

# POLICY FOR THE PREVENTION AND MANAGEMENT OF ML/TF/FPWMD RISK

## 1. GUIDELINE

C.I. PROINGRA S.A.S. is committed to managing and overseeing all its commercial activities through a risk management system for Money Laundering (ML), Terrorist Financing (TF), and Financing of the Proliferation of Weapons of Mass Destruction (FPWMD), including all related activities. This commitment ensures compliance with applicable legal regulations and focuses on the objectives, goals, and control of risks identified in the risk matrix.

## 2. OBJECTIVE

To define the control guidelines that must govern the company's operations for the prevention and control of ML/TF/FPWMD risks, aiming to avoid the materialization of risks connected to these activities within our operations, and to prevent the company from being used, directly or indirectly, as a vehicle for illicit activities.

## 3. SCOPE

This policy applies to all business associates (clients, suppliers, employees, partners, and contractors) currently linked to or seeking to establish a future relationship with C.I. PROINGRA S.A.S.

## 4. DEFINITIONS

### Assets:

Economic resources are currently controlled by the Company because of past events.

### Geographical Area:

The area or territory where the Company carries out its activities.

### Ultimate Beneficial Owner (UBO):

The natural person(s) who ultimately owns or controls a client or the natural person on whose behalf a transaction is conducted. This also includes individuals who exercise effective and/or final control, either directly or indirectly, over a legal entity or other structure without legal personality.

UBOs of a legal entity include:

- a. A natural person who, acting individually or jointly, exercises control over the legal entity in accordance with Article 260 and subsequent of the Commercial Statute.
- b. A natural person who, acting individually or jointly, be the owner directly or indirectly, owns (5%) or more of the capital or voting rights of the legal entity, and/or benefits from (5%) or more of the profits, earnings, or assets of the legal entity.

c. When no natural person is identified under points (a) and (b), the natural person who serves as the legal representative, unless a person with greater authority in relation to the legal entity's management or direction functions exists.

UBOs of a trust agreement, non-legal entity structure, or similar legal arrangement are the following natural person who hold the status of:

- a. The trustor(s), settlor(s), constituent(s) or similar equivalent role.
- b. The fiduciary committee, financial committee, or equivalent.
- c. The trustee(s), beneficiary(ies), or conditional beneficiaries.
- d. Any other natural person who exercises effective and/or final control or has the right to enjoy and/or dispose of the assets, benefits, results, or profits.

**Counterparty:**

Any natural or legal person with whom the Company has commercial, business, contractual, or legal relationships of any kind. Counterparties include:

- Associates
- Employees
- Clients
- Contractors
- Product Suppliers of the Company.

**Due Diligence:**

The process through which the Company takes measures to understand the Counterparty, their business, operations, products, and transaction volume, as defined in section 5.3.1 of Chapter X of the Legal Basic Circular issued by the Superintendence of Companies.

**Enhanced Due Diligence:**

The process through which the Company applies additional and more intense measures to understand the Counterparty, their business, operations, products, and transaction volume, in accordance with section 5.3.2 of Chapter X of the Legal Basic Circular.

**Company:**

A commercial company, sole proprietorship, or branch of a foreign company supervised by the Superintendence of Companies.

**Obligated Company:**

A Company that must comply with Chapter X, as listed in section 4 of said chapter.

**Terrorist Financing (TF):**

The criminal offense regulated under Article 345 of the Colombian Penal Code (or any regulation that modifies or replaces it). It refers to the process of obtaining legal or illegal resources that support and are used to conduct terrorist activities. Terrorism: *"To provide, collect, deliver, receive, manage, contribute, safeguard, or store funds, assets, or resources, or to carry out any other act that promotes, organizes, supports, maintains, finances, or economically sustains armed groups operating outside the law."*

**Financing of the Proliferation of Weapons of Mass Destruction (FPWMD):**

Any act that provides funds or uses financial services, wholly or partially, for the manufacture, acquisition, possession, development, export, transfer of materials, fragmentation, transportation, transfer, deposit, or dual use for unlawful purposes, in contravention of national laws or international obligations, when applicable.

**ML/TF/FPWMD Risk Factors:** These are the potential elements or causes that generate the risk of Money Laundering, Terrorist Financing, or the Financing of the Proliferation of Weapons of Mass Destruction (ML/TF/FPWMD) for any Obligated Company. The Obligated Company must identify these factors by considering, among others, its Counterparties, Products, activities, channels, and jurisdictions.

**FATF (Financial Action Task Force):** An intergovernmental body created in 1989 with the purpose of issuing standards for countries in the fight against Money Laundering (ML), Terrorist Financing (TF), and the Financing of the Proliferation of Weapons of Mass Destruction (FPWMD).

**GAFILAT (Latin American Financial Action Task Force):** A regional body of the FATF, established in 2000, of which Colombia is a member.

**Total Income:** Refers to all revenue recognized in the statement of income for the reporting period, serving as the main source of information regarding the financial activity of a Company during that period.

In accordance with disclosure standards, this includes **Ordinary Operating Income**, other income, gains (other items that meet the definition of income but are not considered Ordinary Operating Income), and financial income.

**Ordinary Operating Income:** Income generated during the Company's core business activities.

**ML/TF/FPWMD:** For the purposes of this Manual, this acronym stands for Money Laundering, Terrorist Financing, and Financing of the Proliferation of Weapons of Mass Destruction.

**Money Laundering (ML):** The process through which illicit resources or assets are given the appearance of legality or are introduced into the formal economy—either within the real or financial sector. Illicit origin refers to resources derived from activities such as: migrant smuggling, human trafficking, extortion, illicit enrichment, kidnapping, rebellion, arms trafficking, drug trafficking, crimes against public administration (corruption), and crimes against the financial system. All these are classified under Article 323 of the Colombian Criminal Code.

**Binding Lists:** These are lists of individuals and entities associated with terrorist organizations that are binding for Colombia under Colombian law (Article 20 of Law 1121 of 2006) and pursuant to international law. This includes, but is not limited to, United Nations Security Council Resolutions 1267 of 1999, 1373 of 2001, 1718 and 1737 of 2006, 1988 and 1989 of 2011, and 2178 of 2014, along with any resolutions that amend, expand upon, or complement them. It also includes any other list binding for Colombia, such as the U.S. Department of Treasury's terrorist lists, the European Union list of terrorist organizations, and the EU list of individuals designated as terrorists. The Superintendence of Companies shall maintain on its website a reference list of Binding Lists applicable in Colombia as a guide, without it being exhaustive.

**ML/TF/FPWMD Risk Matrix:** This is one of the tools that allows a Company to identify, differentiate, segment, assess, and control the ML/TF/FPWMD Risks to which it may be exposed, in accordance with the identified ML/TF/FPWMD Risk Factors.

**Reasonable Measures:** Actions that are sufficient, appropriate, and measurable in both quality and quantity to mitigate ML/TF/FPWMD Risk, considering the inherent risks of the Obligated Company and their materiality.

**Compliance Officer:** The natural person appointed by the Obligated Company who is responsible for promoting, developing, and ensuring compliance with the specific procedures for the prevention, updating, and mitigation of ML/TF/FPWMD Risk, whose profile is described later in this Manual.

**Unusual Transaction:** A transaction whose amount or characteristics do not correspond to the ordinary or regular economic activity of the Obligated Company or which, due to its frequency, amount, or nature, does not fall within the normal standards or usual business practices of a particular sector, industry, or type of Counterparty.

**Suspicious Transaction:** An Unusual Transaction that, in addition to its nature, cannot be reasonably justified based on the customary practices of the activity in question. This includes attempted or rejected transactions that exhibit characteristics that qualify them as suspicious.

**PEP (Politically Exposed Person):** Refers to public officials within any system of nomenclature and job classification of the national and territorial public administration, who, in the positions they hold, have — either by direct responsibility or delegation — duties involving general management, the formulation of institutional policies, the adoption of plans, programs, and projects, and the direct handling of State assets, funds, or resources.

Such duties may include, among others, budget execution, public procurement, investment project management, payments, settlements, and administration of movable and immovable property. This definition also includes Foreign PEPs and PEPs from International Organizations.

**PEPs from International Organizations:** Natural persons who hold senior management positions in international organizations, such as the United Nations, the Organization for Economic Co-operation and Development (OECD), the United Nations Children's Fund (UNICEF), and the Organization of American States (OAS), among others (e.g., directors, deputy directors, board members, or any individual performing an equivalent role).

**Foreign PEPs (Politically Exposed Persons):** These are natural people who perform prominent and significant public functions in a foreign country. In particular, this includes:

- (i) Heads of state, heads of government, ministers, vice-ministers, or secretaries of state;
- (ii) Members of congress or parliament;
- (iii) Members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are not ordinarily subject to appeal, except under exceptional circumstances;
- (iv) Members of central bank boards or tribunals;
- (v) Ambassadors;
- (vi) Chargés d'affaires;
- (vii) Senior military officials;

- (viii) Members of administrative, management, or supervisory bodies of state-owned enterprises;
- (ix) Members of reigning royal families;
- (x) Senior leaders of political parties or movements; and
- (xi) Legal representatives, directors, deputy directors, senior management members, and board members of an international organization (e.g., heads of state, senior government, judicial, or military officials, and high-ranking executives of state-owned enterprises).

**ML/TF/FPWMD Policy:** Refers to the general guidelines that each Obligated Company must adopt to be able to identify, assess, prevent, and mitigate ML/TF/FPWMD Risk and associated risks. Each stage and component of the SAGRILAFT must include clear and effectively applicable policies. These policies must be incorporated into the company's procedures manual to guide the conduct of its employees in the operation of the SAGRILAFT system and must establish consequences and sanctions for non-compliance.

**Products:** The goods and services produced, marketed, processed, or offered by the Company, or acquired from third parties.

**FATF Recommendations:** These are the 40 recommendations issued by the Financial Action Task Force (FATF), along with their interpretive notes, aimed at preventing ML/TF/FPWMD Risk. These recommendations were reviewed in February 2012 and updated in June 2019. The result of this review is the document titled *"International Standards on Combating Money Laundering, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction."*

**Comprehensive Risk Self-Control and Management Regime for ML/TF/FPWMD:** Refers to the SAGRILAFT system and the Minimum Measures Regime, collectively.

**Minimum Measures Regime:** Refers to the obligations related to self-management and control of ML/TF/FPWMD Risk, as provided in section 8 of Chapter X of the Legal Basic Circular.

**ML/TF/FPWMD Risk:** Refers to the possibility of loss or damage that a Company may suffer due to its potential to be used, either directly or through its operations, as an instrument for Money Laundering and/or the channelling of resources toward terrorist activities or the Financing of the Proliferation of Weapons of Mass Destruction.

This also includes instances where the concealment of assets originating from such activities is intended. The contingencies inherent to ML/TF/FPWMD risk materialize through exposures such as Contagion Risk, Legal Risk, Operational Risk, Reputational Risk, and other associated risks that may negatively impact the Company's financial stability when it is used for such illicit purposes.

**Contagion Risk:** The potential loss a Company may incur, directly or indirectly, because of the actions or experiences of a Counterparty.

**Legal Risk:** The potential loss a Company may face when sanctioned or required to pay damages due to breach of laws, regulations, or contractual obligations.

It may also arise from failures in contracts and transactions caused by malicious conduct, negligence, or unintentional acts that affect the execution or formalization of such contracts or transactions.

**Operational Risk:** The potential for losses arising from deficiencies, failures, or inadequacies in human resources, processes, technology, infrastructure, or the occurrence of external events. This definition includes Legal Risk and Reputational Risk associated with such factors.

**Reputational Risk:** The potential loss a Company may incur due to reputational damage, poor public image, or negative publicity—whether true or not—about the organization and its business practices, resulting in the loss of clients, reduced income, or legal proceedings.

**Inherent Risk:** The level of risk inherent to an activity, without considering the mitigating effects of controls.

**Residual Risk:** The level of risk remains after applying the established controls.

**SAR (Suspicious Activity Report):** A report concerning a transaction which, due to its number, volume, or characteristics, does not align with the normal system or business practices within a given industry or sector and based on customary business behavior, cannot be reasonably justified.

**SIREL:** The online reporting system managed by the UIAF. It is a web-based tool that allows reporting entities to upload and/or submit information regarding their sector-specific regulatory obligations efficiently and securely, available 24 hours a day, 7 days a week, 365 days a year.

**SAGRILAF:** The self-control and comprehensive risk management system for ML/TF/FPWMD established under Chapter X of the Legal Basic Circular.

**SMLMV (Legal Monthly Minimum Wage):** The current legal monthly minimum wage in force.

**UIAF (Financial Information and Analysis Unit):** Colombia's financial intelligence unit, responsible for intervening in the economy to prevent and detect ML/TF/FPWMD activities.

## 5. POLICY GUIDELINES

In alignment with the policy established under the Self-Control and Comprehensive Risk Management System for ML/TF/FPWMD, the Organization declares the following guidelines:

**5.1.** Comply with the Colombian regulations applicable to our organization in matters concerning the prevention of Money Laundering (ML), Terrorist Financing (TF), and the Financing of the Proliferation of Weapons of Mass Destruction (FPWMD), as well as the United Nations conventions and treaties aimed at addressing criminal activities related to ML/TF/FPWMD. These include:

- **1988 Vienna Convention:** United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Approved by Law 67 of 1993 – Ruling C-176 of 1994).
- **1989 United Nations Convention for the Suppression of the Financing of Terrorism** (Approved by Law 808 of 2003 – Ruling C-037 of 2004).
- **2000 Palermo Convention:** United Nations Convention Against Transnational Organized Crime (Approved by Law 800 of 2003 – Ruling C-962 of 2003).



- **2003 Merida Convention:** United Nations Convention Against Corruption (Approved by Law 970 of 2005 – Ruling C-172 of 2006).
- **Recommendations issued by the Financial Action Task Force (FATF)** for combating money laundering and terrorist financing, including those established through its regional group, GAFILAT.
- **Law 599/2000 – Colombian Criminal Code:** Classification of crimes that give rise to Money Laundering.
- **Law 747/2002:** Amendments to the Criminal Code (Law 599 of 2000), which established the criminal offense of human trafficking and set forth other related provisions.
- **Decree 3420 of 2004:** Amended the structure and functions of the Inter-Institutional Coordination Commission for Anti-Money Laundering.
- **Law 1121 of 2006:** Provisions for the prevention, detection, investigation, and sanctioning of terrorist financing and other related regulations.

**5.2.** Maintain the position of Compliance Officer and allocate the necessary human, technical, financial, and operational resources required for the proper performance of their duties.

**5.3.** All employees are obligated to safeguard the general interest of the Organization and comply with this Policy to prevent the materialization of ML/TF/FPWMD risks. Any violation thereof shall be considered a serious offense, in accordance with the provisions of the Internal Work Regulations.

**5.4.** C.I. PROINGRA S.A.S. shall not establish any relationship with individuals, legal entities, or any other third party listed in the binding restrictive lists applicable in Colombia that indicate a connection to ML/TF/FPWMD activities or related offenses, whether nationally or internationally. If, during a commercial relationship, it is discovered that the counterparty is involved in illicit activities or is included in the OFAC or UN lists, such commercial relationship shall be terminated.

**5.5.** C.I. PROINGRA S.A.S. shall not enter any business or other type of relationship with individuals or legal entities where there is reasonable doubt about the legality of the operations, or the origin and/or use of the resources involved. Likewise, the company's name shall not be used to carry out business or financial transactions on behalf of third parties outside the scope of its corporate purpose.

**5.6.** C.I. PROINGRA S.A.S. is committed to conducting responsible and secure business. Accordingly, it establishes clear and mandatory procedures for the selection, evaluation, and due diligence of all its business associates, with the aim of determining their risk level and criticality and ensuring the proper due diligence process in all stages of engagement, updating, and disengagement.

**5.7.** C.I. PROINGRA S.A.S. shall only establish relationships with natural or legal persons whose identity and background can be verified, as a prerequisite to access the products it offers or sells, and likewise, for any purchases it makes. If a natural or legal person fails to provide any type of information required for due diligence, the company must abstain from establishing a relationship in order to protect itself from ML/TF/FPWMD risks.

**5.8.** The execution of activities, business transactions, or contracts without the corresponding internal or external documentation is prohibited. All transactions with clients, suppliers, employees, partners, or third parties must be carried out through the information systems made available by the company, ensuring that proper evidence and records are maintained.

**5.9.** If Politically Exposed Persons (PEPs) are identified during the client, supplier, employee, and/or partner due diligence processes, additional controls must be implemented, and any operation and/or business activity must be approved by a higher authority within the company.

**5.10.** The information of business associates who maintain an active relationship with the company must be updated and evaluated annually. If these natural or legal persons fail to provide the required information for the corresponding update, the Compliance Officer and General Management must assess each case individually to decide whether to continue the commercial relationship.

**5.11.** C.I. PROINGRA S.A.S. shall train all its employees to ensure the timely reporting of unusual and suspicious activities related to ML/TF/FPWMD. These training sessions shall be held at least once a year and led by the Compliance Officer.

**5.12.** All payments made by C.I. PROINGRA S.A.S. through bank transfers and/or checks in the ordinary course of its business shall be made exclusively to the name and/or bank account of the rightful beneficiary. Any exceptions, due to specific events, must be documented in writing and authorized solely by the Legal Representative.

**5.13.** Employees who become aware of a criminal offense must comply with their civic duty to report it. The filing of a Suspicious Activity Report (SAR) does not exempt the obligation to report, where applicable, as stated in Article 27 of the Colombian Penal Code.

**5.14.** Control of Perimeter Barriers:

- Implement access control for personnel and vehicles.
- Keep all doors closed to prevent unauthorized entry.
- Monitor and maintain perimeter barriers at least every 12 months to ensure they remain in proper condition.

**5.15.** The information and documents managed by C.I. PROINGRA S.A.S. in matters related to ML/TF/FPWMD are confidential in nature.

Accordingly, employees who have access to such information must handle it in a confidential manner and shall not use it for their own benefit or for the benefit of third parties.

(Policy Code – Version 02 – July 2nd, 2024)