

Anti-Money Laundering Policy

> INTRODUCTION

IXM Holding SA together with all its directly or indirectly controlled or majority-owned subsidiaries (collectively, "IXM") commits to maintaining a high level of ethical and legal conduct in all jurisdictions in which we operate.

This Policy **sets out IXM commitments and standards** regarding:

- Anti-money laundering (AML)
- Combatting the financing of terrorism (CFT)
- Circumvention of sanction laws

It is also intended to set forth the **approach taken by IXM to ensure compliance** with all applicable laws and regulations related to AML/CFT as well as to protect IXM from being involved in transactions that lead to money laundering, terrorist financing, or circumvention of sanctions laws.

If not addressed properly, money laundering can pose serious risks to IXM operations including reputational damage and/or investigations from law enforcement or regulators which can further lead to fines and penalties to the company and involved individuals.

IXM's Risk Committee designates an **Appointed Officer** with necessary experience and capability to be responsible for the overseeing and enforcement of this Policy.

> SCOPE

This Policy is **applicable to all IXM operations globally**. It applies to all IXM directors, officers, employees, as well as its agents and consultants acting on behalf of IXM.

IXM takes breaches of AML Policy seriously and any breach will be subject to internal disciplinary measures which could range from warning to contractual termination. In addition, individuals violating AML Laws may be subject to specific penalties or fines imposed by local government authorities in the relevant jurisdictions.

> WHAT IS MONEY LAUNDERING?

Money laundering is **defined by the Financial Action Task Force (FATF)** as the processing of criminal proceeds with the aim to disguise or conceal their illegal origin. The techniques used to launder money are often similar to those used to conceal the sources of terrorist financing or the circumvention of sanctions programs.

In addition to the involvement of the financial system and physical movement of cash, criminals often exploit the international trade system and its enormous volume of trade flows to transfer assets using methods such as the issuance of false documentation and the misdeclaration of traded goods and services. This is referred to as Trade-Based Money Laundering (TBML).

Money laundering is associated with a wide range of criminal activities such as drug trafficking, illegal arms sales, bribery, terrorism, tax evasion, smuggling, sanctions circumvention, among others.

Money Laundering may aim to achieve a number of different illicit objectives including, but not limited to:

- Concealing the true source of funds in a transaction
- Concealing the ultimate recipient or destination of disposition of funds in a transaction
- Eliminating an audit trail such that it appears that the funds came from legitimate sources
- Avoiding income or other taxes in any jurisdictions

The process of money laundering typically involves three steps:

- 1. Placement** => Introduction of the funds gained from criminal activities into banking and financial system
- 2. Layering** => Placing the funds that have entered the financial system through a series of financial operations to disguise the source and give these funds the appearance of having a legal origin. It also aims to confuse and mislead potential investigations.
- 3. Integration** => Re-introduction of the funds into the legal economy with the appearance that the funds originate from legitimate activities. Funds are then returned to the original source where they can be deployed directly or indirectly into real-estate, luxury assets, business ventures, etc.

> OUR COMMITMENTS

IXM has zero-tolerance for money laundering or terrorist financing and is committed to conduct its activities in compliance with all applicable AML/CFT laws and regulations in all jurisdictions in which IXM operates.

IXM also has zero-tolerance for tax evasion including the facilitation of tax evasion of any form and in any country.

- We do not assist, permit, or facilitate any form of money laundering or terrorist financing.
- We do not engage in transactions or accept proceeds that are known or suspected to involve any kind of criminal activity.
- We do not engage in, assist, permit, or facilitate transactions or arrangements that are intended to circumvent or evade sanctions laws applicable to IXM.
- We do not participate in or knowingly facilitate tax evasion.

As a global trading company, IXM recognizes that it faces the risk of being targeted and used by ill-intentioned third parties in their money laundering or sanctions circumvention schemes. We have implemented procedures and processes to identify any suspicious transactions and protect IXM from becoming inadvertently and unknowingly involved in money laundering and sanctions circumvention activities.

> IXM APPROACH

IXM's AML/CFT program includes several procedures and processes that are implemented following a risk-based approach.

Counterparty Due-Diligence (CDD)

IXM systematically conducts due-diligence and requests Know-Your-Counterparty (KYC) documentation when onboarding potential commercial counterparts to identify and understand:

- Full name and address of the counterpart
- Identification number and/or government-issued documentation proving the existence of the counterpart
- Nature and location of business of the counterpart
- Ultimate beneficial owners with 10% or more of equity interest

IXM's due-diligence process is supported by documentation provided by the counterpart and/or using reliable, independent sources.

Above represents the minimum information required but IXM defines certain factors that will trigger an Enhanced Counterpart Due Diligence (Enhanced CDD). These factors include, among others:

- Link to a **High-Risk country** such as countries with poor AML/CFT systems, countries subject to sanctions/embargoes, jurisdictions listed as non-cooperative for tax purpose, etc. IXM regularly reviews this list using internationally recognized sources (e.g. FATF, OECD)
- Link to a **Politically Exposed Person (PEP)** defined as an individual who is or has been entrusted with a prominent public function which place them in position that can potentially be abused for the purpose of committing money laundering and other related offences such as corruption and bribery.

Third-Party Payment Process

IXM requires that payments received and made under our commercial contracts are done on a bank account held by our contractual counterpart and located in our counterpart's country of establishment.

We have implemented an AML payment matrix that clearly defines the rules and the escalation procedure in case of any requested exceptions.

Transaction Approval Process

Consistent with its risk-based approach, IXM also utilizes a transaction approval process requiring systematic review by IXM compliance team of any new transaction involving a **High-Risk country**. The objective is to identify any suspicious AML red flags and take appropriate measures.

All IXM employees need to go through an **internal training on this AML Policy** at least once a year.

We require our employees to be alert to any suspicious arrangements and transactions which could expose IXM to the risk of money laundering or the facilitation of tax evasion and sanction circumvention, and to report such arrangements to IXM Compliance team.

➤ ACCOUNTABILITY

IXM Anti-Money Laundering Policy is published on IXM's website and communicated internally and externally as applicable. The IXM HoCIR (Head of Compliance, Insurance and Risk) has overall responsibility for the Policy implementation.

IXM will track the performance and review the effectiveness of the Anti-Money Laundering Policy and procedures, supporting the implementation of the Policy, and make necessary updates to the procedures at least annually or where there is a significant change of circumstances to ensure its continuous improvement.

➤ EFFECTIVENESS AND INTERPRETATION

This Policy shall come into force on the date of signing by IXM CEO. This Policy shall be interpreted by the Compliance Department of IXM.

➤ REPORTING VIOLATIONS OF THIS POLICY

All our stakeholders are encouraged to report any grievances linked to this Policy or suspected violations of it via IXM [Raising Concerns](#) tool. The complaints can be made anonymously and IXM will ensure protection of the reporting person from any form of retaliation.