ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND COUNTER-PROLIFERATION FINANCING POLICY

Wallera FZE

Trading as: Wallera

Registered Address: Business Centre, Sharjah Publishing City Free Zone, Sharjah, United Arab Emirates

Effective Date: 1 January 2026

1. REGULATORY FRAMEWORK

This Policy has been developed in accordance with the following regulatory instruments and international standards:

- Federal Decree-Law No. (10) of 2025 Regarding Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing;
- Cabinet Decision No. (134) of 2025 concerning the Executive Regulations of Federal Decree-Law No. (10) of 2025;
- Central Bank of the UAE regulatory circulars and guidance;
- Financial Action Task Force (FATF) Recommendations;
- Sharjah Publishing City Free Zone regulatory requirements and applicable UAE free zone legislation.

Wallera FZE commits to periodic review and updates of this Policy to maintain alignment with evolving regulatory requirements.

2. PURPOSE AND SCOPE

The primary objectives of this Policy are to establish a comprehensive framework for preventing the misuse of Company services for money laundering (ML), terrorist financing (TF), or proliferation financing (PF) activities, ensure full compliance with applicable laws and regulatory guidelines, and create clear procedures for detection, reporting, and management of suspicious activities.

This Policy applies to all employees, contractors, and agents of the Company who are involved in establishing business relationships, executing transactions, or monitoring customer activities.

3. UNDERSTANDING MONEY LAUNDERING

Money laundering refers to the process by which illegally obtained funds are transformed to appear legitimate. This criminal activity involves processing illicit proceeds through various financial channels to obscure their criminal origins.

3.1 Phases of Money Laundering

Placement Phase: The initial introduction of illicit funds into the legitimate financial system. Common methods include structured deposits (smurfing), informal value transfer systems, electronic payment mechanisms, conversion to tangible assets, physical transportation of currency, and securities transactions.

Layering Phase: The separation of illicit funds from their source through multiple complex transactions. Techniques involve offshore financial institutions, corporate vehicles without genuine business activities, trust arrangements, automated transfer accounts, and professional intermediaries.

Integration Phase: The reintroduction of laundered funds into the economy as apparently legitimate assets. Methods include trade-based manipulation, cash-intensive business operations, real property transactions, fictitious consulting arrangements, and sophisticated corporate financing structures.

4. TERRORIST FINANCING AND PROLIFERATION FINANCING

Terrorist financing encompasses any form of financial support provided to terrorist organizations or individuals who plan, facilitate, or execute terrorist activities. Unlike traditional money laundering, terrorist financing may involve both legitimate and illegitimate fund sources.

Proliferation financing refers to the provision of funds or financial services used for the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery, in contravention of applicable laws and international obligations. The Company maintains heightened vigilance against all three forms of financial crime: money laundering, terrorist financing, and proliferation financing.

5. RISK-BASED APPROACH

The Company employs a risk-based methodology to determine appropriate due diligence measures based on the assessed risk level of customers, products, services, and geographical factors.

5.1 Customer Risk Indicators

- Presence on international sanctions lists (UN, EU, OFAC, or equivalent);
- Political exposure status and associated relationships;
- Use of intermediaries or representatives for transactions;
- Third-party beneficial ownership arrangements;
- Complex or opaque ownership structures;
- Inconsistencies between stated business activity and transaction patterns;
- Cash-intensive business operations;
- Presence of nominee arrangements.

5.2 Geographical Risk Factors

The Company maintains a list of high-risk jurisdictions based on factors including inadequate AML/CFT/CPF regulatory frameworks, elevated corruption indices, presence of organized criminal networks, involvement in weapons proliferation, and application of international sanctions.

5.3 Prohibited Jurisdictions

The Company does not establish business relationships with individuals or entities from the following jurisdictions:

- Afghanistan, American Samoa, Aruba, Bahamas, Bangladesh, Botswana, Burkina Faso, Burundi;
- Cambodia, Central African Republic, Congo, Congo Democratic Republic, Cuba;
- Dominican Republic, El Salvador, Equatorial Guinea, Eritrea, Ethiopia;
- Fiji, Ghana, Guam, Guinea, Guinea-Bissau, Guyana, Haiti;
- Iran, Iraq, Jamaica;
- Laos, Lebanon, Libya;

- Mali, Moldova, Morocco, Mozambique, Myanmar;
- Nicaragua, Niger, Nigeria, North Korea;
- Oman;
- Pakistan, Palestine, Panama;
- Russian Federation (Crimea region only);
- Samoa, Sierra Leone, Somalia, South Sudan, Sri Lanka, Sudan, Syria;
- Trinidad and Tobago, Tunisia, Turkmenistan;
- Uganda, US Virgin Islands, United States of America;
- Venezuela;
- Yemen;
- Zambia, Zimbabwe.

This list is subject to periodic review and updates based on changes in international sanctions regimes, FATF assessments, and regulatory guidance.

5.4 Prohibited Business Activities

The Company declines to provide services to businesses engaged in the following activities:

- Charitable organizations, non-profit entities, or NGOs engaged in collecting donations;
- Dating services (particularly newly incorporated or unestablished entities);
- Drug paraphernalia, illicit substances, steroids, or controlled substances;
- Activities that encourage, promote, facilitate, or instruct illegal conduct;
- Extractive industries;
- High-risk file hosting, sharing services, or cyberlockers;
- Infringement of registered copyrights, trademarks, or intellectual property rights;
- Unregulated pharmaceuticals or unlicensed drug-related activities;
- High-yield investment programs or schemes promising unrealistic returns;
- Oil and gas industries;
- PC support services sold via outbound telemarketing;
- Pyramid schemes, Ponzi schemes, or multi-level marketing with recruitment focus;
- Trade in dangerous, hazardous, or restricted goods;
- Manufacture or sale of replica or counterfeit products;
- Sale or production of government identification documents;
- Services associated with prostitution or escort services;
- Trade in stolen goods, including digital and virtual items;
- Unlicensed lottery, gambling, or betting operations;
- Unregulated cryptocurrency exchanges or virtual asset service providers;
- Unregulated foreign exchange (Forex) trading platforms;
- Weapons, firearms, ammunition, or explosives trade;
- Any activity that violates applicable laws, statutes, or regulations.

6. CUSTOMER DUE DILIGENCE PROCEDURES

Due diligence is mandatory when establishing new business relationships, conducting occasional transactions at or above AED 55,000 (single or linked), processing wire transfers at or above AED 3,500, detecting indicators of potential ML/TF/PF, questioning the accuracy of previously collected information, and during periodic reviews.

6.1 Standard Due Diligence Requirements

For Individuals:

- Full legal name as per official identification;
- Date and place of birth;
- Current nationality;
- Residential and business addresses;
- Contact information;
- Government-issued identification document;
- PEP status declaration;
- Tax residency information.

For Legal Entities:

- Complete legal name and any trading names;
- Registered office and principal business addresses;
- Jurisdiction of incorporation;
- Valid trade license or registration certificate;
- Identification of directors, authorized signatories, and key personnel;
- Ultimate beneficial ownership information;
- Constitutional documents.

6.2 Enhanced Due Diligence Circumstances

Enhanced verification procedures apply when: business relationships exhibit unusual characteristics, transactions lack apparent economic rationale, customers operate holding structures for personal assets, ownership structures are complex or non-transparent, bearer share arrangements exist, or when dealing with cash-intensive enterprises.

Additional requirements for enhanced due diligence include:

- Photographic verification (selfie with identification);
- Video verification interview;
- Proof of residential address;
- Recent bank statements;
- Documented source of funds and wealth;
- Expected transaction volume and patterns.

6.3 Politically Exposed Persons

Individuals holding prominent public positions, their immediate family members, and known close associates require enhanced scrutiny due to elevated corruption risks. PEP categories include heads of state and government, senior government officials, parliamentarians and legislators, senior judiciary members, central bank officials, ambassadors and military officers, and executives of state-owned enterprises. Enhanced measures include senior management approval, source of wealth verification, custom transaction limits, and intensified monitoring.

7. TRANSACTION MONITORING

The Company implements systematic monitoring procedures combining real-time screening and retrospective analysis to identify suspicious patterns.

7.1 Monitoring Indicators

- Transactions involving sanctioned parties or PEPs;
- Payments to or from high-risk jurisdictions;
- Third-party payment arrangements;
- Large round-sum transactions;
- Unusual increase in account activity;
- Multi-currency transactions without business justification;
- Transaction patterns inconsistent with customer profile.

8. COMPLIANCE OFFICER

The Board appoints a designated Compliance Officer responsible for: collecting and analyzing information regarding unusual or suspicious transactions, filing Suspicious Transaction Reports (STRs) with the Financial Intelligence Unit, providing periodic compliance reports to the Board, implementing training programs, and maintaining appropriate control mechanisms. The Compliance Officer ensures the Company's compliance with all AML/CTF/CPF requirements.

Reports may be filed through the goAML system at https://services.cbuae.gov.ae/

9. RECORD RETENTION

The Company maintains the following records:

- Customer screening documentation (sanctions, PEP, and proliferation checks);
- Identity verification evidence for five years following relationship termination;
- Transaction records for five years from execution date;
- AML/CTF/CPF training records;
- Suspicious activity report documentation;
- Compliance Officer decision records.

Wallera FZE

Effective: 1 January 2026