SAGRILAFT

MANUAL

SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM

AL/FT/FPWMD

Version 24/08/2021

Integral S.A.

Integral
INGENIEROS CONSULTORES

Impacto Positivo

TABLE OF CONTENTS

CHAPTER I: GENERAL ASPECTS

1. INTRODUCTION

The risk of asset laundering, also known as money laundering, and the Financing of Terrorism, are determining factors in the possibility of loss or damage that a company may suffer due to its propensity to be used directly or through its operations as an instrument for the channeling of resources to carry out terrorist activities, or when it is intended to conceal assets derived from such activities.

Asset laundering and the financing of terrorism, hereinafter AML/CFT, is one of the greatest exposure risks for companies, and it also generates negative consequences for the country's economy and in particular for companies in the real sector of the economy, affecting their competitiveness, productivity and durability with tendencies to destabilize entire societies and economies; these risks can be of a Legal, Reputational, Operational and Contagion type.

Due to this, it corresponds to INTEGRAL S.A., hereinafter the Company, dedicated to developing comprehensive engineering solutions for public and private entities, participating in all phases of the development of projects, from their identification and basic conception to their commissioning, to undertake the design and implementation of a Self-Control and Comprehensive Risk Management System of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD).

In this sense, INTEGRAL S.A has designed and implemented the policy of the Self-Control and Comprehensive Risk Management System of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD) in accordance with the criteria and regulatory duties defined by the Superintendency of Companies as stipulated in chapter X of the Basic Legal Circular, and the regulation that may modify or replace it, and good corporate governance practices.

The purpose of this Manual is, through the clear and effective definition of policies, procedures and controls in the Self-Control and Comprehensive Risk Management System of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD), to minimize the probability of risk to which the

company may be exposed, in case of being used through the products and services offered for asset laundering and financing of terrorism. Due to this, this manual is a tool to generate culture and awareness in all employees of the company, and is available for permanent consultation, in order to address doubts or concerns regarding the functions and responsibilities in matters of AML/CFT/FPWMD.

2. SCOPE

The Self-Control and Comprehensive Risk Management System of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD) designed by INTEGRAL S.A is of mandatory compliance, without exception, for all employees, positions of directive and managerial level, and even for shareholders or partners of the company. They will be responsible for the observance of the policy in what corresponds to their profile, for as long as the relationship lasts, except with respect to the duty of confidentiality and reserve that subsists after the termination of the relationship.

3. OBJECTIVES

3.1. General Objective

I. Provide policies, procedures and controls for the different processes of the company to allow reduce the probability of occurrence or impact of risk events related to AML/CFT/FPWMD, and tools to all employees to enable them to clearly comply with policies and procedures in an effective manner, identifying and foreseeing actions contrary to the regulation and the legal framework in force.

3.2. Specific Objectives

I. Design a System based on policies and procedures for the prevention and control of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD), in accordance with legal regulations and the company's internal procedures.

II. Design the Self-Control and Comprehensive Risk Management System of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD), allowing to manage in an effective and timely manner the risks to which the company could be exposed.

III. Establish rules of conduct for related persons, regardless of the form and nature of their relationship, and thus commit all employees of the company to comply with the policies of the Self-Control and Comprehensive Risk Management System of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD).

IV. Make known to all employees the importance of preventing and controlling Asset Laundering, the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction, and the consequences that this entails for the company.

V. Institute procedures for knowledge, linkage and updating of customers, suppliers, employees, associates and any other source of risk.

4. REGULATORY FRAMEWORK

4.1. International Norms and Standards on AML/CFT/FPWMD[1]

Colombia has ratified, among others, the following United Nations conventions and agreements, in order to confront criminal activities related to AML/CFT/FPWMD.

The following is the name of the convention, the law approving it and the ruling on its constitutionality issued by the Constitutional Court within the ratification process:

- Vienna Convention of 1988: United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Approved by Law 67 of 1993, Ruling C-176 of 1994).
- United Nations Convention for the Suppression of the Financing of Terrorism of 1999 (Approved by Law 808 of 2003, Ruling C-037 of 2004).
- Palermo Convention of 2000: United Nations Convention Against Transnational Organized Crime (Approved by Law 800 of 2003, Ruling C-962 of 2003).

[1] Circular 100-000016 of December 24, 2020.

- Merida Convention of 2003: United Nations Convention Against Corruption (Approved by Law 970 of 2005, Ruling C-172 of 2006).

For its part, the FATF [Financial Action Task Force] designed the FATF Recommendations, in which such intergovernmental body urged the countries to identify the AML/CFT/FPWMD Risks to which their financial institutions and DNFBPs [Designated Non-Financial Businesses and Professions] are exposed and, based on that risk, to adopt measures to mitigate it, with a risk-based supervisory approach, with more flexible measures and in line with the nature of the risks duly identified (FATF Recommendation No. 1).

The interpretative note to FATF Recommendation No. 1 states that, in implementing a risk-based approach, DNFBPs should have processes in place to identify, assess, monitor, manage and mitigate AML/CFT/FPWMD Risks. The general principle of a risk-based approach is that, where major risks exist, intensified measures should be implemented to manage and mitigate those risks; and, for their part, where the risks are minor, the application of simplified measures may be allowed. In any case, simplified measures are not allowed when there is a suspicion of AML/CFT/FPWMD.

In turn, FATF Recommendation No. 15 urges the countries to take measures to manage and mitigate the AML/CFT/FPWMD Risks associated with Virtual Assets, for which they must regulate Virtual Asset service providers and, in order for them to be subject to effective monitoring systems, comply with the FATF Recommendations, among them the one of Due Diligence (Cf. Rec. 10).

In addition, FATF Recommendation No. 28, paragraph (b), states that the countries should ensure that DNFBPs are subject to effective regulatory and supervisory systems. This activity should be carried out by a supervisor or by an appropriate self-regulatory body, provided that such body can ensure that its members comply with their obligations to combat AML/CFT/FPWMD.

Finally, FATF considers that, for a supervisory system to have effective results, the countries must ensure effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, applicable to natural or legal persons that fail to comply with the measures to combat AML/CFT/FPWMD, including their directors and senior management.

4.2. National Standards[1]

Law 526 of 1999 created the Financial Information and Analysis Unit, as a Special Administrative Unit of a technical nature, attached to the Ministry of Finance and Public Credit, whose functions will be of intervention of the State in order to detect practices associated with asset laundering.

Likewise, Law 1121 of 2016 issued a series of regulations with the purpose of preventing, detecting, investigating and sanctioning the financing of terrorism; without prejudice to Laws 599 of 2000 (Criminal Code) and Law 906 of 2004 (Code of Criminal Procedure), which regulate in a precise manner the conducts characterized in this matter and their sanction, as well as the rest of the subsequent laws that modify the Criminal Code in a precise manner, and that, for the special case, it is necessary to exemplify with Law 747 of 2002, which created the criminal offense of "trafficking in persons" as a source crime for the criminal offense of asset laundering.

Decree 1068 of 2015 established that public and private entities, among them the real sector of the economy, must report suspicious transactions to the Financial Information and Analysis Unit (UIAF [for its Spanish acronym]) in accordance with the provisions set forth for this purpose in the Organic Statute of the Financial System when the UIAF may request and in the form and opportunity that it may require. In this regard, Decree 1023 of 2012 established that the Superintendency of Companies should instruct the entities subject to its supervision on the measures to be adopted for the prevention of AML/CFT risk. For this reason, the National Council for Economic and Social Policy (CONPES [for its Spanish acronym]) approved the CONPES Document 3793 of 2013, which established the guidelines for the implementation of the national anti-AML/CFT policy with the objective of achieving a single, coordinated, dynamic and effective system for the prevention, detection, investigation and prosecution of AML/CFT.

Likewise, in the year 2009, the Superintendency of Companies adopted a series of recommendations through Circular 100-004 to prevent the risk of asset laundering and the

financing of terrorism, until reaching Circular 100-000016 of 2020, which has the purpose of providing guidelines to companies in the real sector to develop a Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD -SAGRILAFT [for its Spanish acronym]-.

CHAPTER II: DEFINITIONS

For the correct application and understanding of this manual, it is necessary to take into account the definitions established in Chapter X of the Basic Legal Circular of the Superintendency of Companies and other definitions applicable to Integral S.A.:

Virtual Asset: is the digital representation of value that can be traded or transferred digitally and can be used for payments or investments. Virtual assets do not include digital representations of fiat currency, securities and other financial Assets that are already covered elsewhere in the FATF Recommendations[1].

Assets: is a present economic resource controlled by the Company as a result of past events.

DNFPPs: are the designated non-financial businesses and professions of Companies, which for the purposes of this circular are the following: i) sector of real estate agents; (ii) sector of marketing of precious metals and stones; (iii) sector of accounting services; and (iv) sector of legal services.

Geographical Area: is the area of the territory where the Company develops its activity.

Final Beneficiary(ies): is(are) the natural person(s) who ultimately own(s) or control(s) a customer or the natural person on whose behalf a transaction is made. This also includes the person(s) exercising effective and/or final control, directly or indirectly, over a legal person or other structure without legal personality. The following are Final Beneficiaries of the legal person:

a. Natural person who, acting individually or jointly, exercises control over the legal person, in the terms of article 260 and subsequent articles of the Code of Commerce; or

[1] Definition contained as an attachment, interpretative note to FATF Recommendation No. 15 - New FATF Technologies, available at: http://gafilat.info/index.php/es/biblioteca-virtual/3486-recomendaciones-y-metodologia-act-jul-19-publico

b. 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 person, and/or benefits in five percent (5%) or more from the return, profits or Assets of the legal person;
c. When no natural person is identified in paragraphs 1) and 2), the natural person who holds the position of legal representative, unless there is a natural person who holds greater authority in relation to the management or direction functions of the legal person.

The Final Beneficiaries of a trust contract, of a structure without legal personality, or of a similar legal structure, are the following natural persons who hold the status of:

i. Trustor(s), settlor(s), constituent(s) or similar or equivalent position;
ii. Trust committee, financial committee or similar or equivalent position;
iii. Trustee(s), beneficiary(ies) or conditional beneficiaries; and
iv. Any other natural person who exercises effective and/or final control, or who has the right to enjoy and/or dispose of the Assets, benefits, results or profits.

Counterparty: is any natural or legal person with whom the Company has commercial, business, contractual or legal ties of any kind. Among others, the associates, employees, customers, contractors and suppliers of the Company's Products are counterparties.

Due Diligence: is the process by which the Company adopts measures for the knowledge of the Counterparty, its business, operations, and Products and the volume of its transactions, which is developed established in paragraph 5.3.1 of this Chapter X.

Intensified Due Diligence: is the process by which the Company adopts additional and more intense measures for the knowledge of the Counterparty, its business, operations, Products and the volume of its transactions, as established in paragraph 5.3.2 of this Chapter X.

Company: is the commercial company, sole proprietorship or branch of a foreign company supervised by the Superintendency of Companies.

Obligated Company: is the Company that must comply with the provisions of this Chapter X and which is listed in number 4 of this chapter.

Financing of Terrorism or FT: is the crime regulated in article 345 of the Colombian Criminal Code (or the regulation that may substitute or modify it).

Financing of the Proliferation of Weapons of Mass Destruction or FPWMD: is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fractionation, transportation, transfer,

deposit or dual use for illegitimate purposes in contravention of national laws or international obligations, when the latter is applicable[1].

AML/CFT/FPWMD Risk Factors: are the possible elements or causes generating the Risk of AML/CFT/FPWMD for any Obligated Company. The Obligated Company shall identify them taking into account the Counterparties, Products, activities, channels and jurisdictions, among others.

FATF: is the Financial Action Task Force. Intergovernmental group created in 1989 in order to issue standards to the countries for the fight against AL, FT and FPWMD.

GAFILAT: is the Financial Action Task Force of Latin America [for its Spanish acronym], a regionally based body of the FATF, created in the year 2000 and in which Colombia is a member.

AML/CFT/FPWMD: Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction.

Asset Laundering or AL: is the crime characterized in article 323 of the Colombian Criminal Code (or the regulation that may substitute or modify it).

Binding Lists: are those lists of persons and entities associated with terrorist organizations that are binding on Colombia under Colombian law (article 20 of Law 1121 of 2006) and in accordance with international law, including, among others, Resolutions 1267 of 1999, 1373 of 2001, 1718 and 1737 of 2006, 1988 and 1989 of 2011, and 2178 of 2014 of the United Nations Security Council, and all those that may succeed, relate to or complement them, and any other list binding on Colombia (such as the lists of terrorists of the United States of America, the European Union list of Terrorist Organizations and the European Union list of Persons Cataloged as Terrorists).

AML/CFT/FPWMD Risk Matrix: is one of the instruments that allows the Company to identify, individualize, segment, evaluate and control the AML/CFT/FPWMD Risks to which it could be exposed, according to the identified AML/CFT/FPWMD Risk Factors.

Reasonable Measures: are the sufficient and appropriate actions, measurable in quality and quantity to mitigate the AML/CFT/FPWMD Risk, taking into account the Obligated Company's own risks and their materiality.

[1] https://www.uiaf.gov.co/sistema_nacional_ala_cft/lavado_activos_financiacion_29271/financiacion_proliferacion_armas_30528

Compliance Officer: is the natural person designated by the Obligated Company who is in charge of promoting, developing and ensuring compliance with the specific procedures for the prevention, updating and mitigation of the AML/CFT/FPWMD Risk.

Unusual Operation: is the operation whose amount or characteristics are not related to the ordinary or normal economic activity of the Obligated Company or which, due to its number, quantity or characteristics, is not framed within the guidelines of normality or ordinary business practices in a sector, in an industry or with a class of Counterparty.

Suspicious Operation: is the Unusual Operation that, in addition, according to the uses and customs of the activity in question, could not be reasonably justified. This type of operation includes attempted or rejected operations that contain characteristics that give them the character of suspicious.

PEPs: means politically exposed persons, that is, they are the public servants of any system of nomenclature and classification of jobs of the national and territorial public administration, when in the positions they occupy they have, in the functions of the area to which they belong or in those of the description of the job they occupy, under their direct responsibility or by delegation, the general direction, the formulation of institutional policies and the adoption of plans, programs and projects, or the direct management of goods, money or securities of the State. These can be through expenditure management, public procurement, investment project management, payments, settlements, or administration of movable and immovable property. It also includes Foreign PEPs and PEPs of International Organizations.

PEPs of International Organizations: are those natural persons who perform managerial functions in an international organization, such as the United Nations Organization, the Organization for Economic Cooperation and Development, the United Nations Children's Fund (UNICEF) and the Organization of American States, among others (for example, directors, deputy directors, members of the board of directors or any person performing an equivalent function).

Foreign PEPs: are those natural persons who perform prominent and outstanding public functions in another country. In particular, the following persons: (i) heads of state, heads of government, ministers, undersecretaries or secretaries of state; (ii) congressmen or parliamentarians; (iii) members of supreme courts, constitutional courts or other high judicial bodies whose decisions do not normally admit appeal, except in exceptional circumstances; (iv) members of tribunals or of boards of directors of central banks; (v) ambassadors; (vi) business managers; (vii) senior officials of the armed forces; (viii) members of administrative, managerial or supervisory bodies of state-owned companies; (ix) members of reigning royal families; (x)

prominent leaders of political parties or movements; and (xi) legal representatives, directors, deputy directors, members of senior management and members of the Board of an international organization (for example, heads of state, politicians, high-ranking governmental, judicial or military officials, and senior executives of state-owned companies).

Products: are the goods and services that the Company produces, markets, transforms or offers or acquires from a third party.

AML/CFT/FPWMD Risk: is the possibility of loss or damage that a Company may suffer due to its propensity to be used directly or through its operations as an instrument for Asset Laundering and/or channeling of resources to carry out terrorist activities or for the Financing of the Proliferation of Weapons of Mass Destruction, or when it is intended to conceal Assets derived from such activities. The contingencies inherent to AML/CFT/FPWMD materialize through risks such as Contagion Risk, Legal Risk, Operational Risk, Reputational Risk and others to which the Company is exposed, with the consequent negative economic effect that this may represent for its financial stability, when it is used for such activities.

Contagion Risk: is the possibility of loss that a Company may suffer, directly or indirectly, from an action or experience of a Counterparty.

Legal Risk: is the possibility of loss incurred by a Company when it is sanctioned or obligated to compensate damages as a result of noncompliance with rules or regulations and contractual obligations. It also arises as a consequence of failures in contracts and transactions, derived from malicious actions, negligence or involuntary acts that affect the formalization or execution of contracts or transactions.

Operational Risk: is the possibility of incurring losses due to deficiencies, failures or inadequacies in human resources, processes, technology or infrastructure, or due the occurrence of external events. This definition includes the Legal Risk and the Reputational Risk associated with such factors.

Reputational Risk: is the possibility of loss incurred by a Company due to loss of prestige, bad image, negative publicity, true or not, with respect to the organization and its business practices, causing loss of customers, decrease in revenues or judicial processes.

Inherent Risk: is the own risk level of the activity, without taking into account the effect of controls.

Residual Risk: is the risk level resulting after applying the controls.

ROS: is the Suspicious Operation Report [for its Spanish acronym]. Such is an operation which, due to its number, quantity or characteristics, is not framed within the normal system and

practices of the business, of an industry or of a certain sector and which, in addition, according to the uses and customs of the activity in question, could not be reasonably justified.

SAGRILAFT: is the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD [for its Spanish acronym], established in Chapter X of the Basic Legal Circular of the Superintendency of Companies.

UIAF: is the Financial Information and Analysis Unit [for its Spanish acronym], which is the financial intelligence unit of Colombia, with the functions of intervening in the economy to prevent and detect AML/CFT/FPWMD.

CHAPTER III: POLICIES FOR THE ADMINISTRATION OF THE SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM FOR AML/CFT/FPWMD

1. GENERAL POLICIES

In order to mitigate the AML/CFT/FPWMD risk, the following are the general guidelines adopted by INTEGRAL S.A., seeking the efficient, effective and timely development of the Self-Control and Comprehensive Risk Management System for Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD), aiming to make the best decisions with respect to its exposure.

I. Risks, risk generating factors and controls for the mitigation of the ALFT [Asset Laundering and Financing of Terrorism] risk will be included in the company's risk matrix.

II. The controls for risk mitigation will have a periodic follow-up in order to know the effective and timely implementation.

III. The decision to assume AML/CFT/FPWMD risks must be submitted for approval to the Board of Directors or to whom the Board may delegate this function. In the case of PEPs, the decision to assume risks will be made by the Chief Executive Officer.

IV. The Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD will be known to all employees of the company.

V. Employees must comply with the procedures established in the manual to prevent and control behaviors related to LA/FT/FPWMD.

VI. Compliance will be given to the guidelines established by the Board of Directors in matters of Prevention and control of AML/CFT/FPWMD and the Chief Executive Officer in relation to the contracting of PEPs.

VII. There will be a Compliance Officer who will be provided with the human, technical, financial and operational resources to develop and monitor the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD.

VIII. Relevant information will be requested in the linking of counterparties to avoid risks associated with AML/CFT.

IX. There will be collaboration with the competent authorities through the delivery of the required information.

X. The employees of INTEGRAL S.A. are responsible for identifying the risks related to AML/CFT/FPWMD and determining the applicable control in accordance with the established matrix.

XI. The risk rating is based on the impact that the event would generate in economic and reputational matters for the company.

XII. The controls implemented by the company seek to reduce the probability of occurrence and/or impact of AML/CFT/FPWMD risk.

XIII. An express and justified record must be kept of the risks assumed with respect to AML/CFT/FPWMD by the Board of Directors or its delegate.

XIV. Training and/or communications will be provided to the company's employees, according to their level of exposure and link to the risk factor, in order to generate organizational culture and contextualize employees in the identification of risks associated with AML/CFT/FPWMD and the procedure to be followed to mitigate them.

XV. A follow-up report will be issued on the Self-Control and Risk Management System for AML/CFT/FPWMD, for which the compliance officer will be in charge.

XVI. Effective processes will be in place to facilitate the timely detection of unusual and/or suspicious operations.

XVII. The compliance officer will report to the UIAF in a timely manner, that is, once the suspicious transaction has been identified; it will be reported immediately.

2. COMPREHENSIVE POLICIES WITH INTERNAL REGULATIONS

The policies adopted by the company in relation to the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD, are linked to the Internal Work Rules prescribed by INTEGRAL S.A., which state that employees must comply with general duties and special obligations; and any conduct of breach or violation of obligations and/or prohibitions contained therein will be sanctioned in accordance with the procedure provided for in the law and in the Internal Work Rules.

CHAPTER IV: CONTROL MECHANISMS

1. IDENTIFICATION OF SOURCES OF RISK SUBJECT TO ADMINISTRATION AND CONTROL

According to the *n*ature of Integral S.A.'s risk, the following are identified as risk factors:

Counterparties: which, by virtue of the business, contractual or legal relationship they have with the company, intervene in the development of its main and related corporate purpose, namely:

I. Public and private sector customers, domestic and foreign.
II. Suppliers of domestic and foreign goods and services.
III. Employees and personnel in the selection process.
IV. Business partners or associates, domestic and foreign.
V. Shareholders.

Jurisdictions: The territorial jurisdiction where the counterparties are domiciled is considered as a risk factor, in case they are exposed to the risk of AML/CFT/FPWMD. High-risk jurisdictions will be those identified as non-cooperating countries.

Channel: Since there are no identified sales channels, this risk factor will not be taken into account.

Products: Considering that the company offers two types of services (Design – Auditing) and there is no risk differentiation for both, this is considered as a general risk and does not have an attribute to establish higher levels of control.

Activities: As part of the risk factors, the economic activity carried out by the counterparty will be taken into account. In this aspect, the provisions of the Superintendency of Companies regarding activities of greater risk will be consulted.

2. POLICIES AND CONTROLS

The following general guidelines on self-control and comprehensive risk management of Asset Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (AML/CFT/FPWMD), aim to achieve the proper functioning of the SAGRILAFT and guide the work of managers, advisors, employees, trainees, agents, and, in general, of any natural or legal person acting duly authorized on behalf of the company or legally or contractually related to it.

2.1. Counterparty knowledge policies

I. In order to start contractual and/or commercial relations with natural or legal persons, information contained in the Knowledge Form provided by the company and the respective attachments must be requested.
II. In the case of public sector customers, bidding procedures must be complied with, determining the customer's requirements for the service. These may be specified in a document, communicated by another means, or may have been agreed with

the customer, but always in compliance with the parameters determined in the management system procedures established by the company and in accordance with the procedures established by the standard in force at the time of the awarding of the contract.

III. No counterparties may be linked or maintain commercial relationships, whether natural or legal persons, which are on restrictive lists such as those of OFAC, UNO and other binding lists of risk in matters of AML/CFT established in Chapter X of the Basic Legal Circular.

IV. The verification in restrictive lists of legal entities will also be carried out with respect to the members of the highest corporate body, Associates (Partners/Shareholders) with participation equal to or greater than 5%, Legal Representatives, Statutory Auditor, among others.

V. In order to carry out the due diligence of counterparties, the completion of the counterparty knowledge form provided by the company must be requested, which must be fully filled out. In the event that a field is not applicable to the third party, the third party must state it in this way: **(N/A).**

VI. Compliance with the requirements established in the procedure will be verified; for this purpose, a record will be made with the name of the person responsible and the date of the review.

VII. The counterparty knowledge form may be completed physically and/or digitally and sent with the attached documentation, namely, Single Tax Registry (RUT [for its Spanish acronym]) **(mandatory)**, Certificate of Existence and Legal Representation with validity not older than **30 days** and other required documents.

VIII. A declaration of origin of the resources will be requested from all counterparties, natural or legal persons, with a relationship with the company.

IX. For both natural and legal persons, once the form has been completed, and sent digitally or by e-mail, these data messages will have the probative value established in Law 527 of 1999 or in the regulations that may replace, modify or be added to this law.

X. Advanced due diligence activities will be performed, when alerts are found in the initial verification.

XI. In the case of customers who are Politically Exposed Persons (PEPs), measures of greater diligence will be required. Therefore, there will be verification in restrictive lists and authorization to link them will be requested from the Chief Executive Officer or whoever the latter may designate.

XII. Updates of customer and supplier data will be made once (1) a year, without prejudice to updates that may arise due to the commercial relationship and be presented as a novelty.

XIII. A counterparty will be considered inactive when a period of one (1) year elapses without any contractual and/or commercial relationship existing. In cases in which it is intended to reactivate the relationship with the company, there must be compliance with all the requirements demanded for such purpose.

XIV. The compliance officer must ensure, through semi-annual verifications, that the procedure defined by the company to link counterparties is complied with.

XV. The employees of INTEGRAL S.A. have the obligation to follow all the mechanisms of knowledge of counterparties. The **exceptions** to these procedures must be approved by the **presidency** and be supported by documents or must be related to the exception policies that may be implemented.

XVI. For counterparties located in a territorial jurisdiction with restrictions or located in zones with the influence of illegal groups, an advanced due diligence must be urged, not only complying with the procedure established for the knowledge of the customer, but also having each one of the counterparty's operations subject to constant follow-up.

2.2. Policy on knowledge of employees and personnel in the selection process:

I. It will not be possible to link personnel or maintain an employment relationship with employees who are on restrictive lists such as those of OFAC, UNO and other binding lists of risk in matters of AML/CFT established in Chapter X of the Basic Legal Circular.

II. The selection of employees will conform to the comprehensive management selection procedure established by the company to provide its areas with human resources.

III. The personnel working for the company must provide verifiable information. If changes are produced in the information initially provided, they must report them to the Human Resources area.

IV. The personnel that were selected to join the company will carry out their annual update while they are working in the company, in Physical and/or digital form, attaching the required documentary supports.

V. The compliance officer must ensure, through semi-annual verifications, that there is compliance with the procedure defined by the company for knowledge of employees and personnel in the selection process.

VI. The employees of Integral S.A. have the obligation to follow all the mechanisms of knowledge of employees and personnel in the selection process. The **exceptions** to these procedures must be approved by the **board of directors** or by whoever it authorizes and be supported by documents or must be related to the exception policies that may be implemented.

VII. The linking of employees who are PEPs will require measures of greater diligence. Therefore, there will be verification in restrictive lists and authorization to link them will be requested from the Chief Executive Officer or whoever the latter may designate.

VIII. To keep employee data up to date, information updating strategies will be established that seek to keep the information current at least once a year.

IX. In compliance with the due diligence, all employee hirings will be subject to the verification process, which will also include the declaration of the origin of their resources. Without exception, the information declared will be analyzed and each one of the attached documents will be reviewed. A record of the analysis conducted will be kept with the name of the person responsible for the review and the date of entry.

2.3. Shareholder knowledge policy

I. For the admission of new shareholders, the provisions of the bylaws regarding the Right of First Refusal for the acquisition of shares will be maintained.

II. In the event that new shareholders are admitted, they must fill out the shareholder knowledge form. If they are legal persons, their shareholders or associates with a stake equal to or greater than 5% of the share capital, Legal Representatives, Statutory Auditor, among others, will also be verified.

III. No new shareholders may be linked, whether natural or legal persons, which are on restrictive lists such as those of OFAC, UNO and other binding lists of risk in matters of AML/CFT established in Chapter X of the Basic Legal Circular.

IV. For both natural and legal persons, once the form has been completed, it must be sent electronically through the information system provided for this purpose and by e-mail, attaching the documentary supports required for each case, with these data messages having the probative value established in Law 527 of 1999 or in the regulations that may replace, modify or be added to this law.

2.4. Handling of individual cash transactions and operations

I. All transactions will be carried out through the means authorized by financial institutions, such understood as electronic transfer, PSE [Spanish acronym for Secure Online Payment] Button Payment, Barcode Payment, ATH [Spanish acronym for Around the Clock] Payment, Payment Agreement, Payment by check, among others.
II. There may be operations and/or transactions which in the ordinary course of business involve payments by delivery or receipt of cash only with respect to the amounts existing in petty cash. Any exception to this provision must be authorized by the board of directors or its designee.

2.5. Identification of warning signs

The following are some of the warning signs that can help in the detection of unusual and/or suspicious transactions of natural or legal persons:

Customers/Suppliers

I. They are domiciled in non-cooperating countries or within their operations they carry out transactions or have links with non-cooperating countries with AML/CFT prevention issues.
II. They are reluctant or annoyed when asked for proper identification or completion of the Knowledge Forms.
III. They have a very low subscribed capital and/or a very broad corporate purpose.
IV. They act on behalf of third parties attempting to conceal the identity of the counterparty or real user.
V. They threaten or attempt to bribe the employee of the entity to accept incomplete or false information or not to fill out the information registration form.
VI. They have very good economic solvency, but they find it difficult to obtain references or co-debtors.
VII. They record the same address and/or telephone number of other persons with which they have no apparent relationship.
VIII. They define their economic activity as "independent", "trader" and handle large amounts of money.
IX. They refuse to support an operation or to update basic information.

X. They provide false, difficult to verify or insufficient information.
XI. They are nervous when asked for the required information, hesitate in their answers and/or bring the requested information in writing.
XII. They offer products or services for prices below normal market costs, or higher purchases.
XIII. Constant modifications of the corporate purpose, name or business name and of their representatives or administrators.

Employees

I. They refuse to provide the information required on the employee knowledge form.
II. They have an alert in the restrictive lists in which the risk verification is carried out.
III. Finding inconsistent information between the completed form and the verification carried out.
IV. Finding apparent or simulated information in the completed forms.
V. Impossibility to verify the information entered in the single knowledge form.
VI. High frequency of changes in the basic data provided.
VII. Reluctance to enjoy holidays.
VIII. Reluctance to accept a promotion or change of activity.
IX. Standard of living that does not correspond to the income received.
X. They prevent other employees from serving certain customers or suppliers.

Financial operations

I. Transfers received of a good or service which due to its characteristics and market prices would not be necessary or logical to purchase in another country.
II. Transfers received from a country other than the one where the purchase/sale of a good or service was made, without apparent justification.
III. Transfers received for the purchase/sale of a good or service from a country considered to have low controls against asset laundering and/or financing of terrorism.
IV. Transfers received for the purchase/sale of a good or service in which the documents or contracts constantly present errors, inconsistencies, incoherences, or are not related to the exported goods or services.

V. Transfers received for the purchase/sale of a good or service that are immediately withdrawn from the bank accounts by means of multiple checks or local transfers with signs of fractionation or with irregularities.

VI. Transfers received for the purchase/sale of a good or service that are withdrawn from the bank accounts by means of multiple checks or local transfers in favor of persons which are not suppliers or service providers of the exporting company.

VII. Transfers received for the purchase/sale of a good whose total amount represents a lower value of the quantity of goods declared. That is, it is a fictitious export.

VIII. Transfers received for the purchase/sale of a good or service in which the administrators of the exporting company are very young or lack knowledge and experience in the sector and additionally participate in the management of other similar companies.

IX. Transfers received for the purchase/sale of a good or service in which the corporate purpose or commercial activity of the purchaser does not coincide with or is not related to the good or service that is being paid.

2.6 Intensified due diligence policy

I. An intensified due diligence will be carried out on those persons regarding which, within the initial knowledge, some type of alert has been determined.

II. The persons classified as PEPs will be asked to expand the information by means of a form where the following information will be requested:
   a. Spouses or life partners of the PEP.
   b. Relatives of the PEPs, up to the second degree of consanguinity, second degree of affinity and first civil degree.
   c. Members of a PEP, when the PEP is a partner of, or is associated with, a legal person and, in addition, directly or indirectly owns a stake of more than 5% of the legal person, or exercises control of the legal person, in the terms of Article 261 of the Code of Commerce.

III. Persons located in Countries classified as non-cooperating. In the case of requiring contracting with a person located in a country classified by the FATF as non-cooperating, the approval of the board of directors must be requested for their contracting and a rigorous study must be made by a specialized external company.

IV. Persons that have investments in virtual assets or that received, as part of the capital contribution, virtual assets, must be asked to do the following:
   a. Request a certificate of partners or shareholders.
   b. They will be asked to update data and documentation on an annual basis.
   c. A declaration of Origin of Funds will be requested.

2.7 Information management policy

I. The policy of the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD must be kept in the files of the compliance officer, as a guarantee of its integrity, timeliness, reliability and availability.

II. The documentary records that will support the operations, businesses and contracts, the reports, briefs, and other supports associated with the SAGRILAFT, must be stored for a period of ten (10) years in order to have the evidentiary material of due diligence.

III. The conservation of documents will be carried out in a sequential and chronological manner, and it will be sought, to the extent possible, to support it through a digital copy stored in a technological tool.

IV. Each employee or person in charge of establishing the link with the counterparty is responsible for the integrity, veracity, reliability and confidentiality of the information collected.

V. Only each person responsible and the control bodies for AML/CFT risk management, in particular the compliance officer or the competent authority if required, shall have access to the consultation of the counterparty's information.

2.8 Training policies

I. The compliance officer will design the company's training strategy. This training will be carried out at least once a year in person or virtually by the compliance officer or by the compliance officer’s designee.

II. Additional training sessions may be provided to the specific area that may require them, prior request to the compliance officer.

III. Training for new employees will be included in the induction process.

IV. If there is an update to the "Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD", a communication will be sent to the strategic personnel, as well as in case of a modification to the applicable regulation. This communication will be a Newsletter of the company, sent through the corporate e-mail and posted on billboards. These updates, in turn, will be disseminated by strategic employees to the personnel under their charge.

V. Area directors will communicate warning signs, risks or a more effective control mechanism different from those indicated in the SAGRILAFT to the compliance officer, through institutional mail.

VI. In these trainings there will be dissemination of the policies, procedures, roles and responsibilities with respect to the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD, of each one of the areas related to counterparties or "risk factors" of AML/CFT/FPWMD.

VII. The trainings will be mandatory for those employees who have responsibilities within the system and for those who are considered strategic (Managers and Directors).

VIII. Attendance at trainings carried out will be documented, stating the date, the subject matter covered and the name of the attendees.

IX. The Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD for external stakeholders, especially with authorities, customers and suppliers, will be carried out through the company's website.

2.9 Reporting policies for attempted and/or suspicious transactions

I. If there are reasonable grounds, evidence or doubts regarding sources of risk that could be using the company for asset laundering and/or financing of terrorism, the procedures established in this manual must be followed.

II. The employees of the company must put compliance with regulations on AML/CFT prevention and control before the particular interests of an area or unit.

III. In case of a conflict of interest, because the spouse, life partner, relatives within the second degree of consanguinity, second degree of affinity or first civil degree of the employee are linked to or involved in these situations, the superior must be informed for him/her to take charge of the procedure in accordance with the provisions of this manual.

IV. Employees and personnel linked to the company, in compliance with their functions, must be vigilant for the detection and reporting of all warning signs, attempted or unusual operations and reports that may be generated or detected on the occasion of the controls implemented in accordance with this manual; this report will be made by the area in charge and will be sent to the compliance officer, that is, once the event is detected by the employee, he/she must report this situation to his/her immediate supervisor, who in turn will deliver the duly documented report to the compliance officer, who will perform the pertinent analysis of the event and will determine the relevance and appropriateness of reporting it to the UIAF.

The report that must be delivered by the area director must contain at least:

- Full identification of the source of risk.
- Cause of the report and detailed description of the event.
- Procedure used for detection.
- Material that supports the report.
- Additional information for analysis (if applicable).

These reports must be made in writing and sent by e-mail to the compliance officer.

From the analysis performed by the compliance officer, in addition to determining the appropriateness of the report to the competent body, the compliance officer will respond to the reporting area with the determination to follow, either:

- Monitor the source of risk permanently, performing advanced due diligence processes.
- Reject the linkage, operation, transaction, negotiation or contracting with the source of risk.
- Terminate the transaction, negotiation or contracting with the source of risk.

V. The compliance officer, through the follow-up or the reports made, in case of detecting a suspicious or attempted operation within the company to give the appearance of legality to resources linked to AML/CFT or to finance practices associated with this phenomenon, will determine the appropriate action to be taken after conducting an analysis of these and will communicate it to the reporting area and, if pertinent, will immediately report to the UIAF and the other competent authorities, in accordance with the instructions designed by the entity for this purpose. It is not necessary for the compliance officer to be certain that it is a criminal activity, to identify the type of crime or to investigate suspicious transactions; it suffices to report them to the competent entity.

VI. In the event that no suspicious transactions are reported, the compliance officer will report this fact to the UIAF.

VII. Internal and external reports must be properly documented. The documents that support them must be filed chronologically, and the information that is in the custody of the compliance officer must be kept confidential.

VIII. Reports made to the UIAF must be kept for ten (10) years.

IX. Under no circumstances will the sources of risk (counterparties or third parties) be informed of the causes that gave rise to the control implemented, which has been the subject of internal analysis and/or report to the competent authority.

2.10 Policy for the provision of information to competent authorities

I. In case a suspicious, unusual or attempted operation is generated, in accordance with the established warning signs and the respective analysis, the compliance officer will report to the competent authority; for this purpose, to the UIAF.
II. If an authority requests the provision of information, it will be delivered as long as this is in compliance with the legal provisions on the matter.
III. In case of a conflict of interest, because the spouse, life partner, relatives within the second degree of consanguinity, second degree of affinity or first civil degree of the compliance officer are linked to or involved in these situations, the legal representative must be informed for him/her to take charge of the procedure in accordance with the provisions of this manual.
IV. The compliance officer will be the one in charge of delivering the information required by the requesting entities, after the fulfillment of the legal requirements.

2.11 Monitoring and control policy

The Statutory Auditor's Office and the Risk and Compliance Directorate will annually evaluate the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD, and will determine the possible failures that it may present. The findings will be documented and delivered to the compliance officer.

3. UPDATE OF THE MANUAL AND ATTACHED PROCEDURES

The policies and procedures contained in this manual will be updated after the analysis of the regulatory modifications made and of the procedures for risk mitigation, prevention and control, the context of the company and the operations carried out by it.
If the company enters a new market or acquires new products, an identification of the risks associated with AML/CFT/FPWMD must be carried out with the purpose of implementing additional controls, if required, to reduce the probability of occurrence of risk events.

CHAPTER V: ORGANIZATIONAL STRUCTURE FOR PREVENTION AND SELF-CONTROL OF AML/CFT RISKS

1. BOARD OF DIRECTORS

The main functions of this body in the field of prevention of AML/CFT/FPWMD are:

I. Establish and approve an AML/CFT/FPWMD Policy for the Obligated Company.
II. Approve the SAGRILAFT and its updates, submitted by the legal representative and the Compliance Officer.
III. Approve the SAGRILAFT procedure manual and its updates.
IV. Select and appoint the Compliance Officer and his/her respective alternate, when appropriate.
V. Analyze in a timely manner the reports on the operation of the SAGRILAFT, on the proposals for corrections and updates presented by the Compliance Officer, and make decisions regarding all the issues discussed therein. This should be recorded in the minutes.
VI. Timely analyze the reports and requests submitted by the legal representative.
VII. Make pronouncements on the reports submitted by the statutory auditor or the internal and external audits, related to the implementation and operation of the SAGRILAFT, and follow up on the observations or recommendations included. This follow-up and its periodic progress must be recorded in the corresponding minutes.
VIII. Order and ensure the technical, logistical and human resources necessary to implement and maintain the SAGRILAFT in operation, according to the requirements made by the Compliance Officer for this purpose.
IX. Establish the criteria to approve the linking of a Counterparty when it is a PEP.
X. Establish guidelines and determine those responsible for conducting audits on the compliance and effectiveness of the SAGRILAFT, in case it so determines.
XI. Verify that the Compliance Officer has the availability and capacity necessary to perform his/her functions.
XII. Verify that the Company, the Compliance Officer and the legal representative carry out the activities designated in this Chapter X and in the SAGRILAFT.
XIII. And other complementary functions.

2. EXECUTIVE PRESIDENCY AND/OR LEGAL REPRESENTATIVES

The main functions of this body in the field of prevention of AML/CFT/FPWMD are:

I. Submit with the Compliance Officer, for approval by the board of directors or the highest corporate body, the proposal of the SAGRILAFT and its updates, as well as its respective procedures manual.
II. Study the results of the AML/CFT/FPWMD Risk assessment carried out by the Compliance Officer and establish the corresponding action plans.
III. Efficiently allocate the technical and human resources, determined by the board of directors or the highest corporate body, necessary to implement the SAGRILAFT.
IV. Verify that the Compliance Officer has the availability and capacity necessary to perform his/her functions.
V. Provide effective, efficient and timely support to the Compliance Officer in the design, direction, supervision and monitoring of the SAGRILAFT.
VI. Submit to the board of directors, or the highest corporate body, the reports, requests and alerts that it considers that should be addressed by such bodies and that are related to the SAGRILAFT.
VII. Ensure that the activities resulting from the development of the SAGRILAFT are duly documented, so that it may allowed to have the information meet the criteria of integrity, reliability, availability, compliance, effectiveness, efficiency and confidentiality.
VIII. Certify to the Superintendency of Companies the compliance with the provisions of this Chapter X, when so required.
IX. Verify that the SAGRILAFT procedures develop the AML/CFT/FPWMD Policy adopted by the board of directors.
X. And other complementary functions.

3. COMPLIANCE OFFICER

The natural person designated as Compliance Officer must meet at least the following requirements:

I. Be a University professional in administrative or related areas.
II. Prove a minimum experience of 6 months in SAGRILAFT or similar positions.
III. Prove the completion of courses, diplomas courses, specializations, congresses or others that give him/her the knowledge to perform the position.
IV. Have the ability to make decisions to manage the AML/CFT/FPWMD Risk.
V. Have sufficient knowledge of risk management and understand the ordinary course of business of the Company.
VI. Have the support of a human work team and technical resources, according to the AML/CFT/FPWMD Risk and the size of the Company.

VII. Not to belong to the administration or to the corporate bodies, nor to internal or external audit or control bodies or those that perform similar functions or act in their stead in the Company.

The main functions of this body in the field of prevention of AML/CFT/FPWMD are:

I. Ensure effective, efficient and timely compliance with the SAGRILAFT.
II. Submit, at least once a year, reports to the board of directors or, in its absence, to the highest corporate body. At a minimum, the reports must contain an evaluation and analysis of the efficiency and effectiveness of the SAGRILAFT and, if applicable, propose the respective improvements. Likewise, demonstrate the results of the management of the Compliance Officer, and of the administration of the Company, in general, in the compliance with the SAGRILAFT.
III. Promote the adoption of corrections and updates to the SAGRILAFT, when circumstances may so require and at least once every two (2) years. To this end, it must submit to the board of directors or the highest corporate body, as the case may be, the proposals and justifications of the corrections and updates suggested to the SAGRILAFT.
IV. Coordinate the development of internal training programs.
V. Evaluate the reports submitted by the internal audit or whoever performs similar functions or acts in its stead, and the reports submitted by the statutory auditor or the external audit, if applicable, and adopt Reasonable Measures with respect to the deficiencies reported. If the measures to be adopted require authorization of other bodies, it must promote that these matters be brought to the attention of the competent bodies.
VI. Certify to the Superintendency of Companies the compliance with the provisions of this Chapter X, as required by the Superintendency of Companies.
VII. Verify compliance with the Due Diligence and Intensified Due Diligence procedures applicable to the Company.
VIII. Ensure the proper filing of documentary supports and other information related to management and prevention of the AML/CFT/FPWMD Risk.
IX. Design the methodologies for classification, identification, measurement and control of the AML/CFT/FPWMD Risk that will be part of the SAGRILAFT.
X. Carry out the assessment of the AML/CFT/FPWMD Risk to which the Company is exposed.
XI. Make the Report of Suspicious Operations to the UIAF and any other report or brief required by the provisions in force, as established by said rules and this Chapter X.
XII. And other complementary functions.

4. RISK AND COMPLIANCE DIRECTORATE

The main functions of this body in the field of prevention of AML/CFT/FPWMD are:

I. Strategic and operational direction of the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD.
II. Evaluate the inconsistencies and failures detected in the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD within the area as well as in other areas that are transversally responsible for the management thereof.
III. Inform the Compliance Officer of the results of the evaluations performed and present the pertinent recommendations for the improvement of the effectiveness of the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD.
IV. Support the compliance officer in the decisions that he/she must make to prevent and manage the company's AML/CFT/FPWMD associated risks.
V. Manage before the General Secretariat the cases that merit a legal opinion to allow determine the viability of the relationship with third parties.
VI. Keep confidentiality.

5. STATUTORY AUDITOR'S OFFICE

The main functions of this body in the field of prevention of AML/CFT/FPWMD are:

I. Evaluate the inconsistencies and failures detected in the Self-Control and Risk Management System for AML/CFT.
II. Inform the Compliance Officer of the results of the evaluations performed and present the pertinent recommendations for the improvement of the effectiveness of the Self-Control and Risk Management System for AML/CFT.
III. Propose and generate controls to detect breaches in the mechanisms and instructions given for the management of risks in the field of asset laundering and financing of terrorism.
IV. Monitor the SAGRILAFT.
V. Keep confidentiality.

6. ACCOUNTING DIRECTORATE

I. Be vigilant for the detection and reporting of all warning signs, attempted or unusual operations, and reports generated or detected on the occasion of its functions, and report them to the compliance officer.
II. Guard the information sent by customers and suppliers, and the requests made by customers for the modification of data.
III. Conserve the documentation that it must guard in the exercise of its functions.
IV. Keep confidentiality.

7. DIRECTORATE OF GENERAL SERVICES AND PROJECT MANAGERS

I. Request suppliers to comply with the requirements demanded for the knowledge of the supplier.
II. Verify the information provided by the suppliers and keep a record of the person responsible for the review.
III. Request the update of the information of suppliers, every twelve (12) months, by sending an e-mail to the address provided by the supplier.
IV. Perform the financial analysis of the suppliers in the process of being linked that meet the established criteria.
V. Comply with the requirements regarding quotations, approval of purchases, legalization of contracts and other aspects reiterated in the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD, in accordance with the purchasing procedure established by the company.
VI. Deliver to the compliance officer the updated information of the registered suppliers, the goods or services offered and their average price.
VII. Report to the compliance officer the suspicious, unusual or attempted operations that are detected.
VIII. Provide the database of suppliers, in accordance with the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD adopted by the company, for the verification of risks in restrictive lists.
IX. Conserve the documentation that they must guard in the exercise of their functions.
X. Keep confidentiality.
XI. And other complementary functions.

8. COMMERCIAL AND MARKETING MANAGEMENT AND PROJECT MANAGERS

I. Request customers to comply with the requirements demanded for counterparty knowledge.
II. Verify the information provided by customers and keep a record of the person responsible for the review.
III. Request the update of the information of customers, every twelve (12) months, by sending an e-mail to the address provided by the customer.
IV. Deliver to the compliance officer the updated information of the registered customers and the value of the purchases made by them.
V. Report to the compliance officer the suspicious, unusual or attempted operations that are detected.
VI. Provide the customer database, in accordance with the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD adopted by the company, for the verification of risks in restrictive lists.
VII. Request to the compliance officer the verification of risks of customers in restrictive lists.
VIII. Conserve the documentation that they must guard in the exercise of their functions.
IX. Keep confidentiality.
X. And other complementary functions.

9. HUMAN MANAGEMENT DIRECTORATE

I. Request employees and personnel in the process of selection to comply with the requirements demanded for the knowledge thereof.
II. Verify the information provided by employees and personnel in the process of selection and keep a record of the person responsible for the review.
III. Make the changes requested by employees to the data recorded in the personnel master file.
IV. Deliver to the compliance officer the updated information of the employees and personnel in the process of selection.
V. Report to the compliance officer the suspicious, unusual or attempted operations that are detected.
VI. Provide the database of employees and personnel in the process of selection, in accordance with the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD adopted by the company, for the verification of risks in restrictive lists, as applicable.

VII. Conserve the documentation that it must guard in the exercise of its functions.
VIII. Keep confidentiality.
IX. And other complementary functions.

10. MANAGERS, PROJECT DIRECTORS AND AREA DIRECTORS

I. Report to the compliance officer the suspicious, unusual or attempted operations detected by the personnel under their charge.
II. Accompany the employees under their charge in the implementation of the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD adopted by the company.
III. Attend the trainings that are scheduled.
IV. Keep confidentiality.
V. And other complementary functions.

11. COMPANY PERSONNEL IN GENERAL

I. Know the Self-Control and Comprehensive Risk Management System AML/CFT/FPWMD.
II. Identify the risks related to AML/CFT and determine the applicable control.
III. Promote the implementation of the Self-Control and Comprehensive Risk Management System for AML/CFT/FPWMD adopted by the company.
IV. Report to the area director the suspicious, unusual or attempted operations that are detected.
V. Attend the trainings that are scheduled.
VI. Comply with the requirements and requests made by the compliance officer.
VII. Inform the area director in case of a conflict of interest in a control or procedure associated with AML/CFT.
VIII. Refrain from informing the sources of risk of the causes that gave rise to the control implemented, which has been the subject of internal analysis and/or report to the competent authority.
IX. Keep confidentiality.

CHAPTER VI: SANCTIONS

Employees have the institutional and personal obligation to comply with the procedures and policies established in this manual and in the applicable regulation for the prevention

and control of asset laundering and the Financing of Terrorism and the financing of the proliferation of weapons of mass destruction (AML/CFT/FPWMD).

The procedure for sanctions imposed will be in accordance with the PROCEDURE FOR VERIFICATION OF FAULTS AND FORM OF APPLICATION OF DISCIPLINARY SANCTIONS included in the internal rules of the company.

Failure to comply with or omission of the established procedures may result in disciplinary sanctions up to the termination of the employment contract or the contractual relationship, without compensation; without prejudice to the criminal, administrative or civil sanctions provided by Law.

The company, when necessary, will inform the competent authorities when its employees directly or indirectly facilitate, allow or contribute to the company serving as an instrument to launder assets or finance terrorism.

The imposition of sanctions will be carried out guaranteeing the right of defense; that is, once the breach of the policy is detected, the compliance officer will inform the immediate superior of the person involved and the human resources area, the employee allegedly involved will be summoned and his/her version of the facts will be heard to have elements of judgment to allow making a decision with respect to the sanction. Once heard, the immediate superior, the compliance officer and the human resources directorate will analyze the fault and establish the reasons for the decision made with respect to the sanction, which must be adjusted to the internal work rules.

When a sanction is to be applied, after having carried out the respective disclaimer process, the employee will be notified in writing of the fault and the sanction, so that the sanctioned person may appeal the decision adopted.

CHAPTER VII: DUTY OF RESERVE

The information obtained in the development of the procedures and practices that make up the Self-Control and Risk Management System for AML/CFT is subject to reserve, which means that it can only be known by the Financial Information and Analysis Unit (UIAF [for its Spanish acronym]) of the Ministry of Finance and Public Credit and by the Office of the Attorney General of the Nation upon request.

Therefore, all bodies, areas and employees of Integral S.A. that have responsibilities assigned to them in this manual and the procedures that derive from it, have the

obligation to guard and limit the use of such information to the strictly established purposes.

It is forbidden to all employees to inform the counterparties or third parties, except to competent authorities that make requirements in accordance with legal provisions, of the causes that gave rise to the control implemented, which has been the subject of internal analysis and/or report to the competent authority.

CHAPTER VIII: CONTACT

Any employee or third party who suspects an activity of asset laundering or financing of terrorism in Integral S.A., must immediately notify the company's compliance officer, Andrea Estefanía Vanegas Ruda, through the e-mail aevanegas@integral.com.co, and the alternate compliance officer, Yesica Viviana Ramírez Morales, through the e-mail yvramirez@integral.com.co.

Change Control							
Version	Nature of Change	Prepared		Reviewed		Approved	Date
		Name	Position	Name	Position	Name	
0	Initial version	Beatriz Fernández	Secretary General	Martha Nelly Rojas	Director of Internal Control	Board of Directors Minutes # 528	20/12/2016
1	Authorization of PEPs by the Presidency Committee headed by the Executive President	Martha Nelly Rojas Giraldo	Director of Internal Control	Cielo Elejalde Álvarez	Secretary General	Board of Directors Minutes # 534	25/06/2017
2	Authorization of PEPs to the Presidency	Martha Nelly Rojas	Director of Internal Control	Esteban Posada Jaramillo	Secretary General	Board of Directors Minute # 567	28/01/2020
3	Update of regulatory reference, authorization of exceptions.	Martha Nelly Rojas	Director of Internal Control	Esteban Posada Jaramillo	Secretary General	Board of Directors Minutes # 583	29/01/2021
4	Update according to Circular 100-000016 of December 24, 2020 and Circular 100-000004 of April 4, 2021	Martha Nelly Rojas	Director of Risks and Compliance	Esteban Posada Jaramillo	Secretary General	Board of Directors Minutes # 593	24/08/2021

Integral

CONSULTING ENGINEERS

MAIN OFFICE:
MEDELLÍN-COLOMBIA

CARRERA 46 N°52-36

PBX: (574) 511 54 00 EXT. 4509-4353

FAX: (574) 251 71 91

www.integral.com.co

Positive Impact