Chabahar International Bank (Offshore)

AML-CFT Policy

An Excerpt

Introduction

Chabahar International Bank (Offshore) is committed to preventing and detecting money laundering and the financing of terrorism in accordance with applicable national legislation, international standards, and regulatory directives. The Bank adopts a risk-based approach to customer identification, transaction monitoring, and internal controls to safeguard the integrity of the financial system and ensure compliance with AML/CFT obligations.

1. Regulatory Framework and Compliance Obligations

The Bank's AML/CFT measures are implemented pursuant to:

- The Anti-Money Laundering and Counter-Terrorist Financing Laws of the Islamic Republic of Iran;
- Regulations and guidelines issued by the Central Bank of Iran and the High Council for Combating and Preventing Money Laundering and Terrorist Financing;
- FATF recommendations, Basel Committee principles, and Wolfsberg Group standards;
- Operational coordination with the Financial Intelligence Unit (FIU).

All applicable regulations relating to KYC, suspicious transaction reporting, correspondent banking, sanctions screening, and risk-based monitoring are observed.

2. AML/CFT Organizational Measures

The Bank's AML/CFT Unit is responsible for:

1. Initial and full identification of customers based on valid documents;
2. Prohibiting services to anonymous, shell, or sanctioned persons;
3. Continuous monitoring of financial activities;
4. Risk-based customer classification;
5. Oversight of correspondent banking relationships;
6. Supervisory procedures for internal AML/CFT controls;
7. Obtaining customer declarations and legal attestations where required;
8. Reporting suspicious transactions to the FIU;
9. Staff training on AML/CFT requirements;
10. Performing any other duties assigned by regulation.

3. Customer Acceptance Policy

The Bank establishes business relationships only after complete and verified identification of the customer. Where full identification is not possible, or where legal or regulatory restrictions apply, the relationship is declined. Customers are classified according to their assessed risk profile, which determines the frequency of identity document updates and level of due diligence applied.

4. KYC & Customer Identification

The Bank conducts customer identification under two levels:

- **Initial Identification** for non-basic services (obtaining and verifying identity information of natural persons and legal entities and their authorized representatives).
- **Full Identification / CDD** for basic services (verification of occupation/business activity, beneficial ownership, expected transaction profile, sanctions screening, and background checks).

KYC obligations apply to both domestic and foreign customers, including politically exposed persons (PEPs).

5. Customer Risk Assessment

Risk classification is based on three dimensions:

- **Demographic risk** (nationality, occupation, PEP status, financial background, alignment of declared activity with expected levels of transactions);
- **Geographic risk** (jurisdictional exposure and location of business relationship);
- **Service risk** (type of product, delivery channel, and volume of transactions).

This risk-based classification drives the level of due diligence and monitoring applied.

6. Initial Customer Identification Process

At onboarding, the following documents and forms are collected and reviewed by the Bank teller and subsequently approved by the AML/CFT Department:

- Customer Information Form
- Document Submission Checklist
- Verification Checklist

Where deficiencies exist, the branch must remedy them before proceeding.

7. Customer Due Diligence (CDD) Process

Customers are categorized as **low-**, **medium-**, or **high-risk**, and CDD is applied accordingly. High-risk customers require full due diligence for any service. For basic services and international transfers, a three-level approval workflow is required:

1. Bank user/supervisor verification
2. Compliance specialist review
3. Compliance manager approval

The Bank verifies:

- Applicant and beneficiary identities,
- Purpose and nature of transaction,
- Goods type (especially for dual-use restrictions),
- Connections with sanctioned or prohibited entities,
- Correspondent banks against domestic and international blacklists.

8. Politically Exposed Persons (PEPs)

In accordance with applicable regulatory directives, enhanced due diligence is required for foreign PEPs before account opening or granting of basic services.

- High-risk foreign PEPs may not receive basic banking services.
- Services to ordinary foreign PEPs are permitted, but must be immediately reported to the Central Bank.
- Opening non-profit or foreign currency time deposit accounts for foreign PEPs requires full due diligence.

Ongoing monitoring is mandatory for PEPs identified as high-risk.

9. Suspicious Transaction Reporting (STR)

The Bank identifies and reports suspicious activity through:

1. Continuous monitoring of customer transactions;
2. Confidential internal escalation by staff to the AML/CFT Unit;
3. Use of Central Bank-approved AML detection systems;
4. Timely response to FIU and regulatory inquiries;
5. Filing STRs with the FIU in accordance with prescribed standards.

The obligation to report applies regardless of transaction value or completion.

10. Correspondent Banking Controls

Before establishing correspondent banking relationships, the Bank performs a risk assessment of the foreign institution, including:

- Ownership and management structure;
- Financial statements and regulatory standing;
- Jurisdictional AML/CFT requirements;
- Policies for high-risk customers and PEPs;
- Exposure to sanctions and high-risk geographies;
- Confirmation of no relationship with shell banks.

Correspondent banking relationships are continuously monitored.

11. Monitoring and Internal Controls

AML/CFT oversight is carried out through:

- Real-time and periodic monitoring of customer activity;
- A risk-based approach in all AML/CFT controls;
- Ongoing supervision of international transfers and cross-border payments;
- Review by the internal audit department and compliance function.

12. Record Keeping

Documents related to customer identification, due diligence, and transactions are retained for **at least 10 years**, in line with Article 7 of the AML Law and Article 13 of the Counter-Terrorist Financing Law. Records must remain accessible to supervisory authorities.

13. Training and Awareness

All staff are required to complete:

- Initial AML/CFT induction training,
- Annual refresher programs,
- Specialized training for high-risk functions.

Training records are maintained by the Compliance Officer and are subject to audit.

14. Scope, Approval, and Updates

This policy applies to all employees of Chabahar International Bank (Offshore). New employees must confirm their review and adherence in writing. The policy is reviewed annually, or more frequently if regulatory changes occur, and must be approved by the Board of Directors following endorsement by the High Compliance Committee.