

	TYPE OF DOCUMENT POLICY	Code	PG-02-2025-01
		Version	1
	NAME GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

## INTRODUCTION

Recognizing that Money Laundering, Terrorism Financing, and the Financing of the Proliferation of Weapons of Mass Destruction are criminal phenomena that generate negative consequences for the economy and society as a whole—and that it is evident that criminal organizations currently seek to use legally established companies and institutions to achieve illicit purposes contrary to current regulations—TEAM COMMUNICATIONS S.A. considers it necessary and of vital importance to adopt measures, policies, and procedures to prevent participation in the commission of these crimes.

For this reason, TEAM COMMUNICATIONS S.A. will make every effort to avoid becoming a target of organized crime and to prevent, by all possible means, criminal organizations from using TEAM COMMUNICATIONS S.A. to give a veneer of legality to assets derived from criminal activities or to channel lawful or unlawful resources toward the execution of terrorist activities.

Accordingly, TEAM COMMUNICATIONS S.A. has designed and implemented a Risk Management System for ML/TF/FPWMD, aimed at preventing illicit activities within the company and ensuring compliance with current regulations governing this matter.

TEAM COMMUNICATIONS S.A. understands and acknowledges that the only way to faithfully uphold its commitment to society is by defining effective procedures and policies that involve all natural and/or legal persons who have any relationship with the company.

### I. OBJECTIVE

Define the measures and procedures that promote the development of sound and transparent business relationships, ensuring the good reputation and credibility of TEAM COMMUNICATIONS S.A., while reducing the likelihood that resources derived directly or indirectly from Money Laundering, Terrorism Financing, or the Financing of the Proliferation of Weapons of Mass Destruction enter the company.

### II. DEFINITIONS

- **SAGRILAFT:** This is a Risk Management System designed to identify and manage the risks of Money Laundering, Terrorism Financing, and the Financing of the Proliferation of Weapons of Mass Destruction that may arise within the company.
- **ML/TF/FPWMD:** This abbreviation refers to Money Laundering, Terrorism Financing, and the Financing of the Proliferation of Weapons of Mass Destruction.
- **COUNTERPARTY:** Refers to any natural or legal person with whom the Company has commercial, business, contractual, or legal relationships of any kind. Among others, counterparties include the Company's associates, employees, clients, contractors, and product suppliers.
- **RISKS FACTORS ML/TF/FPWMD:** These are the possible elements or causes that generate LA/FT/FPADM risk for any Company. The organization must identify them by taking into account Counterparties, Products, Activities, Channels, and Jurisdictions, among other relevant factors.

	TYPE OF DOCUMENT POLICY	Code	PG-02-2025-01
		Version	1
	NAME GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

- **BINDING OR RESTRICTIVE LISTS:** These are national and international databases that compile information, reports, and background records from various organizations regarding natural and legal persons who may be involved in suspicious activities, investigations, legal proceedings, or convictions for the crimes of Money Laundering (ML) and Terrorism Financing (TF).
- **COMPLIANCE OFFICER:** The natural person designated by the Company who is responsible for promoting, developing, and ensuring compliance with the specific procedures for the prevention, updating, and mitigation of Money Laundering (ML), Terrorism Financing (TF), and Financing of the Proliferation of Weapons of Mass Destruction (FPWMD) risks.
- **DUE DILIGENCE:** This is the process through which the Company adopts measures to gain knowledge of the Counterparty, its business, operations, products, and the volume of its transactions.
- **ENHANCED DUE DILIGENCE:** This is the process through which the Company adopts additional and more rigorous measures to gain a deeper understanding of the Counterparty, its business, operations, products, and the volume of its transactions.
- **INCOME FROM ORDINARY ACTIVITIES:** These are revenues generated in the course of the Company's main business activities.
- **ML/TF/FPWMD RISK MATRIX:** This is one of the tools that enables a Company to identify, classify, segment, assess, and control the Money Laundering (ML), Terrorism Financing (TF), and Financing of the Proliferation of Weapons of Mass Destruction (FPWMD) risks to which it may be exposed, in accordance with the identified ML/TF/FPWMD Risk Factors.
- **REASONABLE MEASURES:** These are sufficient, appropriate, and quantifiable actions—both in quality and quantity—implemented to mitigate ML/TF/FPWMD risk, taking into account the Company's inherent risks and their materiality.
- **UNUSUAL TRANSACTION:** A transaction whose amount or characteristics do not correspond to the Company's ordinary or normal economic activity, or which, due to its number, volume, or nature, falls outside the normal patterns or customary business practices within a sector, industry, or type of Counterparty.
- **SUSPICIOUS TRANSACTION:** This refers to an Unusual Transaction that, in addition, according to the customary practices of the relevant activity, cannot be reasonably justified. This type of transaction includes attempted or rejected transactions that exhibit characteristics giving them a suspicious nature.
- **PEP:** It refers to Politically Exposed Persons (PEPs), meaning public officials within any system of job classification and nomenclature of the national or territorial public administration, who, by virtue of their positions, have —either directly or by delegation— responsibility for general management, the formulation of institutional policies, and the adoption of plans, programs, and projects, as well as the direct management of State assets, funds, or valuables. These responsibilities may include, among others, budget execution, public procurement, investment project management, payments, settlements, and the administration of movable and immovable property. This category also includes Foreign PEPs and PEPs from International Organizations.
- **POLICIES:** These are the guidelines that the Company must adopt to be able to identify, assess, prevent, and mitigate ML/TF/FPWMD risks and their associated risks. Each stage and element of the SAGRILAFT must have clear and effectively applicable policies. These policies must be incorporated into the procedures manual, which guides the actions of the Company's personnel

	TYPE OF DOCUMENT POLICY	Code	PG-02-2025-01
		Version	1
	NAME GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

for the proper functioning of the SAGRILAFT, and must establish the consequences and sanctions applicable in cases of non-compliance.

- **CONTAGION RISK:** This is the possibility of loss that a Company may suffer, directly or indirectly, as a result of the actions or experiences of a Counterparty.
- **LEGAL RISK:** This is the possibility of loss incurred by a Company as a result of being sanctioned or required to pay damages due to non-compliance with laws, regulations, or contractual obligations. It may also arise from deficiencies in contracts and transactions caused by malicious actions, negligence, or unintentional acts that affect the formalization or execution of such contracts or transactions.
- **OPERATIONAL RISK:** This is the possibility of incurring losses due to deficiencies, failures, or inadequacies in human resources, processes, technology, infrastructure, or as a result of external events. This definition includes Legal Risk and Reputational Risk associated with such factors.
- **REPUTATIONAL RISK:** This is the possibility of loss incurred by a Company due to disrepute, poor image, or negative publicity—whether true or not—regarding the organization and its business practices, which may result in loss of clients, decreased revenue, or legal proceedings.
- **INHERENT RISK:** It is the level of risk inherent to an activity, without considering the effect of controls.
- **RESIDUAL RISK:** This is the level of risk that remains after the application of control measures.
- **STR (Suspicious Transaction Report):** This refers to a transaction that, due to its number, amount, or characteristics, does not fall within the normal system or business practices of a given industry or sector and, furthermore, cannot be reasonably justified according to the customary practices of the relevant activity.
- **SIREL:** This is the online reporting system managed by the UIAF. It is a web-based tool that allows reporting entities to upload and/or submit online information related to the obligations established by the regulations of each sector in an efficient and secure manner. It is available 24 hours a day, 7 days a week, 365 days a year.
- **UIAF:** The Financial Information and Analysis Unit is Colombia's Financial Intelligence Unit (FIU), responsible for intervening in the economy to prevent and detect Money Laundering (ML), Terrorism Financing (TF), and the Financing of the Proliferation of Weapons of Mass Destruction (FPWMD).
- **FINAL BENEFICIAL OWNER:** Refers to the natural person(s) who ultimately own or control a client or the natural person on whose behalf a transaction is conducted. It also includes the person(s) who exercise effective and/or ultimate control, directly or indirectly, over a legal entity or other structure without legal personality. The following are considered Final Beneficial Owners of a legal entity:
  - a. A natural person who, acting individually or jointly, exercises control over the legal entity, in accordance with the provisions of Article 260 and subsequent articles of the Commercial Code; or
  - b. A natural person who, acting individually or jointly, owns directly or indirectly five percent (5%) or more of the capital or voting rights of the legal entity, and/or benefits by five percent (5%) or more from the income, profits, or assets of the legal entity;
  - c. When no natural person is identified under items (a) and (b), the natural person holding the position of legal representative, unless there is another natural person who holds greater authority in relation to the management or direction of the legal entity.

	TYPE OF DOCUMENT  POLICY	Code	PG-02-2025-01
		Version	1
	NAME  GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

The Final Beneficial Owners of a trust agreement, a structure without legal personality, or a similar legal structure are the natural persons who hold any of the following roles:

- i. Trustor(s), settlor(s), grantor(s), or any similar or equivalent position;
- ii. Trust committee, financial committee, or any similar or equivalent position;
- iii. Trustee(s), beneficiary(ies), or contingent beneficiary(ies); and
- iv. Any other natural person who exercises effective and/or ultimate control, or who has the right to enjoy and/or dispose of the assets, benefits, proceeds, or profits.

### III. SCOPE OF APPLICATION

All the provisions and guidelines contained in this document are mandatory for TEAM COMMUNICATIONS S.A., its Employees, Shareholders, Members of the Board of Directors, Managers, Executives, Compliance Officer, Internal Audit, and Statutory Auditor, and are issued in compliance with the requirements and regulations established by the Superintendence of Companies.

### IV. PUBLICATION AND UPDATING

This document is mandatory and available to all employees and staff of TEAM COMMUNICATIONS S.A. It must be updated in accordance with regulatory requirements or at least once every two (2) years and must be approved by the Company's General Shareholders' Meeting.

### V. UNSAFE BEHAVIOR

TEAM COMMUNICATIONS S.A. classifies as risky or unsafe any transaction or business conducted without complying with the Due Diligence and Enhanced Due Diligence Measures established by TEAM COMMUNICATIONS S.A. for the onboarding or engagement of Employees, Shareholders, Members of the Board of Directors, Clients, Suppliers, and Contractors.

### VI. POLICIES

In line with the Company's commitment to combating Money Laundering (ML), Terrorism Financing (TF), and the Financing of the Proliferation of Weapons of Mass Destruction (FPWMD), TEAM COMMUNICATIONS S.A. declares and commits to complying with the following guidelines:

- TEAM COMMUNICATIONS S.A. undertakes to establish the conditions, guidelines, and requirements for the initiation and development of commercial, corporate, and labor relationships with its Employees, Shareholders, Clients, Suppliers, and Contractors.

	TYPE OF DOCUMENT  POLICY	Code	PG-02-2025-01
		Version	1
	NAME  GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

- Faithfully comply with the Legal Basic Circular (100-000016), Chapter X of 2020 issued by the Superintendence of Companies, as well as with all other regulations enacted for the prevention of Money Laundering (ML), Terrorism Financing (TF), and the Financing of the Proliferation of Weapons of Mass Destruction (FPWMD).
- Promote within the Company a culture of prevention and awareness regarding Employees, Shareholders, Members of the Board of Directors, Suppliers, Contractors, and Clients, through training programs and any other available means.
- TEAM COMMUNICATIONS S.A. shall not initiate or renew any commercial, labor, or corporate relationship in which an Employee, Shareholder, Supplier, Contractor, or Client fails to meet the requirements established by the Company or by law for such purposes.
- TEAM COMMUNICATIONS S.A. establishes the requirements that all counterparties (Employees, Temporary Workers, Shareholders, Members of the Board of Directors, Suppliers, Contractors, and Clients) must meet for their engagement with the Company and defines the frequency with which Counterparty information must be updated.
- TEAM COMMUNICATIONS S.A. shall not engage in any service and/or product transactions with suppliers or contractors who have not complied with the onboarding or information update procedures established by the Company.
- No relationship of any kind shall be established with any Counterparty (Employee, Shareholder, Member of the Board of Directors, Supplier, Contractor, or Client) when there are elements that give rise to reasonable doubts regarding the legality of the operations, the origin of the funds, and/or their intended use.
- When a Counterparty (Employee, Temporary Worker, Shareholder, Member of the Board of Directors, Supplier, Contractor, or Client) fails to provide sufficient information to properly assess their situation, the Company must refrain from proceeding with their engagement.
- All employees of TEAM COMMUNICATIONS S.A. must strive to comply with this policy. In the event of non-compliance by any employee, sanctions will be applied in accordance with the provisions set forth in the Company's Internal Work Regulations.
- The General Shareholders' Meeting, the Legal Representative, the Compliance Officer, and other Company collaborators must comply with and be accountable for the obligations and responsibilities applicable to them regarding the implementation of the Self-Control and Comprehensive Risk Management System for ML/TF/FPWMD.
- The information managed by TEAM COMMUNICATIONS S.A. is strictly confidential, and all employees must handle it with the utmost transparency and honesty.
- TEAM COMMUNICATIONS S.A. must cooperate with the authorities by providing any information requested during investigations related to Money Laundering (ML), Terrorism Financing (TF), and/or the Financing of the Proliferation of Weapons of Mass Destruction (FPWMD).
- If, during an employment, commercial, or corporate relationship, it becomes known that a Counterparty (Employee, Temporary Worker, Shareholder, Member of the Board of Directors, Supplier, Contractor, or Client) has been involved in illicit activities or included in restrictive or binding lists, whether national or international, the Compliance Officer shall evaluate the situation and determine the appropriate corrective measures to be taken.
- Counterparty information must be updated annually, in accordance with the Due Diligence measures established by the Company for this purpose.

	TYPE OF DOCUMENT  POLICY	Code	PG-02-2025-01
		Version	1
	NAME  GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

- Implement the role of Compliance Officer and allocate the necessary human, technical, financial, and operational resources for the proper execution of their duties.
- TEAM COMMUNICATIONS S.A. must apply enhanced or detailed due diligence measures when entering into contracts or conducting transactions with Counterparties from countries that do not comply with the recommendations of the Financial Action Task Force (FATF).
- It is the duty of all employees to inform the Compliance Officer, who in turn must immediately and adequately report to the Financial Information and Analysis Unit (UIAF) any relevant information concerning the management of funds whose amount or characteristics do not correspond to the economic activity of the Company's clients or suppliers, or which, due to their number, transaction amounts, or particular features, could reasonably lead to the suspicion that the Company is being used to manage, utilize, or invest funds or resources derived from criminal activities or intended for their financing.
- It is the obligation of all Company employees to be familiar with and strictly apply the criteria and regulations contained in the document Self-Control and Comprehensive Risk Management System for Money Laundering, Terrorism Financing, and Financing of the Proliferation of Weapons of Mass Destruction (SAGRILAFT), as well as to recognize and respond appropriately to the red flags outlined therein.
- TEAM COMMUNICATIONS S.A., upon becoming aware of any crime detected by individuals associated with the Company in the course of their duties, must fulfill the obligation to report such acts to the appropriate authorities.
- All payments by transfer must be made only to accounts in the name of the payment beneficiary, except in specific cases, which must be clearly detailed in writing and authorized in accordance with the policies established by the Company for that purpose.
- The Company, through its Compliance Officer, must submit a Quarterly AROS Report to the UIAF in the event that no suspicious transactions have occurred during the specified period.
- Conduct Enhanced Due Diligence when carrying out international operations whose origin or destination is a country classified as a "tax haven," when counterparties are domiciled in such jurisdictions, or when any of the requirements set out in the Company's procedure for this purpose are met.
- The Company has guidelines and methodologies in place to segment, identify, measure, control, and monitor the ML/TF/FPWMD risk factors associated with the organization.
- The Company has policies in place to regulate cash payments, refunds, and payments to third-party accounts not related to the organization.
- The Company has established Policies for Conflict of Interest Management, regulation of Donations and Political Contributions, recordkeeping and preservation of SAGRILAFT-related information, program monitoring, confidentiality of SAGRILAFT information, internal and external reporting, and dissemination and training on SAGRILAFT.

	TYPE OF DOCUMENT POLICY	Code	PG-02-2025-01
		Version	1
	NAME GENERAL POLICY AGAINST LA/FT/FPADM RISKS	Issue date	31/05/2025

## VII. CHANGE CONTROL

VERSION	DATE	CHAGEN MADE	RESPONSIBLE FOR THE CHANGE/POSITION
1. File issued	31/05/2025	N/A	Compliance Officer