TACTOFX ANTI-MONEY LAUNDERING (AML) POLICY

---

1. INTRODUCTION

1.1 Purpose of This Anti-Money Laundering Policy

This Anti-Money Laundering Policy outlines the framework, procedures, controls, standards, and compliance measures implemented by TactoFX to prevent, detect, identify, monitor, investigate, and report activities associated with:

money laundering;
terrorist financing;
fraud;
financial crime;
sanctions violations;
corruption;
identity theft;
and other illicit financial activities.

TactoFX is committed to maintaining a secure, transparent, and compliant trading environment while protecting the integrity of its operations, Clients, financial systems, and business ecosystem.

This Policy establishes the procedures used by TactoFX to:

verify client identities;
conduct Know Your Customer ("KYC") procedures;
assess financial crime risks;
monitor transactions;
identify suspicious activities;
comply with applicable AML obligations;
and support lawful financial operations.

1.2 Commitment to Financial Crime Prevention

TactoFX maintains a zero-tolerance approach toward:

money laundering;
fraud;
terrorist financing;
sanctions evasion;
forged documentation;
identity manipulation;
and unlawful financial activities.

The Company seeks to implement commercially reasonable controls, technologies, monitoring systems, compliance procedures, and operational safeguards designed to reduce exposure to financial crime risks.

---

2. DEFINITIONS

2.1 Money Laundering

Money laundering refers to activities intended to conceal, disguise, transfer, convert, or legitimize funds obtained through unlawful or criminal activities.

Money laundering commonly involves:

a) Placement

Introducing illicit funds into the financial system.

b) Layering

Conducting transactions intended to obscure the origin of funds.

c) Integration

Reintroducing criminal proceeds into the legitimate economy.

2.2 Terrorist Financing

Terrorist financing refers to the provision, collection, movement, or use of funds intended to support terrorist organizations, unlawful groups, or prohibited activities.

2.3 Politically Exposed Person (PEP)

A Politically Exposed Person (“PEP”) refers to an individual entrusted with a prominent public position, including:

- government officials;
- senior politicians;
- judicial officials;
- military officers;
- state-owned enterprise executives;
- and their close associates or family members.

PEPs may present elevated financial crime risks requiring enhanced due diligence.

2.4 Suspicious Activity

Suspicious activity refers to transactions or behaviours that appear unusual, inconsistent, deceptive, fraudulent, or potentially connected to financial crime.

---

3. SCOPE OF THIS POLICY

3.1 Persons Covered

This Policy applies to:

- Clients;
- prospective Clients;
- employees;
- affiliates;
- partners;
- introducing brokers;
- contractors;
- vendors;
- and any person or entity interacting with TactoFX services.

3.2 Services Covered

This Policy applies to all services provided by TactoFX including:

- trading accounts;
- deposits and withdrawals;

forex trading;
CFD trading;
cryptocurrency-related services;
payment processing;
partner programs;
and operational systems.

---

4. KNOW YOUR CUSTOMER (KYC) PROCEDURES

4.1 Identity Verification Requirements

Before activating certain services or permitting trading activities, TactoFX may require Clients to complete identity verification procedures.

Clients may be required to provide:

government-issued identification;
passport;
national identity card;
driver’s license;
proof of address;
banking documentation;
source-of-funds information;
selfies or biometric verification;
and additional supporting records.

4.2 Proof of Address Verification

Clients may be required to provide documents confirming residential address including:

utility bills;
bank statements;
government correspondence;
tax documentation;
or official residential confirmations.

Documents may be subject to validity periods and formatting requirements.

4.3 Enhanced Verification Procedures

Additional verification measures may apply in cases involving:

- high-risk jurisdictions;
- unusually large transactions;
- suspicious activities;
- politically exposed persons;
- sanctions concerns;
- or elevated compliance risks.

Enhanced due diligence may include:

- source-of-wealth verification;
- additional identity checks;
- financial background reviews;
- and ongoing monitoring.

---

5. CUSTOMER DUE DILIGENCE (CDD)

5.1 Risk-Based Approach

TactoFX applies a risk-based approach to compliance monitoring.

Clients may be categorized according to risk factors including:

- geographic location;
- transaction behaviour;
- account activity;
- payment methods;
- trading patterns;
- occupation;
- and business relationships.

5.2 Ongoing Monitoring

The Company may continuously monitor:

- transaction activity;
- trading patterns;
- withdrawal behaviour;
- deposit activity;

device usage;
IP addresses;
account access;
and operational activity.

Monitoring systems may identify unusual or suspicious behaviour requiring review.

5.3 Source of Funds Verification

Clients may be required to demonstrate the legitimate source of deposited funds.

Acceptable evidence may include:

salary records;
bank statements;
investment records;
business income documentation;
tax filings;
or asset sale records.

---

6. SANCTIONS COMPLIANCE

6.1 Sanctions Screening

TactoFX may screen Clients, transactions, and counterparties against:

sanctions lists;
watchlists;
regulatory databases;
politically exposed person databases;
and international compliance records.

6.2 Restricted Jurisdictions

The Company may restrict or prohibit services in jurisdictions considered:

high-risk;
sanctioned;
politically unstable;

non-compliant with international AML standards;
or subject to legal restrictions.

6.3 Prohibited Persons

TactoFX may refuse services to individuals or entities associated with:

sanctions programs;
criminal organizations;
terrorist groups;
fraud schemes;
financial crime;
or unlawful activities.

---

7. TRANSACTION MONITORING

7.1 Monitoring Systems

TactoFX may use manual and automated systems designed to identify:

suspicious transaction patterns;
unusual trading behaviour;
abnormal deposits;
rapid withdrawals;
account manipulation;
payment irregularities;
and potentially fraudulent conduct.

7.2 Indicators of Suspicious Activity

Indicators may include:

inconsistent transaction behaviour;
use of multiple accounts;
rapid movement of funds;
unusual trading activity;
mismatched identity information;
forged documents;
unexplained wealth;

or attempts to evade compliance procedures.

7.3 Cryptocurrency Monitoring

Cryptocurrency-related transactions may be subject to enhanced review due to elevated risks involving:

- anonymity;
- blockchain obfuscation;
- mixer services;
- wallet irregularities;
- and cross-border transaction complexity.

---

8. REPORTING OF SUSPICIOUS ACTIVITIES

8.1 Internal Reporting Procedures

Employees may be required to report suspicious activities internally to designated compliance personnel.

Reports may involve:

- suspicious transactions;
- identity inconsistencies;
- unusual client behaviour;
- fraud indicators;
- or sanctions concerns.

8.2 Regulatory Reporting

Where required by applicable law or regulatory obligations, TactoFX may report suspicious activities to:

- regulatory authorities;
- financial intelligence units;
- law enforcement agencies;
- or authorized governmental bodies.

8.3 Confidentiality of Reports

Suspicious activity investigations and reports may remain confidential.

Clients may not necessarily be informed where investigations or reports are conducted.

9. RECORD KEEPING

9.1 Retention of Records

TactoFX may maintain records relating to:

- identity verification;
- transaction history;
- compliance reviews;
- communication logs;
- suspicious activity investigations;
- and financial records.

9.2 Retention Periods

Records may be retained for periods considered reasonably necessary for:

- regulatory compliance;
- financial crime prevention;
- dispute resolution;
- legal obligations;
- and operational administration.

10. EMPLOYEE COMPLIANCE AND TRAINING

10.1 Compliance Responsibilities

Employees are expected to:

comply with AML procedures;
identify suspicious activities;
maintain confidentiality;
cooperate with investigations;
and follow internal compliance protocols.

10.2 AML Training Programs

TactoFX may provide AML-related training concerning:

financial crime risks;
sanctions compliance;
fraud prevention;
suspicious activity indicators;
identity verification procedures;
and regulatory responsibilities.

---

11. FRAUD PREVENTION MEASURES

11.1 Fraud Detection Controls

The Company may implement systems designed to identify:

account takeovers;
payment fraud;
forged documents;
identity theft;
unauthorized access;
bonus abuse;
and deceptive activities.

11.2 Security Measures

Security measures may include:

multi-factor authentication;
device monitoring;

encryption systems;
transaction verification;
behavioural analytics;
and cybersecurity protections.

---

12. ACCOUNT RESTRICTIONS AND SUSPENSIONS

12.1 Temporary Restrictions

TactoFX reserves the right to impose restrictions where suspicious activity is identified.

Restrictions may include:

withdrawal holds;
account limitations;
additional verification requirements;
transaction reviews;
or temporary suspension.

12.2 Account Termination

The Company may terminate accounts where it reasonably suspects:

money laundering;
fraud;
sanctions violations;
identity manipulation;
terrorist financing;
or unlawful conduct.

---

13. THIRD-PARTY RELATIONSHIPS

13.1 Partner Due Diligence

TactoFX may conduct compliance reviews involving:

introducing brokers;
affiliates;
payment providers;
vendors;
and operational partners.

13.2 Monitoring External Risks

Third-party relationships may be monitored to reduce exposure to:

financial crime risks;
reputational risks;
compliance failures;
and operational vulnerabilities.

---

14. CLIENT RESPONSIBILITIES

14.1 Accurate Information Obligations

Clients are responsible for providing:

accurate information;
authentic documentation;
truthful disclosures;
and updated account information.

Submission of false information may result in:

account suspension;
service termination;
regulatory reporting;
or legal action.

14.2 Cooperation with Compliance Requests

Clients may be required to cooperate with reasonable requests involving:

verification;
transaction explanations;

source-of-funds evidence;
and compliance reviews.

Failure to cooperate may impact account access.

---

15. DATA PROTECTION AND CONFIDENTIALITY

15.1 Confidential Handling of Information

Compliance information may be handled confidentially and accessed only by authorized personnel where reasonably necessary.

15.2 Data Protection Measures

TactoFX may implement safeguards designed to protect:

personal information;
financial records;
compliance documentation;
and confidential operational data.

---

16. REGULATORY COOPERATION

16.1 Cooperation with Authorities

TactoFX may cooperate with:

regulators;
law enforcement agencies;
courts;
financial intelligence units;
and governmental authorities

where legally required or reasonably necessary.

16.2 Information Sharing

The Company may disclose information where permitted or required for:

- fraud prevention;
- AML investigations;
- sanctions compliance;
- legal obligations;
- or regulatory cooperation.

---

17. LIMITATIONS

17.1 No Guarantee Against Financial Crime

While TactoFX implements commercially reasonable AML controls, the Company cannot guarantee the complete prevention of all unlawful activities.

Financial crime risks may evolve continuously and involve sophisticated methods.

17.2 Operational Discretion

The Company reserves discretion regarding:

- verification requirements;
- compliance reviews;
- account restrictions;
- transaction approvals;
- and risk assessments.

---

18. POLICY REVIEWS AND AMENDMENTS

TactoFX reserves the right to amend, modify, update, or replace this AML Policy at any time.

Updated versions become effective upon publication on the official website.

Continued use of TactoFX services constitutes acceptance of revised terms.

---

19. CONTACT INFORMATION

For AML or compliance-related inquiries, Clients may contact:

TactoFX Compliance Department

Email:
Website: www.tactofx.com

FINAL STATEMENT

TactoFX is committed to maintaining a secure, transparent, and compliance-focused financial environment through rigorous Anti-Money Laundering procedures, identity verification systems, transaction monitoring controls, and financial crime prevention measures.

The Company seeks to uphold operational integrity, protect its ecosystem from unlawful activities, and support responsible participation within the global financial markets.