BRAND USE POLICY

The policies detailed below meet the basic guidelines for the correct use and application of Logiztik Alliance Group's brand. These policies must be applied by all those responsible and/or interested in applying the brand or logo of the company in any medium.

Logiztik Alliance Group is a registered trademark, the use and application of the brand or logo must be accepted by the marketing department. The area will determine if you can make use of the brand and period for which it can be used. To obtain this approval of use, you must send a request to marketing@logiztikalliance.com

If the use of the brand is approved, it must be accompanied by the words that indicate the type of relationship Logiztik Alliance has with you.

Additionally, you must commit to making proper use of our image, complying with the corporate visual identity manual. For this reason, each of the pieces that contain our image must be previously sent to marketing@logiztikalliance.com for approval.

For more information and to obtain the corporate visual identity manual, consult marketing@logiztikalliance.com

PERSONAL DATA PROCESSING POLICY

This data processing policy applies to all employees at all levels of the Company, customers, suppliers, contractors, and business partners with whom the Logiztik Alliance Group establishes a working or commercial relationship. It also applies to all databases and personal information files held by Logiztik Alliance Group.

PROCESSING OF PERSONAL INFORMATION

In addition to the processing of the information set out in the Privacy Policy, the following items of personal information processing are established:

1. Administration of Logiztik Alliance Group customers' and suppliers' transactions and information.
2. Additional information that benefits and optimizes the operation and delivery of products and services.
3. Store information associated with requests for products and services that you as a customer consider important to know in order to reaffirm the business relationship.
4. To deal with requests, complaints, or claims.
5. Sending communications related to Logiztik Alliance Group's commercial activities, such as services, products, offers, news, invitations to events, job offers and/or surveys about our products or services.
6. Manipulation of data on the use of products and services for statistical purposes, marketing or data analysis for supply and demand purposes related to Logiztik Alliance Group.
7. Other activities related to the corporate purpose that must necessarily use personal information.

RIGHTS OF THE OWNER

The employee, client, supplier, or business partner may exercise the following rights about the information currently held in the Logiztik Alliance Group databases:

1. To know, update, rectify, and authorize the handling of personal data in relation to Logiztik Alliance Group. This right may be exercised, among others, in the case of partial, inaccurate, incomplete, incomplete, fractioned, misleading data, or data whose processing is expressly prohibited or has not been authorized.

2. Request proof of the authorization granted to Logiztik Alliance Group. Except when expressly exempted as a requirement for the processing.

3. File complaints before the Superintendence of Industry and Commerce for infringements of the provisions of this Law and other regulations that modify, add, or complement it.

4. To revoke the authorization and/or request the deletion of the data when the Processing does not respect the constitutional and legal principles, rights and guarantees. The revocation and/or deletion shall proceed when the Superintendence of Industry and Commerce has determined that the processing of the information has been carried out in a manner contrary to the Law and the Constitution.

5. Access free of charge to their personal data that have been subject to processing.

OBLIGATIONS

Obligations of Logiztik Alliance Group:

1. Registration before the Superintendence of Industry and Commerce, the databases handled by the Company in accordance with the legal requirements.

2. To guarantee to the Data Subject, always, the full and effective exercise of the right of Habeas Data.

3. Request and keep, under the conditions provided for in Law 1581 of 2012, a copy of the respective authorization granted by the Data Subject.

4. Duly inform the Data Subject about the purpose of the collection and the rights to which he/she is entitled by virtue of the authorization granted.

5. Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, use, or unauthorized or fraudulent access.

6. Ensure that the information provided to the Data Processor is truthful, complete, accurate, current, verifiable, and understandable.

7. Update the information, communicating in a timely manner to the Data Processor, all developments with respect to the data previously provided and take other necessary measures to keep the information accurate and reliable.

8. Rectify the information when it is incorrect and communicate the relevant information to the Data Processor.

9. Provide to the Data Processor, as the case may be, only data whose Processing has been previously authorized in accordance with the provisions of this Law.

10. Require the Data Processor at all times to respect the security and privacy conditions of the Data Subject's information.

11. To inform the Data Controller when certain information is under discussion by the Data Subject, once the claim has been filed and the respective process has not been completed.

12. Inform upon request of the Data Subject about the use given to his/her data.

13. Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

- **Duties of the database administrators appointed for the processing of information by the Logiztik Alliance Group:**

14. To guarantee the Data Subject, at all times, the full and effective exercise of the right of habeas data.

15. To keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.

16. To update, rectify or delete data in a timely manner under the terms of this Law.

17. Update the information reported by the data controllers.

18. Process queries and claims made by data subjects under the terms set out in this Law.

19. Insert in the database the legend "information under judicial discussion" once notified by the competent authority about judicial proceedings related to the quality of the personal data.

20. Refrain from circulating information that is being disputed by the Data Subject and whose blocking has been ordered by the Superintendence of Industry and Commerce.

21. Allow access to the information only to those persons who may have access to it, subject to a confidentiality agreement.

22. Inform the Superintendence of Industry and Commerce when there are violations to the security codes and there are risks in the administration of the data subjects' information.

The area responsible for the attention of requests, queries, and claims before which the holder of the information can exercise their rights to know, update, rectify and delete the data and revoke the authorization via email:
col-administrative3@logiztikalliance.com, registered at the following address: Av. El Dorado #106-39, Bogotá - Colombia. Office 305.

AUTHORIZATION

By accepting this Policy, the USER voluntarily, expressly, and informedly authorizes Logiztik Alliance Group to collect, record and process all data and information that the USER voluntarily provides at the time of registration. Based on the above, Logiztik Alliance Group and other persons or companies with whom it contracts such activities, by sending e-mail, text message (SMS and/or MMS) or through any analogous and/or digital means of communication, known or to be known, may reproduce, translate, adapt, extract or compile the data or information

provided, as well as dispose of the data or information for a fee or free of charge in accordance with and under the terms of Law 1581 of 2012 and Decree 1377 of 2013.

COMPREHENSIVE POLICY

Logizitk Alliance Group, a company dedicated to providing air, sea, and land cargo transportation services, establishes as its Comprehensive Policy: ensuring the allocation of technological and human resources necessary to guarantee compliance with the Integrated Management System, the goods and interests of customers and stakeholders, the integrity of processes, and compliance with legal requirements, thus ensuring safety, risk and hazard prevention, and satisfaction of our customers within and outside the country.

Therefore, the Presidency, Vice Presidencies, Management, and Employees of the company commit to:

- Verify compliance with the policy and integrated management objectives.
- Implement an Integrated Management System that effectively addresses any deviation in the provision of services, the safety of employees, and/or illicit activities such as drug trafficking, money laundering, terrorism financing, the proliferation of weapons of mass destruction, corruption, bribery, or any other type of illicit activity that may affect the company's image.
- Promote secure trade by complying with the regulatory and statutory requirements applicable to the integrated management system and its economic activity.
- Allocate the necessary resources to develop, implement, and maintain the Integrated Management System.
- Identify hazards, assess and evaluate risks, establish controls, and continuously monitor them.
- Protect the safety and health of all workers, minimizing the risk of workplace accidents and work-related illnesses.
- Implement actions through the use of information technologies.
- Promote continuous improvement of the integrated management system.

"This policy is reviewed by top management, company committees, IMS, and OSHMS, will be updated annually and/or in case of regulatory changes, will be disclosed and made available to all personnel, contractors, and other stakeholders."

CORPORATE SOCIAL RESPONSIBILITY POLICY

Through corporate values, management systems, and best practices, we conduct our work responsibly towards our collaborators, clients, shareholders, regulatory entities, society, and all stakeholders involved in our business operations.

We are committed and aligned with:

- Strengthening and embodying corporate values:
  - Communication.
  - Service.
  - Integrity.
  - Diversity and Talent.
  - Collaboration.
  - Innovation.
  - Continuous Improvement.
  - Passion and Enthusiasm.

- Contributing to the development of professional competencies of our collaborators.
- Ensuring respect and dignified treatment.
- Rejecting all forms of labor abuse.
- Promoting and protecting human rights.
- Rejecting any form of discrimination based on gender, religion, place of origin, identity, political opinion, or any other nature.
- Developing corporate guidelines for inclusion and social well-being.
- Strengthening business relationships with clients and suppliers.
- Rejecting child labor and forced labor.
- Ensuring compliance with applicable legal requirements.

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY

Logiztik Alliance Group, in the course of its activities and following its Comprehensive Policy, is committed to providing security and confidence. To achieve this, the company has established the Comprehensive Anti-Money Laundering and Combating the Financing of Terrorism System (SARLAFT). This system will be disseminated to ensure understanding, implementation, and maintenance at all levels, fostering a risk prevention culture and offering transparent, reliable, and timely operations.

Risk analysis to prevent money laundering allows the detection of suspicious transactions that may be linked to the channeling of funds from criminal sources to the commission of punishable activities or the concealment of assets derived from illicit activities.

1. Purpose: Define and apply guidelines, controls, and actions necessary to protect against the risk of Money Laundering and Financing of Terrorism, involving all counterparts of LOGIZTIK ALLIANCE GROUP.

2. Scope: Applies to all processes where Money Laundering and Financing of Terrorism (ML/FT) risk factors are present. The counterparts that involve a risk factor in this regard and on which these guidelines are determined are:

- Clients
- Suppliers
- Partners or shareholders
- Company employees

3. Definitions:

- Risk factors: Elements that generate ML/FT risk to be considered in identifying situations that may lead to economic or reputational losses.
- National and international lists: Lists of individuals who, according to the publishing authority, may be linked to money laundering or financing of terrorism. Examples include the United Nations Security Council lists, which are binding for Colombia. Additionally, other lists such as OFAC, INTERPOL, National Police, among others, can be consulted.
- Financing of terrorism: A crime sanctioned by Article 345 of the Penal Code, related to the provision, collection, delivery, receipt, administration, contribution, custody, or storage of funds, goods, or resources to promote, organize, support, maintain, finance, or economically sustain organized crime groups, illegal armed groups, or their members, or national or foreign terrorist groups or terrorist activities.
- Money laundering: A crime described in Article 323 of the Penal Code, committed by a natural or legal person when acquiring, safeguarding, investing, transporting, transforming, storing, preserving, safeguarding, or managing assets with their immediate or mediate origin in activities such as human trafficking, extortion, illicit enrichment, extortionate kidnapping, rebellion, arms trafficking, trafficking of minors, financing of terrorism and administration of resources related to terrorist activities, drug trafficking, crimes against the financial system, crimes against public administration, or linked to the product of crimes executed in concert to commit crimes,

or giving the appearance of legality to assets from such activities, or legalizing, concealing, or covering up the true nature, origin, location, destination, movement, or right to such assets, or performing any other act to hide or cover up their illicit origin.

- Attempted operation: Awareness of the intention to carry out a suspicious operation, which is not completed either because the person attempting it abandons it or because the established controls do not allow its completion. These operations must be reported to the Financial Information and Analysis Unit (UIAF).
- Unusual operation: One whose amount or characteristics are not related to the economic activity of the counterparts or, due to its amount, the amounts transacted, or its particular characteristics, deviates from established normal parameters.
- Suspicious operation: One that, due to its amount, quantity, or characteristics, does not fit within the normal systems and practices of business, industry, or a specific sector. It cannot be reasonably justified according to the customs and practices of the activity. These operations must be reported to the UIAF.
- External reports: Reports generated for external entities, mainly the UIAF or other competent authorities.
- Internal reports: Reports generated for internal use and decision-making in AML/CFT matters.
- Early warning indicators: A set of indicators that allow the timely identification of atypical behaviors previously defined by the Foundation.
- Financial Information and Analysis Unit (UIAF): A special administrative unit, of a technical nature, created by Law 526 of 1999, modified by Law 1121 of 2006, with the objective of preventing and detecting operations that may be used for money laundering or the financing of terrorism. It also imposes reporting obligations on certain economic sectors.

4. Policies: As part of the implementation of the Anti-Money Laundering and Combating the Financing of Terrorism risk prevention system, LOGIZTIK ALLIANCE GROUP has established the following policies:

Policy 1: Collaborate in the fight against Money Laundering and Financing of Terrorism, promoting the proper functioning of the Anti-Money Laundering Prevention System.

- Do not use the company's name to conduct business or money movements for third parties.
- For all payments by transfer and check, only transfer or issue to the payee named in the payment.
- Provide complete and sufficient evidence of all transactions involving financial products.
- Adopt mechanisms that allow full identification of the origin of funds entering the company.

Policy 2: Employee Action Criteria: The performance of all company members in preventing Money Laundering and Financing of Terrorism will always be in line with corporate principles and values, which are framed in the highest ethical standards. The following specific criteria are defined:

- Knowledge of related third parties: Every LOGIZTIK ALLIANCE GROUP worker involved in national or international operations or transactions is obliged to apply the control

measures established by the company, both in this policy and in the procedures, for the proper and diligent identification of third parties within the scope of their duties.

- Collaboration to achieve objectives: All LOGIZTIK ALLIANCE GROUP workers are obliged to collaborate in the verifications or collection of information required for the Anti-Money Laundering and Financing of Terrorism Prevention System. They are also required to report operations that, within the normal course of their work and as defined in this policy, correspond to an unusual or suspicious Money Laundering or Financing of Terrorism operation.
- Confidentiality of information: No LOGIZTIK ALLIANCE GROUP employee may disclose to third parties' information about Anti-Money Laundering or Financing of Terrorism procedures or controls, as well as reports sent to competent authorities.
- Doubt any business proposal that represents unjustified and unjustifiable returns.
- Doubt suppliers providing products at prices equal to or lower than their cost, and even much lower than those normally offered in the market.

Policy 3: Principles of Relationship with Related Third Parties: LOGIZTIK ALLIANCE GROUP provides its services based on the following principles:

- Compliance with current national and international laws, as well as the rules and regulations applicable to activities related to Money Laundering and Financing of Terrorism.
- Adherence to the fundamental principles of the United Nations Global Compact.
- Adherence to the Business Ethics Code.
- Transparency in the execution of tasks and the results obtained in company activities.
- Responsible, reasonable, and sustainable risk management.
- Reporting unusual and suspicious operations to the UIAF.
- Before contracting with a client or supplier, documentation will be requested to guarantee its origin.
- Conduct periodic visits to client and supplier facilities.
- Check potential clients and suppliers against binding lists, at least: OFAC or Clinton List - INTERPOL - Attorney General's Office - Comptroller General's Office - National Police - RUES - Financial backgrounds (BDME).

Policy 4: Analyze, review, and report when applicable payments received from tax havens according to Decree 1966 of October 7, 2014, and from non-cooperative jurisdictions following the Financial Action Task Force (FATF).

The general aspects described in this policy must be integrated into all procedures related to (payments, acquisitions, personnel selection, clients, suppliers).