions.

IV. CUSTOMER RE-IDENTIFICATION AND VERIFICATION POLICY

The Bank must regularly proceed with a new identification and investigation of the Customer and determination of the identity of the holder of the economic right as follows:

- Updating Customer's data on the basis of Customer's classification in terms of risk (every year for high-risk accounts, every 3 years for medium-risk accounts, every 4 years for low-risk accounts).
- Upon the discovery of an inconsistency between the data submitted by the Customer and the transactions executed by the latter, the Bank must not wait until the date the updating is required, but rather immediately update the data, to check whether natural changes in

the Customer's data or the data of the holder of the economic right have occurred, or if the transactions involve money laundering or terrorism financing.

- Making sure that all the relevant accounts meet all the required forms and documents.

4. BANKING TRANSACTIONS MONITORING PROCEDURES

Following Financial Action Task Force (FATF) recommendations, the Bank takes a risk-based approach to transaction monitoring compliance and performs assessments on all its customers, and then deploys a compliance response proportionate to the risk they present.

Transactions involving higher risk customers may be subject to more stringent transaction monitoring measures while lower risk customers may require simpler measures, a transaction monitoring is supported by the following measures and controls:

- **Customer due diligence (CDD):** In order to gauge transactions against risk profiles, the Bank establish and verify customers' identities by conducting appropriate due diligence. The customer due diligence (CDD) process requires the Bank to collect identifying information including names, addresses, dates of birth, company incorporation details,........
- **Sanctions screening:** the Bank screens customers on an ongoing basis against relevant sanctions and watch lists to ensure no dealing with sanctioned persons or entities.
- **PEP screening:** Politically exposed persons (PEPs), including elected and government officials, the Bank screens customers on an ongoing basis to establish their PEP status.
- **Adverse media monitoring:** the Bank monitors adverse media stories from screen, print, and online sources, to ensure its risk profiles remain as accurate as possible.

  The bank uses a monitoring system integrated with Dow Jones for this purpose.

<u>**Cash Payments**</u>

- The Bank will carefully scrutinize all available data regarding the cash payments before the execution, in order to insure that it's nature and amount are compatible with both the economic activities of the concerned customers and the activity of their accounts. If the depositor / drawer is not the account holder, the bank obtains the name of the depositor / drawer and verify his relationship with the account holder.

  Accordingly, the bank will refrain from executing the transaction in case of incomplete or illogical information.
- The Bank must request the customer to provide information about the source of funds and their destination in case of a cash transaction or in the event of several cash transactions connected with each other whose value exceeds a certain amount,
- If the holder of the economic right of the transaction is not the account holder, a declaration form identifying the holder of the economic right of the transactions executed on behalf of third parties, must be filled-in.

- transactions must be monitored and tested with the money laundering and terrorism financing indicators.
- Should the Bank be unable to obtain promptly any missing Originator Information, then details of the transactions shall be summarized and forwarded immediately to the MLRO for further action as a possible suspicious transaction, which may be reported to the Combating Money Laundering & Terrorism Financing Commission.
- The AML/CFT unit (within the compliance department) monitors all cash transactions using specific reports to ensure that the mentioned required information is provided, and that its nature and amount are compatible with both the economic activities of the concerned customers and the activity of their accounts.

Transfers

- The Bank will carefully scrutinize all available data regarding the incoming/outcoming transfers before the execution, in order to insure that:
  - It is completely sufficient and contain the following information:
    - The name of the payer/beneficiary.
    - The address of payer/beneficiary.
    - The account number or unique customer identification number of the payer/beneficiary.
    - The purpose of the transfer.
  - The transfer's nature and amount are compatible with both the economic activities of the concerned customers and the activity of their accounts.

    Accordingly, the bank will refrain from executing the transfer in case of incomplete or illogical information.
- Should the Bank be unable to obtain promptly any missing Originator Information, then details of the transfer shall be summarized and forwarded immediately to the MLRO for further action as a possible suspicious transaction, which may be reported to the Combating Money Laundering & Terrorism Financing Commission.
- The AML/CFT Unit (within the compliance department) monitors all transfers using specific reports to ensure that the mentioned required information is provided, and that its nature and amount are compatible with both the economic activities of the concerned customers and the activity of their accounts.
- Moreover, AML/CFT Unit makes sure that the Bank does not deal with any entity or person included on international black lists, through a special program directly linked to the "SWIFT" system.

5. FOREIGN CORRESPONDENT BANKING RELATIONSHIP POLICY

The Bank must ensure that normal customer due diligence measures are carried out on respondent banks and that the Bank has sufficient information about the respondent to fully understand its business. The following information must be collected before entering into any correspondent banking relationship:

- Information on the respondent’s ownership structure and management.
- Major business activities of the respondent and its location as well as the location of its parent (where applicable) and reputation in terms of combating money laundering and terrorism financing.
- Money laundering and financing of terrorism prevention and detection controls.
- Purpose of the account.
- The extent to which the respondent performs ongoing due diligence on customers and the condition of regulation and supervision in the respondent’s country.
- Confirmation that the respondent bank is able to provide relevant customer identification data on request to the correspondent bank.
- Investigations into whether the respondent bank has been subject to a money laundering or terrorist financing investigation.

Further, the bank must ensure that, prior to opening a correspondent banking relationship:

- The establishment of the correspondent banking relationship has the approval of the Bank’s board of directors.
- A correspondent relationship has not been entered into or maintained with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell bank).
- Making sure that the respondent bank does not provide correspondence services to any shell bank.

6. REPORTING SUSPICIONS

- It is the duty of every member of management and staff to report any suspicious transactions to the Money Laundering Reporting Officer (MLRO).
- All internal Suspicious Transaction Reports must reach the MLRO and must not be blocked.
- The MLRO will investigate the report and will decide on the basis of all available information and additional enquiries whether or not the transaction or instruction remains suspicious or whether there is some additional information that removes the suspicion.
- If the MLRO considers the suspicion to be justified, he will prepare a report for the Commission for Combating Money Laundering and Financing of Terrorism.
- The name of the individual member of staff who made the report will not be revealed.
- Once a report has been made to the MLRO, all officers and employees of the Bank are prohibited from communicating directly or indirectly, in any manner or by any means to any person, the fact that the suspicious transaction report was made ('tipping off').

7. Anti-Bribery & Corruption

- The Bank is committed to conducting business in an honest, ethical, and transparent manner. The Bank has a zero-tolerance policy toward bribery and corruption and is dedicated to acting professionally, fairly, and with integrity in all its business dealings and relationships.
- Employees must report any suspicion or evidence of bribery or corruption to the Compliance manager - MLRO or via the Whistleblower Hotline.
- All reports will be treated confidentially and without retaliation.
- Compliance department and Internal Audit department conduct an Internal investigation of the suspected violation.
- Violations may result in disciplinary action, including termination.
- Legal reporting obligations to regulators and law enforcement will be followed.

8. Fraud

- The Bank is committed to the highest standards of honesty, integrity, ethical conduct and is dedicated to preventing, detecting, and responding to fraudulent activity.

- Fraud includes theft of funds or assets, forgery or alteration of documents, misrepresentation of facts, unauthorized use of bank resources, and any act intended to deceive for financial gain.
- All suspected fraud must be reported immediately to the Compliance Manager - MLRO or through the Bank's Whistleblower Hotline. Reports will be handled confidentially and without retaliation.
- Compliance department and Internal Audit department conduct an Internal investigation of the suspected violation, confirmed fraud may result in disciplinary action, including termination and legal proceedings.
- The Bank maintain internal controls, conduct fraud risk assessments, and ensure segregation of duties to reduce the risk of fraud.

9. Data protection

The bank process personal data with all due care so that only necessary and accurate personal data are processed by authorized employees, in a legitimate, secure and transparent manner, and for specific and limited purposes. To this end, the Bank is committed to the following principles regarding the processing of personal data:

1. Lawful and Fair Processing
Personal data will be collected and processed only for legitimate business purposes with clear consent or legal basis.

2. Data Minimization
Only data necessary for specific purposes will be collected and retained.

3. Accuracy
The bank ensures that personal data is accurate and kept up to date.

4. Storage Limitation
Personal data will not be stored longer than necessary for its intended purpose or legal requirements.

5. Integrity and Confidentiality
The bank implements appropriate technical and organizational measures to protect data from unauthorized access, loss, or damage.

6. Access and Rights
Data subjects have the right to access, correct, or request deletion of their data, subject to legal obligations.

7. Third-Party Sharing
Personal data will only be shared with trusted third parties under strict data protection agreements.

All employees and contractors must adhere to this policy. Violations may result in disciplinary action, including termination or legal action

The Bank is committed to collecting and processing customer data for Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) purposes in accordance with applicable data protection laws and regulations.
All personal information obtained through Know Your Customer (KYC) and transaction monitoring procedures is handled with strict confidentiality and used solely for lawful and legitimate purposes.

10. WHISTLEBLOWER PROTECTION

The Bank is committed to fostering a safe and transparent environment where employees and stakeholders can report concerns related to AML, CTF, fraud, bribery and corruption without fear of retaliation. This policy ensures that all whistleblowers are protected from any form of adverse treatment or discrimination as a result of their good-faith reporting. Confidentiality will be strictly maintained throughout the investigation process to encourage openness and integrity.

11.AUDITING AND INDEPENDENT TESTING

- The Bank is subject to periodical audit review by the Regulators, the Bank's Internal Audit and on yearly basis by the external auditors in order to verify that the Bank is complying with applicable laws and regulations in terms of combating money laundering and terrorism financing as well as related internal policies and procedures.
- In addition, the Bank's Compliance department performs a periodic self-assessment in order to test the overall effectiveness of the Bank's AML/CFT policies and procedures to identify, assess and mitigate any related risks, in addition to ensure that all branches and departments are applying the Bank's AML/CFT Policies and procedures properly.

12. EDUCATION AND TRAINING

The Bank will provide appropriate training to all employees. Such training will focus on:

- The identification and prevention of money laundering and terrorist financing.
- Follow-up procedures for unusual or suspicious activities.
- Material changes in the applicable customer due diligence laws and regulations.
- Their responsibilities under the AML/CFT laws and regulations.
- The identity and responsibility of the MLRO.
- The current AML/CFT policies and procedures.
- Money laundering and terrorist financing typologies and trend.

- The type of customer activity or transaction that may justify an internal suspicious transaction report.
- The potential effect on the Bank, its employees and customers, of any breach of the AML/CFT Law or the AML/CFT Regulations.
- The procedures for making an internal suspicious transaction report.
- Customer due diligence measures with respect to establishing new business relationships with customers.

13. RECORD KEEPING

The Bank will keep adequate records and identification documents for the following specific periods:

Type of document	Hard copy	Electronic copy	Comments
• In relation to evidence of identity and business relationship records**.**	**5 years**	**10 years**	from the end of the Bank's relationship with the customer.
• Documents of customers' transactions.	**5 years**	**10 years**	from the date when the transaction was completed.
• Reports made to, or by, the MLRO and records of consideration of those reports and any action taken as a consequence.	**10 years**	**10 years**	from the date of report, or the date of action taken.
• Compliance reports by the auditors (AML/CFT external & internal auditing results).	**10 years**	**10 years**	from the date of auditing report.
• Dates when AML/CFT training was provided, the nature of the training and the names of the staff who received the training.	**5 years**	**5 years**	from the date of training.

All records must be available for prompt access by the relevant authorities, when required.

Compliance Manager: MHD Waseem Nadar