Better research, better policy, better reform

CESD | CENTER FOR ECONOMIC & SOCIAL DEVELOPMENT

Global Think-Tank

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

The Policy was approved by the CESD LLC Board Members on December 12, 2025

Center for Economic and Social Development (CESD)
Dadash Bunyadzada str.13, apt. 56, Yasamal,
Baku, Azerbaijan
Phone: (99412) 5943665
Fax: (99412) 5943665
Email: info@cesd.az
URL: www.cesd.az

Baku, 2025

1. PURPOSE

The purpose of this Policy is to establish the framework, principles, and internal controls adopted by CESD LLC to prevent, identify, detect, and report money laundering and terrorist financing activities.

The Institution is committed to complying with applicable laws, regulations, regulatory requirements, and internationally recognized AML/CFT standards.

2. SCOPE

This Policy applies to:

- Board members and Senior Management.
- All employees and business units.
- Branches and subsidiaries, where applicable.
- Customers and business relationships.
- Financial transactions and services.
- Agents, intermediaries, and relevant third parties.

3. REGULATORY FRAMEWORK

The Institution shall comply with applicable national AML/CFT legislation and regulatory requirements, including relevant requirements concerning:

- Prevention of money laundering.
- Countering terrorist financing.
- Targeted financial sanctions.
- Suspicious transaction reporting.
- Customer due diligence.
- Beneficial ownership transparency.
- Recordkeeping and retention.

The Institution shall also consider applicable FATF Recommendations and relevant international standards.

4. GOVERNANCE AND RESPONSIBILITIES

4.1 Board of Directors

The Board shall approve the AML/CFT framework, oversee its implementation, and ensure adequate resources are allocated to compliance activities.

4.2 Senior Management

Senior Management shall ensure that AML/CFT controls are implemented effectively and that identified deficiencies are addressed.

4.3 Compliance Officer / MLRO

The Compliance Officer or MLRO shall:

- Oversee AML/CFT compliance.
- Monitor implementation of internal policies.
- Review and investigate suspicious activities.
- Submit reports to competent authorities where required.
- Monitor regulatory developments.
- Coordinate AML/CFT training.
- Report significant compliance matters to Senior Management.

4.4 Employees

Employees must comply with AML/CFT requirements, identify suspicious activities, and promptly escalate concerns to the Compliance Department.

5. RISK-BASED APPROACH

The Institution shall apply a risk-based approach to identify, assess, understand, and mitigate money laundering and terrorist financing risks.

Risk assessments shall consider:

- Customer risk.
- Geographic and country risk.
- Product and service risk.
- Transaction risk.
- Delivery channel risk.
- Ownership and control structures.
- Industry and business activity risks.

Customers and business relationships shall be classified according to their risk levels.

6. CUSTOMER DUE DILIGENCE AND KYC

The Institution shall implement appropriate customer identification and verification measures in accordance with its separate KYC Policy and applicable legal requirements.

Customer due diligence shall include:

- Customer identification and verification.
- Understanding the purpose and intended nature of the business relationship.
- Identification of beneficial owners.
- Assessment of customer risk.
- Ongoing monitoring of business relationships.

7. ENHANCED DUE DILIGENCE

Enhanced Due Diligence shall be applied to customers and transactions presenting higher risks.

Such customers may include:

- Politically Exposed Persons (PEPs).
- Customers from high-risk jurisdictions.
- Customers with complex ownership structures.
- Customers involved in high-risk business activities.
- Customers with unusual or suspicious transaction patterns.

Additional measures may include establishing source of funds and source of wealth, obtaining additional documentation, increased monitoring, and senior management approval where required.

8. SANCTIONS COMPLIANCE

The Institution shall maintain appropriate screening procedures to identify individuals, entities, and transactions subject to applicable sanctions.

Potential matches shall be reviewed and investigated promptly.

Confirmed matches shall be handled in accordance with applicable legal requirements, including asset-freezing and transaction-prohibition obligations.

9. TRANSACTION MONITORING

The Institution shall maintain appropriate transaction monitoring controls to identify unusual, complex, or potentially suspicious activities.

Monitoring shall include:

- Transactions inconsistent with customer profiles.
- Unusual payment patterns.
- Transactions involving high-risk jurisdictions.
- Unexplained transfers.
- Potential structuring and layering.
- Transactions potentially related to terrorist financing.

Identified unusual activities shall be escalated to the Compliance Officer or MLRO.

10. SUSPICIOUS TRANSACTION REPORTING

All employees must promptly report suspicious activities internally.

The Compliance Officer or MLRO shall assess the circumstances and determine whether a report must be submitted to the competent authority.

The Institution shall comply with applicable reporting deadlines and confidentiality requirements and shall prohibit tipping-off where required by law.

11. PROHIBITED BUSINESS RELATIONSHIPS

The Institution shall not knowingly establish or maintain business relationships or conduct transactions prohibited by applicable laws and regulations.

This includes prohibited relationships involving sanctioned persons, shell banks where prohibited, anonymous accounts, and other prohibited activities.

The Institution shall assess shell companies and complex ownership arrangements to understand their legitimate business purpose and beneficial ownership.

12. RECORDKEEPING AND RETENTION

The Institution shall maintain appropriate AML/CFT records, including:

- Customer due diligence documentation.
- Transaction records.
- Beneficial ownership information.
- Sanctions screening results.
- Suspicious activity investigations.
- Internal compliance reports.
- Relevant correspondence and approvals.

Records shall be retained for the periods prescribed by applicable laws and regulations.

13. AML/CFT TRAINING

The Institution shall provide regular AML/CFT training to employees, appropriate to their roles and responsibilities.

Training shall cover money laundering risks, terrorist financing, customer due diligence, sanctions, suspicious transaction identification, and reporting obligations.

14. INTERNAL CONTROLS AND AUDIT

The Institution shall maintain appropriate internal controls to assess the effectiveness of its AML/CFT framework.

Independent reviews and internal audits shall be conducted periodically, and identified deficiencies shall be addressed within appropriate timeframes.

15. POLICY REVIEW

This Policy shall be reviewed at least annually or whenever significant regulatory, operational, or risk-related changes occur.

16. APPROVAL

This Policy shall become effective upon approval by the Board of Directors or other authorized governing body.