PROCEDURES MANUAL FOR THE TRANSPARENCY AND ETHICS PROGRAM

Table of Contents

I. INTRODUCTION 3

II. GENERAL OBJECTIVE 3

III. SPECIFIC OBJECTIVES. 3

IV. SCOPE 3

V. DEFINITIONS 4

1. BUSINESS TRANSPARENCY AND ETHICS PROGRAM 4

1.1 Commitment of Management or Senior Management 4
1.2 Assessment of Risks Related to Corruption and Transaction Bribery 4
Management Model 4
2. CLASSIFICATION AND SEGMENTATION OF RISK FACTORS. 5
2.1 Segmentation 6
2.2 Identification of Risk Events. 6
2.3 Risk Analysis and Assessments. 7
2.4 Controls. 8
2.5 Mitigation. 10
2.6 Monitoring 10
2.7 Improvement Actions. 12
3. STRUCTURE AND FUNCTIONING OF THE BUSINESS TRANSPARENCY AND ETHICS PROGRAM. 13
3.1 Governance of the Business Transparency and Ethics Program 13
3.1.1 General rules. 13
3.1.2 Administration and Management of Conflicts of Interest Regarding the BTEP Organizational Structure 14
Disqualifications and Incompatibilities 14
Compliance Officer Profiles 14
3.1.3 Specific Rules for Governing, Administrative and Control Bodies 14
3.1.3.1 Board of Directors. 14
3.1.3.2 Chief Executive Officer 15
3.1.3.3 Compliance Officer. 15
3.1.3.4 Ethics Committee 17
3.1.3.5 Employees. 17
3.1.3.6 Internal Audit and Statutory Auditor 18
4. PROCEDURES OF THE BUSINESS TRANSPARENCY AND ETHICS PROGRAM 18

+57 (1)7943999 www.canalclima.com
Carrera 11B # 99 - 25 canalclima
Piso 10 - Edificio Wework
Bogotá, Colombia

4.1 Procedure for Desing, Approval, and Updated of the Business Transparency and Ethics Program 18
4.2 Compliance Audit Procedure 19
4.3 Due Diligence Procedures 19
4.4 Warning Signals 19
4.5 Communication and Training Programs 21
4.5.1 Communication Strategy. 21
4.5.2 Training Plan 21
4.5.3 Reporting and Investigation Channels 22
Internal Reporting Channel 22
Reporting Channel of the Superintendence of Companies and Matters Related to Transnational Bribery. 23
4.5.4 Sanctions Procedure 23
4.5.5 Document Management Procedure 23
ANNEX 1. GLOSSARY. 25

+57 (1)7943999
Carrera 11B # 99 - 25
Piso 10 - Edificio Wework
Bogotá, Colombia
www.canalclima.com
canalclima

I. INTRODUCTION

CANAL CLIMA S.A. ("Canal Clima" or the "Company") has voluntarily adopted the Business Transparency and Ethics Program (Programa de Transparencia y Ética Empresarial – PTEE) and has established this Procedures Manual in accordance with Chapter XIII of the Basic Legal Circular.

This Manual sets forth the policies and procedures that make up the Business Transparency and Ethics Program ("Program" or "PTEE") and aligns them with the RFC Group Code of Conduct and Ethics, with the purpose of effectively preventing, detecting, and correcting the risk of Corruption, Bribery, and Transnational Bribery, hereinafter referred to as C/TB

II. GENERAL OBJECTIVE

To establish the principles and guidelines for the implementation of the Business Transparency and Ethics Program – PTEE, aimed at ensuring an ethical, transparent, and honest organizational culture, free from risks of corruption and transnational bribery.

III. SPECIFIC OBJECTIVES.

- To design strategies and measures for the identification, detection, prevention, and mitigation of acts of Corruption, including Transnational Bribery, hereinafter referred to as C/TB, in order to reduce the likelihood that the Company may be used as an instrument for its Employees, Senior Management, Suppliers, Contractors, or Counterparties to commit any act that may be considered corrupt.
- To establish the commitment of the Company and its Senior Management to ethical and transparent conduct in its operations and in its dealings with Stakeholder Groups, acting under a philosophy of **zero tolerance** toward any conduct that may be considered Bribery or that may in any way be corrupt.
- To establish the organizational structure of the Business Transparency and Ethics Program through the regulation of potential Conflicts of Interest, the assignment of roles and responsibilities to processes, and the establishment of a regime of disqualifications and incompatibilities.
- To define the C/TB Risk Management Model and the corresponding segmentation of risk factors.
- To define Due Diligence measures in accordance with the established segmentation.
- To regulate and align the procedures, policies, guidelines, roles, and functions established by the Company for an effective Business Transparency and Ethics Program.
- To define the foundations for effective communication and training in order to promote a culture of compliance through an environment of self-control of C/TB risks.

IV. SCOPE

This Manual is addressed to Senior Management, Employees, Suppliers, or third parties representing the Organization, and compliance with it is mandatory for all of them.

Its application and compliance are compulsory, and lack of knowledge of its content or procedures may not be alleged to justify any conduct that deviates from it.

V. DEFINITIONS.

The expressions written with an initial capital letter in this document that require a special definition are defined in the Glossary.

1. BUSINESS TRANSPARENCY AND ETHICS PROGRAM

1.1 Commitment of Management or Senior Management

The Company is committed to promoting a culture of transparency and integrity in which corruption and transnational bribery are generally considered unacceptable. For this reason, Senior Management promotes and supports business transparency and ethics policies aimed at conducting business with transparency, honesty, responsibility, and integrity, in compliance with the Law and with the highest ethical principles.

Furthermore, each Employee (regardless of their position, functions, or responsibilities) is expected and encouraged to adopt an attitude involving a sense of belonging to the Company, whereby they embrace and implement efforts to collectively build work environments free from corruption, transnational bribery, and other corrupt practices, in which the corporate values of Justice, Equity, Respect, Trust, Transparency, and Fair Competition serve as guiding principles governing their conduct.

1.2 Assessment of Risks Related to Corruption and Transaction Bribery

Management Model

The principle of assessing the risk of Corruption and Transnational Bribery constitutes the foundation of the Business Transparency and Ethics Program. Therefore, this principle requires the adoption of assessment procedures proportional to the size, structure, nature, jurisdictions of operation, and specific activities of the Organization.

In other words, this Program applies the concept of a risk-based approach, and for this purpose a Risk Management Model is established, as described below.

The model establishes a risk management methodology composed of systematic and interrelated steps through which C/TB risks are managed.

The model consists of five (5) phases, namely:

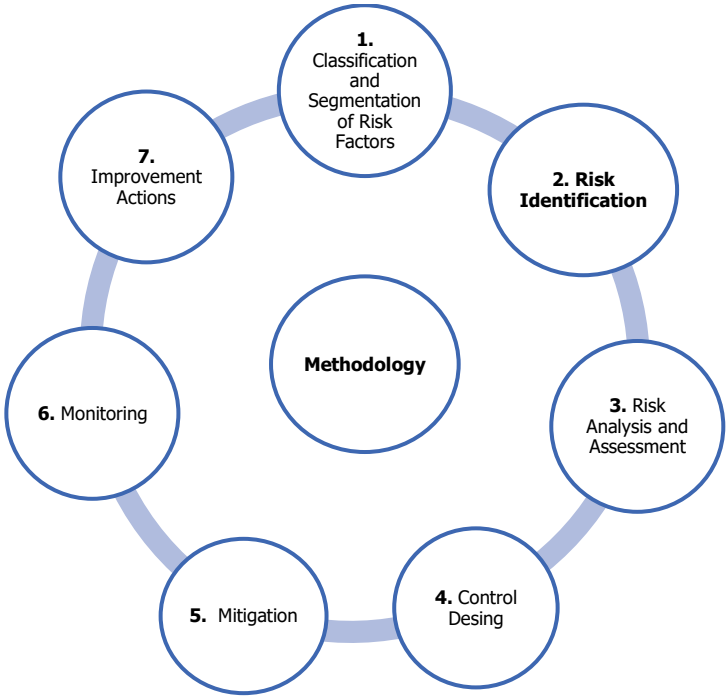
a. Identification

b. Measurement
c. Control
d. Monitoring
e. Improvement

To manage each of these phases a Risk Matrix and a heat Map will be used, enabling the integration and documentation of the activities carried out in each phase.

As a development methodology, the following steps will be addressed, the evaluation of which is continuous and recurring:

1. Classification and Segmentation of Risk Factors
2. Risk Identification
3. Risk Analysis and Assessment
4. Control Desing
5. Mitigation
6. Monitoring
7. Improvement Actions



2. CLASSIFICATION AND SEGMENTATION OF RISK FACTORS.

The identification and classification of risk factors or sources stem from an understanding of the dynamics of all businesses, operations, and processes that manage the Organization's activities, as well as the internal and external relationships that the Company establishes with Employees and Third

Parties, which present vulnerabilities or threats to the occurrence of Corruption and/or Transnational Bribery risk events.

As a result of this analysis, and upon reviewing the reality of the operations carried out by the Company and its specific aspects of engagement with Third Parties, the countries in which it operates or where Third Parties are located, and the economic sectors in which it participates, the following risk factors have been identified for the Company:

- Economic Sector
- Third Parties
- High-Risk Countries
- Operations

2.1 Segmentation

The application of a Risk-Based Approach (RBA or EBR) determines the proportionality of measures according to the level of risk represented by each factor and sub-factor.

In accordance with the activities carried out by the Company, certain characteristics (criteria or segmentation variables) have been identified that imply a higher exposure to C/TB risks (Corruption and/or Transnational Bribery). Therefore, the application of enhanced measures for Third-Party due diligence, as well as monitoring and traceability of operations, is required.

Segmentation variables are defined as those characteristics which, when applied to homogeneous groups, result in subgroups to which more stringent measures must be applied.

The segmentation variables and the measures established within the Due Diligence processes are set forth in the Annex entitled **Due Diligence and Segmentation Procedure.**

2.2 Identification of Risk Events.

To identify risk events, the Company relied on interviews with process owners and prepared a list of potential risk events; that is, incidents or occurrences derived from internal or external sources that may generate risks associated with C/TB.

Once the list of events was identified, an analysis was conducted considering possible causes. This makes it possible to identify the circumstances that could materialize the risk and that must be controlled to prevent their occurrence.

The risk identification stage must be carried out in advance whenever there is a modification of risk factors, such as entering a new market through an investment or initiating operations in new jurisdictions.

2.3 Risk Analysis and Assessments.

The analysis of C/TB risks involves measuring the probability or likelihood of occurrence of the risk inherent to the activity, as well as the impact should it materialize through associated risks.

Impact consequences and probabilities are combined to produce the risk level.

For risk measurement, the following measurement levels and corresponding criteria are used, which may also be applied by a group of experts with experience and knowledge of the sector in which the Company operates, and who are also familiar, both retrospectively and prospectively, with its dynamics and evolution.

Chart 1 Risk Probability Assessment.

Probability		
Qualification	**Descriptor**	**Description**
5	**Imminent**	May occur in 90% or more of cases. May occur within the company.
4	**Very Likely**	May occur in 70% to 89.9% of cases. May occur within the sector.
3	**Likely**	May occur in 50% to 69.9% of cases. May occur in a sector related to the Company's line of business.
2	**Unlikely**	May occur in 25% to 49.9% of cases. May occur in other sectors.
1	**Remote**	May occur in less than 0.1% to 24.9% of cases. There is no known record of occurrence.

Chart 2. Risk Impact Assessment.

Impact					
Qualification	**Descriptor**	**Operative**	**Economic**	**Legal**	**Reputational**
5	Very High	Closure of operations for more than 30 days or	Losses equal to or greater than 5% of equity.	Administrative liability of the legal entity. Imprisonment of Legal	Media exposure > 30 days. Extensive international coverage.

		permanent shutdown		Representatives or Employees.	
4	High	Temporary closure of operations for up to 30 days	Losses ranging from 1% to 4.99% of equity.	Administrative fines imposed on Legal Representatives or Employees.	Media exposure < 30 days. Extensive regional or national coverage.
3	Medium	Partial closure of operations for up to 29 days.	Losses ranging from 0.5% to 0.9% of equity.	Internal disciplinary measures, including termination for just cause.	Media exposure <15 days. Event disclosed locally on an isolated basis.
2	Low	Partial closure of operations for up to 15 days	Losses ranging from 0.1% to 0.49% of equity.	Internal disciplinary measures or administrative requirement.	Known and addressed at the Company level.
1	Very Low	Partial closure of operations for up to 7 days	Losses of less than 0.09% of equity.	Response to an administrative requirement.	Known and addressed internally within a specific area or work team.

The results of the application of these criteria are consolidated; however, the **Coefficient of Variation** is also used as a statistical measure which, in the context of Risks, helps determine the level of dispersion among the individual opinions of each of the experts who applied the voting criteria for each risk.
In the event that the coefficient of variation is very high (>70%), the experts must conduct the voting process again in order to reach consensus.

For this purpose, the results of multiplying probability and impact magnitude are plotted on a heat map, where inherent risks can be observed according to their level of exposure or severity as low, moderate, high, or extreme.

The risk analysis and assessment shall be conducted on a biennial basis or whenever required by the Company due to changes in its business model.

2.4 Controls.

Understood as **Reasonable Measures**, controls must be designed according to the level of risk, recognizing that the higher the risk, the more robust the controls must be.
Their design must ensure that the control is sufficient, appropriate, and measurable. Accordingly, the following criteria are established to address these attributes.

Sufficiency: Determined by the combination of the form and type of control:

Chart 3. Sufficiency Framework.

Type	Description
Manual	Refers to controls in which one or more individuals are involved in their execution.
Semi-automated	Refers to controls that involve a combination of an information system and the execution of manual activities by one or more individuals.
Automated	Refers to controls in which an information system operates from start to finish and does not require any human intervention for their execution or verification.

Chart 4. Sufficiency Control Type.

Type	Description
Preventive	Controls that reduce the causes generating risks, thereby decreasing the frequency with which they occur.
Detective	Controls that identify the causes of risks after incidents have occurred. In a way, they serve to assess the effectiveness of preventive controls.
Corrective	Controls that remedy errors, omissions, or malicious acts once they have been detected.

The sufficiency of controls is assessed based on the combination of the control form and control type, as follows:

Chart 5. Sufficiency Assessment.

Forma de control	Tipo de control	Combination	Calcification
Automated	Preventive	Automated and Preventive	5
Semi-automated	Preventive	Semi-automated and Preventive	4
Manual	Preventive	Manual and Preventive	3
Automated	Detective	Automated and Detective	4
Semi-automated	Detective	Semi-automated and Detective	3
Manual	Detective	Manual and Detective	2
Automated	Corrective	Automated and Corrective	4
Semi-automated	Corrective	Semi-automated and Corrective	3
Manual	Corrective	Manual and Corrective	2

Appropiate (suitable or right for a particular situation or occasion): For the determination of this attribute, the following criteria are applied with their respective assessments:

Chart 6. Appropriate Attribute Ratings

Criteria	The control addresses the cause of the risk.	The control is applied within the process cycle (Implemented).	Evidence of the results of its application is maintained (Documented).	Are the controls currently being applied (operating effectiveness) ?	Does the control require improvements?
YES	5	5	5	5	0
NO	0	0	0	0	5

From the evaluation of controls, a control can be classified as:

- ✓ Strong: Controls are adequate and operate correctly.
- ✓ Moderate: Weaknesses exist in their design and/or implementation, requiring modifications—opportunities for improvement.
- ✓ Weak: Controls are not at an acceptable level.

Any recommendations generated must be managed by the process owners.

2.5 Mitigation.

Due to the nature of C/TB risks, the effectiveness of controls influences the probability of their occurrence, resulting in the following residual risks:

Chart 7. Types of Residual Risks.

Resulting probability according to % of control mitigation	Initial probability	If it mitigates more than 0.74	If it mitigates between 0.74 and 05.1	If it mitigates less than 0,51
	Remote	Remote	Remote	Remote
	Unlikely	Remote	Remote	Unlikely
	Likely	Remote	Unlikely	Likely
	Very likely	Unlikely	Likely	Very likely
	Imminent	Likely	Very likely	Imminent

2.6 Monitoring.

Once the residual risks have been determined, the system must be monitored for improvement. In this regard, risks and, in general, the model itself must be continuously tracked.
For this purpose, the heat map should be analyzed, considering the effect of controls on inherent risk, according to the following guidelines:

Chart 8. Residual Risk Controls

Residual Severity Level	Policy	Treatment
Extreme	Under no circumstances is a risk of this level acceptable. Therefore, any activity where a risk event of this level occurs will be suspended while the appropriate treatment is applied. These risks require high-priority attention from the management responsible for the event to immediately reduce its severity.	Immediate action required; treatment plans must be implemented and reported to the Board of Directors and Legal Representative.
High	Requires priority actions in the short term by directors and managers responsible for the areas or processes where the event occurs, due to the significant impact it could have on the Company.	Must be addressed within three (3) months of identification through treatment plans implemented and reported to the corresponding directors.
Moderate	Activities must be carried out to manage this risk in the medium term by assistants or area coordinators where the event occurs.	Acceptable risk managed with standard control procedures; treatment required within six (6) months of identification, reported to the corresponding directors.
Low	The risk has low severity and does not justify additional resource investment. Current actions should be maintained to keep the risk level. These risks are monitored and reviewed quarterly to ensure the level has not increased.	Managed with routine procedures. Insignificant risk; no action required.

Based on the results obtained in the previous phase, an effective monitoring process must be carried out to enable the rapid detection and correction of deficiencies in the model, at least on an annual basis; ensuring that controls comprehensively cover all risks and that they operate in a timely, effective, and efficient manner.

During this stage, the Compliance Officer must track the established risk profile.

This Monitoring phase includes the following activities:

- Ensure that residual risks remain within the levels of acceptance established by the Organization.

- Monitor risks by measuring them according to the established methodology. Likewise, mitigation controls will be evaluated to verify their sufficiency and timeliness.
- Based on this new measurement, risk variations will be established to determine their behavior over time.
- These variations will be analyzed by risk factor and associated risk across different periods, including mitigation during the same period. Improvement plans will be developed according to the results.
- Ensure that controls for all risks are comprehensive. A qualitative assessment will be performed according to the nature of each risk, considering manual, automated, and technology-dependent controls, as well as their operational effectiveness. Walkthrough tests and representative sampling will be included in the supervision and monitoring plans, based on criteria such as: realized risks, audit reports, and reported warning signals.
- Track and compare Inherent Risk and Residual Risk for each risk factor and associated risks, including Strategic, Legal, Reputational, and Operational Risks.
- Establish descriptive and/or forward-looking indicators that highlight potential risk sources.
- Evaluate the relevance of the indicators.
- Analyze the data reported by the indicators.
- Assess the results of indicator diagnostics and monitor them against previous results.
- Communicate outcomes to the responsible manager.
- Prepare reports on the results obtained.

Additionally, when the Company enters new sectors, the related risks—including C/TB risks—must be evaluated. For this purpose, the Compliance Officer, with the support of the person responsible for the new business, will conduct the analysis and document the findings.

2.7 Improvement Actions.

The consolidation of improvement actions corresponds to a formal and documented process, coordinated by the Compliance Officer, aimed at implementing measures that reduce the severity of residual risks.

This stage must be carried out prior to the launch of any new business line, modification of its characteristics, entry into a new market, or the opening of operations in new jurisdictions.

The following sources should be considered when defining improvement actions:

- ✓ Reports of operations submitted to the Compliance Officer (confirmed events). In this regard, all Employees must be trained to detect irregularities in the Company's operations and report them to the Compliance Officer.
- ✓ Audit and statutory auditor reports.
- ✓ Written significant experiences.
- ✓ Management reports.

- ✓ Documentation from regulatory entities.
- ✓ Requests from authorities.
- ✓ Media reports.
- ✓ Information reported by the Organization's process leaders.

Additionally, to identify risks that lack written evidence, the DELPHI methodology (Helmer & Gordon) can be used. This involves open surveys directed at individuals with knowledge of the environment in which the Company operates. Participants provide input through self-assessment questionnaires structured by the Compliance Officer, allowing expert information to be collected for the construction of risks recorded in the Corruption and Transnational Bribery Risk Identification Matrix.

Participants for the survey are selected based on their experience and knowledge of the processes or businesses under evaluation. If this methodology is applied, at least two (2) successive surveys are conducted to achieve consensus on the opinions provided.

The Improvement Action Plan identifies responsibilities, timelines, proposed actions, and the established review process. To ensure effective monitoring of control strengthening aimed at reducing the frequency and impact of risks, the Compliance Officer records the Improvement Action Plan in the Matrix.

3. STRUCTURE AND FUNCTIONING OF THE BUSINESS TRANSPARENCY AND ETHICS PROGRAM.

3.1 Governance of the Business Transparency and Ethics Program

3.1.1 General rules.

his Manual establishes the governance of the BTEP (Business Transparency and Ethics Program), and for this purpose:

- Defines responsibilities and specific functions considered critical in the direction, management, and control of the Program, in coordination with the Compliance Officer.
- Identifies the Compliance Officer as the person responsible for the development, monitoring, verification of effective functioning, and implementation of the Business Transparency and Ethics Program.
- Assigns process owners the duty to integrate Corruption and Bribery risks into their risk assessments when hiring or performing their functions, and, in coordination with the Compliance Officer, identify potential events to apply the corresponding controls.
- Establishes guidelines for the prevention and resolution of Conflicts of Interest that may arise in the assignment of functions and responsibilities for the proper design, implementation, and monitoring of the Business Transparency and Ethics Program.

Thus, to clearly assign responsibility for exercising the necessary functions and duties throughout the execution of the Program's stages, elements, and activities, the following directives are established:

3.1.2 Administration and Management of Conflicts of Interest Regarding the BTEP Organizational Structure

Disqualifications and Incompatibilities

In accordance with applicable regulations, the following rules are established to avoid Conflicts of Interest in the implementation, development, and application of the Business Transparency and Ethics Program:

a) No member of management, administration, or control may assume the responsibilities of Compliance Officer for managing the BTEP.

b) Specifically, regarding the Compliance Officer profile, the individual may not be:

- Shareholder
- Board Member
- Legal Representative
- Internal Auditor
- Statutory Auditor
- Officer responsible for administration or business processes
- Related by consanguinity or civil kinship to Board Members or Legal Representatives
- Anyone who has held a position in the past two (2) years in public entities responsible for oversight, control, and sanctioning of Money Laundering and Terrorism Financing crimes, such as the Superintendence of Companies, the Financial Information and Analysis Unit (UIAF), the Prosecutor's Office, or Criminal Judges.

Compliance Officer Profiles

The profile of the Compliance Officer will be determined in the regulations, Chapter XIII of the Circular Básica Jurídica of the Superintendence of Companies, and by the Board of Directors.

3.1.3 Specific Rules for Governing, Administrative and Control Bodies

3.1.3.1 Board of Directors.

The Board of Directors is responsible for:

a) Committing to the prevention of Corruption and Transnational Bribery, as well as any other corrupt practices, so that the Company can conduct its business ethically, transparently, and honestly.
b) Appointing the Compliance Officer and their alternate, and defining their profiles to ensure suitability, experience, and leadership required to establish an effective program for preventing Corruption and Transnational Bribery risks.
c) Issuing and defining the Compliance Policy adopted by the Company as the **Anti-Corruption Policy**.
d) Approving the Business Transparency and Ethics Program, which includes the policies and this Manual of Procedures.

e) Receiving and evaluating, through the Audit and Conflicts of Interest Committee, the report submitted by the Compliance Officer regarding the Company's risk situation and the implementation and execution of the Program.
f) Ordering appropriate actions against associates in management or administration positions if they violate the provisions of the Program.
g) Reviewing semiannually, through the Audit and Conflicts of Interest Committee, reports submitted by the Internal Auditor, with follow-up on recommendations documented in the minutes.
h) Ensuring provision of financial, human, and technological resources required by the Compliance Officer to fulfill their duties and implement/maintain the Program.
i) Leading an effective communication and training strategy to ensure dissemination and understanding of the Policies and Program among Employees, Shareholders, Contractors, and other identified stakeholders. The Board approves the Communication and Training Plan submitted by the Compliance Officer.

3.1.3.2 Chief Executive Officer

The CEO, as Legal Representative, must:

a) Submit, together with the Compliance Officer and alternate, the proposed BTEP for Board approval.

b) Ensure the BTEP aligns with the Transparency and Ethics Policy adopted by the Board.

c) Provide effective, efficient, and timely support to the Compliance Officer in designing, directing, supervising, and monitoring the Program.

d) Certify compliance with External Circular No. 100-000011 of 2021 before the Superintendence of Companies, when required.

e) Certify that the Compliance Officer and alternate meet the requirements in Chapter XIII of the *Circular Básica Jurídica* within 15 business days of appointment or ratification.

f) Ensure that all activities resulting from the BTEP are properly documented and meet criteria of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality.

3.1.3.3 Compliance Officer.

The Compliance Officer, or their alternate in temporary or absolute absence, is responsible for:

a) Submitting, together with the President, the BTEP proposal and updates to the Board, especially when higher C/TB exposure is identified.

b) Presenting at least once a year a report on the Program's operation and management to the Audit and Conflicts of Interest Committee. Reports must include an evaluation of program

efficiency and effectiveness and propose improvements, if necessary, while demonstrating the results of the Compliance Officer and overall management.

c) Ensuring the Program aligns with the **Anti-Corruption Policy** adopted by the Board.

d) Overseeing the effective, efficient, and timely execution of the Program.

e) Implementing and updating a **Corruption and Transnational Bribery Risk Identification Matrix** according to needs, risk factors, C/TB materiality, and the **Anti-Corruption Policy**.

f) Defining, adopting, and monitoring actions and tools for detecting C/TB Risk in accordance with the **Anti-Corruption Policy and Risk Matrix.**

g) Ensuring the implementation of appropriate channels for confidential and secure reporting of Program violations or suspicious activities related to Corruption.

h) Verifying the application of whistleblower protection policies and, for Employees, compliance with labor harassment prevention policies.

i) Establishing internal investigation procedures to detect Program violations and acts of Corruption.

j) Coordinating internal training programs.

k) Ensuring **Due Diligence** processes are applied according to the **Due Diligence and Segmentation Procedure.**

l) Safely archiving all documentation and information related to C/TB risk management and prevention for at least 10 years.

m) Designing methodologies for classification, identification, measurement, and control of C/TB Risk within the Program.

n) Evaluating compliance with the Program and assessing the Organization's exposure to C/TB Risk.

o) Executing, as approved by the Board, internal and external communication strategies to effectively disseminate the **Program and Anti-Corruption Policy to Employees**, clients, suppliers, and contractors, emphasizing consequences of noncompliance.

p) Ordering internal investigations using internal resources or specialized Third Parties.

q) Acting on conclusions of the Ethics Committee regarding reports received through various channels and, if necessary, reporting to relevant authorities.

r) Implementing corrective actions ordered by the Board, evaluating reports from the Internal Auditor, and taking measures regarding reported deficiencies.

s) Addressing and coordinating any requests or inquiries from competent judicial or administrative authorities in this matter.

3.1.3.4 Ethics Committee

The Ethics Committee is responsible for promoting, overseeing, and enforcing the Code of Conduct, acting as a consultative body for ethical or reputational dilemmas, managing reports of unethical behavior, and participating in the evaluation of compliance with ethical standards. All actions aim to ensure a culture of integrity, transparency, and adherence to organizational values. These responsibilities include the COLCX Program, in accordance with **the Ethics Committee Regulations** and the **COLCX Program Governance Model.**

The Committee is composed of the CEO, a Board Member, the Administrative and Financial Manager, and the Compliance Officer, except when issues related to the COLCX Program are under review.

If a situation or report impacts the COLCX business line, the Committee's composition changes: the Administrative and Financial Manager will not participate, and an external advisor or consultant with expertise in reputational matters and carbon project businesses will be invited, according to the Ethics Committee Regulations.

Functions of the Ethics Committee include:

a) Analyzing and taking necessary actions regarding cases reported through the Compliance Officer or other communication channels concerning suspected or actual instances of Bribery or Corruption, or any circumstances impacting the reputation of CANAL CLIMA or the COLCX Program.

b) Investigating violations of Policies or actions contrary to anti-corruption standards based on complaints received through the Compliance Officer, the Ethics Line, or any other means.

c) Determining sanctions upon verification of a Policy breach, in accordance with the Policy and the Organization's Internal Work Regulations.

d) Ensuring that events constituting criminal offenses are reported to the competent authorities.

e) Guaranteeing the right of defense for reported individuals, including the submission of explanations and evidence, applying the principle of presumed innocence until proven otherwise.

f) Implementing the whistleblower protection policy or guidelines.

g) Addressing or analyzing issues affecting the COLCX Program, including complaints or reports that may harm its reputation or involve unethical conduct.

3.1.3.5 Employees.

Employees of the Company are required to:

a) Understand and familiarize themselves with the components of the Program and its procedures.
b) Know the processes applicable to their responsibilities and implement the corresponding measures and controls for risk prevention.
c) Comply with this document and the Refocosta or RFC **Group Code of Conduct and Ethics**.
d) Prevent any acts of Corruption or Transnational Bribery by employees exposed to these risks and report any suspected or observed instances through the designated channels.
e) Communicate requests, complaints, claims, or commendations regarding the Business Transparency and Ethics Program.
f) Maintain ethical behavior inside and outside their role in the Organization, guided by corporate principles and values.

3.1.3.6 Internal Audit and Statutory Auditor

The Audit function has the following responsibilities:

a) Include in the Annual Audit Plan the verification of compliance and effectiveness of the transparency and ethics programs.

b) The Statutory Auditor must report to criminal, disciplinary, and administrative authorities any acts of Corruption or alleged offenses against public administration, economic and social order, or economic property detected during their duties.

c) The Statutory Auditor must evaluate the Business Transparency and Ethics Program and provide an opinion on it.

d) Report Corruption incidents to the Ethics Committee within six (6) months from the time the Statutory Auditor became aware of them..

4. PROCEDURES OF THE BUSINESS TRANSPARENCY AND ETHICS PROGRAM

4.1 Procedure for Desing, Approval, and Updated of the Business Transparency and Ethics Program

For the design, approval, and updates of the Program, the Compliance Officer must follow these rules:

- The design or update must be based on a thorough evaluation of the Organization's specific characteristics and exposure to Corruption and/or Transnational Bribery Risks.
- The Program must be structured to identify, detect, prevent, and mitigate Corruption and/or Transnational Bribery Risks. It must reflect a Risk-Based Approach (RBA) through a C/TB risk management model that enables identification, assessment, control, and monitoring to prevent risk materialization in operations and Third-Party relationships.
- The Program draft must be presented jointly by the CEO and Compliance Officer to the Board of Directors for approval, which must be recorded in the meeting minutes.

- This procedure also applies when updating the Program and must occur at least every two (2) years, unless earlier updates are required due to regulatory changes, creation or elimination of a business line, business model changes, increased exposure to C/TB risk, or similar causes.

4.2 Compliance Audit Procedure

To maintain effective functioning of the Business Transparency and Ethics Program and identify necessary improvements, program monitoring is the responsibility of the Compliance Officer or, in their temporary or absolute absence, the alternate.

The Compliance Officer will carry out periodic supervision to verify effective program functioning. The supervision plan applies different levels of review:

a) Evaluations or self-assessments to measure the ethical environment or compliance level through surveys or compliance certifications by responsible parties or Third Parties exposed to risks.

b) Verifications including review of annual Conflict of Interest declarations, gift, hospitality, and entertainment records, donation and political contribution documentation, Ethics Line reports, among others.

c) Audits to ensure proper application of the **Due Diligence and Segmentation Procedure** and treatment of reported warning signals.

Additionally, the Company establishes control and audit systems allowing the Statutory Auditor to verify accounting accuracy and ensure that monetary transfers between the Company and Third Parties do not conceal direct or indirect payments related to Bribery or other corrupt conduct.

4.3 Due Diligence Procedures

Review processes are conducted periodically and proportionally to the risk level presented by each Counterparty or Contractor, and according to the segmentation established for risk factors.

Counterparties or Contractors representing higher C/TB risk exposure will be subject to additional due diligence measures, following the **Due Diligence and Segmentation Procedure.**

Enhanced measures for traceability and monitoring of operations are applied when Warning Signals are identified.

4.4 Warning Signals

A warning signal is any fact, situation, event, amount, quantitative or qualitative indicator, financial reasoning, or other information that may reveal atypical behavior of variables defined by the Organization.

Responsibility for identifying and verifying warning signals primarily lies with Employees controlling normal business operations and those in regular contact with Third Parties.

Based on identified risk factors, the following warning signals are established, without limiting Employees or responsible parties from identifying others:

a. Accounting Records, Operations, or Financial Statements:

- Invoices that appear false, do not reflect actual transactions, are inflated, or contain excessive discounts or refunds.
- Foreign operations with highly sophisticated contractual terms.
- Transfers to countries considered tax havens without apparent justification.
- Operations lacking logical, economic, or practical explanation.
- Transactions outside the ordinary course of business.
- Operations with unclear parties or unclear source of funds.
- Assets or rights recorded in financial statements without real value or non-existent.

b. Corporate Structure or Corporate Purpose:

- Complex or international legal structures without apparent commercial, legal, or tax benefits, including entities without a commercial objective, particularly if abroad.
- Legal entities with national trusts, foreign trusts, or non-profit foundations.
- Offshore entities or offshore bank accounts.
- Non-operating companies per Law 1955 of 2019, or entities considered “paper” companies.
- Companies declared fictitious suppliers by DIAN.
- Legal entities without identified Ultimate Beneficiaries.

c. Transactions or Contracts:

- Frequent use of consultancy, intermediary contracts, or joint ventures.
- Contracts with Contractors or government entities appearing legal but lacking precise obligations.
- Contractors providing services to a single client.
- Unusual gains or losses in contracts or unjustified significant changes.
- Contracts with unreasonable variable remuneration or payments in cash, virtual assets, or in-kind.
- Payments to PEPs or persons close to PEPs.
- Payments to related parties (Associates, Employees, Subsidiaries, branches, etc.) without apparent justification.

Detection of a warning signal must be reported to the Compliance Officer or Internal Audit.

The Compliance Officer must analyze and provide recommendations for appropriate management of the warning signal, which should be included in the applicable due diligence procedure.

4.5 Communication and Training Programs

4.5.1 Communication Strategy.

The dissemination of this Manual is carried out through its publication on the Company's intranet. Additionally, the Group RFC **Anti-Corruption Policy** and **Code of Conduct** and Ethics are published on the Company's website so that Contractors, Third Parties, and Stakeholders are aware of the guidelines, as well as the responsibilities of Senior Management regarding the prevention of Corruption and Bribery, financial controls, gift and donation policies, available reporting channels, and the sanctions regime for non-compliance with the Business Transparency and Ethics Program.

The Compliance Officer will develop a communication and dissemination plan covering topics related to the Business Transparency and Ethics Program, which will be communicated through:

- Emails
- Any other medium deemed effective for transmitting this information

During the onboarding of new counterparties (employees, suppliers, clients, and contractors), they must sign the forms provided in the Due Diligence procedure, confirming that they have read and understood the Group RFC Code of Ethics and Anti-Corruption Policy.

The Business Transparency and Ethics Program must be disseminated within the Company and to other relevant stakeholders identified by the Compliance Officer based on risk factors, with the frequency and method required to ensure proper compliance, at least once a year.

4.5.2 Training Plan

To raise awareness of the C/TB risks to which the Company is exposed and to ensure the Program is adequately understood by Employees, the Compliance Officer, with the support of Human Resources when applicable, must coordinate training plans that meet the following requirements:

a) Delivered as awareness sessions during the induction process for new Employees, raising awareness of the threats posed by Corruption and Bribery.

b) When a Third Party, Contractor, or Supplier acts on behalf of the Company or provides an essential service to operations, they must also receive training on the Business Transparency and Ethics Program to ensure alignment of their internal processes with the system.

c) Provided periodically to all Employees, at least once a year.

d) Training plans must be continuously reviewed and updated.

e) After training, Employees must complete an assessment to ensure comprehension of the concepts.

f) A minimum of 60% correct responses is required to consider the concepts understood. If below this threshold, the assessment must be repeated.

g) If the passing percentage is not achieved after three attempts, the Compliance Officer must notify the Employee's direct supervisor and Human Resources to incorporate this into performance evaluations.

h) Documentation of the training materials, attendance, and assessment results must be maintained.

i) Attendance at trainings is mandatory for all individuals who are called to participate.

4.5.3 Reporting and Investigation Channels

Internal Reporting Channel

The Company has an internal Ethics Line enabling anyone to confidentially and securely report violations of policies or suspected unethical conduct, ensuring confidentiality and anonymity, with no risk of direct or indirect retaliation. The operation of the Ethics Line is based on the principles of Independence, Confidentiality, Feedback, Monitoring, Transparency, and Non-Retaliation.

The Compliance Officer also receives inquiries, complaints, and reports regarding potential violations of procedures, anti-corruption policies, and unethical conduct.

The Ethics Line is managed by an independent third party, guaranteeing confidentiality, anonymity, and information security. It is available 24 hours a day, 7 days a week.

Toll-Free Line: 01-800-752-2222 Option 1 for an operator, Option 2 for recorded message.

Email: lineaetica.rfc@resguarda.com

Website: www.resguarda.com/lineaeticagruporfc

WhatsApp: +57 1 7868154

The Company does not accept false or frivolous complaints or reports. If it is determined that a report is false, frivolous, or not made in good faith, such conduct will be considered a violation of the Group RFC Code of Conduct and Ethics.

In coordination with the Compliance Officer, the Ethics Committee conducts investigations regarding Employees as needed to determine the facts related to the reports and decides on their handling, evaluating the applicable sanctions according to the Internal Work Regulations.

Reporting Channel of the Superintendence of Companies and Matters Related to Transnational Bribery.

In addition to the internal reporting channel, the Company recognizes the existence of and promotes the use of institutional channels available for filing complaints, such as:

- For reports related to Transnational Bribery:
  - https://www.supersociedades.gov.co/delegatura_aec/Paginas/Canal-de-Denuncias-Soborno-Internacional.aspx

- For reports of acts of Corruption:
  - https://portal.paco.gov.co/

The Compliance Officer, in the dissemination of the Business Transparency and Ethics Program (conducted at least once a year), includes the promotion of these reporting channels.

4.5.4 Sanctions Procedure

Any situation of non-compliance with the policies and procedures of the Business Transparency and Ethics Program by a Company Employee entails the application of disciplinary sanctions in accordance with the Internal Work Regulations.

The severity of the violation must be analyzed by the Human Resources manager and the Compliance Officer.

Proportionate to the seriousness of the violation, one of the following sanctions is applied:

- Warning
- Formal Reprimand
- Written Memorandum
- Disciplinary Suspension
- Termination of Employment for Just Cause

Regardless of the analysis of the violation, failure to timely report or failure to report an Unusual Transaction or a Suspicious Transaction constitutes a serious offense.

Disciplinary sanctions under the Internal Work Regulations do not exclude or exempt the responsible party from facing any applicable civil or criminal penalties.

4.5.5 Document Management Procedure

All activities resulting from the implementation of the Business Transparency and Ethics Program must be documented so that the information meets criteria of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality.

In compliance with regulations, information related to the Business Transparency and Ethics Program must be retained for 10 years, in any physical or digital medium, provided its reproduction is guaranteed.

Since this does not constitute a criminal complaint, the Company must file the corresponding report when a criminal offense is identified.

+57 (1)7943999
Carrera 11B # 99 - 25
Piso 10 - Edificio Wework
Bogotá, Colombia
www.canalclima.com
canalclima

ANNEX 1. GLOSSARY.

Agent: Any person authorized to act, directly or indirectly, on behalf of the Organization. Agents include advisors, consultants, contractors, lawyers, service providers, intermediaries, or any person acting on behalf of the Organization..

Senior Executives: Natural or legal persons appointed in accordance with the corporate bylaws, any internal provision of the legal entity (Organization), or Colombian law, as applicable, to manage and direct the legal entity, whether as members of collegiate bodies or individually.

Associates: Natural or legal persons who have contributed money, work, or other assets of monetary value to a company in exchange for shares, interests, or any other form of participation allowed under Colombian law.

Close Associates: Legal entities whose administrators, shareholders, controllers, or managers are PEPs (Politically Exposed Persons), or that have established autonomous patrimonies or trusts for them, or with whom commercial relationships are maintained; due diligence is applied according to current regulations.

Self-Control: The willingness of the entrepreneur and administrators to detect, control, and efficiently manage the risks to which the Organization is exposed.

Compliance Audit: A systematic, critical, and periodic review regarding the proper implementation of the Business Ethics Program.

Hospitality (Attentions): Refers to payments for travel or accommodation offered by a Third Party or provided to them by an Employee.

Beneficial Owner: The natural person(s) who ultimately owns or controls a client or the natural person on whose behalf a transaction is conducted. It also includes any person who exercises final and/or effective control, directly or indirectly, over a legal entity or other non-legal structure. Beneficial owners of a legal entity include:

a. A natural person who, individually or jointly, exercises control over the legal entity under Articles 260 et seq. of the Colombian Commercial Code;

b. A natural person who, individually or jointly, holds, directly or indirectly, 5% or more of the capital or voting rights of the legal entity, and/or benefits from 5% or more of the profits, income, or assets;

c. When no natural person is identified in (a) or (b), the natural person holding the position of legal representative, unless another person holds greater authority regarding management or direction.

For fiduciary contracts, non-legal structures, or similar legal structures, beneficial owners include natural persons holding positions such as: settlors, trustees, beneficiaries, fiduciary committee members, or any person exercising effective control or the right to enjoy/dispose of assets, benefits, or profits.

Employee: An individual who provides personal services under the Organization's subordination in exchange for compensation.

Counterparty: For purposes of anti-money laundering, counter-terrorism financing, and WMD proliferation risk prevention, any natural or legal person with whom the Organization has commercial,

business, contractual, or legal relationships. This includes agents, shareholders, employees, suppliers, and grantees.

Contractor: In the context of a business or transaction, any third party providing services to the Organization or having a contractual legal relationship with it. Contractors may include suppliers, intermediaries, agents, distributors, advisors, consultants, and parties in joint ventures, temporary unions, consortia, or risk-sharing arrangements.

Ethics Committee: Composed of the General Director, Administrative and Financial Manager, and Compliance Officer. Responsible for receiving, processing, investigating, recording, and analyzing any case of suspected corruption or transnational bribery or any violation of the Code of Conduct and Ethics.

Conflict of Interest: Occurs when the personal, familial, or commercial interests, direct or indirect, of an Employee may conflict with the Organization's interests, interfere with the Employee's obligations, or affect performance or impartiality. Conflicts also exist when Employees receive undue personal benefits from their position.

Corruption: Any act that harms the Organization's interests or assets and violates the Code of Conduct. Includes bribery and acts constituting offenses against public administration, economic order, environment, and other forms of corruption.

Other Forms of Corruption: Includes:

- **Private Corruption:** Promising, offering, or giving an unjustified benefit to managers, employees, or advisors to obtain favor for oneself or a third party (Art. 16, Anti-Corruption Statute, Law 1474/2011).
- **Mismanagement:** Administrators, partners, employees, or advisors abusing functions for personal or third-party benefit, causing economic harm (Art. 17, Anti-Corruption Statute, Law 1474/2011).
- **Collusion:** Restrictive competition practices aimed at manipulating public tenders or award results.
- **Facilitation Payments:** Sums offered to expedite routine procedures by public officials.

Due Diligence: The process through which the Organization takes measures to understand a Counterparty, their business, operations, products, and transaction volumes.

Enhanced Due Diligence: Additional and more intensive measures applied to higher-risk Counterparties, their business, operations, products, and transaction volumes, based on established segmentation.

Government Entity: Any national or international government authority or body, public institutions, decentralized entities, judicial offices, state-owned or controlled commercial enterprises, and international organizations (e.g., World Bank, Red Cross), including public agencies and subdivisions at any territorial level.

Entertainment: Invitations to social, cultural, or sporting events attended by the Third Party with the Organization's Employee.

Terrorism Financing (TF): Activities aimed at channeling lawful or unlawful resources to provide, collect, deliver, receive, manage, or support organized crime, armed groups, terrorists, or terrorist activities, nationally or internationally.

Financing of WMD Proliferation (FPWMD): Any act providing funds or financial services, wholly or partially, for the illegitimate production, acquisition, possession, development, export, transfer, or dual-use of materials against national or international laws.

C/ST Risk Factors: Potential elements or causes generating Corruption/Transnational Bribery risk.

AML/TF/FPWMD Risk Factors: Potential elements or causes generating Anti-Money Laundering, Terrorism Financing, and WMD proliferation risks. Factors consider Counterparties, products, activities, channels, and jurisdictions.

Government Official: Any person acting on behalf of a Government Entity, including employees of state-owned companies, political parties, or international public organizations.

Stakeholders: Groups affected directly or indirectly by the Organization, capable of affecting the Organization's operations. Internal: Employees, shareholders, clients, executives, and Group RFC subsidiaries. External: Third Parties, suppliers, contractors, Government Entities, Government Officials, and certification bodies.

High-Risk Jurisdictions or Zones:

- Countries or jurisdictions classified as high risk by FATF: UIAF List
- Countries with high corruption indices (Transparency International CPI): https://www.transparency.org
- Areas with public order issues according to public sources.

Compliance Officer: Natural person appointed to promote, develop, and oversee compliance with procedures to prevent, update, and mitigate risks of Money Laundering, Terrorism Financing, Corruption, and Bribery.

AML/TF/FPWMD: Money Laundering, Terrorism Financing, and Financing of WMD Proliferation.

Money Laundering: Crime defined in Article 323 of the Colombian Penal Code (or subsequent amendments).

Law 1778 / Anti-Bribery Law: Law 1778 of February 2, 2016, establishing liability of legal persons for acts of transnational corruption and related provisions.

Ethics Line: Anonymous, independent channel for reporting violations of internal policies or ethical standards. Managed by a third party, ensuring confidentiality, anonymity, and 24/7 availability.

Toll-Free Line: 01-800-752-2222 Option 1 for an operator, Option 2 for recorded message.

Email: lineaetica.rfc@resguarda.com

Website: www.resguarda.com/lineaeticagruporfc

WhatsApp: +57 1 7868154

Binding List: Lists of persons and entities associated with terrorist organizations that are binding for Colombia under Colombian law (Article 20, Law 1121 of 2006) and in accordance with international law. This includes, but is not limited to, UN Security Council Resolutions 1267 (1999), 1373 (2001), 1718 and 1737 (2006), 1988 and 1989 (2011), 2178 (2014), and any successors, related or complementary lists, as well as any other lists binding in Colombia, such as the U.S. terrorist lists, the EU list of terrorist organizations, and the EU list of persons designated as terrorists.

Risk Matrix: A tool used to identify risks of Corruption, Transnational Bribery, Money Laundering, Terrorism Financing, and Financing of the Proliferation of Weapons of Mass Destruction.

Reasonable Measures: Sufficient, appropriate, and measurable actions in quality and quantity to mitigate ML/TF/WMD risks, taking into account the Organization's inherent risks and materiality.

International Business or Transactions: Any business or transaction of any nature with foreign natural or legal persons, whether public or private.

Anti-Corruption and Anti-Bribery Standards: The regulatory framework defining conduct considered criminal related to corruption and transnational bribery, including the Anti-Corruption Statute, Law 1778 of 2016, the Colombian Penal Code, and Law 2195 of 2022.

Compliance Officer: Refers to the Organization's Employee responsible for promoting and developing specific procedures to prevent, update, and mitigate the risk of money laundering, terrorism financing, corruption, and domestic or transnational bribery.

Unusual Transaction: A transaction whose amount or characteristics are inconsistent with the Company's ordinary economic activity, or that, due to number, amount, or characteristics, falls outside normal business practices in a sector, industry, or with a type of Counterparty.

Suspicious Transaction: An Unusual Transaction that cannot be reasonably justified according to the customs and practices of the relevant activity. Includes attempted or rejected transactions that display suspicious characteristics.

Politically Exposed Person (PEP): Public officials at any level of national or territorial administration who are assigned or delegated functions such as drafting regulations, general management, policy formulation, plan implementation, management of state assets, administration of justice, or administrative sanctioning. Also includes individuals managing resources in political parties or movements. Functions may be exercised through budget management, public contracting, investment project management, payments, asset administration, etc. Examples include:

- President, Vice President, ministers, vice ministers, advisors, directors, and sub-directors of administrative departments.
- General Secretaries, Treasurers, CFOs of ministries, administrative departments, and supervisory bodies.

- Directors, managers, CFOs, treasurers of public establishments, special administrative units, public service companies, state social enterprises, industrial and commercial state companies, and mixed-economy companies.
- Superintendents and Deputy Superintendents.
- Senior military and police officials empowered to authorize spending or commit resources.
- Governors, mayors, deputies, councilors, treasurers, CFOs, and general secretaries at local and departmental levels.
- Senators, members of the House, general secretaries, committee secretaries, and administrative directors of Congress.
- Managers and co-directors of the Central Bank.
- Directors and financial controllers of regional autonomous corporations.
- National Civil Service Commissioners and commissioners of regulatory commissions (energy, water, communications).
- Judges, magistrates, prosecutors, and related high-level judicial officers.
- Comptrollers, attorneys general, ombudsmen, auditors, and their deputies or delegates.
- Treasurers and budget approvers of high courts, tribunals, attorney general, comptroller, ombudsman, and audit offices.
- Electoral council magistrates, national civil registrar, and delegated registrars.
- Notaries and urban curators.
- Budget approvers in public universities.
- Legal representatives, presidents, directors, and treasurers of political parties and movements.
- Settlors of autonomous patrimonies or trusts managing public resources.

*Note***:** PEP status applies during tenure and for two (2) years after leaving office, resignation, dismissal, annulment, or termination of any contract.

PEP of International Organizations: Individuals holding executive functions in international organizations such as the UN, OECD, UNICEF, and the Organization of American States (e.g., directors, deputies, board members, or equivalent roles).

Foreign PEPs: Individuals performing prominent public functions in another country, including heads of state/government, ministers, legislators, high court judges, central bank board members, ambassadors, military leaders, state enterprise managers, royalty, political party leaders, and senior executives of international organizations.

Compliance Policies: Adopted as the Anti-Corruption Policy, these are the Organization's general policies to conduct business ethically, transparently, and honestly, while identifying, preventing, and mitigating corruption or transnational bribery risks.

Supplier: Any individual or entity that sells or provides goods or services to the Organization in exchange for monetary or in-kind compensation.

Gifts: Items of value such as discounts, gift cards, favors, subsidies, goods, equipment, or services given by Employees to third parties or vice versa.

Contagion Risk: The potential loss the Organization may suffer, directly or indirectly, due to the actions or experiences of a Counterparty.

Corruption Risks: The possibility that public administration purposes are diverted or public assets are misused for private benefit.

Legal Risk: Potential losses from penalties or obligations to compensate for breaches of laws, regulations, or contracts, including errors from negligence, malintent, or involuntary acts affecting contracts or transactions.

Operational Risk: The possibility of loss from deficiencies in human resources, processes, technology, infrastructure, or external events. Includes Legal and Reputational Risk.

Reputational Risk: Potential loss from damage to the Organization's image or negative publicity affecting income or legal proceedings.

Inherent Risk: Risk level intrinsic to an activity, without considering controls.

Residual Risk: Risk remaining after applying controls.

Transnational Bribery Risk (ST Risk): The possibility that a legal entity, directly or indirectly, gives, offers, or promises money, valuable items, or other benefits to a foreign public official in exchange for performing, omitting, or delaying acts related to their functions in connection with an international business or transaction.

Suspicious Activity Report (SAR/ROS): A report of transactions outside normal business patterns or industry practices that cannot be reasonably justified.

SAGRILAFT: Self-control and integrated risk management system for ML/TF/WMD.

Warning Sings: Qualitative or quantitative indicators signaling the possible occurrence of unusual or suspicious events outside ordinary operations.

Bribery: Offering, promising, or giving money, valuable items, or other benefits to a private party or public official to induce or delay actions related to their functions and an Organization-related business.

Transnational Bribery: When the Organization, through employees, administrators, associates, contractors, or subsidiaries, gives, offers, or promises money, valuable items, or benefits to a foreign public official to influence acts in connection with an international business or transaction.

Third Party: Any natural or legal person with whom the Organization has a commercial relationship other than an employment relationship.

Financial Intelligence Unit (UIAF): Colombia's Financial Intelligence Unit responsible for intervening in the economy to prevent and detect ML/TF/WMD.