



# ANTI-MONEY LAUNDERING POLICY

WEB VERSION

(UPDATED 04 JULY 2022)

# Contents

Introduction	2
General Requirements for the Company	3
Identity Verification	3
Anti-Money Laundering Compliance Officer	4
Transaction Monitoring	4
Risk Assessment	4
Sanctions	5

## Introduction

XCL International LLC (or “the Company”) Anti-Money Laundering and Know Your Customer Policy (hereinafter - the “AML/KYC Policy”) is designed to prevent and mitigate possible risks of the Company being involved in any kind of illegal activity.

This document is a short extract of key principles from the Company's Internal Policy and should not be viewed as a full AML/KYC Policy.

Domestic and international regulations require XCL International LLC to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity on the part of its clients.

The AML/KYC Policy covers the following matters:

- Appointing an Anti-Money Laundering Compliance Officer (AMLCO) and making sure that employees know to report any suspicious activity to them;
- Identifying the responsibilities of senior managers and providing them with regular information on money laundering risks;
- Training employees on their anti-money laundering responsibilities;
- documenting and updating anti-money laundering policies, controls and procedures;
- Introducing measures to make sure that the risk of money laundering is taken into account in the day-to-day business operations;
- Forwarding/reporting all sustained suspicions to the appropriate authority;
- Promptly responding to all communication from the appropriate authority.

## General Requirements for the Company

Before the Company can execute any transaction for any new client, a number of procedures need to be in place and carried out:

- AML procedures, including customer identification, record-keeping, discovering and monitoring of unusual or suspicious transactions and, as appropriate, internal/external reporting and control;
- Ensuring that all employees know and understand their responsibilities and the Company's procedures;
- Ensure that appropriate training is undertaken;
- All relevant requests from outside sources are forwarded directly to the AMLCO.

## Identity Verification

Whenever the Company requests and receives supporting documents related to a new client's identity, it needs to be completely satisfied that they demonstrate the existence of the new client as a real natural or legal person and that the client is indeed who they say they are.

Although the Company will at times rely on third party sources as part of its fact-checking procedure when onboarding clients, the Company bears the ultimate legal responsibility for the checks being conducted accurately.

Client's identification information will be collected, securely stored, shared and protected strictly in accordance with the Company's Privacy Policy and related regulations that correspond to the GDPR requirements.

## Anti-Money Laundering Compliance Officer

The AMLCO is ultimately responsible for implementing regulations concerning Anti-Money Laundering. For the sake of ease of navigating this document 'Compliance Officer' and 'AMLCO' refer to the same person; however, the specific tasks of each role are different.

As noted above, the AMLCO is a person of authority with access to any and all relevant information for the performance of their duties.

You can contact the Company's AMLCO department by emailing us at: [support@xcoex.org](mailto:support@xcoex.org).

## Transaction Monitoring

The constant monitoring of the clients' accounts and transactions is an imperative element in effectively controlling the risk of Money Laundering and Terrorist Financing. In this respect, the AMLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company.

## Risk Assessment

The Company shall apply appropriate measures and procedures by adopting a risk-based approach, so as to focus its efforts in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

Further, the AMLCO shall monitor and evaluate the effectiveness of the measures and procedures of this Policy on an on-going basis.

The adopted risk-based approach that is followed by the Company and described in the full AML Policy has the following general characteristics:

- Recognizes that the money-laundering or terrorist financing threat varies across clients, countries, services and financial instruments;
- Allows the board of directors to differentiate between clients of the Company in a way that matches the risk of their particular business;
- Allows the board to apply its own approach in formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics;
- Helps to produce a more cost-effective and efficient system;
- Promotes prioritization of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the Company's services.

The risk-based approach adopted by the Company, and described in the Policy, involves specific measures and procedures in assessing the most cost effective and appropriate way to identify and manage the Money Laundering and Terrorist Financing risks faced by the Company.

## Sanctions

The Company is prohibited from transacting with individuals, companies and countries that are under international sanctions. The Company will therefore screen all new and existing clients against the United Nations, European Union, UK Treasury and US Office of Foreign Assets Control (OFAC) sanctions lists.

The Company does not provide services to persons residing in:

- Afghanistan
- Austria
- Bahamas
- Belgium
- Bosnia and Herzegovina
- Botswana

- Burundi
- Canada
- Central African Republic
- China
- Congo, Democratic Republic of the
- Cuba
- Egypt
- Ethiopia
- Ghana
- Gibraltar
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Iran
- Iraq
- Japan
- Lao, People's Democratic Republic of
- Lebanon
- Libya
- Mali
- Myanmar
- Nicaragua
- North Korea
- Pakistan
- Russia (Russian Federation)
- Serbia
- Somalia
- Sri Lanka
- South Sudan
- Sudan
- Syria
- Trinidad and Tobago
- Tunisia
- Uganda
- United States of America

- Vanuatu
- Venezuela
- Virgin Islands, USA
- Yemen
- Zimbabwe

The above list may be updated at any time with or without updating this document by a decision of the Compliance officer.