INTRODUCTION

Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, Magnum Zona Franca S.A.S., and Logística S.A.S., which for the purposes of this document shall be referred to as the Companies, acknowledge that, as part of their corporate responsibility, they must act in compliance with the Political Constitution, the laws of the Republic, the regulations governing their operations, and the ethical values and principles defined by the organization.

The Transparency and Business Ethics Program – PTEE is intended to reflect the commitment of the Companies, their administrators, directors, and employees to act ethically, transparently, and responsibly toward all their stakeholders, promoting a culture of integrity in the development of their operations, business relationships, and other own or complementary activities.

The Companies have zero tolerance for any act, conduct, operation, transaction, agreement, or omission that goes against their principles, corporate values, internal policies, and other guidelines adopted to prevent and mitigate risks associated with corruption, national bribery, transnational bribery, fraud, or any practice contrary to the law, business ethics, and transparency.

All employees and other stakeholders of the Companies are responsible for knowing, complying with, and supporting the implementation of the Transparency and Business Ethics Program – PTEE, according to their role and relationship with the organization.

1. OBJECTIVE

To establish the policies, guidelines, responsibilities, procedures, and mechanisms of the Transparency and Business Ethics Program – PTEE, in order to identify, prevent, manage, and mitigate the risks of corruption and transnational bribery to which the Companies may be exposed in the development of their operations, including related conducts that may facilitate or materialize such risks.

2. SCOPE

The Transparency and Business Ethics Program – PTEE applies to Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, Magnum Zona Franca S.A.S., and Logística S.A.S., in accordance with the comprehensive compliance model adopted by the organization and with the regulatory obligations applicable to each company.

The program is mandatory for shareholders, legal representatives, directors, employees, contractors, suppliers, clients, and other stakeholders who have a direct or indirect relationship with the Companies, according to the type of relationship, role, and responsibilities applicable to them.

The PTEE is articulated, as applicable, with the ML/TF/FPWMD risk management systems applicable to each company, including SAGRILAFT for Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, and Magnum Zona Franca S.A.S., and SARLAFT for Logística S.A.S., as well as with the Code of Ethics, Conduct and Good Governance, corporate policies, the risk matrix, procedures, instructions, reporting channels, training mechanisms, disclosure, monitoring, auditing, and other documents of the Integrated Management System.

3. DEFINITIONS

Total Assets: All current and non-current assets recognized in the statement of financial position that correspond to the present economic resources controlled by the Company.

Acts/Events of Corruption: All actions or omissions that may give rise to a benefit or the satisfaction of an interest related to the commission of crimes against public administration or public assets, or to the commission of Transnational Bribery conducts.

Senior Management: Natural or legal persons appointed in accordance with the corporate bylaws or any other internal provision of the legal entity and Colombian law, as applicable, to administer and direct the Legal Entity, whether as members of collegiate bodies or as individually considered persons.

Risk Analysis: The systematic use of available information to determine the possibility of occurrence of an event and the magnitude of its consequences.

Associates: Natural or legal persons who participate in a company through contributions in money, work, or other assets appreciable in money, in exchange for shares, quotas, interest participation, or any other form of participation provided by law. An associate is also understood as a person who decides to incorporate a legal entity, join an existing one, or contribute to the joint development of the corporate purpose approved in its bylaws.

Compliance Audit: The systematic, critical, and periodic review of the proper execution of the Transparency and Business Ethics Program.

Beneficial Owner(s): The natural person(s) who ultimately own(s) or control(s), directly or indirectly, a client and/or the natural person on whose behalf a transaction is carried out. This also includes the natural person(s) who exercise effective and/or final control, directly or indirectly, over a legal entity or another structure without legal personality.

The following are beneficial owners of a legal entity:

The legal entity, under the terms of Article 260 of the Commercial Code, subrogated by Article 26 and following articles of Law 222 of 1995.

Indirectly, five percent (5%) or more of the capital or voting rights of the legal entity, and/or who benefits from five percent (5%) or more of the returns, profits, or assets of the legal entity, under the terms of Article 16 of Law 2155 of 2021.

The natural person who holds the position of legal representative must be identified, unless there is a natural person who holds greater authority regarding the management or direction functions of the legal entity, under the terms of Article 16 of Law 2155 of 2021.

Reporting Channel: Instruments, tools, or alert systems that allow employees, clients, users, contractors, partners, members of boards of directors, and other counterparties to confidentially communicate and report activities or events that may possibly be considered acts of corruption or conducts that may potentially threaten transparency and ethics.

Contractor: In the context of an international business or transaction, this refers to any third party that provides services to a legal entity or has any type of contractual legal relationship with it. Contractors may include, among others, suppliers, intermediaries, agents, distributors, advisors, consultants, and persons that are part of collaboration or joint venture contracts with the company.

Corruption: Conducts aimed at allowing the Company to benefit, seek a benefit or interest, or be used as a means in the commission of crimes against public administration or public assets, or in the commission of Transnational Bribery conducts.

Private Corruption: According to Article 250A of the Criminal Code, added by Article 16 of Law 1474 of 2011, this is understood as the conduct of anyone who, directly or through an intermediary, promises, offers, or grants to directors, administrators, employees, or advisors of a company, association, or foundation a gift or any unjustified benefit so that such person favors them or a third party.

Basic Legal Circular: Basic Legal Circular No. 100-000005 of 2017 of the Superintendence of Companies, including its amendments, additions, or any regulations that replace it.

Code of Ethics, Conduct and Good Governance: The document or set of guidelines that establishes principles, values, rules of conduct, good governance guidelines, reporting channels, reporting duties, whistleblower protection mechanisms, and consequences for non-compliance, in order to guide the ethical and transparent conduct of the employees, administrators, contractors, and other stakeholders of the Companies.

Companies: For the purposes of this document, Companies shall mean Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, Magnum Zona Franca S.A.S., and Logística S.A.S., as applicable.

Conflict of Interest: A situation in which personal, family, economic, political, labor, or any other type of interests may interfere, or appear to interfere, with a person's objective judgment, independence, or decision-making in the performance of their duties within the organization.

Counterparty or Stakeholder: Any natural or legal person with whom the Company has commercial, business, contractual, labor, operational, or legal relationships of any kind. Among others, counterparties may include shareholders, administrators, employees, clients, suppliers, contractors, drivers, owners, holders, intermediaries, allies, authorities, and other related third parties.

Due Diligence: The process of identifying, knowing, reviewing, and evaluating current or potential counterparties through the verification of information, supporting documents, and other necessary elements, according to the corruption and transnational bribery risks to which the Company may be exposed.

Enhanced Due Diligence: The process through which additional and more in-depth measures are adopted to know a counterparty, its business, operations, products, transaction volume, beneficial owners, source of funds, and other relevant aspects, when a more detailed analysis is required due to its risk level.

Whistleblower: A person who reports the circumstances of time, manner, and place of a specific act that results in a risk, unlawful act, or malpractice that may affect business integrity or the general interest and, therefore, may cause administrative, disciplinary, tax, and/or criminal consequences for the legal or natural person involved.

Enterprise: According to Article 25 of the Commercial Code, it is "any organized economic activity for the production, transformation, circulation, administration, or custody of goods or for the provision of services. Such activity shall be carried out through one or more commercial establishments."

Non-Profit Entity: A legal entity capable of exercising rights and assuming civil obligations, and of being represented judicially and extrajudicially, in which there is no capitalist concept of return on investment. Therefore, no distribution of surpluses or benefits obtained by the obligated subject is made in favor of any natural or legal person. The surpluses obtained by this type of organization at the end of each fiscal year must be reinvested in its corporate purpose.

Employee: A natural person who provides personal services to the Company or any of its related companies, under an employment relationship or any other form of relationship permitted by law.

Business Ethics: The set of principles, values, actions, and behaviors promoted by the organization, within the framework of a responsible business culture, in order to encourage lawful, transparent, and respectful actions toward employees, clients, suppliers, contractors, investors, authorities, and other stakeholders.

Risk Factors: The possible elements, circumstances, or causes that generate corruption and transnational bribery risks for the Company. For their identification, among others, counterparties, activities, products or services, channels, geographic areas, operations, processes, and other characteristics of the business may be considered.

Joint Venture: A business collaboration agreement through which two or more parties join together to develop a specific project, business, or operation, sharing resources, responsibilities, risks, and benefits, either through the creation of a new company or through a contract, without necessarily losing their legal independence.

Law 1778 or Anti-Bribery Law: Law 1778 of February 2, 2016, which establishes rules on the liability of legal entities for acts of transnational corruption and issues other provisions regarding the fight against corruption.

Lobbying: The performance of actions aimed at influencing, promoting, or managing before authorities, public entities, trade associations, or other actors, decisions favorable to the interests of a Company, sector, or association, in accordance with the law, transparency, and internal policies.

International Businesses or Transactions: International businesses or transactions are understood as businesses or transactions of any nature with foreign natural or legal persons, whether governed by public or private law.

Risk Matrix: The tool that allows the Company to identify, analyze, evaluate, control, and monitor corruption and transnational bribery risks to which it may be exposed, as well as the controls, responsible parties, treatments, and follow-ups defined for their management.

Compliance Manual: The document that contains the Transparency and Business Ethics Program of the Companies, their policies, procedures, responsibilities, controls, and other elements necessary for its implementation, monitoring, and improvement.

Businesses or Transactions: All operations of any nature with natural or legal persons governed by public or private law.

OECD: The Organisation for Economic Co-operation and Development.

Compliance Officer: A natural person responsible for leading and managing the PTEE, in accordance with the functions, requirements, and obligations established in the applicable regulations of the Superintendence of Companies and the Superintendence of Transportation, including any rules that amend, add to, or replace them.

Politically Exposed Person or PEP: Corresponds to the definition established in Article 2.1.4.2.3 of Decree 1081 of 2015, as amended by Article 2 of Decree 830 of July 26, 2021.

Compliance Policies: The general policies adopted by the Senior Management of the company so that the latter may conduct its business ethically, transparently, and honestly, and be able to identify, detect, prevent, and mitigate corruption risks or Transnational Bribery risks.

Legal Entity: In accordance with Article 633 of the Civil Code, this refers to "a fictitious person, capable of exercising rights and assuming civil obligations, and of being represented judicially and extrajudicially," including non-profit entities, public law entities, and civil and commercial companies.

Obligated Legal Entity: Those subject to inspection, surveillance, and control under Article 34-7 of Law 1474 of 2011, added by Article 9 of Law 2195 of 2022, and which, by determination of the corresponding Superintendencies and authorities, must adopt Transparency and Business Ethics Programs.

Transparency and Business Ethics Program – PTEE: The document that contains the Compliance Policy and the specific procedures under the responsibility of the Compliance Officer, aimed at implementing the Compliance Policy in order to identify, detect, prevent, manage, and mitigate Corruption Risks or Transnational Bribery Risks to which the Company may be exposed, in accordance with the risk matrix, applicable regulations, and internal documents defined by the organization.

Suspicious Transaction Report – STR: The report filed before the Financial Information and Analysis Unit – UIAF, when, after the corresponding analysis, operations, events, or situations are identified that may be considered suspicious, in accordance with the applicable regulations.

Corruption Risks: The possibility that, by action or omission, the purposes of public administration may be diverted toward a private benefit, public assets may be affected, or conducts may arise that could compromise transparency, business ethics, or compliance with the PTEE.

Transnational Bribery or Transnational Bribery Risk or TB Risks: The act or possibility that the Company, directly or through its employees, administrators, associates, contractors, subordinate companies, or any related third party, gives, offers, or promises to a foreign public official, directly or indirectly, sums of money, objects of pecuniary value, or any benefit or advantage, so that such foreign public official performs, omits, or delays any act related to their duties and in connection with an international business or transaction.

CO/TB Risks: Corruption Risk and/or Transnational Bribery Risk, according to the terminology used by the Superintendence of Companies and the Superintendence of Transportation, as applicable.

Inherent Risk: The level of risk inherent to the activity, without considering the effect of controls.

Residual Risk: The resulting level of risk after applying controls.

Foreign Public Official: Has the scope provided in the First Paragraph of Article 2 of Law 1778. In general terms, it includes any person who holds a legislative, administrative, or judicial position in a foreign State, its political subdivisions or local authorities, or who performs a public function for a foreign State, foreign state entity, or international public organization.

Risk Management System for Transnational Bribery and Other Corrupt Practices: The system aimed at properly articulating the Compliance Policies with the Business Ethics Program and ensuring its adequate implementation in the Legal Entity.

SIREL: The Online Reporting System managed by the Financial Information and Analysis Unit – UIAF, through which the corresponding reports are made, in accordance with the applicable regulations.

Bribery: Offering, giving, or promising, or authorizing someone to offer, give, or promise, an undue benefit, directly or indirectly, with the intention of influencing or rewarding someone's behavior in order to obtain or retain a business advantage.

Subordinate Company: Has the scope provided in Article 260 of the Commercial Code and any other regulations that amend, add to, or replace it.

Supervised Company: A company, sole proprietorship, or branch of a foreign company subject to the surveillance of the Superintendence of Companies, under the terms provided in Article 84 of Law 222 of 1995.

Obligated Subject: A legal entity that, because it is subject to inspection, surveillance, or control by a competent authority and meets the applicable regulatory criteria, must adopt, implement, maintain, and update a Transparency and Business Ethics Program – PTEE, according to its activity, risk level, supervisory authority, and applicable regulations.

Financial Information and Analysis Unit – UIAF: A special administrative unit of the Colombian State responsible for receiving, centralizing, systematizing, and analyzing information related to suspicious transactions and other reports defined by the applicable regulations.

4. REGULATORY FRAMEWORK

This Transparency and Business Ethics Program – PTEE is based on the applicable national and international regulations regarding transparency, business ethics, prevention of corruption, transnational bribery, and other conducts that may affect the legality and integrity of the Companies' operations.

The PTEE is adopted and implemented in accordance with the regulatory obligations applicable to each company, considering its activity, supervisory authority, risk level, operation, and other particular conditions.

4.1. International Rules and Standards

In furtherance of Colombia's efforts to combat Corruption and transnational bribery, an international legal framework has been adopted, which includes the following conventions and agreements:

- The Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of the Organisation for Economic Co-operation and Development – OECD.
- The Inter-American Convention against Corruption of the Organization of American States – OAS.
- The United Nations Convention against Corruption – UNCAC.
- The Criminal Law Convention on Corruption of the Council of Europe.
- The Civil Law Convention on Corruption of the Council of Europe.
- The African Union Convention on Preventing and Combating Corruption.
- The OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance.

Some of the above instruments expressly promote the adoption of compliance programs, codes of conduct, internal audit mechanisms, anti-corruption controls, and policies aimed at preventing transnational bribery and other corrupt practices.

4.2. National Regulations

At the national level, the PTEE takes into account the applicable legal and regulatory provisions regarding transparency, business ethics, prevention, and the fight against corruption, including:

- **Law 222 of 1995:** Establishes, among other aspects, the supervisory powers of the Superintendence of Companies. In particular, paragraph 3 of Article 86 states that such Superintendence may impose sanctions or fines on those who fail to comply with its orders, the law, or the bylaws.
- **Law 1474 of 2011 – Anti-Corruption Statute:** Contains measures aimed at strengthening mechanisms for the prevention, investigation, and punishment of acts of corruption. It also incorporates provisions related to private corruption.

- **Law 1778 of 2016 – Anti-Bribery Law:** Establishes the administrative liability regime of legal entities for acts of transnational bribery. Additionally, Article 23 establishes the duty of the Superintendence of Companies to promote, among the companies subject to its surveillance, the adoption of transparency and business ethics programs, internal anti-corruption mechanisms, internal audit rules, and mechanisms for the prevention of transnational bribery conducts.
- **Decree 1736 of 2020:** Assigns to the Superintendence of Companies the function of instructing the entities subject to its supervision on the measures they must adopt to promote transparency and business ethics in their business practices and to have internal mechanisms for the prevention of acts of corruption.
- **CONPES 4070 of 2021:** Defines guidelines aimed at strengthening a culture of integrity, legality, trust, and the fight against corruption.
- **Law 2195 of 2022:** Adopts measures regarding transparency, prevention, and the fight against corruption. This law added Article 34-7 to Law 1474 of 2011, establishing that legal entities subject to inspection, surveillance, or control must adopt Transparency and Business Ethics Programs, in accordance with the guidelines defined by the competent authority.
- **Circular No. CIR24-00000089 / GFPU 13130000 of the Transparency Secretariat of the Presidency of the Republic and the Propositive Guide for the Preparation and Implementation of Transparency and Business Ethics Programs – PTEE:** These are used as references to strengthen a culture of integrity, transparency, trust, and compliance in the business sector.
- **Decree 1081 of 2015, as amended by Decree 830 of 2021:** Contains the definition and guidelines related to Politically Exposed Persons – PEP, which are considered within due diligence procedures.
- **Law 2155 of 2021:** Contains provisions related to the identification of beneficial owners, a relevant aspect within counterparty knowledge and due diligence processes.

4.3. Applicable Regulations of the Superintendence of Companies

For Magnum Logistics S.A.S., the PTEE follows the applicable provisions issued by the Superintendence of Companies regarding the prevention of corruption and transnational bribery risk.

Within this regulatory framework, the following are mainly considered:

- **External Circular 100-000003 of July 26, 2016,** through which the Superintendence of Companies issued the guide intended to implement business ethics programs for the prevention of transnational bribery conducts.
- **Basic Legal Circular No. 100-000005 of 2017 of the Superintendence of Companies,** including its amendments, additions, or any regulations that replace it.

- **External Circular 100-000011 of August 9, 2021,** through which External Circular 100-000003 of 2016 was fully amended and Chapter XIII of the Basic Legal Circular was added, related to the Transparency and Business Ethics Program – PTEE.
- **External Circular 100-000012 of August 9, 2021,** through which the Superintendence of Companies established its supervision policy for Transparency and Business Ethics Programs – PTEE.
- **External Circular 100-000003 of September 11, 2023,** through which the Superintendence of Companies established the requirements and deadlines for filing Report 75 — SAGRILAFT and PTEE, integrating the former Report 50 on ML/TF/FPWMD risk prevention and Report 52 on the Transparency and Business Ethics Program — PTEE.

This regulation establishes, among other aspects, the importance of having a written PTEE, a risk matrix, compliance policies, a Compliance Officer, due diligence procedures, disclosure, training, reporting channels, and monitoring and audit mechanisms.

4.4. Applicable Regulations of the Superintendence of Transportation

For Logística S.A.S., the PTEE incorporates the guidelines applicable to the transportation sector, according to its activity, operation, and supervisory authority.

Within this regulatory framework, the following are mainly considered:

- **Decree 2409 of 2018:** Establishes the inspection, surveillance, and control functions of the Superintendence of Transportation over the subjects under its supervision.
- **Resolution 14673 of September 18, 2025 of the Superintendence of Transportation,** through which Chapter 10 of Title V of the Single Circular of Infrastructure and Transportation was added, related to the Transparency and Business Ethics Program – PTEE.
- **Resolution 7038 of May 15, 2026 of the Superintendence of Transportation,** through which Chapter 10 of Title V of the Single Circular of Infrastructure and Transportation was amended, related to the Transparency and Business Ethics Program – PTEE.

These resolutions establish and update the guidelines that legal entities subject to inspection, surveillance, and control by the Superintendence of Transportation must observe for the implementation of the PTEE. In particular, they establish provisions related to the minimum content of the program, compliance policies, procedures manual, code of ethics and good governance, organizational structure, obligations of the highest corporate body, legal representative, Compliance Officer or Compliance Responsible Person, statutory auditor, internal audit, PTEE stages, risk matrix, reports, disclosure, training, and document retention.

For Logística S.A.S., the PTEE must be articulated with SARLAFT and with the other documents, controls, procedures, instructions, and mechanisms defined in the Integrated Management System, as applicable.

5. POLICY ON PREVENTION AND ZERO TOLERANCE AGAINST CORRUPTION, TRANSNATIONAL BRIBERY, AND RELATED CONDUCTS

The Companies are committed to preventing acts of corruption and transnational bribery in the development of their businesses, operations, and relationships with third parties. For this reason, all their actions must be carried out under the principles of legality, transparency, business ethics, good faith, and compliance with the applicable regulations.

The Companies have zero tolerance for any act, conduct, operation, transaction, agreement, or omission that may be related to corruption, transnational bribery, or any practice contrary to the law, corporate values, corporate principles, and internal policies. This commitment also includes related conducts such as fraud, national bribery, improper payments, unauthorized benefits, or any action that may facilitate or materialize corruption risks.

Shareholders, legal representatives, administrators, employees, clients, suppliers, contractors, and other stakeholders are prohibited from offering, promising, giving, requesting, accepting, or authorizing, directly or indirectly, money, gifts, favors, benefits, economic advantages, or any item of value, for the purpose of unduly influencing a decision, obtaining an advantage, retaining business, expediting a procedure, or favoring a natural or legal person.

This prohibition applies to relationships with national or foreign public officials, authorities, public entities, control bodies, clients, suppliers, contractors, intermediaries, and other third parties.

Any breach of this policy must be reported through the channels defined by the Companies and shall be evaluated in accordance with this PTEE, the Internal Work Regulations, contracts, internal policies, and applicable regulations, without prejudice to any administrative, civil, criminal, or disciplinary liabilities that may arise.

5.1. Design, Approval, and Allocation of Resources

For the design and update of the Transparency and Business Ethics Program – PTEE, the Companies take into account the applicable regulations, materiality, the nature of their operations, the services they provide, their structure, their processes, their counterparties, and the risk factors associated with corruption and transnational bribery, as well as any related conducts that may facilitate or materialize such risks.

The PTEE is structured under a risk-based approach and is articulated with the comprehensive risk matrix, procedures, instructions, policies, controls, and other documents of the Integrated Management System that may be applicable.

The highest corporate body, as applicable, shall approve the PTEE, its policies, procedures, risk matrix, Code of Ethics and Good Governance, and other documents that form an integral part of the program.

For Magnum Logistics S.A.S., such approval and the appointment of the Compliance Officer shall be carried out in accordance with the applicable provisions of the Superintendence of Companies. For Logística S.A.S., the approval of the PTEE and the appointment of the Compliance Officer shall be carried out in accordance with the guidelines established by the Superintendence of Transportation.

For Agencia de Aduanas ML S.A.S. Nivel 1 and Magnum Zona Franca S.A.S., the PTEE shall be approved or ratified as a good corporate practice, without prejudice to any legal, regulatory, or supervisory obligations that may be applicable to them.

The Companies, through their competent bodies and legal representatives, shall guarantee the human, technological, financial, and operational resources necessary for the Compliance Officer to properly and timely perform their duties.

The policies, procedures, instructions, protocols, and other guidelines defined in this PTEE shall be mandatory for administrators, legal representatives, employees, contractors, suppliers, clients, and other stakeholders, according to the role, relationship, and responsibility applicable to them.

6. COMPLIANCE POLICIES OF THE TRANSPARENCY AND BUSINESS ETHICS PROGRAM – PTEE

The following policies develop the general policy on prevention and zero tolerance against corruption, transnational bribery, and related conducts. Their application shall be carried out in coordination with the procedures, instructions, forms, matrices, and other documents of the Integrated Management System that may be applicable.

These policies are mandatory for the shareholders, administrators, legal representatives, employees, clients, suppliers, contractors, intermediaries, and other stakeholders of the Companies, according to their role, relationship, and level of responsibility.

6.1. Whistleblower or Reporting Person Protection and Non-Retaliation Policy

The Companies promote the timely and good-faith reporting of any situation that may be related to acts of corruption, transnational bribery, fraud, national bribery, conflicts of interest, improper payments, unauthorized benefits, breaches of the PTEE, or conducts contrary to business ethics.

The Companies shall not discriminate against or retaliate against employees, counterparties, or third parties who report possible breaches, red flags, or concerns raised in good faith.

However, making false or malicious reports, or providing information knowing that it does not correspond to reality, is considered contrary to this policy.

Reports may be made through the channels defined by the Companies, which allow situations to be reported confidentially and, where possible, anonymously. The information received shall be handled with confidentiality, care, and traceability.

Reports shall be reviewed by the Compliance Officer or by the competent bodies, in accordance with the internal procedures defined by the Companies. Where appropriate, the applicable preventive, corrective, disciplinary, contractual, or legal actions shall be adopted.

6.2. Policy Against Money Laundering, Terrorist Financing, and Financing of the Proliferation of Weapons of Mass Destruction

The Companies maintain their commitment to the prevention of risks associated with money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction – ML/TF/FPWMD.

This policy is articulated with the risk management systems applicable to each company, including the SARLAFT of Logística S.A.S. and the SAGRILAFT of Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, and Magnum Zona Franca S.A.S., as well as with the internal procedures related to client selection and documentation, purchasing and supplier selection, human talent, suspicious activity reports, document control, and record control of the Integrated Management System.

No operation, commercial, contractual, or labor relationship may be used to facilitate, conceal, or channel resources associated with illegal activities, corruption, transnational bribery, improper payments, or any conduct contrary to the law and internal policies.

6.3. Policy Regarding Counterparties or Stakeholders

The Companies shall inform, through their communications and onboarding or update forms, as applicable, their commitment to the prevention of corruption, transnational bribery, and conducts contrary to business ethics.

The Companies shall not contract or conduct business with a counterparty when an unmanaged risk of non-compliance with applicable anti-corruption or transnational bribery laws, or with the prohibitions established in this PTEE, is identified.

The Companies shall not use clients, suppliers, contractors, agents, drivers, owners, holders, or other third parties as a means to commit, facilitate, or conceal acts of corruption, transnational bribery, improper payments, or unauthorized benefits.

Before establishing, maintaining, or renewing a commercial, contractual, labor, or legal relationship, the Companies shall apply reasonable due diligence measures to know their counterparties, validate their information, identify beneficial owners, evaluate red flags, and determine their level of risk exposure.

These measures are developed, among others, through the Human Talent procedure, the Client Selection and Documentation Instructions, the Purchasing Procedure, the supplier criticality matrix, the SARLAFT/SAGRILAFT systems, and other documents of the Integrated Management System that may be applicable.

6.4. Conflict of Interest Policy

A conflict of interest is understood as any situation in which the personal, family, economic, labor, commercial, or any other type of interests of shareholders, administrators, employees, contractors, or other stakeholders may be opposed to the legitimate interests of the Companies, or may affect the objectivity, independence, and transparency with which they must act in the performance of their duties or responsibilities.

A conflict of interest may arise in different ways. Therefore, employees, administrators, and other related persons must act with good judgment, transparency, responsibility, and a sense of belonging, avoiding participation in decisions or actions where personal or third-party interests may interfere with the interests of the Companies.

Any real, potential, or apparent conflict of interest must be promptly reported to the immediate supervisor, the Compliance Officer, the Human Talent area, or the competent body, so that it may be analyzed and the corresponding management measures may be defined.

In personnel onboarding processes, the Companies have mechanisms to identify possible family relationships, internal recommendations, or other links that may generate conflicts of interest. This information shall be reviewed by the Human Talent area, in accordance with the applicable internal procedures.

Among others, the following situations are considered events that may generate a conflict of interest:

- Receiving undue personal benefits as a result of the position, function, or relationship with the Companies.
- Taking advantage of business opportunities, information, assets, resources, or contacts of the Companies for personal benefit or for the benefit of third parties.

- Participating in decisions related to relatives, friends, partners, clients, suppliers, contractors, or third parties with whom there is a personal, economic, or commercial interest.
- Working for, advising, representing, or holding an interest in competing entities or entities that may affect the interests of the Companies.
- Favoring a client, supplier, contractor, or third party to the detriment of another party or of the Companies.
- Using the position to obtain additional benefits for oneself, relatives, friends, or third parties.
- Exceeding assigned duties or carrying out improper acts, even when arguing that they are for the benefit of the Companies.
- Offering, requesting, or accepting incentives, commissions, gifts, benefits, or courtesies outside the normal and authorized conditions for conducting business.
- Accepting courtesies, in money or in kind, that may affect independence, objectivity, or freedom of decision regarding what is most convenient for the Companies and their clients.

Persons facing a possible conflict of interest must refrain from intervening in the corresponding decision or management until the situation is reviewed and the applicable measures are defined. The handling of these cases must leave the corresponding traceability.

6.5. Policy on the Companies' Relationship with Their Employees

The Companies shall ensure fair and dignified treatment of their employees, promoting a respectful and transparent work environment aligned with corporate values, the Internal Work Regulations, internal policies, and applicable regulations.

Employees must act with honesty, responsibility, good faith, and adherence to the procedures defined by the Companies. Likewise, they must refrain from requesting, receiving, offering, or giving undue benefits, altering documents, concealing relevant information, signing documents without authorization, improperly using confidential information, or engaging in any conduct contrary to the PTEE.

Employees whose duties expose them to corruption or transnational bribery risks must strictly comply with the controls, procedures, authorizations, and reporting duties defined by the Companies.

Any breach of the PTEE, the Internal Work Regulations, employment contracts, or internal policies may give rise to the corresponding disciplinary, contractual, or legal measures, in accordance with the applicable regulations and the internal due process.

6.6. Policy on Relationships with the State, Authorities, and Public Officials

The Companies and their employees shall act with honesty, good faith, respect, and adherence to the legal rules governing their activities before the State, authorities, public entities, control bodies, and national or foreign public officials.

Any relationship with public officials shall be carried out in strict compliance with the law, applicable regulations, internal procedures, and the principles of transparency, traceability, and business ethics.

The Companies shall cooperate with state entities at the international, national, departmental, municipal, or district level when they conduct investigations, requests, visits, audits, or proceedings related to corruption, transnational bribery, regulatory compliance, or any matter within their authority.

It is prohibited to make payments, offers, gifts, favors, courtesies, benefits, or informal arrangements for the purpose of unduly influencing public, administrative, regulatory, contractual, operational, or supervisory decisions.

6.7. Lobbying Policy

Lobbying, advocacy, interest management, or institutional relationship activities shall be carried out in a lawful, transparent, respectful, and documented manner, and in accordance with the corporate principles, applicable regulations, and internal policies of the Companies.

Lobbying may not be used for corrupt or illegal purposes, nor to unduly influence decisions that represent an improper advantage for the Companies or for a third party.

When the Companies participate in projects, regulatory initiatives, procedures, sector-related actions, or relationship spaces with authorities, trade associations, local or regional governments, public corporations, inspection, surveillance and control entities, control bodies, regional autonomous corporations, political organizations, or other public actors, they shall act transparently and leave sufficient traceability of the management carried out.

The person carrying out lobbying or advocacy activities on behalf of the Companies shall report any real, potential, or apparent conflict of interest that may affect the objectivity or transparency of the activity.

It is not permitted to make payments, offers, gifts, favors, courtesies, benefits, or any improper arrangement to public officials, authorities, intermediaries, or third parties in order to obtain favorable decisions, expedite procedures, avoid controls, modify results, receive improper benefits, or improperly influence public or private actions.

Courtesies, gifts, travel, meals, lodging, or entertainment that may arise within the framework of commercial or institutional relationships shall be governed by the specific policy defined in this PTEE for such matters.

6.8. Policy on Government Contracting

When the Companies participate directly or indirectly in government contracting processes, bids, invitations, agreements, arrangements, or any contractual relationship with public entities, they shall act under the principles of legality, transparency, objectivity, free competition, and compliance with applicable requirements.

Any conduct aimed at obtaining undue advantages, directing processes, altering or falsifying documents, providing inaccurate information, entering into unauthorized agreements, offering improper benefits, engaging in collusion, unfair competition, or irregularly influencing decisions of public officials, public entities, or related third parties is prohibited.

The responsible areas shall keep traceability of the actions, supporting documents, approvals, communications, and documents related to this type of process, in order to evidence the transparency and legality of the management carried out.

6.9. Policy on Financing Political Campaigns

The Companies shall not make contributions, donations, funding, or financing to political campaigns, parties, political movements, candidates, or significant groups of citizens, unless there is express authorization from the General Management and the highest corporate body or competent authority, compliance with applicable regulations, and traceability of the operation.

Before any authorized political contribution is made, due diligence shall be conducted on the candidate, party, political movement, or beneficiary, as well as an analysis of possible conflicts of interest, especially when current or future relationships may exist with public contracting, procedures, permits, authorizations, or decisions by authorities.

Under no circumstances may political contributions be made for the purpose of obtaining commercial, contractual, regulatory, operational, or any other improper benefit for the Companies or for a third party.

Administrators, directors, employees, or collaborators who make political contributions in their personal capacity shall prevent such action from being confused with participation, support, or financing carried out on behalf of the Companies. When a possible conflict of interest exists, they shall report it through the channels defined by the Companies.

6.10. Policy on Donations, Sponsorships, and Contributions

All donations, sponsorships, or contributions made by the Companies shall have a lawful, transparent, and verifiable purpose and shall be aligned with the corporate principles, internal policies, and, when applicable, the Companies' corporate social responsibility or sustainability programs.

Sponsorships, donations, or contributions may not be used to receive commercial advantages, influence decisions of authorities or third parties, conceal improper payments, favor private interests, or materialize acts of corruption or transnational bribery.

Any donation, sponsorship, or contribution shall have prior approval from the General Management. Before approval, the purpose of the contribution, the reasonableness of the support, the identification of the beneficiary, the destination of the resources, possible conflicts of interest, and any red flag that may represent a risk for the Companies shall be validated.

The disbursement or delivery shall be made through traceable means, be duly supported, and have sufficient evidence to verify the purpose and recipient of the contribution made.

The improper use of donations, sponsorships, or contributions shall give rise to the applicable internal, contractual, or legal measures.

6.11. Policy on Gifts, Courtesies, Travel Expenses, Meals, Lodging, and Entertainment

Employees of the Companies shall not request, offer, give, receive, or accept gifts, benefits, favors, money, or any advantage in money or in kind from clients, suppliers, contractors, authorities, or third parties when these may influence, or appear to influence, a commercial, contractual, administrative, operational, or authority-related decision.

Only souvenir-type items or advertising materials of reasonable value may be accepted, such as calendars, notebooks, planners, keychains, pens, or other similar items with a corporate logo, provided that they are not intended to unduly influence a decision.

Invitations to training sessions, advisory meetings, conferences, or events directly related to the employee's position or duties may also be accepted, provided that they have a legitimate purpose and do not affect the independence, objectivity, or transparency of the action.

Business courtesies, dinners, travel, meals, lodging, or entertainment may only take place when they have a legitimate purpose, do not seek to obtain an undue advantage, and have prior approval from the General Management, Regional Management, or Administrative and Financial Management, as applicable.

Travel expenses, per diem, advances, reimbursements, or expense settlements shall be related to a real need of the authorized operation or management, have the corresponding supporting documents, and comply with the internal policies in force. Each employee shall apply good judgment when requesting, authorizing, or using the Companies' resources.

Any request, delivery, receipt, return, or exception related to these matters shall be justified and supported.

Until the Companies define a specific limit for these types of matters, any situation other than souvenirs, advertising material of reasonable value, or training related to the position shall be previously consulted and approved by the General Management, Regional Management, or Administrative and Financial Management, as applicable.

When the situation involves public officials, authorities, public entities, PEPs, contracting processes, procedures, audits, inspections, sensitive negotiations, possible conflicts of interest, or any red flag, the Compliance Officer shall be consulted beforehand.

6.12. Policy on Remuneration, Commission Payments, and Incentives

The Companies shall pay their employees in accordance with the employment contract, internal policies, and current labor regulations.

Commissions, incentives, or recognitions shall apply only to the positions, conditions, amounts, and procedures authorized by the Companies, in accordance with the internal documents defined for such purpose.

For commercial executives, commissions shall be calculated in accordance with OD-TH-04 Commission Policy for Commercial Executives, or the internal rule that amends, replaces, or updates it. This policy establishes the methodology applicable by company, the conditions to access commissions, profitability criteria, collection, accounts receivable, approval, and other rules defined by the Companies.

It is prohibited to use remuneration, bonuses, commissions, recognitions, variable payments, or any employment benefit to conceal improper payments, favor third parties, compensate decisions contrary to business ethics, or materialize acts of corruption.

When payments, commissions, incentives, or recognitions are agreed upon with associates, contractors, intermediaries, or third parties, they must be duly supported, justified, approved, recorded, and related to a real, lawful, and verifiable operation.

6.13. Financial, Accounting, Payments, and Records Management Policy

The Companies shall comply with the Corporate Policies of the Financial Area and the Corporate Policies of the Accounting Area, located in the Integrated Management System.

All financial and accounting operations, payments, advances, reimbursements, expense settlements, commissions, discounts, refunds, transfers, and other economic movements must be duly authorized, supported, recorded, and related to a real, lawful, and verifiable operation.

It is prohibited to alter, conceal, split, simulate, or improperly record payments, expenses, invoices, commissions, benefits, donations, courtesies, or any operation for the purpose of concealing acts of corruption, improper payments, favoritism, or breaches of the PTEE.

Payments shall not be made to unauthorized third parties, unregistered accounts, natural or legal persons other than the actual counterparty, or without sufficient supporting documentation, unless there is a valid justification, approval from the competent body, and complete traceability.

Accounting records must faithfully, completely, and timely reflect the operations carried out by the Companies. Under no circumstances may accounting records, money transfers, intercompany payments, payments to subordinate companies, intermediaries, or third parties be used to conceal bribes, gifts, kickbacks, improper payments, or other corrupt conducts.

7. CODE OF ETHICS AND GOOD GOVERNANCE

The Companies incorporate this Code of Ethics and Good Governance as an integral part of the Transparency and Business Ethics Program – PTEE, for the purpose of guiding the conduct of administrators, legal representatives, employees, contractors, suppliers, clients, allies, and other stakeholders, in accordance with the organizational culture, principles, values, and commitments defined in the Integrated Management System.

This Code seeks to promote ethical, transparent, responsible conduct that is consistent with the higher purpose of the Companies: to serve the world, creating opportunities and connecting solutions. Likewise, it is articulated with the mission, vision, corporate policies, Internal Work Regulations, procedures of the Integrated Management System, and other applicable internal documents.

Every person linked to or related to the Companies is jointly responsible for acting in accordance with this Code, the PTEE, and internal policies, with the support of Senior Management to act in accordance with ethical principles, legality, transparency, and the prevention of acts of corruption and transnational bribery.

7.1. Principles of Conduct

The principles adopted by the Companies constitute a guideline for action for all personnel and other stakeholders. These principles guide the way decisions are made, operations are carried out, and relationships with clients, suppliers, authorities, coworkers, and third parties are managed.

Principle of Equality: This consists of providing all persons, including coworkers, clients, suppliers, authorities, and the community in general, with equal, respectful, and

non-discriminatory treatment, guaranteeing equal opportunities to exercise their rights and carry out their activities.

Principle of Honesty and Transparency: This consists of acting with integrity, consistency, objectivity, and clarity between what is thought, said, and done, following regular channels, complying with current regulations, and avoiding any conduct that may generate corruption, transnational bribery, fraud, or any action that may call into question the ethical conduct of the Companies.

Principle of Prevalence of the Common Good: This consists of guiding decisions and actions toward the legitimate benefit of the Companies, their clients, authorities, employees, stakeholders, and the community in general, avoiding private interests that may affect the transparency, objectivity, or integrity of management.

Principle of Professionalism: This consists of maintaining and strengthening the knowledge, skills, and abilities required for the position, applying them with responsibility, quality, diligence, and commitment in the provision of services.

7.2. Corporate Values

The Companies develop their principles through the following corporate values:

Respect: Acting by recognizing the rights and dignity of people, institutions, and the environment.

Integrity: Doing things well, being consistent in what is thought, said, and done, even when no one is watching.

Trust: The foundation of every relationship. It is the security we convey to our clients because we will make the best possible decision.

Humility: It consists of keeping our virtues silent and allowing others to discover them.

7.3. General Rules of Conduct

Administrators, legal representatives, employees, contractors, and other stakeholders must act in accordance with the following general rules of conduct:

- Comply with the law, the PTEE, the Internal Work Regulations, corporate policies, procedures of the Integrated Management System, and other applicable internal guidelines.
- Act with honesty, transparency, good faith, responsibility, and respect in all commercial, labor, contractual, operational, and institutional relationships.
- Refrain from offering, promising, giving, requesting, accepting, or authorizing payments, gifts, favors, benefits, or undue advantages.

- Avoid and promptly report any real, potential, or apparent conflict of interest.
- Protect confidential, privileged, or sensitive information of the Companies, clients, suppliers, employees, and other stakeholders.
- Properly use the resources, assets, documents, systems, passwords, accesses, and tools provided by the Companies.
- Maintain traceability of the actions, approvals, supporting documents, communications, and decisions, as applicable.
- Report any situation that may be contrary to business ethics, the PTEE, internal policies, or the law.
- Attend and participate in the training, awareness, or disclosure spaces defined within the PTEE.

7.4. Management of Ethical Dilemmas

In the performance of their duties, employees, administrators, contractors, and other related persons may face situations in which it is not clear how to act or where there is pressure to make decisions contrary to the principles of the Companies.

When an ethical dilemma arises, the person must act prudently, consult the internal guidelines, and, when necessary, seek guidance from their immediate supervisor, the Compliance Officer, Human Talent, Legal, or the competent area.

Before making a decision, it is recommended to evaluate, among others, the following aspects:

- Whether the action is legal and permitted by internal policies.
- Whether the decision is transparent and can be clearly explained.
- Whether there is any personal, family, economic, or commercial interest that may affect objectivity.
- Whether the action may generate an undue benefit for the person, the Company, or a third party.
- Whether the situation may affect the reputation, trust, or integrity of the Companies.
- Whether the necessary supporting documents, authorizations, and traceability are available.

When there is doubt, the person must refrain from acting until guidance is received from the competent body.

7.5. Conducts Contrary to the Code of Ethics and Good Governance

The following conducts, among others, are considered contrary to this Code:

- Participating in, facilitating, concealing, or tolerating acts of corruption, transnational bribery, fraud, national bribery, improper payments, or unauthorized benefits.
- Offering, requesting, receiving, or giving gifts, favors, courtesies, commissions, travel, money, or any benefit that may unduly influence a decision.
- Altering, concealing, destroying, manipulating, or improperly using documents, records, supporting documents, reports, communications, or information.
- Using the position, role, or relationship with the Companies to obtain personal benefits or to unduly favor third parties.
- Intervening in decisions when there is an undeclared or unmanaged conflict of interest.
- Making improper payments, offers, gifts, or courtesies to public officials, authorities, clients, suppliers, contractors, or third parties.
- Failing to report red flags, suspicious conducts, breaches of the PTEE, or situations contrary to business ethics.
- Retaliating against those who report possible breaches or unethical conduct in good faith.
- Using confidential, privileged, or sensitive information for personal benefit or for the benefit of third parties.
- Acting outside the assigned duties, internal authorizations, or procedures defined by the Companies.

7.6. Procedure for Unethical Conducts

When an employee, administrator, contractor, supplier, client, or third party becomes aware of a situation that may be contrary to this Code, the PTEE, internal policies, or the law, they must report it through the channels defined by the Companies.

Reports shall be received and reviewed by the Compliance Officer or by the competent body, depending on the nature of the case. When necessary, the General Management, Administrative and Financial Management, Human Talent, Legal, Integrated Management Systems, or the corresponding area may participate.

The reported situations shall be analyzed with confidentiality, objectivity, and traceability, ensuring the proper handling of information, the protection of the good-faith whistleblower, and the adoption of the preventive, corrective, disciplinary, contractual, or legal measures that may be applicable.

When the case involves labor or disciplinary matters, it shall be handled in accordance with the Internal Work Regulations, employment contracts, internal policies, and applicable regulations.

7.7. Body Responsible for Handling Situations Contrary to the Code

The Compliance Officer shall be the body responsible for receiving, reviewing, and managing reports related to possible breaches of the PTEE, acts of corruption, transnational bribery, or conducts contrary to business ethics.

Depending on the reported situation, the Compliance Officer may rely on the General Management, Administrative and Financial Management, Human Talent, Legal, Integrated Management Systems, or any other competent area, in order to analyze the facts and define the corresponding treatment.

If the report involves the Compliance Officer or if there may be a conflict of interest in its management, the case must be escalated to the General Management or to the Administrative and Financial Management, in order to guarantee objectivity, independence, and traceability in its review.

7.8. Channels for Reporting Unethical Conducts

The Companies have internal channels to report possible breaches of the PTEE, unethical conducts, acts of corruption, transnational bribery, fraud, conflicts of interest, improper payments, unauthorized benefits, or any situation contrary to internal policies.

The reporting channels, their method of use, confidentiality, anonymity, and handling are defined in the corresponding section of this PTEE and in I-RF-03 Instructions for Reporting Suspicious Activities and Incentive Program.

The Companies guarantee the protection of the good-faith whistleblower and prohibit any type of retaliation, discrimination, pressure, threat, or unfavorable treatment against anyone who responsibly reports a situation.

7.9. Evaluation of Ethical Culture and Internal Perception

The Companies shall conduct evaluations, surveys, reviews, feedback sessions, or similar activities that make it possible to understand the perception of employees, managers, and directors regarding business ethics, compliance with the PTEE, transparency in actions, and dilemmas that may arise in the performance of their duties.

These activities may be carried out through internal surveys, training evaluations, meetings, audits, awareness sessions, mechanisms of the Integrated Management System, or any other means defined by the Companies.

The results may be used to strengthen training, update policies, improve controls, identify improvement opportunities, and reinforce the culture of compliance.

7.10. Mandatory Awareness and Training

Attendance and participation in awareness, training, or disclosure sessions related to the PTEE, the Code of Ethics and Good Governance, the prevention of corruption, transnational bribery, conflicts of interest, reporting channels, and other internal policies shall be mandatory for employees and other persons to whom such activities are addressed.

The Companies shall retain the supporting documents of training, attendance, disclosure, or evaluation that make it possible to evidence the knowledge and appropriation of this Code and the PTEE.

7.11. Breach of the Code of Ethics and Good Governance

A breach of this Code, the PTEE, or internal policies may give rise to preventive, corrective, disciplinary, contractual, or legal measures, depending on the nature of the facts, the relationship of the person involved, and the applicable regulations.

In the case of employees, the measures shall be applied in accordance with the Internal Work Regulations, employment contracts, internal policies, and the corresponding due process.

In the case of contractors, suppliers, clients, allies, or third parties, the Companies may adopt the contractual, commercial, or legal measures that may apply, including termination of the relationship, suspension of operations, reporting to competent authorities, or any other action permitted by law and the applicable contractual documents.

8. ORGANIZATIONAL STRUCTURE, FUNCTIONS, RESPONSIBILITIES, AND PTEE COMPLIANCE AUDIT

The Companies have a defined organizational structure for the implementation, execution, monitoring, auditing, updating, and improvement of the Transparency and Business Ethics Program – PTEE.

The functions and responsibilities described in this section shall apply according to the nature of each company, its activity, risk level, supervisory authority, and applicable regulations. Accordingly, Magnum Logistics S.A.S. shall comply with the applicable provisions of the Superintendence of Companies; Logística S.A.S. shall incorporate the guidelines of the Superintendence of Transportation; and Agencia de Aduanas ML S.A.S. Nivel 1 and Magnum Zona Franca S.A.S. shall apply the PTEE as part of the comprehensive compliance model and good corporate practice, without prejudice to any legal, regulatory, or supervisory obligations that may apply to them.

For the purposes of this PTEE, when reference is made to administrators or persons with management and administrative functions, this shall include, as applicable, legal representatives, managers, directors, and other persons who perform management, administration, or decision-making functions within the Companies.

8.1. Highest Corporate Body or Board of Directors

The highest corporate body or the board of directors, as applicable, shall be responsible for approving, supporting, and monitoring the PTEE, its policies, and the other documents that comprise it.

Its main functions and responsibilities are:

- Issue, define, approve, and update the PTEE Compliance Policies.
- Define the profile of the Compliance Officer, in accordance with the applicable regulations and the needs of the Companies.
- Appoint the main and alternate Compliance Officer, when applicable, in accordance with the applicable regulations and the internal decisions of each company.
- Approve the PTEE, its Procedures Manual, risk matrix, Code of Ethics and Good Governance, procedures, controls, and other documents that form an integral part of the program.
- Assume a commitment aimed at preventing corruption and transnational bribery risks, so that the Companies conduct their business ethically, transparently, and honestly.
- Ensure the provision of the human, technological, financial, and operational resources necessary for the Compliance Officer to properly perform their duties.
- Review and evaluate the reports submitted by the Compliance Officer, Legal Representative, Statutory Auditor, Internal Audit, Integrated Management System, or whoever acts in such capacity.
- Order the preventive, corrective, disciplinary, contractual, or legal actions that may apply when breaches of the PTEE are identified by shareholders, administrators, legal representatives, managers, directors, employees, contractors, or other stakeholders.
- Lead and support a communication and educational strategy that enables the effective disclosure and knowledge of the PTEE and its Compliance Policies.
- Guarantee the existence of appropriate, secure, and confidential channels to report possible breaches of the PTEE, acts of corruption, transnational bribery, or conducts contrary to business ethics.
- Leave record in the corresponding minutes of the decisions related to approval, updating, reports, appointment of the Compliance Officer, allocation of resources, corrective actions, and other relevant PTEE matters.

8.2. Legal Representative

The Legal Representative shall be responsible for supporting the implementation, operation, monitoring, and updating of the PTEE, in coordination with the Compliance Officer and the responsible areas, in accordance with the regulations applicable to each company.

Its main functions and responsibilities are:

- Submit, together with the Compliance Officer, the proposal for the PTEE and its updates for approval by the board of directors or the highest corporate body, when applicable.
- Ensure that the PTEE is articulated with the Compliance Policies adopted by the board of directors or the highest corporate body.
- Provide effective, efficient, and timely support to the Compliance Officer in the design, direction, implementation, supervision, monitoring, and updating of the PTEE.
- Study the results of the corruption and transnational bribery risk assessment carried out by the Compliance Officer and support the definition of the corresponding action plans.
- Ensure that the activities resulting from the development of the PTEE are duly documented, so that the information meets criteria of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality. Documentary supports must be retained in accordance with the applicable regulations and internal document management procedures.
- Promote that employees, managers, directors, contractors, and other stakeholders know and apply the PTEE, its policies, procedures, and reporting channels.
- Certify compliance with the PTEE before the competent authority, when required.
- In cases where there is no board of directors, propose the person who will perform the role of Compliance Officer, for appointment by the highest corporate body, when the applicable regulations so require.

8.3. Compliance Officer

The Compliance Officer shall be the natural person appointed by the competent body to lead, manage, execute, monitor, and verify compliance with the PTEE.

In order to avoid the suspension of program activities, the Companies may appoint an alternate Compliance Officer when the applicable regulations, the competent body, or internal needs so determine.

Its main functions and responsibilities are:

- Submit, together with the Legal Representative, the proposal for the PTEE and its updates for approval by the board of directors or the highest corporate body, when applicable.
- Ensure the effective, efficient, and timely compliance with the PTEE, guaranteeing its proper functioning.
- Ensure that the PTEE is articulated with the Compliance Policies adopted by the board of directors or the highest corporate body.
- Carry out or coordinate the assessment of corruption and transnational bribery risks to which the Companies may be exposed.
- Design, update, implement, and monitor the PTEE, its policies, procedures, controls, and risk matrix.
- Implement and update the risk matrix according to the needs of the Companies, their risk factors, operation, materiality, and level of exposure.
- Define, adopt, and monitor actions and tools for the identification, measurement, control, detection, prevention, and mitigation of corruption and transnational bribery risks.
- Submit reports to the highest corporate body or board of directors at least once a year, or with the frequency required by the applicable regulations. These reports must include the evaluation of the efficiency and effectiveness of the PTEE, the results of the management carried out, identified developments, corrective actions, progress, and improvement recommendations.
- Ensure the performance of audits on the operation of the PTEE at least once a year, when the applicable regulations so require. The audit report must be submitted to the highest corporate body or board of directors, in order to make the adjustments, corrective actions, or improvements that guarantee the effective operation of the program.
- Ensure the update of the PTEE at least every two years, or earlier when relevant changes occur in the operation, regulations, structure, risk factors, controls, or conditions of the program. For this purpose, the Compliance Officer must submit to the highest corporate body or board of directors the proposals and justifications for the corresponding corrective actions, updates, or improvements.
- Ensure the implementation of appropriate channels so that any person may confidentially and securely report possible breaches of the PTEE, acts of corruption, transnational bribery, or conducts contrary to business ethics.
- Verify the application of the whistleblower or reporting person protection and non-retaliation policy.
- Coordinate the review, analysis, or internal investigation of the reports received, in order to detect possible breaches of the PTEE or acts of corruption.
- Coordinate the development of internal training, awareness, and disclosure programs regarding the PTEE.
- Verify compliance with due diligence and enhanced due diligence procedures, when applicable.
- Ensure the proper filing, retention, and traceability of documentary supports and other information related to the management and prevention of corruption and transnational bribery risks.

- Evaluate the reports submitted by Internal Audit, Statutory Audit, Integrated Management System, or whoever acts in such capacity, and propose the corresponding action plans or corrective measures.
- Report to the Transparency Secretariat of the Presidency of the Republic any cases that may be associated with corruption or transnational bribery, when applicable.
- Carry out or manage the Suspicious Transaction Reports – STR before the UIAF, when the corresponding analysis determines that the report is appropriate in accordance with the applicable regulations.
- Certify compliance with the PTEE before the competent authority, when required.

The Compliance Officer may rely on the General Management, Administrative and Financial Management, Human Talent, Legal, Security, Integrated Management Systems, and/or the corresponding areas, according to the nature of the matter.

8.4. Minimum Requirements, Disqualifications, and Incompatibilities of the Compliance Officer

The Compliance Officer must comply with the minimum requirements, disqualifications, and incompatibilities established in the regulations applicable to each company and in the internal decisions of the Companies.

In general terms, the Compliance Officer must comply, as applicable, with the following requirements:

- Be domiciled in Colombia.
- Have the capacity to make decisions related to the management of corruption and transnational bribery risks, have direct communication, and report directly to the board of directors or to the highest corporate body, when there is no board of directors, for matters related to the PTEE.
- Have sufficient knowledge of C/ST or CO/ST risk management and understand the ordinary course of the Companies' activities.
- Accredit education, experience, or training in risk management, when the applicable regulations so require.
- For Logística S.A.S., the Compliance Officer must be a technician, technologist, or professional and must accredit training in risk management through a diploma course of at least ninety (90) hours or a specialization, in accordance with the guidelines of the Superintendence of Transportation.
- Have the necessary human, technical, and operational support, according to the risk level, size, and operation of the Companies.
- Not belong to the administration, corporate bodies, statutory audit, nor act as internal auditor or as whoever performs similar functions or acts in such capacity in the obligated company or in the Company to which the obligation applies.
- Have no background related to fraud, corruption, bribery, or conducts that may affect their suitability for the position.

- Not act as Compliance Officer in entities that represent incompatibility, conflict of interest, or unauthorized competition, in accordance with the applicable regulations.
- Not act as Compliance Officer in more than ten (10) obligated companies, except for the exceptions permitted by the applicable regulations, especially when there is a business group or control situation.
- The SARLAFT Compliance Officer may also perform the functions of PTEE Compliance Officer, provided that they are not subject to disqualifications or incompatibilities and meet the requirements established by the applicable regulations.
- The appointment of the Compliance Officer must be recorded in the minutes of the board of directors or of the highest corporate body, as applicable.
- The corresponding company must certify that the appointed Compliance Officer has the suitability, experience, knowledge, training, and leadership required to manage corruption and transnational bribery risks.
- When the applicable regulations so require, the company must inform the competent authority of the appointment, change, or update of information of the Compliance Officer within the corresponding term, submitting the required data, minutes, résumé, or documents.
- Due to the difference in functions between the Statutory Auditor, the Legal Representative, and the Compliance Officer, the Statutory Auditor or the Legal Representative shall not be appointed as Compliance Officer when there is an incompatibility in accordance with the applicable regulations.

8.5. Statutory Audit

The Statutory Audit, when applicable, shall perform the duties assigned by law, especially those set forth in Article 207 of the Commercial Code and other applicable regulations, as well as those related to the verification of the proper functioning of internal, accounting, and compliance controls related to the PTEE.

In the performance of their duties, the Statutory Auditor shall pay special attention to red flags that may be related to possible acts of corruption, transnational bribery, fraud, suspicious transactions, improper payments, or breaches of the PTEE.

Their main functions and responsibilities are:

- Verify, within the framework of their legal duties, that the accounting and records properly reflect the operations carried out by the Companies.
- Inform the Compliance Officer, Legal Representative, and highest corporate body or board of directors, as applicable, of any inconsistencies, deficiencies, red flags, or weaknesses identified in relation to the operation of the PTEE or the established controls.
- Submit an annual report to the highest corporate body or board of directors and to the Compliance Officer on the inconsistencies or weaknesses detected

regarding the operation of the PTEE or the established controls, when required by the applicable regulations.
- Report to the competent criminal, disciplinary, and administrative authorities any acts of corruption or the alleged commission of crimes detected in the performance of their duties, in accordance with the applicable regulations.
- Inform the corporate bodies and management of the company of any relevant facts identified that may represent risks of corruption, transnational bribery, fraud, or breach of the PTEE.
- Report to the UIAF any suspicious transactions identified in the ordinary course of their duties, when applicable in accordance with the law.
- Request a username and password in SIREL, managed by the UIAF, for the submission of Suspicious Transaction Reports – STR, when applicable.
- Maintain independence, objectivity, confidentiality, and traceability in the performance of their duties.

8.6. Internal Audit

The Integrated Management System area, through the Internal Audit process, shall support the review, monitoring, and improvement of the PTEE, in accordance with the internal procedures defined by the Companies.

The annual internal audit plan shall include, when applicable, the verification of knowledge, application, and compliance with the policies, procedures, controls, and responsibilities established in the PTEE by the employees and responsible areas.

The results of the audits, reviews, or validations carried out shall be documented and communicated to the Legal Representative, the Compliance Officer, and the highest corporate body or board of directors, as applicable, in order to identify developments, weaknesses, improvement opportunities, and define the relevant actions.

The Integrated Management System area, through the Internal Audit process, shall monitor the action plans derived from findings related to the PTEE and support the continuous improvement of the program.

8.7. Managers, Directors, and Other Process Leaders

Managers, directors, and other process leaders are responsible for supporting the implementation of the PTEE in the areas and operations under their responsibility. As persons knowledgeable about their processes, they shall manage and control the risks associated with their activities, with the support of the Compliance Officer and the Integrated Management System, when applicable.

Their main functions and responsibilities are:

- Promote compliance with the PTEE, its policies, and procedures within their work teams.
- Apply the controls defined in the risk matrix and in the documents of the Integrated Management System.
- Participate, when applicable, in the identification, review, and update of risks, controls, and action plans associated with their processes.

- Report to the Compliance Officer any red flag, breach, conflict of interest, unethical conduct, or situation that may represent a risk of corruption or transnational bribery.
- Ensure that decisions, approvals, operations, and actions under their responsibility have sufficient support and traceability.
- Facilitate the participation of their teams in training, audits, reviews, or activities related to the PTEE.
- Support the implementation of corrective, preventive, or improvement actions derived from audits, reports, investigations, or monitoring of the PTEE.
- Report any weaknesses that the PTEE may have and contribute to its continuous improvement.

8.8. Employees

All employees of the Companies are responsible for knowing, complying with, and applying the PTEE, its policies, procedures, controls, and other internal guidelines applicable to them according to their position, duties, and level of risk exposure.

Their main functions and responsibilities are:

- Ensure transparent management in their respective areas and in the Companies in general.
- Know and comply with the PTEE, the Code of Ethics and Good Governance, the Internal Work Regulations, and the policies, instructions, and procedures that form part of the Integrated Management System.
- Act with legality, transparency, honesty, good faith, and respect for corporate principles and values.
- Refrain from participating in acts of corruption, transnational bribery, fraud, improper payments, undeclared conflicts of interest, or any conduct contrary to business ethics.
- Promptly report, through the means defined by the Companies, any unusual transaction, suspicious situation, red flag, breach, conflict of interest, improper request, or conduct contrary to the PTEE.
- Participate in the training, awareness, and activities scheduled by the Companies regarding the PTEE.
- Preserve the traceability and supporting documents of the activities, approvals, and controls under their responsibility.
- Apply the controls defined for their process, especially when related to clients, suppliers, authorities, payments, operations, sensitive information, or critical decisions.
- Respond to information requests made by the Compliance Officer, Internal Audit, Statutory Audit, Management Systems, or the competent body, in the development of the PTEE.
- Report any weaknesses that the PTEE may have and contribute to its improvement.

8.9. Suppliers, Clients, and Other Stakeholders

Suppliers, clients, and other stakeholders shall act in accordance with the law, contracts, applicable internal policies, and the principles of transparency, business ethics, and prevention of corruption.

Their main responsibilities are:

- Know and comply, to the extent applicable to them, with the provisions of the PTEE and the Compliance Policies of the Companies.
- Not carry out and reject any act of fraud, corruption, national bribery, transnational bribery, improper payments, or unauthorized benefits toward the Companies or toward the counterparties with whom they have a relationship.
- Refrain from offering, requesting, giving, or accepting payments, gifts, favors, benefits, or undue advantages.
- Provide clear, complete, truthful, and updated information in onboarding, update, or due diligence processes.
- Promptly report any situation that may represent a conflict of interest, red flag, contractual breach, act of corruption, transnational bribery, or conduct contrary to business ethics.
- Allow, when applicable, the verification of information and supporting documents required by the Companies.
- Comply with contractual clauses, statements, certifications, or commitments related to business ethics, anti-corruption, transnational bribery, and regulatory compliance.

Failure to comply with these obligations may give rise to contractual, commercial, or legal measures, including termination of the relationship, suspension of operations, reporting to competent authorities, or any other measure permitted by law and the applicable contractual documents.

9. STAGES FOR THE MANAGEMENT OF CORRUPTION AND TRANSNATIONAL BRIBERY RISK

The stages of the Transparency and Business Ethics Program – PTEE constitute a systematic, structured, and interrelated process through which the Companies identify, evaluate, control, monitor, and update the corruption and transnational bribery risks to which they may be exposed in the development of their operations.

For the management of these risks, the Companies adopt the methodology defined in P-PE-03 Risk Management Procedure and the comprehensive risk matrix managed in the Integrated Management System – IMS, under the RISICAR method, which allows estimating inherent and residual risk, defining controls, assigning responsible parties, establishing action plans, and monitoring the effectiveness of the implemented measures.

The management of corruption and transnational bribery risk is articulated with strategic planning, the process-based approach, and the comprehensive management model of the Companies. For this purpose, the needs and expectations of stakeholders, legal and complementary requirements, management indicators, organizational structure, process map, services offered, geographic areas of operation, relationships with counterparties, and other elements that may affect the level of risk exposure are taken into account.

Likewise, the risk analysis considers the macro-processes defined in the Integrated Management System: strategic processes, productive or mission-related processes, and support processes, considering that corruption and transnational bribery risks may materialize in any of them, depending on the activities, decisions, controls, third parties involved, and assigned responsibilities.

9.1. Analysis of the Internal and External Context

The analysis of the internal and external context makes it possible to understand the strategic, operational, legal, commercial, geographic, and organizational conditions that may influence the Companies' exposure to corruption and transnational bribery risks.

This analysis may consider, among other aspects:

- The organizational structure and business model of each Company.
- The strategic, productive or mission-related, and support processes.
- The services provided and activities carried out.
- Relationships with clients, suppliers, contractors, employees, shareholders, authorities, and other third parties.
- Geographic areas, jurisdictions, ports, free trade zones, and other places where operations are carried out.
- The regulatory framework applicable to each company.
- Red flags, materialized events, audit findings, investigations, internal reports, or relevant situations.
- Changes in the environment, operations, processes, counterparties, or applicable regulations.

This analysis shall be used as input for the identification, evaluation, treatment, and monitoring of corruption and transnational bribery risks.

9.2. Identification of Corruption and Transnational Bribery Risk

The identification stage is intended to timely recognize situations, events, processes, activities, relationships, or factors that may expose the Companies to corruption and transnational bribery risks.

Risk identification shall be carried out with the participation of process leaders, the Compliance Officer, the Integrated Management System, and the responsible areas, according to the knowledge that each process has of its activities, controls, and possible exposure scenarios.

Each identified risk shall be recorded in the comprehensive risk matrix, indicating at least the risk factor, type of risk, risk situation, generating agent, process where it may materialize, company to which it applies, cause, consequence, existing controls, responsible parties, inherent rating, residual rating, and action or contingency plans, when applicable.

9.2.1. Internal and External Risk Factors to Be Evaluated

During the identification of corruption and transnational bribery risks, the Companies shall consider internal and external factors that may increase their level of exposure, according to the nature of their operations, processes, counterparties, services, geographic areas, and other particular conditions.

The risk factors to be evaluated include:

The operation: Risks derived from internal processes, such as commercial, administrative, logistics, financial, accounting, operational, or investment activities. This includes the review of procedures, controls, human and technological resources, and possible situations that may facilitate acts of corruption or transnational bribery.

Countries or jurisdictions of operation: Risks associated with countries or jurisdictions where the Companies carry out direct or indirect activities, maintain commercial, financial, or contractual relationships, or execute international operations. Factors such as levels of corruption, tax havens, international sanctions, conflicts, institutional weakness, or high-risk jurisdictions shall be considered.

Type of business: Business model, economic activity, or sector in which the Companies operate. Some businesses may present greater exposure due to the nature of their operations, level of regulation, interaction with authorities, use of intermediaries, or contractual complexity.

Goods and/or services offered: Evaluation of whether the services provided by the Companies may be used, directly or indirectly, to conceal improper payments, unauthorized benefits, corrupt practices, or non-transparent business relationships.

Commercialization or relationship channels: Means used to offer services, manage clients, suppliers, contractors, or third parties. Some channels may generate greater exposure when there is less traceability, intermediation, non-face-to-face operations, or dependence on third parties.

Geographic areas where the Companies operate: Regions, cities, ports, free trade zones, logistics corridors, or places where the Companies have a physical, commercial, or operational presence. Variables such as institutional presence, exposure to illicit economies, corruption, smuggling, conflict, or risks inherent to the environment shall be considered.

Counterparties: Natural or legal persons with whom the Companies maintain labor, commercial, contractual, or legal relationships, such as clients, suppliers, contractors, shareholders, employees, allies, intermediaries, and other third parties. Their profile, reputation, economic activity, behavior, source of funds, and level of risk exposure are evaluated.

Beneficial owners of counterparties: Natural persons who ultimately own, control, or benefit from a counterparty. Their identification makes it possible to detect complex structures, lack of transparency, possible conflicts of interest, links with PEPs, or exposure to higher-risk jurisdictions.

Third parties and intermediaries: Agents, advisors, managers, representatives, contractors, allies, or any third party acting on behalf of the Companies or participating in their operations. This factor is relevant due to the risk that such third parties may facilitate improper payments, irregular management, or acts of corruption.

Size and structure of the Companies: Level of organizational complexity, volume of operations, number of employees, geographic coverage, available resources, and control capacity.

Legal and corporate nature: Corporate type, corporate purpose, shareholding composition, ownership structure, participation of related or subordinate companies, and other aspects that may affect transparency, effective control, or decision-making.

Specific activities: Activities that, by their nature, may generate greater exposure to corruption or transnational bribery risks, such as relationships with authorities, procedures, permits, inspections, government contracting, international operations, intermediation, or handling of sensitive payments.

Economic sectors: Sectors to which the Companies or their counterparties belong. Some sectors may represent greater risk due to their level of regulation, interaction with public entities, exposure to foreign trade, transportation, logistics, infrastructure, government contracting, or cross-border operations.

These factors shall be considered in the comprehensive risk matrix, in accordance with the methodology defined by the Companies in the Integrated Management System and in P-PE-03 Risk Management Procedure.

9.3. Description and Recording of the Risk

Each identified risk shall be described clearly, completely, and traceably in the comprehensive risk matrix. For this purpose, at least the following elements shall be documented:

- **Risk situation:** Event or scenario that may generate exposure to corruption or transnational bribery.
- **Generating agent:** Source, person, process, third party, condition, or circumstance that may originate the risk.
- **Area or process where it may materialize:** Internal process or activity in which the risk may arise.
- **Company to which it applies:** Company or companies to which the risk corresponds.
- **Cause:** Condition that allows the existence of the risk or increases its probability of occurrence.
- **Consequence:** Effect that could arise in the event of materialization, including legal, reputational, operational, or contagion impacts.
- **Existing controls:** Measures, procedures, policies, verifications, or tools implemented to prevent, detect, protect against, or correct the risk.
- **Responsible parties:** Areas or positions responsible for managing the risk, applying controls, and following up.
- **Action or contingency plans:** Activities defined to strengthen controls, mitigate the risk, or act in the event of materialization.

9.4. Risk Measurement or Evaluation

The measurement or evaluation stage is intended to determine the probability of occurrence and the impact that could result from the materialization of a corruption or transnational bribery risk.

For these purposes, the Companies shall apply the criteria defined in the risk management methodology and in the comprehensive risk matrix managed in the IMS. The evaluation shall be carried out considering frequency and impact criteria.

Frequency makes it possible to estimate the probability of occurrence of the risk, according to the following ranges:

- **Low:** Once a year.
- **Medium:** Between 2 and 3 times a year.
- **High:** Between 4 and 5 times a year.
- **Very high:** More than 5 times a year.

Impact makes it possible to assess the severity of the consequences in the event of materialization, taking into account the following dimensions:

- **Legal:** Possible fines, sanctions, legal expenses, or compensation.
- **Reputational:** Impact on image, trust, institutional relationships, or third-party perception.
- **Operational:** Suspension, impact, or interruption of operations.
- **Contagion:** Direct or indirect impact on other companies of the group, processes, related third parties, or stakeholders.

The impact rating may be slight, moderate, severe, or catastrophic, according to the ranges defined in the comprehensive risk matrix.

The evaluation shall determine the level of risk at two points:

- **Inherent risk:** The level of risk existing before applying controls, actions, or countermeasures.
- **Residual risk:** The resulting level of risk after applying the controls, actions, or countermeasures defined by the Companies.

The risk rating shall allow classification according to the ranges defined in the comprehensive risk matrix:

- **Acceptable:** 5.
- **Tolerable:** 10, 15, or 20.
- **Serious:** 30, 40, 50, or 60.
- **Unacceptable:** 80, 100, 150, or 200.

The Companies shall also evaluate corruption and transnational bribery risks when they enter new markets, modify their services, establish new relationships with third parties, participate in new operations, identify relevant regulatory changes, or when situations arise that may modify their level of exposure.

9.5. Risk Control and Treatment

Once the level of risk has been determined, the Companies shall define the necessary treatment measures to prevent, detect, protect against, correct, or reduce exposure to corruption and transnational bribery risk.

Treatment measures shall be proportional to the identified level of risk, under the risk-based approach principle: the higher the risk, the greater the control; the lower the risk, simplified measures may be applied, provided they are sufficient and reasonable.

In accordance with the methodology and risk matrix of the IMS, risk treatment strategies may include:

- **Accept the risk:** Assume the risk when it is within the levels permitted by the Companies and does not require additional measures.
- **Avoid the risk:** Eliminate, suspend, or refrain from carrying out the activity, relationship, operation, or situation that generates an unacceptable risk.
- **Transfer the risk:** Fully or partially transfer the risk to a third party, when feasible, for example, through insurance policies, guarantees, contractual clauses, or other permitted mechanisms.
- **Protect the company:** Implement measures aimed at reducing the impact in the event of risk materialization.
- **Prevent the risk:** Implement controls, barriers, procedures, or measures that reduce the probability of occurrence of the risk.
- **Retain losses:** Assume the losses or effects derived from the risk, when so defined according to the level of exposure, response capacity, and internal criteria.

The controls defined to manage risks may be classified, according to their purpose, as follows:

- **Prevention:** They act on the causes of the risk or generating agents, in order to reduce the probability of occurrence.
- **Detection:** They make it possible to identify alerts, irregular situations, or deviations that may indicate the possible materialization of the risk.
- **Protection:** They neutralize or reduce the immediate effect generated by the materialization of the risk, in order to avoid greater material, economic, legal, reputational, or operational losses.
- **Correction:** They allow the correction of deviations, breaches, or failures identified in a process, especially when the risk has materialized or weaknesses in controls have been detected.

Treatment measures shall be mandatory for risks rated as serious or unacceptable. For acceptable or tolerable risks, additional actions may be defined when the context, operation, red flags, or judgment of the process owner so require.

Controls and treatment plans shall be documented in the comprehensive risk matrix and may include, among others, special approvals, accounting controls, documentary supports, segregation of duties, training, and audits.

9.6. Risk Monitoring and Reassessment

The management of corruption and transnational bribery risk is a cyclical and ongoing process. Therefore, the Companies shall periodically monitor the identified risks, implemented controls, materialized events, and defined action plans, in order to verify their effectiveness and keep the PTEE updated.

Monitoring shall include, among other aspects:

- Verifying compliance with the defined action plans.
- Reviewing risks that have materialized and the actions taken for their treatment.
- Evaluating the effectiveness of existing controls and implemented action plans.
- Identifying whether it was necessary to implement new, different, or additional controls to mitigate the risk.
- Identifying deviations, weaknesses, or improvement opportunities.
- Reviewing responsible parties, dates, progress, and supporting documents of the defined actions.
- Detecting new risks or changes in existing risks.
- Comparing inherent risk against residual risk.
- Verifying that residual risk remains within the levels accepted by the Companies.

Risk reassessment may be carried out ordinarily within the periodic review of the matrix, or extraordinarily when relevant changes occur in the operation, structure, processes, regulations, counterparties, beneficial owners, geographic areas, markets, services, channels, red flags, audit findings, materialized events, or when it is evidenced that existing controls are not sufficient.

Monitoring and reassessment shall be carried out at least annually, or whenever the Compliance Officer, process leaders, the Integrated Management System, or Senior Management deem it necessary.

At the annual meeting with the highest corporate body or board of directors, when applicable, the progress of action plans, materialized risks, effectiveness of controls, implemented adjustments, and PTEE improvement opportunities may be reviewed.

9.7. Matrix Update and Continuous Improvement

The comprehensive corruption and transnational bribery risk matrix shall be updated when new risks are identified, events materialize, audit findings arise, processes change, business conditions are modified, applicable regulations are updated, or it is evidenced that existing controls are not sufficient.

Updates may result in adjustments to the PTEE, its policies, procedures, controls, responsible parties, action plans, red flags, training activities, or other related documents.

The Compliance Officer, with the support of process leaders, the Integrated Management System, and the responsible areas, shall promote the review and continuous improvement of the PTEE, ensuring that the management of corruption and transnational bribery risk remains updated, traceable, and consistent with the operational reality of the Companies.

P-PE-03 Risk Management Procedure develops in greater detail the methodology for the identification, assessment, treatment, monitoring, and verification of the effectiveness of the action plans defined by the Companies.

10. DUE DILIGENCE AND COUNTERPARTY KNOWLEDGE PROCEDURES

The Companies apply due diligence and counterparty knowledge procedures as a mechanism to prevent, identify, control, and monitor risks of corruption, transnational bribery, and conducts contrary to business ethics in their commercial, contractual, labor, corporate, or operational relationships.

Due diligence shall be applied before starting a relationship with the counterparty, during its execution, and in update processes, when document expirations, relevant changes, red flags, database findings, changes in the operation, or any situation that may increase the risk level arise.

For these purposes, the Companies have procedures, instructions, forms, matrices, and records managed in the Integrated Management System – IMS, which develop the step-by-step process for onboarding, updating, consultation, rating, monitoring, and filing of counterparty information. This PTEE does not duplicate such documents, but refers to them as operational support for the execution of due diligence.

Due diligence includes, among other aspects, the identification of the counterparty, verification of information, knowledge of its activity, review of supporting documents, database consultation, identification of beneficial owners when applicable, validation of possible Politically Exposed Persons – PEP, risk rating, analysis of red flags, definition of control measures, approval by the competent body, and retention of the corresponding traceability.

10.1. Knowledge of Clients

The onboarding, updating, and monitoring of clients shall be carried out in accordance with the internal documents defined in the IMS, especially:

- F-GC-02 Client Identification Form.
- I-SC-02 Client Selection and Documentation Instructions.
- I-SC-03 Client Database Consultation Instructions.
- I-SC-05 Client Risk Rating Instructions.
- T-SC-01 Client Risk Rating.
- I-PE-01 Instructions for Conducting Security Studies for Clients and Suppliers.

For the onboarding or updating of clients, the commercial areas, customer service areas, or those designated in the regional offices shall request the applicable documentation, manage the completion of the corresponding form, verify that the information is complete, and submit the supporting documents for publication in SOUL, in accordance with the internal procedures.

All onboarded or updated clients must have database validation. The searches shall be carried out on the corresponding legal entity or natural person, legal representatives, alternates, attorneys-in-fact, controlling parties, partners, shareholders, beneficial owners, and any other persons that must be verified according to the information registered in the Chamber of Commerce, Circular 170, or equivalent documents. The searches must be retained and published in SOUL in the field defined for database validation.

The client risk rating shall be carried out in accordance with the matrix defined by the Companies, taking into account criteria such as security certifications, economic solvency analysis, length of commercial relationship, goods involved in the operations, origins, destinations, main domicile, and type of company. According to the result of the rating, the applicable type of due diligence shall be defined.

When the rating result, type of operation, nature of the client, red flags, or service needs require it, a security study or enhanced due diligence shall be conducted by the Compliance and Risk Management area. This analysis may include document review, additional searches, economic solvency analysis, validation of findings, review of the goods or operation, and issuance of a concept or recommendation on the viability of the relationship.

Client documentation must be kept updated in accordance with the terms defined in the internal procedures. If a client does not provide the required information, submits incomplete or expired documentation, or presents relevant inconsistencies, traceability of the management carried out must be kept and the case must be escalated to the competent body to determine whether onboarding, updating, continuity, restriction, veto, or any other applicable measure is appropriate.

10.2. Knowledge of Suppliers, Contractors, and Third Parties

The onboarding, updating, and monitoring of suppliers, contractors, and third parties shall be carried out in accordance with the purchasing procedures, database consultation, risk rating, and other documents defined in the IMS.

For these purposes, the following internal documents shall be used, among others:

- F-CP-01 Supplier Selection Form.
- P-CP-01 Purchasing Procedure.
- I-CP-04 Database Consultation Instructions for Suppliers.
- I-CP-07 Supplier Risk Rating Instructions.
- T-CP-02 Risk Rating Matrix for Operational and Administrative Suppliers.
- I-PE-01 Instructions for Conducting Security Studies for Clients and Suppliers.

Suppliers, contractors, and third parties must provide complete, truthful, clear, and updated information for their onboarding or updating. The information must allow the Companies to know the identity of the counterparty, its activity, representatives, beneficial owners when applicable, contracting conditions, level of criticality, relationship with the operation, and other aspects necessary to evaluate its risk exposure.

All suppliers that are onboarded or updated must have database validation. The searches must be consolidated into a supporting file and published in the field defined for database validation, in accordance with the applicable instructions.

The supplier risk rating shall be carried out in accordance with the matrix defined by the Companies, taking into account criteria such as access to cargo, access to documentation or confidential information, possibility of document falsification, access to facilities, supplier dependency, and security certifications. According to the result, the supplier may be classified as non-critical, moderately critical, or critical, which will allow the Companies to define the applicable type of due diligence or controls.

During the relationship with suppliers, evaluations or re-evaluations may be carried out, taking into account findings, breaches, service quality, timeliness, security, price, attention, occupational health and safety requirements, environmental requirements, contractual requirements, or any other situation that may affect the operation or represent a risk for the Companies.

When the supplier, contractor, or third party presents red flags, relevant search results, high criticality, relationship with sensitive activities, access to information or critical assets, interaction with authorities, or any condition that increases the risk, enhanced due diligence may be applied or a security study may be requested, leaving the corresponding traceability and approval.

10.3. Knowledge of Drivers, Owners, Holders of Outsourced Vehicles

For operations involving land cargo transportation, the Companies shall apply the procedures defined for the selection, approval, updating, and monitoring of drivers, owners, holders, and outsourced vehicles.

For these purposes, the following internal documents shall be used, among others:

- P-TT-04 Selection, Approval, and Updating of Résumés of Drivers and Outsourced Vehicles.
- I-TT-02 Instructions for Conducting Security Studies for Drivers and Owners.

The information of drivers, owners, holders, and vehicles must be submitted by the areas responsible for the operation, clearly and completely, for the corresponding validations

to be carried out. These shall include searches in public or private databases, background checks, validations in RUNT and RNDC, review of vehicle documents, and other controls defined by Security.

The Head of Security shall be responsible for controlling compliance with the procedure and approving or rejecting the onboarding when findings are identified. When necessary, the case may be analyzed jointly with the Compliance and Risk Management Department and the Land Transportation Department.

The searches, supporting documents, results, and decisions must be kept in the repositories defined by the Companies, guaranteeing traceability, availability, and control of the information.

10.4. Knowledge of Employees and Critical Positions

The onboarding, evaluation, and monitoring of employees shall be carried out in accordance with P-TH-01 Human Talent Procedure, which applies from the personnel request to the termination of the corresponding contract or relationship.

During the selection process, depending on the position and the stage of the process, background validations, interviews, technical tests, values tests, competency tests, document verifications, candidate authorizations, experience analysis, suitability evaluations, and other controls defined by Human Talent may be carried out.

Within the selection process, the Companies carry out background pre-validations in sources such as the Office of the Inspector General, Police, Interpol, UN, legal proceedings, OFAC, SIMIT, RUNT, and any other applicable databases or sources. Likewise, the corresponding authorization is requested from the candidate to continue with the process.

The Companies have the T-TH-04 Position Risk Rating Matrix and the I-TH-30 Position Risk Rating Instructions, through which the criticality levels of positions are identified, according to criteria such as access to cargo, access to documentation or confidential information, personnel under supervision, involvement in key company decisions, and handling of money or financial information.

Each time a new position is created, the corresponding rating must be carried out to identify its level of criticality. Likewise, the Compliance and Human Talent areas shall review the position risk rating matrix at least once a year, in order to validate that the positions are correctly classified, active, and adjusted to the reality of their functions.

According to the level of criticality of the position, additional controls may be applied, such as security tests, alcohol and substance testing, socioeconomic studies, follow-up visits, reliability analysis, or other measures defined by the Companies, always respecting the applicable labor regulations and internal procedures.

10.5. Knowledge of Partners or Shareholders

When a new partner or shareholder is intended to be onboarded, the controls defined by the Companies must be applied in order to know their identity, background, source of funds, beneficial owners, possible conflicts of interest, red flags, and other relevant aspects.

This process shall be carried out in accordance with OD-PE-07 Corporate Policy and any other applicable internal documents.

10.6. Identification of Beneficial Owners

The Companies shall adopt reasonable measures to identify the beneficial owners of counterparties, especially in the case of legal entities, complex corporate structures, partners, shareholders, clients, suppliers, contractors, or third parties that may represent greater risk exposure.

The identification of beneficial owners will make it possible to know the natural persons who ultimately own, control, or benefit from a counterparty, as well as to detect possible opaque structures, lack of transparency, conflicts of interest, links with PEPs, risk jurisdictions, or red flags.

When it is not possible to obtain sufficient information on beneficial owners, or when the counterparty refuses to provide it without a valid justification, the case must be analyzed by the Compliance Officer in order to define whether it is appropriate to continue, condition, suspend, or reject the relationship.

10.7. Identification and Treatment of Politically Exposed Persons – PEP

In onboarding, updating, monitoring, or enhanced due diligence processes, the Companies must identify whether the counterparty, its representatives, shareholders, partners, beneficial owners, or relevant third parties have the status of Politically Exposed Person – PEP, or whether they have a relevant relationship with a PEP.

When a PEP status or a relevant relationship with a PEP is identified, an enhanced analysis of the case must be carried out, considering the type of relationship, public position or function, level of exposure, possible conflict of interest, interaction with the Companies, red flags, jurisdiction, economic activity, and other factors that may affect the risk.

The identification of a PEP does not necessarily imply rejection of the relationship; however, it shall require analysis, traceability, and approval by the General Management, in accordance with the internal procedures.

10.8. Enhanced Due Diligence

Enhanced due diligence consists of applying additional and more in-depth measures for the knowledge of a counterparty when, due to its profile, operation, risk level, red flags, or search results, an enhanced analysis is required before starting, continuing, or updating a commercial, contractual, labor, corporate, or operational relationship.

This due diligence may be applied, among other cases, when the counterparty is classified as higher risk, presents relevant database results, has PEP status or a relevant relationship with a PEP, documentary inconsistencies are identified, refuses to provide information, has reputational background, has complex corporate structures, is related to high-risk jurisdictions or non-cooperative countries, has exposure to virtual assets, or red flags are evidenced that may increase the risk of corruption, transnational bribery, or conducts contrary to business ethics.

Enhanced due diligence may include an expanded review of documentation, additional searches in public or private sources, analysis of beneficial owners, background validation, news review, economic solvency analysis when applicable, verification of economic activity, source of funds, request for clarifications, certifications, additional supporting documents, concept from the Compliance area, and approval by the competent body.

When PEP status is confirmed, the operation involves non-cooperative countries or high-risk jurisdictions, there is relevant management or exposure to virtual assets, or a material red flag is identified, the onboarding, continuity, negotiation, or contracting must have analysis by the Compliance Officer and prior approval from the General Management or the competent body, as applicable.

In the case of clients and suppliers, security studies shall be carried out in accordance with I-PE-01 Instructions for Conducting Security Studies for Clients and Suppliers and other applicable documents of the Integrated Management System. These studies allow the documentation of the review of supporting documents, documentary findings, database searches, financial analysis when applicable, information on the operation, concept or recommendation, and final conclusion.

All actions, analyses, searches, supporting documents, approvals, and decisions derived from enhanced due diligence must be documented in the systems or repositories defined by the Companies, guaranteeing traceability, confidentiality, integrity, and availability of the information.

10.9. Technological Tools and Traceability

The Companies shall use the authorized technological tools, internal systems, and repositories to support the onboarding, updating, consultation, rating, monitoring, filing, and traceability processes of due diligence and enhanced due diligence.

The SOUL system shall be used as the official documentary repository for the publication, consultation, and retention of documents, records, supporting documents, validations, matrices, studies, concepts, and other evidence related to the knowledge of clients, suppliers, contractors, and other counterparties, in accordance with the applicable internal procedures.

The Compliance platform or the tools that replace it may be used to carry out individual or massive searches in binding lists, restrictive lists, public and private databases, and other sources defined by the Companies. When a search cannot be carried out through the corresponding platform, it must be performed manually and the respective support must be retained.

In the case of drivers, owners, holders, and outsourced vehicles, the searches, supporting documents, and results may be kept in the repositories defined by the responsible area, guaranteeing traceability, availability, and control of the information.

The information obtained during due diligence processes must be retained in a complete, available, secure, traceable, and confidential manner, in accordance with the internal procedures for document management, record control, information security, and personal data protection.

10.10. Decisions Regarding Findings or Red Flags

When inconsistencies, red flags, incomplete information, expired documentation, refusal to provide information, relevant database results, links with PEPs, possible conflicts of interest, reputational background, financial findings, or any situation that may increase the risk level are identified during due diligence, updating, monitoring, or security studies, the case must be analyzed by the Compliance Officer or by the competent body, as applicable.

According to the nature and seriousness of the finding, the Companies may adopt measures such as requesting additional information, applying enhanced due diligence, conditioning the relationship, suspending the onboarding, rejecting the counterparty, blocking or vetoing the third party, requiring approval from the General Management, carrying out special monitoring, internally reporting the situation, or adopting any other measure permitted by law and internal procedures.

When confirmed matches are identified in binding and restrictive lists, main control lists, including especially the lists of the United Nations Security Council – UN, applicable in Colombia by legal mandate; the lists of the United States of America related to terrorists, terrorist organizations, and sanctions, including OFAC; and the lists of the European Union on organizations and persons classified as terrorists, the Companies shall not initiate or continue any commercial, contractual, labor, or operational relationship with

such third party. In these cases, traceability of the analysis carried out must be kept, possible homonymies must be ruled out when applicable, and the action must proceed in accordance with the applicable regulatory framework and internal procedures.

Likewise, when confirmed, current, or materially relevant findings related to corruption, national or transnational bribery, fraud, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, crimes against public administration, economic crimes, or related conducts are identified, the onboarding or continuity of the relationship must be suspended until the case is analyzed by the Compliance Officer and defined by the General Management or the competent body. If the finding represents an unacceptable risk for the Companies, the relationship with the counterparty shall not be initiated or continued.

When the identified finding does not represent a material risk, corresponds to a homonymy, requires clarification, or does not imply a restriction for the onboarding or continuity of the relationship, the case must be analyzed and documented, leaving the corresponding justification, supporting documents, and approval when applicable.

All actions, analyses, communications, decisions, approvals, concepts, and supporting documents must be duly documented, in order to evidence the proper and timely diligence of the Companies.

11. RED FLAGS

Red flags are facts, situations, behaviors, operations, documents, amounts, indicators, background information, or any other information that deviates from what the Companies consider normal within their processes, operations, or relationships with counterparties, and that may indicate the possible existence of risks of corruption, transnational bribery, fraud, improper payments, conflicts of interest, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, or other conducts contrary to business ethics.

The red flags described in this section apply to Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, Logística S.A.S., and Magnum Zona Franca S.A.S., according to the nature of their operations, processes, services, counterparties, and level of risk exposure. Some red flags may arise across all Companies, while others shall apply depending on the specific activity of each company, such as logistics, customs, land transportation, free trade zone, foreign trade, administrative, financial, or contractual management.

Red flags do not, by themselves, constitute proof of improper conduct; however, they must be timely analyzed by the Compliance Officer or the competent body, in order to determine whether it is necessary to request additional information, apply enhanced due

diligence, suspend or reject a relationship, adopt additional controls, make internal or external reports, or take any other measure defined by the Companies.

Any employee, contractor, supplier, client, ally, or stakeholder who identifies a red flag must report it through the channels defined by the Companies. The report must be managed with confidentiality, traceability, and without retaliation against the person who reports it in good faith.

11.1. Red Flags in Accounting Records, Financial Operations, and Supporting Documents

The following, among others, are considered red flags:

- Invoices that appear to be false, do not reflect the reality of a transaction, are inflated, or contain unusual discounts, reimbursements, or concepts.
- Operations that do not have a logical, economic, commercial, or practical explanation.
- Operations that fall outside the ordinary course of business or are not related to the activity of the counterparty.
- Operations in which the identity of the parties, the origin, or the destination of the funds is not clear.
- Goods, rights, services, or expenses recorded in the accounting records that do not have a real value, do not exist, or cannot be verified.
- Payments, advances, reimbursements, commissions, fees, or expenses without sufficient support, with inconsistent supporting documents, or with generic descriptions.
- Requests to modify dates, values, concepts, descriptions, or supporting documents so that they do not reflect the reality of the service or operation.
- Requests to make payments to third-party accounts that do not have a clear relationship with the operation.
- Requests to split payments, invoices, contracts, or operations without a reasonable commercial, operational, or accounting justification.
- Use of cash, virtual assets, crypto-assets, or non-traditional payment mechanisms without justification, traceability, or the corresponding approval.
- Transfers of funds to countries considered tax havens, non-cooperative countries, or high-risk jurisdictions, without sufficient justification.

11.2. Red Flags in Corporate Structure, Corporate Purpose, and Beneficial Owners

The following, among others, are considered red flags:

- Complex legal structures, whether national or international, without apparent commercial, legal, or tax benefits.

- Legal entities with structures that make it difficult to identify partners, shareholders, controlling parties, or beneficial owners.
- Legal entities with structures abroad or similar vehicles that make it difficult to know their ownership, control, or purpose, without a clear justification.
- Non-operating or shell companies, or companies that reasonably do not fulfill a real commercial purpose.
- Companies declared as fictitious suppliers by the DIAN.
- Legal entities for which it is not possible to identify the beneficial owner.
- Frequent or unjustified changes in shareholders, legal representatives, domicile, corporate purpose, or ownership structure.
- Unjustified refusal to provide information on shareholding composition, beneficial owners, source of funds, or compliance systems.
- Counterparties with corporate structures involving non-cooperative countries, high-risk jurisdictions, or areas with low transparency.

11.3. Red Flags in Contracts, Negotiations, and Relationships with Counterparties

The following, among others, are considered red flags:

- Frequent or unjustified use of consulting, intermediation, representation, agency, business collaboration, joint venture, or similar contracts.
- Contracts with contractors, intermediaries, or public entities that do not reflect clear duties, obligations, scope, deliverables, or conditions.
- Contracts with contractors that provide services to a single client without reasonable justification.
- Losses, profits, discounts, benefits, or significant changes without commercial justification.
- Contracts that include unreasonable variable remuneration, cash payments, payments in kind, virtual assets, or unauthorized benefits.
- Payments to related parties, employees, associates, related or subordinate companies without apparent justification.
- Requests to generate, modify, conceal, or alter invoices, certifications, supporting documents, contracts, or any document related to the operation.
- Third parties or intermediaries that intend to represent a counterparty without sufficient power of attorney, authorization, contract, or support.
- Clients, suppliers, contractors, or third parties that intend to start operations without completing the onboarding, updating, document validation, or internal approval process.
- A counterparty refusing to provide information or documentation required for onboarding, updating, or due diligence.
- Submission of false, altered, incomplete, expired, inconsistent, or difficult-to-verify documentation.
- The counterparty using intermediaries to carry out transactions without justification.

- The counterparty avoiding visits, validations, audits, or verifications without valid justification.
- Operations carried out that are not consistent with the counterparty's economic activity, financial capacity, experience, infrastructure, or personnel.
- The third party lacking personnel, physical facilities, verifiable operations, or sufficient means to provide the service offered.
- Critical suppliers with repeated breaches, relevant findings, resistance to evaluations, or refusal to correct identified findings.
- Matches in binding, restrictive, or control lists involving the counterparty, its representatives, partners, shareholders, beneficial owners, administrators, or related parties.

11.4. Red Flags Related to Authorities, Public Officials, and PEPs

The following, among others, are considered red flags:

- Knowledge or suspicion of a family, personal, economic, or commercial relationship between an employee, contractor, or third party and a public official who may intervene in decisions related to the Companies.
- Counterparties that have relationships with public officials, authorities, state entities, or PEPs and do not report them in a timely manner.
- Proceedings before authorities carried out by third parties without authorization, traceability, or justification.
- Requests to expedite procedures, obtain permits, avoid controls, modify decisions, or influence actions by authorities through improper payments or benefits.
- Participation of PEPs or persons related to PEPs without proper identification, analysis, and the corresponding approval.
- Payments, gifts, courtesies, favors, travel, lodging, donations, sponsorships, contributions, or benefits directed to public officials, authorities, PEPs, or related persons, without justification, support, or approval.

11.5. Red Flags in Gifts, Courtesies, Donations, Sponsorships, Contributions, and Benefits

The following, among others, are considered red flags:

- Unusual, frequent, or unjustified requests for political contributions, donations, sponsorships, or charitable support.
- Offering or receiving gifts, courtesies, travel, dinners, lodging, entertainment, or benefits during negotiation, contracting, audit, inspection, procedure, claim, or sensitive decision-making processes.

- Donations, sponsorships, or contributions without a clear purpose, without a verifiable beneficiary, without approval, or without sufficient support.
- Benefits offered or received for the purpose of influencing a decision, obtaining an advantage, retaining business, or expediting a procedure.
- Payments, gifts, or courtesies requested by intermediaries or third parties on behalf of authorities, clients, suppliers, or contractors.
- Offering or receiving benefits that may affect the independence, objectivity, or transparency of a decision.

11.6. Red Flags Specific to Operations

The following, among others, are considered red flags:

- Foreign trade operations in which the information on the goods, origin, destination, value, supporting documents, or parties involved is not clear, consistent, or verifiable.
- Clients, suppliers, drivers, owners, holders, or vehicles with documentary inconsistencies, relevant background information, unverifiable information, or refusal to provide data required for the security study.
- Operations involving goods, routes, origins, destinations, values, or conditions that are not consistent with the profile of the client, supplier, or third party.
- Counterparties that request that their identity, the identity of the beneficial owner, the intermediary, or third parties related to the operation be kept confidential.
- Public information linking the counterparty, its representatives, partners, shareholders, beneficial owners, or related parties to corruption, fraud, bribery, transnational bribery, money laundering, terrorist financing, crimes against public administration, economic crimes, or other related crimes.
- Business associates that appear on control lists reviewed by the Companies or have background information related to links with illicit activities.

11.7. Management of Red Flags

When a red flag is identified, the case must be reported to the Compliance Officer or to the competent body, as applicable, for analysis and treatment.

According to the nature of the red flag, the Companies may request additional information, apply enhanced due diligence, carry out complementary searches, suspend the onboarding or continuity of the relationship, reject the counterparty, block or veto the third party, require approval from the General Management, implement additional controls, initiate an internal review, activate the disciplinary procedure, make internal or external reports, or adopt any other measure permitted by law and internal procedures.

When a match is confirmed in binding, restrictive, or main control lists, including especially the lists of the United Nations Security Council – UN, applicable in Colombia

by legal mandate; the lists of the United States of America related to terrorists, terrorist organizations, and sanctions, including OFAC; and the lists of the European Union on organizations and persons classified as terrorists, the Companies shall not initiate or continue any commercial, contractual, labor, or operational relationship with such third party. In these cases, traceability of the analysis carried out must be kept, possible homonymies must be ruled out when applicable, and the action must proceed in accordance with the applicable regulatory framework and internal procedures.

When the red flag, after the corresponding analysis, allows the possible existence of a suspicious transaction, an act of corruption, transnational bribery, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, or another reportable conduct to be inferred, the Compliance Officer must file the reports with the UIAF and/or other competent authorities, when applicable, in accordance with current regulations and internal procedures.

When confirmed, current, or materially relevant findings related to corruption, national or transnational bribery, fraud, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, crimes against public administration, economic crimes, or related conducts are identified, the onboarding or continuity of the relationship must be suspended until the case is analyzed by the Compliance Officer and defined by the General Management or the competent body. If the finding represents an unacceptable risk for the Companies, the relationship with the counterparty must not be initiated or continued.

When the identified finding does not represent a material risk, corresponds to a homonymy, requires clarification, or does not imply a restriction for the onboarding or continuity of the relationship, the case must be analyzed and documented, leaving the corresponding justification, supporting documents, and approval when applicable.

All red flags, analyses, supporting documents, decisions, approvals, reports, and actions adopted must be duly documented, in order to evidence the management carried out and strengthen the continuous improvement of the PTEE.

12. INTERNAL AND EXTERNAL REPORTS

The Companies have mechanisms to receive, analyze, and manage internal and external reports related to red flags, suspicious activities, complaints, materialized events, breaches of the PTEE, conflicts of interest, acts of corruption, transnational bribery, fraud, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, or other conducts contrary to business ethics.

Reports are managed with confidentiality, reserve, timeliness, and traceability. When a report is made in good faith, the Companies guarantee the protection of the reporting person and prohibit any act of retaliation, intimidation, unjustified sanction, or unfavorable treatment derived from the report made.

12.1. Internal and External Reporting Channels

The Companies have channels through which employees, managers, directors, process leaders, contractors, suppliers, clients, allies, counterparties, and other stakeholders may report, openly, confidentially, or anonymously, possible violations of the PTEE, corporate policies, internal procedures, or any irregular conduct.

For these purposes, the Companies have I-RF-03 Instructions for Reporting Suspicious Activities and Incentive Program, applicable to Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, Magnum Zona Franca S.A.S., and Logística S.A.S., through which mechanisms are established, such as the virtual security mailbox, physical security mailboxes at the offices or warehouses where applicable, the email address cumplimiento@magnum.com.co, and direct communication channels with the General Management, Administrative and Financial Management, Management System Department, and/or Compliance Officer.

The current virtual security mailbox is:

https://forms.office.com/Pages/ResponsePage.aspx?id=EQrzs7i81U6B8DXQ6y3NdlIckVjyP55Pu3wOGAGCzNRUMzZQNUlTR0U4S0hQVTI5OVdZUUhQNkJYSi4u

Reports made through the virtual security mailbox generate an alert to the Compliance Officer, who reviews the case and, when applicable, analyzes it with the competent bodies to define the applicable actions. Physical mailboxes, when they exist, are reviewed according to the frequency and responsible parties defined in the internal instructions.

12.2. Reporting of Employees Contacted for Illicit Purposes

The Companies have AN-TH-11 Security Protocol for Employees Contacted for Illicit Purposes, through which guidelines are established to report situations in which an employee is contacted, approached, or required by internal or external persons to participate in illicit acts, provide reserved information, reveal internal functions, facilitate improper operations, or provide information related to the Companies' businesses, clients, operations, goods, routes, processes, or controls.

These reports are made immediately to the direct supervisor, Regional Management, General Management, Administrative and Financial Management, Management System Department, or Compliance Officer, through email, telephone call, direct communication, virtual security mailbox, physical mailbox, or any other channel defined by the Companies.

Abnormal actions by employees, coworkers, third parties, or external persons are also reported, such as unjustified requests for information, strange calls or visits, unusual interest in knowing internal functions, businesses, operations, or any situation that may represent a risk for the Companies.

12.3. Analysis and Management of Reports

The reports received are analyzed by the Compliance Officer or by the competent body, according to the nature of the case. When necessary, the analysis is carried out with the General Management, Administrative and Financial Management, Management System Department, Human Talent Department, Regional Management, responsible areas, or any other persons considered necessary for the proper management of the case.

According to the analysis carried out, the Companies may request additional information, apply enhanced due diligence, suspend or condition a relationship, block or veto a counterparty, activate security protocols, execute contingency plans, initiate internal investigations, apply disciplinary measures, file reports with authorities, or implement corrective, preventive, or improvement actions.

All actions, analyses, communications, decisions, supporting documents, and measures adopted shall be documented.

12.4. Compliance Officer's Management Report

The Compliance Officer shall submit a PTEE management report to the highest corporate body or board of directors, as applicable, at least once a year or with the frequency required by the applicable regulations.

This report shall include, as applicable, the management carried out, results of risk monitoring, update of the risk matrix, controls and action plans, relevant red flags or reports, due diligence results, matches in lists, materialized risks, training sessions, audits, status of action plans, reports to authorities, recommendations, and the need to update the PTEE.

When applicable, the Compliance Officer's management report shall be attached to the financial statements or to the documents that must be submitted to the competent authority.

The decisions, recommendations, or instructions derived from the report shall be documented in the corresponding minutes.

12.5. Reports to Authorities and Confidentiality of Information

When, from the analysis of a red flag, complaint, operation, counterparty, event, or situation received through any of the channels defined by the Companies, the possible existence of a suspicious transaction, act of corruption, transnational bribery, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, or other reportable conduct is determined, the Compliance Officer shall file the corresponding reports with the UIAF and/or the other competent authorities, when applicable.

Reports to authorities are not made automatically for every red flag; they are made when, based on the analysis performed, it is determined that the report is appropriate in accordance with the law, internal procedures, and the judgment of the Compliance Officer.

Regarding the UIAF, when the existence of a suspicious transaction or activity is determined, the Compliance Officer shall file the corresponding report through SIREL, in accordance with I-RF-03 Instructions for Reporting Suspicious Activities and Incentive Program and other applicable internal procedures.

For companies obligated under the regime of the Superintendence of Companies, the applicable reports, management reports, certifications, or requirements shall be addressed, including Report 75 – SAGRILAFT and PTEE, or any report that amends, replaces, or serves the same purpose, when applicable.

For Logística S.A.S., when the analysis performed identifies acts that may be associated with corruption and/or transnational bribery in the ordinary course of its businesses or activities, the Compliance Officer shall file the corresponding reports with the UIAF, the Transparency Secretariat of the Presidency of the Republic, and/or the Superintendence of Companies, according to the nature of the case, in accordance with the guidelines of the Superintendence of Transportation, the instructions of each authority, the applicable regulations, and internal procedures.

In cases where the existence of a suspicious transaction associated with corruption and/or transnational bribery is determined, the report shall be filed with the UIAF through SIREL. In the case of acts that may be associated with corruption and/or transnational bribery, the channels defined by the Transparency Secretariat of the Presidency of the Republic shall be used, and, when the matter corresponds to alleged transnational bribery, by the Superintendence of Companies.

Agencia de Aduanas ML S.A.S. Nivel 1 and Magnum Zona Franca S.A.S. shall address the reports or requirements that may be applicable according to their activity, supervisory authority, legal obligations, and the comprehensive compliance model adopted by the Companies.

When it is necessary to provide information to authorities, certification bodies, clients, suppliers, the media, or other stakeholders, the General Management shall define the corresponding instructions and the person authorized to make the communication, in accordance with internal procedures.

Information related to reports to the UIAF, suspicious transactions, complaints, internal investigations, reports of employees contacted for illicit purposes, or requests from authorities shall be confidential and may only be known by authorized persons.

Under no circumstances shall the counterparty involved be informed about reports filed with authorities, when such communication is prohibited or may affect the reserve, confidentiality, investigation, or management of the case.

The retention, custody, and filing of supporting documents related to internal reports, external reports, and reports to authorities shall be carried out in accordance with the Document and Record Retention section of the PTEE and the applicable internal procedures.

13. DOCUMENT AND RECORD RETENTION OF THE PTEE

Magnum Logistics S.A.S., Agencia de Aduanas ML S.A.S. Nivel 1, Magnum Zona Franca S.A.S., and Logística S.A.S. shall retain, in physical or digital form, the documents, records, and supporting documentation related to the Transparency and Business Ethics Program – PTEE, for a period of ten (10) years, in accordance with the provisions of Article 28 of Law 962 of 2005, or any regulation that amends or replaces it.

The custody of documents and records shall be the responsibility of the areas in charge of the corresponding processes, in accordance with what is defined in the record control of each procedure and in the internal document management guidelines. These areas shall guarantee the integrity, timeliness, reliability, confidentiality, availability, and traceability of the information under their responsibility.

The information provided by counterparties in due diligence and enhanced due diligence processes, as well as the supporting documents for verification, analysis, searches, approvals, and decisions adopted, must be duly documented, with date, responsible party, and sufficient evidence to prove the proper and timely diligence of the Companies.

The Compliance Officer shall be responsible for the custody of the information and supporting documents related to Suspicious Transaction Reports, reports to competent authorities, analysis of red flags, complaints, internal investigations, or actions associated with the PTEE, when applicable. This information shall be confidential and, under no circumstances, shall counterparties have access to or knowledge of such supporting documents when such confidentiality is required by law, internal procedures, or the nature of the report.

14. DISCLOSURE, TRAINING, AND UPDATE OF THE PTEE

The Companies have disclosure, training, and communication mechanisms to make known the Transparency and Business Ethics Program – PTEE, its policies, procedures, reporting channels, and applicable responsibilities.

For employees, the PTEE is disclosed from the corporate induction process and reinforced through annual training and communications sent by email.

The Program, its policies, procedures, instructions, forms, protocols, matrices, and other related documents are published in the Integrated Management System – IMS, located in SOUL, in the route defined for consultation: Document Administration and Consultation / Strategic Planning / Procedures and Programs. This information is available for consultation by the personnel of the Companies.

For clients and suppliers, the Companies disclose relevant information about the PTEE through the corporate website and communications sent by email. Additionally, the onboarding forms include a statement through which the counterparty declares that it knows and accepts compliance with the PTEE and the anti-corruption policies of the Companies.

The Companies shall retain evidence of the training sessions, communications, and disclosures carried out, in accordance with the applicable internal procedures.

The PTEE, its policies, procedures, protocols, instructions, forms, matrices, and other related documents shall be updated when regulatory changes, modifications in the activity, structure, processes, operations, risks, controls, or any situation that may affect the level of exposure to corruption, transnational bribery, or related conduct risks arise. In any case, the Program shall be reviewed and updated at least every two (2) years, in accordance with the applicable provisions of the Superintendence of Companies and the Superintendence of Transportation.

15. POLICIES, PROCEDURES, INSTRUCTIONS, AND RELATED DOCUMENTS

The Transparency and Business Ethics Program – PTEE is articulated with the policies, procedures, instructions, forms, matrices, protocols, and other internal documents that are part of the Integrated Management System – IMS of the Companies.

These documents shall be applied as applicable, according to the company, process, operation, risk, or counterparty involved. The current version shall be the one published and controlled in the IMS, located in SOUL.

The related documents include:

- T-PE-02 Risk Matrix.
- P-PE-03 Risk Management Procedure.
- M-PE-01 Integrated Management System Manual.
- OD-PE-01 Integrated Management System Policy.
- OD-PE-20 Integrated Management Objectives.
- OD-PE-11 Financial Area Policy.
- OD-PE-08 Accounting Area Policy.
- OD-PE-07 Corporate Policy.
- F-GC-02 Client Identification Form.
- I-SC-02 Client Selection and Documentation Instructions.

- I-SC-03 Client Database Consultation Instructions.
- I-SC-05 Client Risk Rating Instructions.
- T-SC-01 Client Risk Rating.
- F-CP-01 Supplier Selection Form.
- P-CP-01 Purchasing Procedure.
- I-CP-04 Supplier Database Consultation Instructions.
- I-CP-06 Supplier Evaluation Instructions.
- I-CP-07 Supplier Risk Rating Instructions.
- T-CP-02 Risk Rating Matrix for Operational and Administrative Suppliers.
- I-RF-03 Instructions for Reporting Suspicious Activities and Incentive Program.
- AN-TH-11 Security Protocol for Employees Contacted for Illicit Purposes.
- I-PE-01 Instructions for Conducting Security Studies for Clients and Suppliers.
- P-TH-01 Human Talent Procedure.
- I-TH-30 Position Risk Rating Instructions.
- T-TH-04 Position Risk Rating Matrix.
- P-TH-03 Disciplinary Process Procedure.
- AN-TH-35 Internal Work Regulations.
- P-TT-04 Selection, Approval, and Update of Résumés of Drivers and Outsourced Vehicles.
- I-TT-02 Instructions for Conducting Security Studies for Drivers and Owners.
- P-PE-08 Self-Control and Comprehensive Risk Management Program for Money Laundering, Terrorist Financing, and Financing of the Proliferation of Weapons of Mass Destruction – SAGRILAFT.
- P-TT-07 SARLAFT Logística S.A.S.

In the event of an update, amendment, or replacement of any of these documents, the current version published in the Integrated Management System – IMS shall apply.

16. SANCTIONS FOR NON-COMPLIANCE WITH THE PTEE

Failure to comply with the Transparency and Business Ethics Program – PTEE, its policies, procedures, instructions, controls, reporting channels, and other internal guidelines may give rise to administrative, disciplinary, contractual, civil, criminal, or regulatory measures, according to the nature of the conduct, the seriousness of the facts, the level of responsibility, and the applicable regulations.

16.1. Administrative Sanctions

Legal entities that engage in acts of transnational bribery, corruption, or conducts subject to sanctions by the competent authorities may be subject to the administrative sanctions provided for in the applicable regulations, including fines, disqualifications, publication of the sanctioning decision, prohibition from receiving incentives or subsidies from the Government, and any other applicable measures.

Failure to comply with the orders, instructions, or obligations related to the PTEE may give rise to the corresponding administrative proceedings and sanctions against the obligated companies, their administrators, legal representatives, statutory auditors, Compliance Officers, or other responsible parties, according to the applicable supervisory authority.

For Logística S.A.S., failure to comply with the guidelines, instructions, or obligations related to the PTEE may give rise to administrative sanctions imposed by the Superintendence of Transportation, in accordance with the applicable regulations, without prejudice to any administrative, civil, criminal, or disciplinary actions that may be carried out by other competent authorities.

16.2. Criminal Sanctions

Conducts related to corruption, transnational bribery, bribery, private corruption, fraud, money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, or other crimes may generate criminal liability for the natural persons involved, in accordance with the Colombian Criminal Code and other applicable regulations.

16.3. Internal Sanctions

For employees, failure to comply with the provisions of the PTEE may be considered a disciplinary offense and shall be managed in accordance with the Internal Work Regulations, P-TH-03 Disciplinary Process Procedure, and other applicable labor regulations.

Based on the analysis of the case, the appropriate disciplinary measures may be adopted, guaranteeing due process, confidentiality, and the corresponding traceability.

16.4. Measures Against Third Parties

When the breach is committed by contractors, suppliers, clients, intermediaries, or other third parties related to the Companies, measures may be adopted such as suspension of the relationship, contractual termination, claims for damages, reporting to competent authorities, or any other action permitted by law and the applicable contractual documents.

All investigations, analyses, decisions, adopted measures, and supporting documents related to breaches of the PTEE must be duly documented, guaranteeing traceability, confidentiality, due process, and reserve of information, as applicable.

17. INSTITUTIONAL REPORTING CHANNELS BEFORE AUTHORITIES

Without prejudice to the reporting channels defined by the Companies in this PTEE, employees, clients, suppliers, contractors, allies, counterparties, and other stakeholders may use the institutional channels made available by the competent authorities to report possible acts of corruption, transnational bribery, or other related conducts.

For cases of transnational bribery, the Superintendence of Companies has a reporting channel enabled to bring to its attention facts or situations related to this conduct.

For possible acts of corruption, the Transparency Secretariat of the Presidency of the Republic has the Colombian Anti-Corruption Portal – PACO, as the institutional channel available to report acts of corruption.

The existence of these institutional channels does not replace the internal and external reporting channels defined by the Companies, nor does it exempt employees from timely informing the Compliance Officer or the competent body about red flags, suspicious activities, breaches of the PTEE, or situations that may represent a risk for the Companies.

The electronic addresses of these channels may be consulted on the official websites of the Superintendence of Companies and the Transparency Secretariat of the Presidency of the Republic.

18. APPROVAL, PUBLICATION, AND VALIDITY OF THE PTEE

The Transparency and Business Ethics Program – PTEE shall be approved by the highest corporate body or board of directors, as applicable, according to the nature of each company and the applicable regulations.

Once approved, the PTEE shall be published in the Integrated Management System – IMS, located in SOUL, for consultation by employees and responsible areas. Likewise, the Companies may disclose relevant information about the Program through the corporate website, internal communications, emails, or other means defined for employees, clients, suppliers, and other stakeholders, as deemed appropriate.

This Program shall enter into force as of its approval and publication, and shall be mandatory for employees, managers, directors, process leaders, suppliers, clients, and other counterparties, as applicable.

Any updates, amendments, or replacements of the PTEE must be managed in accordance with the internal document control procedures of the Integrated Management System

and must be approved by the competent body, when required by the applicable regulations or by the internal provisions of the Companies.

The approved PTEE shall replace previous versions of the Program and shall remain in force until it is formally updated, amended, or replaced.