# MANUAL FOR SELF-MONITORING SYSTEM AND COMPREHENSIVE RISK MANAGEMENT OF MONEY LAUNDERING, TERRORIST FINANCING AND THE FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

## 1. INTRODUCTION

Money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction (ML/TF/WMD-PF) are illegal activities that have a negative impact on the economy. All organizations, regardless of their size or sector, are vulnerable to being used for these criminal activities, posing a serious threat to the business environment as well as to the society at large.

SURA Asset Management S.A. (hereinafter, "SURA AM" or the "Company"), is a commercial company domiciled in Medellín, Colombia, and identified with the TAX ID# 900.464.054-3. Its main corporate purpose is to invest in a portfolio of companies dedicated to asset management, pension fund administration and investment consulting.

SURA AM maintains a zero-tolerance policy on ML/TF/WMD-PF and their source crimes. In accordance with the corporate principles of respect, equity, transparency and responsibility, and in compliance with the requirements of the Basic Legal Circular of the Superintendence of Companies and the guidelines of the Code of Conduct of the SURA Business Group, the Company has designed and implemented a Self-Control and Comprehensive Risk Management System for ML/TF/WMD-PF (SAGRILAFT).

As a starting point, an analysis was carried out considering SURA AM's exposure to all the applicable risk factors in the current context as a holding company. This Manual establishes the guidelines and procedures of this system, with the objective of protecting the organization from being used for criminal activities and guaranteeing transparency and integrity in all its actions.

## 2. OBJECTIVES

### 2.1. General objective

Define the framework of action and the guidelines included in SURA AM's SAGRILAFT. This Manual seeks to provide clear guidance for the implementation, monitoring and

assessment of the necessary controls to prevent the Company, in its role as a holding company, from being used in illicit activities, thus contributing to the protection of its reputation and regulatory compliance.

### 2.2. Specific objectives

a. Establish policies, methodologies, guidelines and procedures for the effective management of any risks related to ML/TF/WMD-PF, in accordance with the nature and risk profile of the Company.

b. Define the stages of identification, assessment, control and monitoring of any risks related to ML/TF/WMD-PF as well as the mechanisms and procedures applicable to each one.

c. Define the organizational structure and assign the roles and responsibilities to the administrative and control bodies and to the employees in the application and surveillance of the SAGRILAFT.

d. Promote a culture of integrity and prevention against the risk of ML/TF/WMD-PF at all levels of the organization.

e. Outline the mechanisms for the documentation, filing and reporting of the SAGRILAFT data, both to the internal control bodies and to the competent authorities when appropriate.

## 3. SCOPE

This Manual is mandatory for all employees, administrators, counterparties and other stakeholders of SURA AM, insofar as it is applicable to each one. Its scope covers all areas, processes, actions and Company transactions, with special emphasis on the management of any ML/TF/WMD-PF risk factors.

## 4. DEFINITIONS

The terms used in this document have the meaning that corresponds to each one according to its nature, the applicable regulation and the definitions purposedly stated as follows.

**Control activities:** Current and operational control measures, implemented with the objective of mitigating one or more risks. They are aimed to attack any failures in the risks they seek to mitigate. These controls provide an operational model of reasonable security in achieving the objectives and are inherent to the roles of all the employees of the Company.

**Risk Management**: Coordinated activities to identify, assess, control and monitor the risks to which the Company is exposed to.

**Risk Analysis**: A process of understanding the nature of the risks to which the Company is exposed to, and determine the frequency of the events that may occur and the magnitude of their consequences, thus determining the level of risk.

**End beneficiary:** A natural person who, as established in the applicable regulation, owns, controls or ultimately benefits from an entity, transaction or contractual relationship. The percentage of participation or control required to be considered an end beneficiary will be determined by the regulations in force.

**Event**: Incident or situation where ML/TF/WMD-PF occurs and takes place in the Company during a certain period of time.

**Risk factors**: the following will be considered in the SAGRILAFT system:

- **Counterparties**: are the third parties with which SURA AM interacts directly at the corporate level in the following categories: suppliers, employees, controlled entities, shareholders, investors and members of the board of directors.
- **Jurisdictions**: correspond to the countries where the Company has its legal domiciles and where its controlled companies are located. These are: Colombia, Chile, Mexico, Peru, Uruguay, the United States and Luxembourg.
- **Products and activities**: taking into account that SURA AM does not offer any type of product or service, the grouping of these categories refers to SURA AM's own corporate activities as a holding company, which include the management of its investments, mergers and acquisitions (M&A) processes, financing and, in general, the execution of contracts and operations necessary for the development of its corporate purpose.

**Binding List**: public lists of persons or entities, whether associated with terrorist organizations or with criminal activities that are of mandatory verification by Colombia, by virtue of international treaties and/or that are binding on the Company.

**ML/TF/WMD-PF Risk and Controls Matrix**: an instrument that allows the identification, individualization, segmentation, evaluation and control of ML/TF/WMD-PF Risks to which the Company could be exposed to, in accordance with the identified
ML/TF/WMD-PF Risk Factors.

**Risk levels**: these are the different levels established by the Company to measure the exposure to any risks and its impacts.

**Unusual Transaction**: is a transaction in which the amounts or characteristics are not related to the ordinary or normal economic activity of SURA AM or which, due to its amount, quantity or characteristics, does not fall within the normal or ordinary business practices of a sector, industry or counterparty class.

**Suspicious Transaction**: is the Unusual Transaction that follows the uses and customs of the activity in question but cannot be reasonably be justified. This type of operation includes attempted or rejected transactions that contain any characteristics that grants the transaction that suspiciousness.

**Risk Profile**: consolidated result of the permanent surveillance of the risks to which the company is exposed to.

**Processes**: set of interrelated activities through which SURA AM executes its corporate purpose as a holding company.

**Risk**: impact and likelihood that an undesired event may affect the achievement of the Company's goals and objectives.

**Risk of contagion** is the possibility that SURA AM may suffer any loss, directly or indirectly, due to an action or experience of a Counterparty.

**ML/TF/WMD-PF Risk**: is the possibility of loss or damage to the image of the Company when used directly or through its activity, employees or related parties, as an instrument for money laundering and/or channeling of resources towards

terrorist activities or the Financing of the Proliferation of Weapons of Mass Destruction.

**Legal Risk**: is the possibility of loss incurred by SURA AM when sanctioned or forced to compensate damages as a result of non-compliance with the rules or regulations and contractual obligations. It also arises as a result of breaches in contracts and transactions, derived from malicious activities, negligence or involuntary acts that affect the formalization or execution of contracts or transactions.

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

**Reputational Risk**: is the possibility of loss incurred by SURA AM due to discredit, bad image, negative publicity, true or not, with respect to the organization and its business practices, which causes the loss of customers, decrease in income or legal proceedings.

**Red Flags**: specific facts and circumstances surrounding the performance of the Company's Counterparties' own operations, from which a careful and detailed study must be carried out by the Company and the Compliance Officer.

**Financial Analysis and Information Unit (UIAF):** autonomous body of the Colombian State responsible for centralizing, systematizing and analyzing data related to Money Laundering operations, that is, the unit serves as an information filter supported by technology that consolidates and adds value to the data collected to detect any operations that may be related to the crime of Money Laundering.

## 5. ML/TF/WMD-PF Risk Management Policies

### 5.1. General Policies

SURA AM follows these general policies as a guiding framework when dealing with any risks of ML/TF/WMD-PF. They seek to implement a self-control and risk management

system that is efficient, effective and timely, in accordance with current regulations and the corporate principles that govern the Company.

- SURA AM's employees must carry out their activities in compliance with the rules and procedures for the prevention of any ML/TF/WMD-PF risks, as well as compliance with ethical principles, in accordance with the provisions of the Code of Conduct.

- The Company will put first the policies adopted for the correct management of a ML/TF/WMD-PF risk before the fulfillment of its goals or the execution of the business objectives.

- The identification and assessment of any risks associated to ML/TF/WMD-PF must be carried out prior to making a new investment, entering a new market or opening operations in new jurisdictions.

- It is the obligation of all the employees to know the objectives, policies and procedures related to the prevention of any ML/TF/WMD-PF risks that have been disclosed by the Company.

- Any action that infringes the policies and procedures contained in the SAGRILAFT Manual and that exposes the Company any associated risks will constitute a misconduct that will be investigated and may have consequences as defined in the applicable norms and internal regulations of SURA AM.

### 5.2. Policies Related to the Stages of the SAGRILAFT

#### 5.2.1. Identification

The Company identifies the inherent risks of ML/TF/WMD-PF considering its corporate purpose and business model as a holding company. This process is based on the analysis of the defined risk factors: Jurisdictions, Counterparties, Products and Activities, and Channels, as well as the risks associated with each one.

Identification is carried out through expert judgment, analysis of the internal and external context, and study of typologies in accordance with the recommendations of the FATF. Includes the segmentation of the counterparties and jurisdictions to establish differentiated levels of exposure. The identified risks are recorded in the ML/TF/WMD-PF Risk Matrix.

#### 5.2.2. Measurement

The Company applies structured methodologies to assess the probability of occurrence and the impact of the identified risks, both in their inherent and residual state. The measurement is carried out through a risk management matrix, documenting risks, causes, impacts and applicable controls. These controls are classified as preventive, detective, or corrective, and must be aligned with the type of risk they mitigate.

#### 5.2.3. Control

The Company establishes control measures to mitigate the identified risks, reducing their probability of occurrence and/or impact. All controls must be documented, operational and have verifiable evidence. The Company must guarantee the technical, human and financial resources for the development of the controls and improvement of the system. Specific controls are included for each risk factor.

#### 5.2.4. Monitoring

The Company implements mechanisms for permanent monitoring of the behavior and evolution of the inherent and residual risk. This monitoring allows for the detection of emerging events, evaluate the effectiveness of the controls and validate the SAGRILAFT parameters. The consolidated risk profile is periodically assessed and reported back to the Board of Directors.

## 6. Guidelines by risk factor

### 6.1. Jurisdictions

The Company assesses the risk associated with the jurisdictions in which it operates, considering international indices and other geopolitical and regulatory factors. Jurisdictions are then segmented by risk level and thus measures are applied according to its classification.

Main Controls:

- Application of risk indices for country risk rating.
- Segmentation of jurisdictions by risk level (low, medium, high).
- Operation restrictions in non-cooperation or high-risk jurisdictions.
- Regular monitoring of relevant regulatory and geopolitical changes.

### 6.2. Counterparties

The Company has assessment, monitoring identification mechanisms of the counterparties it has business relationships with. These include shareholders, investors, suppliers, employees, and controlled entities. They are segmented by type and level of risk and due controls are applied according to their exposure.

Main controls:

- Initial and regular due diligence.
- Segmentation of counterparties by type and level of risk.
- At least once a year consultation of restrictive and binding lists.
- Inclusion of contractual clauses for early termination due to any ML/TF/WMD-PF risks.

### 6.3. Products & Activities

The Company assesses the risk associated with its corporate activities, such as investments, mergers and acquisitions, financing and capital management. These operations are carried out in regulated environments and with institutional counterparties, but they may involve additional risks due to their complexity or international scope.

Main controls:

- Revision of the operations by corporate governance bodies.
- Document traceability of strategic operations.
- Identification of final beneficiaries in investment operations.

## 7. Internal and External Reporting

### 7.1. Internal Reports

All Company employees must be able to report on any activities that do not comply with this Manual and that may indicate an unusual situation of a ML/TF/WMD-PF risk. Employees may report the situation directly to the Compliance Officer or file a

complaint through the ethics line, attaching the supporting documents to the operation and a clear explanation of the activity.

Once this information is received, the Compliance Officer will carry out the due investigation and based on the supporting documentation and will determine if it's an unusual operation or a Suspicious Transaction Report (STR) to then proceed with the report to the UIAF (Financial Information and Analysis Unit).

**Reports to the Board of Directors and General Management:** The Compliance Officer must submit at least once a year a report to the Board of Directors and the Administration, containing at least:

- The results of the management carried out.
- Evaluation and analysis of the efficiency and effectiveness of the ML/TF/WMD-PF risk management system.
- Comply with the submission of reports to the different authorities.
- The identified controls' implementation status as a result of the ML/TF/WMD-PF risk assessment.
- The effectiveness of the mechanisms and instruments in place to rectify the failures of the ML/TF/WMD-PF risk management system.
- Summary of the requirements and responses given to oversight entities.
- Alerts of unusual or suspicious LA/TF/WMD-PF activities.

### 7.2. External Reports

#### 7.2.1. Information requests from authorities:

Requests for information made to SURA Asset Management by the different competent authorities regarding ML/TF/WMD-PF processes will be received by the Compliance Officer.

#### 7.2.2. Suspicious Transaction Reports:

The STRs are carried out by the Compliance Officer on the activity and evidence collected through direct communication with the UIAF. The submission of the STR does not constitute a criminal complaint, the unit in charge of defining whether or not there is an operation related to ML/TF/WMD-PF is the Financial Analysis Unit (UIAF).

The company and the Compliance Officer must guarantee the confidentiality of the report of a STR sent to the UIAF, as provided for in Law 526 of 1999 and other regulations that have added, modified or replaced it.

## 8. Document Storage

The documents containing the result of the controls for the prevention of ML/TF/WMD-PF risks must be kept digitally stored for at least 5 years, complying with the security requirements that guarantee availability, integrity, timeliness, reliability, confidentiality and recoverability over time.

Any requests for documents by a collaborator or oversight entity in regard to the ML/TF/WMD-PF risk prevention processes must be made directly to the Compliance Officer.

## 9. Organizational Structure

The responsibility for managing and controlling the risks of ML/FT/FPADM, preventing the company from being used as an instrument for the materialization of these risks, corresponds to all SURA AM employees, regardless of the process or area in which they work. The main roles and responsibilities of the governing bodies and some specific areas of the Company are described below:

### 9.1. Board of Directors

The Board of Directors has the following responsibilities related to the risk management of ML/TF/WMD-PF:

a. Review and approve the prevention and control policies, strategies, plans and programs submitted for consideration by the Compliance Officer, which include at least the following aspects:

- Efficient and effective policies, procedures and internal controls to ensure the sound functioning of the System.
- Continuous and permanent training programs for the employees that work in sensitive areas in the prevention and control of ML/TF/WMD-PF.

- Efficient and effective mechanisms so that the activities carried out by internal and external auditing can identify, quantify and control any risks to which the systems and activities are exposed to and to be able to make an assessment to identify, measure and prioritize the ML/FT/WMD-PF risks.
- Approve this System Manual and its updates.

b. Receive and analyze the periodic reports prepared by the Compliance Officer, any deficiencies and weaknesses raised, as well as the recommendations suggested to continuously and permanently improve the policies, procedures and internal mechanisms for prevention and control of ML/TF/WMD-PF, to implement the pertinent corrective actions.

c. Give their opinion on the reports presented by the External Audit or the Statutory Auditor related to the implementation or operation of the system and follow up on the observations or recommendations provided by them.

d. Analyze the reports and requests submitted by the legal representative.

e. Provide the physical, administrative, and budgetary resources necessary for the System to be efficient and effective.

f. Select and designate the Compliance Officer and his alternate, if any.

g. Verify that the Compliance Officer has the availability and capacity necessary to perform his or her duties.

h. Determine those responsible and the conditions for carrying out audits to the system.

i. Verify that the Company, the Compliance Officer and the legal representative carry out the activities that correspond to them in relation to the System.

### 9.2. Legal Representative

a. Supervise and control compliance with the obligations assigned to the Compliance Officer.
b. Propose to the Board of Directors the person who will fulfill the role of Compliance Officer.
c. Submit to the Compliance Officer, for approval by the Board of Directors or the highest corporate body, the proposal of the System and its updates (Manual).

d. Study the results of the ML/TF/WMD-PF risk assessment carried out by the Compliance Officer and establish the corresponding action plans.
e. Efficiently allocate the technical and human resources, determined by the Board of Directors, necessary to implement the System.
f. Verify that the Compliance Officer has the availability and capacity necessary to perform his or her duties.
g. Provide effective, efficient, and timely support to the Compliance Officer in the design, management, supervision, and monitoring of the System.
h. Submit to the Board of Directors the reports, requests and alerts that it considers should be dealt with by said bodies.
i. Ensure that the activities resulting from the development of the work are duly documented, so that the information meets the criteria of integrity, reliability, availability, compliance, effectiveness, efficiency and confidentiality.
j. Verify that the System's procedures develop the LA/TF/WMD-PF Manual adopted by the Board of Directors.
k. Certify before the Superintendency of Corporations compliance with the obligations arising from the System when requested by this regulatory agency.

### 9.3. Compliance Officer

The Compliance Officer must actively participate in the design, management, implementation, audit, verification of compliance and monitoring of the system.

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

- Have the ability to make decisions to manage the risks related to ML/TF/WMD-PF.
- Have the necessary knowledge on risk management and understand the normal course of the Company's activities.
- Have the support of a human and technical team, according to the ML/TF/WMD-PF Risk and the size of the Company.
- Not belong to the administration or government bodies, or to internal or external auditing or control or whoever performs similar functions or has this role in the Company.

**Duties of the Compliance Officer**

The Compliance Officer has the following duties:

a. Ensure effective, efficient and timely compliance with the System.
b. Submit annual reports to the Board of Directors, which must contain, in addition to the activities, recommendations for the improvement of the procedures adopted. In whole, present the compliance of the System.
c. Promote the adoption of corrective measures, update the Manual (System) once every two years and submit it to the Board of Directors for approval.
d. Coordinate training activities for all SURA AM employees on the legislation, regulations and internal controls in force, as well as in policies and procedures related to the prevention and control of ML/TF/WMD-PF. Likewise, the development of communication strategies for the stakeholders on the subject matter.
e. Evaluate the reports of Internal Audit and the Statutory Auditor and adopt corrective measures in the face of the deficiencies reported.
f. Verify compliance with the Due Diligence procedures applicable to the different related parties.
g. Increase awareness and supervise full compliance with the current legislation, the Code of Ethics, the rules and procedures aimed at preventing SURA Asset Management from being used to legitimize money coming from illicit activities.
h. Uphold institutional relations with the UIAF and other authorities and control bodies of the Society.
i. Ensure the proper storage of support documents and other information related to the management and prevention of ML/TF/WMD-PF Risks.
j. Design the methodologies to be able to classify, identify, measure and control any ML/TF/WMD-PF Risks that will be part of the system.
k. Accompany the ML/TF/WMD-PF risk evaluation processes that the Company may be exposed to.
l. Submit reports of suspicious and unusual activity to the UIAF as indicated
in the regulation, as well as answers to any inquiries related to the matter that the UIAF or other competent authorities require, within the deadlines established by the laws and communications on request for information.

m. Represent SURA AM, when ordered by the President of the Company, in conventions, events, forums, committees and national and international official meetings on the subject matter.
n. Certify before the Superintendency of Corporations compliance with the obligations arising from the System, at the request of this agency.

To comply with the responsibilities aforementioned, the Compliance Officer must have an appropriate organizational and budgetary structure and the necessary decision-making power, scope and functional authority to be able to carry out the duties assigned.

### 9.4. Internal Audit

a. Evaluate the effectiveness and compliance of the ML/TF/WMD-PF Risk Management System. The result of these audits must be shared with the legal representative, the Compliance Officer and the Board of Directors.
b. Report in a timely manner to the Compliance Officer or his/her alternate, any irregularities that may arise during the operation of the system and the prevention of risks related to ML/TF/WMD-PF.

### 9.5. Procurement Department

The Procurement department will be responsible for collecting the information and the documents, as well as managing the Suppliers' ID file, which will allow it to carry out all Due Diligence of the latter.

### 9.6. Legal and General Secretariat

The General Secretariat, head of the Legal area, will be responsible for collecting the information and the documents, as well as for managing the Shareholders', Board of Directors' and Investors' ID files, which allow it to carry out all Due Diligence of the latter.

Likewise, during any mergers and acquisitions processes, the Legal area will be responsible for collecting the information and the documents to be able to properly identify SURA AM's

counterparties or the businesses in which it invests, which allow it to carry out all Due Diligence of the latter.

### 9.7. Human Talent

The area of Human Talent will be responsible for obtaining the information and documents, as well as for managing the identification file of SURA AM Employees, which will allow it to carry out all Due Diligence of the latter.

### 9.8. Operational Risks

The Operational Risks area will be responsible for accompanying and advising on the activities necessary for the updating of the ML/TF/WMD-PF Risk Matrix and controls; it will also report on the changes in the methodology described in the Comprehensive Risk Management Manual that may affect or modify the Risk and Controls Matrix.

### 9.9. Statutory Auditor

The Statutory Auditor is responsible for verifying the proper implementation and operation of the SAGRILAFT, in accordance with the provisions of the applicable regulation. In addition, it must report in a timely manner to the UIAF any activity that, in the exercise of its functions, may be considered suspicious. To comply with his/her duties, the Statutory Auditor must pay special attention in the analysis of the accounting and financial data and to those indicators that may suggest a possible ML/TF/WMD-PF activity.

## 10. Training and Outreach

The Compliance Officer is required to develop training and outreach programs for SURA AM employees that meet the following characteristics:

1. Must be part of the new employee onboarding program.
2. It must be part of the annual training program.
3. The training program and its content must be reviewed and updated at least every two years, or whenever the regulations require it.
4. Evidence of training and outreach programs should remain.

## 11. Warning Signs

The following warning signs must be considered during counterparty monitoring and contracting processes:

- Submitted ID documents damaged, illegible, incomplete or with inconsistencies.
- Counterparties who present commercial, financial or personal references that are difficult to verify or with inconsistent information.
- Suppliers, strategic partners or counterparties without clear economic activity, without financial history, or whose corporate purpose is unusual for the sector or for the type of relationship with SURA AM.
- Foreign investors or strategic partners whose economic activity is not related to the projects developed by the Company.
- Administrators or legal representatives without relevant experience in the sector, or who participate in multiple companies with similar characteristics.
- Companies that register foreign investment and share information like addresses, telephone numbers, corporate purpose, partners, administrators or tax statutory auditors.
- Counterparties that refuse to disclose details about their activities, end beneficiaries, shareholder structure, or that refuse to provide financial statements or relevant information.

In itself, these warning signs do no constitute evidence of illicit activities, but require further analysis and, if necessary, the application of a broader due diligence procedures and reporting to the competent authorities.

## 12. Due Diligence

To obtain effective, efficient and timely knowledge of current and potential counterparties, the responsible areas (Procurement, General Secretariat, Legal, Compliance, Human Talent, among others defined according to the Company's needs) must carry out a due diligence process for the management of the counterparties' ID file.

This procedure consists of confirming the identity of the counterparty, verifying its documents and data, and doing a cross-reference with restrictive lists, sanctions lists, and relevant public databases, with the objective of identifying any matches or warning signs.

The Compliance Officer has the power to define the scope and enhance the due diligence, determine the information and documents required, as well as the specific criteria and

procedures, according to the nature of the counterparty, the type of relationship and the level of risk identified.

In addition, the jurisdiction in which the counterparty is domiciled or in which it operates, must be registered to determine whether it corresponds to a non-cooperative or high-risk country, as defined by the competent authorities and the applicable regulations on the prevention of money laundering and terrorist financing. Third-party data must be updated periodically in accordance with the procedures defined by the Compliance Officer.

In the event of finding matches in restrictive lists, sanctions lists or public databases, or that the counterparty is domiciled in a non-cooperative or high-risk country, the responsible areas will inform the Compliance Officer who will determine the corresponding course of action. Likewise, it's the duty of the Compliance Officer to approve contracting a Politically Exposed Person (PEPs), in accordance with the procedures and criteria defined by the Company.

## 13. Sanctions

Failure to comply with the obligations stated in this Manual will entail disciplinary measures or be fired from the company, in accordance with the provisions of the Company's Internal Work Regulations.

In addition, and when necessary, the competent authorities will be notified as to initiate the administrative, civil or criminal actions.

## 14. Duties of suppliers towards SAGRILAFT

Suppliers that carry out contractual agreements with SURA AM must comply with the following duties to strengthen the integrity of the business relationship and thus prevent any risks of ML/TF/WMD-PF:

a. Act in accordance with the applicable legislation on the prevention of ML/TF/WMD-PF and source crimes, as well as respect the ethical principles defined in the SURA AM Supplier Code of Conduct.

b. Provide truthful, complete, and up-to-date information during the selection and contracting process as well as during the service provided, including legal, financial, and background checks, end beneficiaries and any other information required by SURA AM for due diligence.

c. State any situation that may represent a real or potential conflict of interest within the scope of the business relationship with SURA AM.

d. Refrain from offering, promising, authorizing, or delivering any type of undue benefit to public officials, Politically Exposed Persons (PEPs), or third parties, to obtain commercial or contractual advantages.

e. Actively cooperate with SURA AM in the event of internal investigations related to possible acts of money laundering and terrorist financing, providing the required information and documentation.

f. Ensure that the resources provided by SURA AM, including payments, donations or sponsorships, are used exclusively for the agreed purposes, avoiding their diversion or improper use.

g. Sign the documents that formalize the compliance with the principles of SAGRILAFT and other internal policies of SURA AM.

h. Attend the training or awareness sessions convened by SURA AM on business ethics, compliance and risk prevention of ML/TF/WMD-PF.

i. Use the channels provided by SURA AM such as the Ethics Hotline, to report any irregular conduct, suspicion of ML/TF/WMD-PF, corruption or non-compliance with ethical principles.

j. Implement internal control, supervision and monitoring mechanisms that contribute towards the prevention of unlawful actions within the framework of the contractual relationship with SURA AM.

## 15. Revision and update of the SAGRILAFT

The operational, economic, physical, technological and resource measures required for the proper implementation of the System will be revised and updated every two years, or if necessary, when there are new legal provisions, regulations, or modifications to policies and procedures.

The Board of Directors of SURA AM is responsible for approving this Manual and its modifications.

| Version | Date of update | Description of changes | Responsible area |
|---|---|---|---|
| 1.0 | May 2021 | Initial version | Legal & Compliance, risks |
| 2.0 | 11/05/2025 | Updated by Internal audit and regulatory adjustments | Compliance |