

# Know Your Customer (KYC) and Anti-Money Laundering (AML) Policy

Policy Reference: BAP-KYC-002 | Version: 3.0 | Effective Date: January 1, 2026

## 1. Introduction and Purpose

This KYC and AML Policy establishes the bank's framework for identifying customers, verifying their identities, and monitoring transactions to prevent money laundering and terrorist financing. The policy applies to all customer relationships and transactions processed by the bank.

## 2. Customer Due Diligence (CDD)

### 2.1 Standard Due Diligence Requirements

All customers must provide the following documentation:

Customer Type	Required Documents	Verification Level
Individual - UAE National	Emirates ID, Passport	Standard
Individual - Expatriate	Passport, Visa, Emirates ID	Standard
Corporate - UAE Registered	Trade License, MOA, Board Resolution	Enhanced
Corporate - Foreign Entity	Certificate of Incorporation, Apostille documents	Enhanced Plus
Government Entity	Official Letter, Authorized Signatory List	Standard
High Net Worth Individual	All standard docs + Source of Wealth	Enhanced

### 2.2 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is required for high-risk customers including:

- Politically Exposed Persons (PEPs) and their family members
- Customers from high-risk jurisdictions identified by FATF
- Non-face-to-face customers and correspondent banking relationships
- Customers with complex ownership structures
- Customers in high-risk business categories (cash-intensive businesses)

- Customers with negative news or adverse media findings

## 2.3 Customer Risk Rating

Risk Category	Risk Score	Review Frequency	EDD Required
Low Risk	1-30	Every 3 years	No
Medium Risk	31-60	Every 2 years	No
High Risk	61-80	Every year	Yes
Very High Risk	81-100	Every 6 months	Yes - Intensive

## 3. Transaction Monitoring

### 3.1 Automated Monitoring System

The bank employs an automated transaction monitoring system that screens all transactions against predefined rules and thresholds:

- Cash transactions exceeding AED 40,000 (approximately USD 10,900) must be reported
- Wire transfers exceeding AED 100,000 require additional documentation
- Unusual transaction patterns trigger automatic alerts for review
- Cross-border transactions to high-risk jurisdictions require enhanced scrutiny
- Structured transactions (smurfing) detection algorithms are applied

### 3.2 Suspicious Transaction Reporting

All suspicious transactions must be reported to the Financial Intelligence Unit (FIU) within 24 hours of detection. Suspicious activity indicators include:

- Transactions inconsistent with customer's known business profile
- Unusual cash deposits followed by immediate wire transfers
- Multiple accounts receiving funds then transferring to single account
- Customer reluctance to provide required documentation
- Transactions just below reporting thresholds (structuring)

## 4. Sanctions Screening

All customers and transactions must be screened against the following sanctions lists:

- UAE Local Terrorist List - updated daily
- UN Security Council Consolidated List
- OFAC (Office of Foreign Assets Control) SDN List
- European Union Consolidated Sanctions List
- Bank's internal watchlist and negative news database

## 5. Training and Awareness

All bank employees are required to complete mandatory AML/KYC training:

- Annual mandatory AML awareness training (minimum 4 hours)
- Role-specific training for front-line staff (minimum 8 hours annually)
- Specialized training for compliance officers (minimum 16 hours annually)

Approved by: Compliance Committee | Next Review Date: January 1, 2027

NOTE: This is a SAMPLE document created for educational purposes only.