KYC & Onboarding Policy

Company: SO Digital Trade FZCO
Registered Address: Unit No: UT-12-CO-362, DMCC Business Centre, Level 12, Uptown Tower, Dubai, UAE
Version: 1.0
Last Updated: 2025

---

1. Purpose of the Policy

This KYC & Onboarding Policy establishes the procedures and standards applied by **SO Digital Trade FZCO** ("the Company") to identify, verify, and onboard clients in compliance with AML/CTF regulations applicable in the UAE and international best practices.

The goal of the Policy is to: - prevent the Company from being used for money laundering or terrorist financing; - ensure the legitimacy of customer identities and activities; - mitigate financial, reputational, and regulatory risks.

---

2. Scope of Application

This Policy applies to: - all individual clients interacting with the Company through P2P trading platforms (Binance, Bybit, OKX, etc.); - all employees involved in onboarding, support, and compliance operations; - any third-party service providers used for identity verification.

---

3. Onboarding Workflow

The onboarding procedure is initiated **before the customer can begin trading** with the Company.

3.1. Client Initiates Trade

The onboarding process begins when the client opens a trade/order with the Company on P2P platforms such as: - Binance P2P, - Bybit P2P, - OKX P2P, - or other supported marketplaces.

3.2. Delivery of the Verification Link

Before executing the trade, the Company sends the client a **one-time verification link** inside the chat of the open order.

The link redirects the client to the verification flow provided by **KYCAID**.

3.3. Completion of KYC

The client must successfully complete the KYCAID verification, including: - ID document upload, - liveliness check (selfie/video), - extraction and validation of personal information.

The verification link is: - single-use; - valid only for the current onboarding session; - tied to the client's order/chat.

3.4. Compliance Review

After KYCAID returns a verification result, the Company performs: - automated risk evaluation, - sanctions list screening, - PEP screening, - fraud/bypass detection review.

If needed, the Compliance team may request additional information.

3.5. Approval / Rejection

Approval – customer may trade normally with defined limits.
Rejection – trade is cancelled and the client is blocked from further cooperation if: - identity cannot be verified, - documents appear forged or tampered, - client is matched on sanctions lists, - client refuses to complete KYC.

---

4. KYC Standards (Know Your Customer)

4.1. Basic Verification (CDD – Customer Due Diligence)

The Company collects and verifies: - Full name - Date of birth - Nationality - Residential address - Valid government-issued ID (passport, ID-card) - Live selfie/liveness - Purpose of transaction (implicit via P2P platform)

4.2. Enhanced Due Diligence (EDD) Cases

EDD is applied when: - customer shows unusual behavior; - large-volume trading beyond thresholds; - high-risk country of origin; - suspected fraudulent actions.

EDD may include: - additional proof of address, - bank statement with name, - proof of funds, - source of wealth.

4.3. Sanctions & PEP Screening

KYCAID + internal compliance tools are used to screen clients against: - UN sanctions lists - EU sanctions lists - OFAC lists - UAE national lists - Global PEP databases

Any sanctioned or high-risk PEP client will be automatically rejected.

---

5. Risk Scoring Model

Each client is assigned a risk level: - **Low Risk:** standard/retail clients with clean verification. - **Medium Risk:** high trading volumes, less common jurisdictions. - **High Risk:** EDD cases, borderline results, unusual transactional activity.

High-risk clients require manual compliance approval.

6. Ongoing Monitoring

The Company performs: - periodic rescreening of clients using KYCAID tools; - monitoring of unusual transaction patterns on P2P platforms; - manual reviews for suspicious behavior.

If suspicious activity is detected, the Company may: - pause trading, - request additional documents, - report activity to relevant authorities.

---

7. Prohibited Clients

The Company does **not** onboard: - clients refusing KYC; - clients using fraudulent or altered documents; - sanctioned individuals or entities; - clients with suspicious behavior (e.g. repeated attempts to avoid verification); - clients from high-risk banned jurisdictions.

---

8. Record Keeping

The Company securely stores: - KYC reports from KYCAID, - communication logs from P2P platforms, - risk evaluations and compliance reviews.

Retention period: **minimum 5 years**.

All data is stored in encrypted form and accessible only to authorized personnel.

---

9. Employee Responsibilities

All staff must: - follow this Policy strictly, - escalate suspicious cases to Compliance, - avoid giving clients any advice on how to bypass verification systems.

---

10. Updates to the Policy

This Policy may be updated in accordance with: - changes in UAE regulatory requirements, - DMCC compliance rules, - AML/CTF international standards, - internal risk assessments.

Version updates must be approved by the Company’s management.

Approved by: Management of SO Digital Trade FZCO