

**PREVENTION AND
IDENTIFICATION OF
OPERATIONS WITH
ILLICIT PROCEEDS
POLICY**

January 2024

INDEX

1.	INTRODUCTION.....	2
2.	OBJECTIVE	2
3.	SCOPE	2
4.	REFERENCES	2
4.1.	Internal.....	2
4.2.	External.....	3
5.	POLICY GUIDELINES	3
5.1.	General.....	3
6.	EXCEPTIONS.....	5
7.	SANCTIONS	6
8.	LIABILITY / OWNERSHIP.....	6
9.	EXHIBITS.....	6

1. INTRODUCTION

In Grupo Traxión, S.A.B. de C.V. (“Traxión” or the “Company”) we are committed to comply with the laws, rules, regulations and other provisions regarding Prevention and Identification of Operations with Illicit Proceeds (hereinafter “Anti-Money Laundering”).

Likewise, we understand the importance of doing business with transparency and integrity; therefore, we consider it essential to ensure that our transactions comply with reasonable measures to prevent and detect transactions involving illicit resources.

Accordingly, we are issuing this Policy in an effort to conduct our business in compliance with applicable anti-money laundering laws.

2. OBJECTIVE

Establish guidelines, criteria and mechanisms to ensure that Traxión and each of its subsidiaries, the Board of Directors and its Committees, executives, directors, officers and third parties that provide a good, service or have any type of interaction with the Group are aware of and comply with the applicable Anti-Money Laundering laws, to avoid possible economic, operational, legal, reputational and associated risks and/or damages for the Group and its collaborators.

3. SCOPE

This Policy applies to Traxión and its Subsidiaries, as well as to third parties that provide a good, service or have any type of interaction with the Group such as agents, suppliers, contractors or others that conduct business with Traxión and/or any of its subsidiaries and/or affiliates in compliance with applicable Anti-Money Laundering Laws.

4. REFERENCES

4.1. Internal

- Traxión’s Code of Ethics
- Compliance Policy.

4.2. External

- Federal Law for the Prevention and Identification of Operations with Resources of Illicit Origin, Rules and Applicable Regulations
- General provisions regarding prevention, operations possibly linked to the crimes of Operations with Resources of Illicit Origin and Financing of Terrorism
- Federal or Local Penal Code as appropriate
- Applicable Tax Regulations
- Bank Secrecy Act and the USA PATRIOT Act of 2001 last renewed 2015
- European Union Directive (EU) 2018/843 of the European Parliament and of the Council, of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for money laundering or the financing of terrorism, and which modifies Directives 2009/138/EC and 2013/36/EU
- Similar laws against money laundering and terrorist financing in force in the countries where the Group operates and/or has business
- Leyes similares contra el lavado de dinero y financiamiento del terrorismo vigentes en los países donde el Grupo opera y/o tenga negocios.

5. POLICY GUIDELINES

5.1. General

- I. Contracts entered into by Traxión and/or any of its subsidiaries with third parties shall be subject to compliance with this Policy.
- II. Traxión and/or any of its subsidiaries may apply the disciplinary measures they deem appropriate to third parties on a case-by-case basis, which may range from the imposition of economic sanctions, temporary or definitive bans.
- III. Third parties that carry out transactions with any company of the Group are required to comply at all times with the provisions applicable to them in the Anti-Money Laundering Laws, Law, Regulations or Rules and General Provisions on prevention, transactions possibly related to the crimes of Transactions with Illicit Proceeds.
- IV. Third parties that provide goods or services to the Group must expressly declare and acknowledge that they are in compliance with their tax obligations, including the obligations included in Form 32-D and, in the case of legal entities, state that the same is

not a Company that Invoices Simulated Operations (“EFOS” for its acronym in Spanish) or that it is a Company that Deducts Simulated Operations (“EDOS” for its acronym in Spanish), a situation that they are required to maintain during the entire term of the contractual relationship with the Group.

- V. It is strictly forbidden to carry out Fraudulent Operations in our transactions, as well as when it is known that they come from or represent the product of an illicit activity.
- VI. The information, presentation of notices and reports and submission of reports that must be sent when any of the companies and subsidiaries of the Group carry out a Vulnerable Activity, must be made in the official format issued by the UIF (Financial Intelligence Unit, for its acronym in Spanish) for such purpose.
- VII. Carry out the due identification of payment instruments in acts and transactions that are subject to laws, rules, regulations and other provisions on Anti-Money Laundering.
- VIII. Payments for acts or transactions may not be made or accepted through the use of coins and banknotes, whether in local and/or foreign currency, or precious metals in any of the activities listed in Exhibit 1, provided they reach the amounts established therein.
- IX. Each Business Unit in conjunction with the Risk area shall conduct an annual assessment of the Group’s risks related to Money Laundering or, in the case of new services or products, such assessment shall be prior to the start of operations, with the objective of efficiently and effectively developing internal control systems that adapt to changes in the operating and business environment, mitigating risks to acceptable levels as the Group’s business evolves and expands. The results of the risk assessment will be shared with the Compliance Officer/Compliance Representative and the Legal Department to evaluate necessary improvements to this Policy.
- X. Maintain, protect, safeguard and prevent the destruction or concealment of the information and documentation that supports the Vulnerable Activity, as well as that which identifies its Clients or Users, for a period of 5 years from the date of the activity.
- XI. Provide the necessary facilities for the Authority to carry out verification visits or requirements on compliance with laws, rules, regulations and other provisions on Anti-Money Laundering.
- XII. When Vulnerable Activities are carried out, to have a document that develops its guidelines for the identification of Clients or

Users, as well as the criteria, measures and internal procedures to comply with the provisions of the laws, rules, regulations and other provisions on Anti-Money Laundering.

- XIII. Prior to the execution of any Vulnerable Activity, whether in a single transaction or in a business relationship, the Client or User shall be required to provide the necessary information for its identification in accordance with the General Rules or Provisions in accordance with the obligated subject, as applicable. The identification documents referred to above and provided must be free of erasures or alterations.
- XIV. Create a single Customer or User Identification file when any of the Group's companies and subsidiaries carry out Vulnerable Activities. Likewise, the documents must be compared with the original or certified copy of the same, prior to their acceptance and integration to the file and may be integrated physically or electronically, in the understanding that either format must contain all the information and documentation of the Client or User.
- XV. Have an anonymous whistleblower communication channel so that, if an employee of the Group knows or suspects a violation of the applicable Anti-Money Laundering Laws or of this Policy, he/she shall promptly report the facts through such channel or communicate his/her doubts or report any suspicion, without fear of retaliation.

6. EXCEPTIONS

Traxión has adopted a zero-tolerance policy with respect to any conduct that violates the Anti-Money Laundering Laws mentioned above, always seeking to do business only with third parties that carry out legitimate activities and are committed to following the guidelines and criteria established in this Policy.

Therefore, the only exceptions to this Policy shall be those established and contemplated in the law itself, in which case the Compliance Officer/Compliance Representative and Traxión's Legal Department must be notified by means of a document stating the reasons for requesting an exception to the Policy, in order for said Department to analyze the case.

In the case of an exception request for the integration of the customer or user's identification file, it must be carried out at the latest during the performance of the act or operation. Neither Traxión nor its subsidiaries will be able to carry out the Vulnerable Activity that is subject to an exception request until it receives a response from the Legal Department, or until it is able to prove to the Legal

Department that it has obtained all the data and documents, thus rendering the exception request null and void.

7. SANCTIONS

Any non-compliance with the provisions of this Policy by members of the Board of Directors and its Committees, executives, directors and/or officers shall be subject to the sanctions determined by the Company's management considering the circumstances of each case.

In the event of non-compliance by third parties that provide a good, service or have any type of interaction with any Group company, the disciplinary measures that the Company's management considers appropriate in each case must be applied, which may range from the imposition of economic sanctions, temporary or definitive bans and the corresponding legal actions.

8. LIABILITY / OWNERSHIP

The Corporate Legal Department through of the Compliance Office are the assigned owners of this policy and are mainly responsible for its content, updating and request for approval by Traxión's Corporate Governance.

9. EXHIBITS

1. Exhibit 1 "Vulnerable Activities and Restriction on the Use of Cash".