

<p align="center">POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING</p>	<p align="center">HOTELES CHARLESTON S.A.S.</p>	
<p>Date of update: JULY 21 2023</p>	<p>Effective: JULY 21 2023</p>	<p>Version: 001</p>

POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING

INTRODUCTION

HOTELES CHARLESTON S.A.S. (hereinafter referred to as THE ORGANIZATION) is committed to implementing strategies to prevent fraudulent, improper or related actions to money laundering and terrorist financing (ML/TF). Therefore, in order to maintain the best practices - in accordance with the parameters established in Chapter X of the Basic Legal Circular of the Superintendency of Corporations¹ - the Organization implements this Policy, which regulates the system of self-control and risk management of money laundering and terrorist financing, in order to ensure transparency of all operations carried out by the Company.

1. ABOUT

The main purpose of the Organization is to operate and invest in hotels and tourism projects in general, inside and outside the country, being able to acquire real estate and personal property to develop its activity.

Business ethics, good industry practices and corporate governance are fundamental values that any organization must take into account to ensure its success and sustainability over time. In this sense, our organization is proud to have an appropriate commitment to these aspects, promoting socially responsible behavior in accordance with current legislation in all areas of its activity. We believe that an ethical and responsible company not only serves its own interests, but also contributes to the development and well-being of society as a whole. Therefore, in each of our decisions and actions, we strive to meet the highest standards of quality and transparency, prioritizing the respect and satisfaction of our customers, employees, suppliers and local communities.

Our company has different compliance base documents that cover different aspects to guarantee an ethical, responsible and quality service in the tourism sector. Among the tools implemented are:

- Customer Service Policy; Modification and Cancellation Policy; Privacy and Confidentiality Policy; Reservation Policy; Locker Use Policy; and Educational Assistance Use Policy.
- National Tourism Registry: The establishment is registered in the Business and Social Registry (RUES), which allows it to carry out the activities of tourist accommodation in a legal and transparent manner.
- Biosafety protocol for the reception of supplies and products: As a service company focused on accommodation and customer service, it recognizes that human talent is its most valuable resource. For this reason, its occupational health and safety policy recognizes the importance of ensuring a safe and healthy working environment for all its employees.
- Code of Business Conduct: The Company has established a Code of Business Conduct that sets forth the practices and procedures necessary to conduct its business in a consistent manner and in accordance with the highest ethical standards. This code enables them to comply with applicable laws and ensure customer satisfaction.

2. OBJETIVE

To establish the guidelines to be followed in the area of money laundering and terrorist financing risk management (hereinafter referred to as the SAGRILAF Policy), in order to minimize the risks that, through the Organization's operations, funds derived from money laundering or terrorist financing may enter, or that, indirectly, instruments may be used to conceal, manage, invest or benefit from any form of money and other assets derived from illicit activities.

¹ Basic Legal Circular: compiles the main general legal instructions issued by the Superintendence of Companies on money laundering, financing of terrorism and financing for the proliferation of weapons of mass destruction.
[https://www.supersociedades.gov.co/nuestra_entidad/normatividad/Documents/Circular%20Basica%20Jur%C3%ADdica%20Mod1%20\(10-08-15\).pdf](https://www.supersociedades.gov.co/nuestra_entidad/normatividad/Documents/Circular%20Basica%20Jur%C3%ADdica%20Mod1%20(10-08-15).pdf)

POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING	HOTELES CHARLESTON S.A.S.	
Date of update: JULY 21 2023	Effective: JULY 21 2023	Version: 001

Similarly, this policy seeks to protect the reputation of the Organization by avoiding, to the extent possible, its association with third parties involved in money laundering or terrorist financing activities.

3. SCOPE

The SAGRILAF policy applies to all employees, whether they perform their duties at the facilities, at home or at any other location, independent contractors, customers and suppliers of products and services that support the operation. Failure to comply with or adhere to any of the measures set forth in this document shall constitute a serious offense for all legal purposes. The foregoing indicates that such non-compliance may result in termination of employment for just cause, subject to appropriate labor disciplinary procedures.

4. DEFINITIONS

- a. **Due diligence:** is the set of precautions that the law or common sense advises to take in an activity in order to avoid foreseeable harm². In the context of the Self-Monitoring and Risk Management System for Money Laundering and Terrorist Financing, due diligence refers to "the practice of knowing the customer"³. In other words, it is the process by which the organization takes measures to know the counterparty, its business, operations, products and volume of transactions.
- b. **Counterparty:** any natural or legal person with whom the Organization has a commercial, business, contractual or legal relationship of any kind. Counterparties include, but are not limited to, the Organization's partners, employees, customers, contractors and product suppliers.
- c. **GAFI:** An intergovernmental body established in 1989 to set standards and promote the effective implementation of legal, regulatory and operational measures to combat money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, and other threats to the integrity of the international financial system⁴.
- d. **ML/FT/PWMD:** refers to the combined concepts of money laundering, terrorist financing and proliferation of weapons of mass destruction.

The Financial Information and Analysis Unit (UIAF) defines money laundering as "the process by which criminal organizations seek to give the appearance of legality to the resources generated by their illicit activities. In practical terms, it is the process of making dirty money look clean so that criminal organizations or criminals can use and, in some cases, profit from these resources"⁵.

At the same time, it defines terrorism as "a method of carrying out repeated violent actions, using individuals, groups or clandestine (semi-)state actors, for ideological, religious or political reasons"⁶.

- e. **Restrictive lists⁷:** are "those national and international databases that collect information, reports and background information from different agencies on natural and legal persons that may represent suspicious activities, investigations,

² Definition taken from the Pan-Hispanic Dictionary of Legal Spanish of the Royal Spanish Academy (RAE) (<https://dpej.rae.es/lema/diligencia-debida>).

³ Definition taken from the Infolaft website, a company specialized in providing information and training to prevent and mitigate the risks of money laundering, terrorist financing, corruption and fraud within companies (<https://www.infolaft.com/que-es-debida-diligencia/>).

⁴ Definition taken from the UIAF website, International Affairs section (https://www.uiaf.gov.co/asuntos_internacionales/organizaciones_internacionales/grupo_accion_financiera_7114).

⁵ https://www.uiaf.gov.co/sistema_nacional_ala_cft/lavado_activos_financiacion_29271/lavado_activos

⁶ The UIAF takes the definition of terrorism from the document A review of sources on terrorist financing. The text quoted here was taken from https://www.uiaf.gov.co/sistema_nacional_ala_cft/lavado_activos_financiacion_29271/financiacion_terrorismo

⁷ Complete list of restrictive lists binding on Colombia at: <https://www.un.org/securitycouncil/es/content/un-sc-consolidated-list>

POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING	HOTELES CHARLESTON S.A.S.	
Date of update: JULY 21 2023	Effective: JULY 21 2023	Version: 001

prosecutions or convictions for the crimes of money laundering⁸ and terrorist financing.

- f. **Binding lists:** are those lists of persons and entities associated with terrorist organizations that are binding on Colombia under Colombian law (Article 20 of Law 1121 of 2006) and international law, including, but not limited to, Resolutions 1267 of 1999, 1373 of 2001, 1718 and 1737 of 2006, 1988 and 1989 of 2011, and 2178 of 2014 of the United Nations Security Council, and all subsequent, related and complementary resolutions, as well as any other list binding on Colombia (such as the terrorist lists of the United States of America, the list of terrorist organizations of the European Union, and the list of persons listed as terrorists of the European Union, among others).
- g. **Monitoring:** is the continuous and systematic process of verifying the efficiency and effectiveness of a policy or process, identifying its achievements and weaknesses, and recommending corrective measures to optimize the expected results⁹.
- h. **Compliance Officer:** is the natural person appointed by the Organization in charge of promoting, developing and ensuring compliance with the specific procedures for the prevention, updating and mitigation of ML/FT/PWMD risks in the Obligated Subjects. In HOTELES CHARLESTON S.A.S., the Compliance Officer is appointed by the General Assembly of Shareholders.
- i. **Unusual transaction:** a transaction whose amount or characteristics are not related to the economic activity of the clients or which, due to its amount, the amounts transacted or its particular characteristics, are outside the established parameters of normality.
- j. **Suspicious Transaction:** is a transaction that, because of its number, quantity or characteristics, does not fall within the normal systems and practices of a business, industry or specific sector and, in addition, could not be reasonably justified according to the customs and practices of the activity in question. These transactions must be reported to the UIAF through a Suspicious Transaction Report.
- k. **Politically Exposed Persons (PEP):** are public servants of any nomenclature and job classification system of the national and territorial public administration, when in the positions they occupy, in the functions of the area to which they belong or in those of the employment record they occupy, they have, under their direct responsibility or by delegation, the general direction, formulation of institutional policies and adoption of plans, programs and projects, the direct management of goods, money or securities of the State. This may be done through the management of expenditures, public contracts, management of investment projects, payments, liquidations, management of movable and immovable property.
- l. **Financial Information and Analysis Unit (UIAF):** is a special administrative unit of the Colombian State, with legal personality, administrative and financial autonomy, of a technical nature, attached to the Ministry of Finance and Public Credit. It is the country's financial intelligence unit, created by Law 526 of 1999 and regulated by Decree 1068 of 2015, to prevent, detect and combat money laundering and terrorist financing¹⁰.

5. SAGRILAFI POLICY GUIDELINES

For a proper operation of the SAGRILAFI policy, the organization implements the following guidelines, which must be respected by all shareholders, management team, direct employees, employees on assignment, contract administrators, customers, suppliers or third parties with whom the company has a relationship:

⁸ <https://www.compliance.com.co/onu-lista-vinculante-para-colombia-las-listas-restrictivas-o-listas-vinculantes/#:~:text=Recordemos%20que%20las%20listas%20Restrictivas,actividades%20sospechosas%2C%20investigaciones%2C%20procesos%20o>

⁹ Definition taken from the Basic Legal Circular of the Superintendence of Corporations.

¹⁰ Definition taken from the UIAF website, section Who we are (https://www.uiaf.gov.co/nuestra_entidad/quienes_somos).

POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING	HOTELES CHARLESTON S.A.S.	
Date of update: JULY 21 2023	Effective: JULY 21 2023	Version: 001

- a. **Prevalence of the SAGRILAFT policy in the achievement of business objectives.**
- b. **Guidelines for the acceptance and association/negotiation/contracting of clients and counterparties.** The Organization shall not have any relationship with any natural or legal person that is included in the international lists binding Colombia, in accordance with international law (United Nations lists), OFAC lists, or other lists of criminals and terrorists, which by their nature are considered high risk activities of ML/FT/PWMD, or if any of its shareholders, partners or administrators are included in restrictive lists.

In the event that any property, asset, product, fund or right of ownership is identified or verified in the name of or under the management or control of any country, person or entity included in the Restrictive Lists, the Compliance Officer shall immediately report it to the UIAF and inform the Attorney General's Office through the channels provided for that purpose.
- c. **Monitoring, Control and Detection of Unusual and Suspicious Transactions.** The Organization shall, at least once a year, monitor, control and detect possible unusual and/or suspicious transactions among its shareholders, management, direct employees, contractors, customers, suppliers or third parties with whom the Company has a relationship.
- d. **Payments and Collections.** All payments and collections, both with customers and suppliers, must be made through electronic transfers and/or checks through banking institutions whose holder must be the natural or legal person with whom the relationship/contract has been established.
- e. **All operations, transactions and contracts must be supported by evidence.** Without exception, it is forbidden to carry out activities, transactions and contracts without the corresponding internal and external supports, duly dated and authorized by those who participate in or prepare them. Such documentation may be contracts, commercial offers or proposals and the corresponding purchase or service order. These documentary supports will serve the Organization to verify the traceability of the transaction and the verification of the process in accordance with the guidelines established in the SAGRILAFT Policy.
- f. **Retention of supporting documents.** All documents evidencing transactions, business or contracts, in addition to being the support for the negotiation and accounting, constitute the evidentiary support for any investigation that may be carried out by the competent authorities and, therefore, must be kept for a period of at least ten (10) years from the date the transaction was identified, in accordance with article 28 of Law 962 of 2005 and chapter X of the Basic Legal Circular of the Superintendence of Corporations.

6. DUE DILIGENCE PROCEDURES

In order to ensure compliance with the guidelines of the SAGRILAFT Policy, the Organization establishes the following due diligence procedure, aimed at preserving institutional integrity and preventing the Organization from being used as a tool for ML/FT/PWMD activities.

- a. **Identification of situations that may give rise to ML/FT/PWMD risks in the organization's operations and business.** The manager of the relevant process shall identify the ML/FT/PWMD risks in its operations or business derived from its corporate purpose. If an ML/FT/PWMD risk is identified, it shall be reported to the Compliance Officer via corporate e-mail, who shall issue a formal and written policy.
- b. **Knowledge of Customers.** The Organization shall establish customer awareness, as well as the mechanisms, forms and tools to implement it. The above as a control mechanism to prevent risks related to ML/FT/PWMD, a possible risk of contagion of activities related to ML/FT/PWMD.
 - Among the basic activities that should be carried out in order to get to know the customer, and whenever the nature of the operation and activity so permits, are, by way of example, the following:

<p align="center">POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING</p>	<p align="center">HOTELES CHARLESTON S.A.S.</p>	
<p>Date of update: JULY 21 2023</p>	<p>Effective: JULY 21 2023</p>	<p>Version: 001</p>

- To know by any legal means the origin of the resources.
 - Verify the customer's identity.
 - Verify and confirm your contact information, your economic activity.
 - Request any additional documentation deemed relevant.
- c. Knowledge of Politically Exposed Persons (PEPs).** The PEP due diligence process requires a higher level of due diligence, as it is more rigorous and requires greater controls. Approval of transactions and business with PEPs is given by a higher authority than the one responsible for the normal counterparty know-your-customer process.
- d. Knowledge of Suppliers.** When associating/negotiating/contracting with suppliers, both natural and legal persons, due diligence and controls must be carried out in accordance with their risks. The above as a preventive measure against a possible risk of contagion of activities related to ML/FT/PWMD risks.
- e. Knowledge of Shareholders.** When new shareholders are admitted, the Compliance Officer, or whoever is in his place, shall carry out due diligence on both natural and legal persons, with the aim of knowing the ultimate beneficiary of the investment and the origin of the new investor's funds, in order to avoid that, in the event that the funds are illicit, the Organization may be harmed. The identification will be carried out in order to validate in lists with ML/FT/PWMD information.
- f. Knowledge of Employees.** The organization must verify the background of its employees and those it intends to hire. It must also update this information at least annually. The Organization shall have policies for selecting, hiring, and maintaining information on all of its employees, who, in the performance of their duties, shall strictly comply with the Internal Work Regulations (RTI) and the Organization's policies, standards, and procedures.
- g. Verification of lists containing ML/FT/PWMD information on customers, suppliers and employees.** The validation of background information (historical, legal and administrative) related to ML/FT/PWMD shall be carried out at least in the following sources:
- UN List issued by the Security Council of the United Nations.
 - OFAC list issued by the Office of Foreign Assets Control of the U.S. Department of the Treasury.
 - Disciplinary Record Certificate issued by the Attorney General's Office of the Nation of the legal entity and its legal representative or the corresponding natural person.
 - In addition, the lists of Interpol and the National Police and the tax records certificate of the Comptroller General of the Republic, among others, may be consulted through the Internet or other technical means.
- To facilitate the task of validating restrictive lists, the Organization has a technological tool that allows it to make individual and mass queries of binding and restrictive lists (OFAC, UN and other risk lists offered in open sources of information) that will be integrated into the different processes of the Organization that so require.
- h. Denial of Products.** In cases where a product or service is denied to a customer due to a report on lists containing ML/FT/PWMD information or due to the detection of a suspicious transaction, no document issued by the organization or oral communication shall state that the denial of the product or service is due to ML/FT/PWMD related antecedents.
- i. Recordkeeping and Due Diligence.** The Organization shall have procedures in place to ensure the appropriate handling, retention and filing of documents and reports related to the risk management systems associated with ML/FT/PWMD, thereby guaranteeing their integrity, timeliness, reliability and availability.
- j. Internal Reports.** At least once a year, the Compliance Officer shall present a report on SAGRILAFT's management to the Shareholders' Meeting. Likewise, the Compliance Officer shall make any report requested by the General Assembly or the Legal Representative.
- k. Collection of Cash Transactions.** All payments and collections of counterparties shall be made through electronic transfers and/or checks through banking institutions, with the exception of collections of lodging and events that are made

<p style="text-align: center;">POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING</p>	<p style="text-align: center;">HOTELES CHARLESTON S.A.S.</p>	
<p>Date of update: JULY 21 2023</p>	<p>Effective: JULY 21 2023</p>	<p>Version: 001</p>

at the payment point of THE COMPANY, whose maximum amount shall not exceed the sum of four (4) current legal minimum monthly wages in cash transactions.

- I. **Verification in control lists of customers and suppliers.** A minimum transaction limit of seventeen (17) current monthly legal minimum wages for legal entities (customers or suppliers) and nine (9) current monthly legal minimum wages for natural persons is established for validation in control lists.

- m. **Risk Factor Segmentation.** For an adequate implementation of the SAGRILAFT Policy, the Organization has segmented the risk factors to be analyzed as follows:
 - **With regard to counterparties**
 - i. Entering into transactions with natural or legal persons who are not fully identified.
 - ii. Accepting new partners, shareholders or employees with a judicial record for any crime, especially those related to money laundering, financing of terrorism or financing the proliferation of weapons of mass destruction.
 - iii. Accepting new partners or shareholders without first verifying the origin of the resources they contribute.

 - **With respect to transactions, business or contracts**
 - i. Transactions involving large amounts of cash without apparent justification.
 - ii. Transactions involving movable or immovable property at prices that differ significantly from normal market prices.
 - iii. Donations.
 - iv. Transactions, deals or contracts that are not in writing.
 - v. Payment of transactions with funds derived from international wire transfers from multiple senders to the same recipient or from the same sender to multiple recipients without any apparent relationship.
 - vi. Transactions with unidentified subcontractors.
 - vii. Commercial transactions or transactions with persons listed in Resolutions 1267 of 1999, 1373 of 2001, 1718 and 1737 of 2006, adopted by the United Nations Security Council or its various committees, and any other resolutions that amend or supplement them.
 - viii. Transactions with counterparties domiciled or located in jurisdictions designated by the FATF as non-cooperative.
 - ix. Transactions involving virtual currencies.

7. RISKS ASSOCIATED WITH ML/FT/PWMD

In accordance with the provisions of Chapter X of the Basic Legal Circular of the Superintendency of Corporations, the risks associated with ML/FT/PWMD are as follows:

- a. **Legal risk:** is the possibility that a company, its officers, directors or other related persons may be sanctioned, fined or required to pay damages as a result of failure to comply with rules or regulations related to the prevention of ML/FT/PWMD.

- b. **Reputational risk:** is the possibility that a company may suffer losses due to loss of prestige, poor image, negative publicity, whether true or not, regarding the institution and its business practices, resulting in loss of customers, decrease in revenues, or being involved in legal proceedings.

- c. **Operational Risk:** is the possibility of being used in ML/FT/PWMD activities due to deficiencies, failures or inadequacies in human resources, processes, technology, infrastructure or the occurrence of external events.

- d. **Contagion Risk:** is the possibility of loss that a company may suffer, directly or indirectly, as a result of an action or experience of a customer, employee, supplier, associate or related party related to ML/FT/PWMD crimes. Related or

POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING	HOTELES CHARLESTON S.A.S.	
Date of update: JULY 21 2023	Effective: JULY 21 2023	Version: 001

associated parties include natural or legal persons who have the ability to exercise influence over the entity.

8. ETHICS LINE

The Organization uses the e-mail lineaethicahcs@hotelescharleston.com as an ethical line, i.e., as a direct communication channel to report and denounce, with verifiable evidence, behaviors and facts suspected of money laundering or terrorist financing. The company guarantees the confidentiality of the information and of the person who denounces and reports.

9. RESTRICTIVE LIST CHECKS

Third parties (customers or suppliers) that are to be linked or are already linked to the organization must be verified once a year in restrictive lists. Once the verification in the lists has been carried out, if any suspicious report comes out, the case must be immediately escalated to the Compliance Officer, who will validate the report and will issue his concept regarding the convenience of continuing or not with the linking process. If the case of suspicion is indeed confirmed by the Compliance Officer, it will be reported to the UAIF and to the Public Prosecutor's Office through the channels provided for this purpose.

10. INCIDENT AND SANCTION MANAGEMENT

In the event of a situation related to ML/FT/PWMD that could not have been previously detected or contained by the Compliance Officer, it must be immediately remedied in accordance with the instructions given by the Shareholders' Meeting. In all cases, a corrective action plan must be presented to ensure that the risk has been managed and controls have been strengthened. Lessons must be learnt from the incident in order to avoid its recurrence, taking into account aspects such as: redesign of processes, improvement plans and updating of the risk assessment, determining whether it is necessary to modify the profile and possible adjustments to controls.

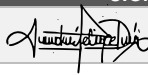

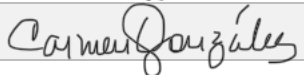
It is the responsibility of each of THE COMPANY'S managers and employees to ensure strict compliance with the laws, regulations and internal procedures that support ML/FT/PWMD risk management.

Such non-compliance implies the possibility of the occurrence of actions that exceed what is normally considered ethical limits or that violate legal restrictions and that are due to irresponsible, permissive, negligent, inefficient or opaque attitudes in the commercial and operational development of THE COMPANY, which may lead to the application of the Penalty Regime. In the event of any violation of the procedures and rules described in this Policy by any legal representative or employee of the Organization, such violation shall be considered a serious labor offense under the employment contract, the Internal Labor Regulations and/or the policies of THE COMPANY.

11. DISSEMINATION

The Organization will carry out internal and external dissemination and training activities on the SAGRILAF policy.

12. SIGNATURES

POSITION	NAME	SIGNATURE
Elaboration: Attorney	PDA ABOGADOS	
Review:	JULIA PRADO - THE COMPLIANCE OFFICER	
Review:	CARMEN GONZALEZ-LEGAL REPRESENTATIVE	

<p align="center">POLICY FOR THE SELF-MONITORING AND RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING AND TERRORIST FINANCING</p>	<p align="center">HOTELES CHARLESTON S.A.S.</p>	
<p>Date of update: JULY 21 2023</p>	<p>Effective: JULY 21 2023</p>	<p>Version: 001</p>

<p>Approval:</p>		
<p>Approval: By the General Meeting of Shareholders of HOTELES CHARLESTON S.A.S. by means of Protocol No. 64 dated 21 of JULY 2023</p>		