POLICY ON THE INTERNAL INFORMATION SYSTEM

Sercotel Hotel Group

TABLE OF CONTENTS

1. INTRODUCTION AND OBJECTIVE

The purpose of this Policy is to promote and strengthen a culture of communication within the SERCOTEL Group as a tool to prevent and detect threats to the public interest, while ensuring and prioritizing the protection of whistleblowers, under Law 2/2023 of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption, which transposes into Spanish law DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of October 23,
2019, on the protection of persons who report breaches of Union law.

The SERCOTEL Group expects both its members and business partners to act at all times in accordance with the principle of good faith in the performance of their duties, which requires, among other things, consistently maintaining a collaborative attitude toward the organization.

As a tool to ensure compliance with the above, the Group's Compliance Committee has established the following internal reporting channel as the preferred means available to all executives, employees, collaborators, suppliers, and customers of the entity, as well as any other third party:compliance@sercotel.com , or by mail to Calle Comte d'Urgell, No. 240, Attic, 08036, Barcelona—to the attention of the Compliance Committee; as well as verbally or via the internal form available on the intranet through Sercotel Connect and the web form via the link https://www.sercotelhoteles.com/es/compliance.

2. SCOPE

This Internal Information System Policy applies to and is binding on all entities comprising the SERCOTEL Group, ensuring the application of its principles across all member entities, without prejudice to any necessary adaptations, where applicable, to comply with applicable regulations in foreign subsidiaries.

Accordingly, this Policy is translated into whatever languages are necessary so that all members of the SERCOTEL Group, as well as its business partners associated with the Group, can understand its scope and content.

3. CONTENT OF COMMUNICATIONS

Through this Internal Reporting System, executives, employees, contractors, suppliers, customers, and other third parties may report, confidentially and anonymously if they so choose, any concerns regarding a possible breach or violation of the provisions of the Code of Conduct or any other internal policy of the organization, or report any irregularity they detect in the performance of their duties, as well as any violation or omission of which they are aware and that may constitute a violation of the law.

the European Union or its financial interests, or even criminal or administrative offenses under Spanish law.

In this regard, this Communication Channel may be used to report actions or omissions that constitute or may constitute violations in the following areas:

- Health alert
- Harassment / Discrimination
- Public procurement
- Confidentiality
- Corruption/Fraud
- Competition
- Corporate Crimes
- Tax / Corporate
- Finance
- Non-compliance with applicable laws
- Non-compliance with Policies / Procedures / Internal Regulations
- Violations of the Code of Ethics and other internal codes
- Labor / Workers' Rights
- Environment
- Radiation protection and nuclear safety
- Intellectual Property/Trade Secrets
- Organizational Protocols and Standards
- Occupational Risk Prevention
- Consumer Protection
- Privacy and Personal Data Protection
- Risks or Suspicions of Money Laundering or Terrorist Financing
- Sustainability
- Public health
- Food and feed safety, animal health, and animal welfare
- Network and information system security
- Product safety and compliance
- Transport safety
- Other

This reporting channel is to be used solely for the purpose described and should not be used as a means for inquiries or complaints.

Internal reporting channels that are authorized to receive any communications or information beyond what is set forth above shall not be covered by the scope of protection provided by this Policy or by Law 2/2023 of February 20, which regulates the protection of individuals who report regulatory violations and combats corruption.

4. ON WHISTLEBLOWERS OR INFORMANTS

The principles, guarantees, and rights set forth in this Policy focus on the protection of whistleblowers, prohibiting retaliation of any kind and promoting support and assistance for them.

In this context, whistleblowers or informants are defined as any individuals who report the violations mentioned in the preceding section, who work in the

private or public sector and who have obtained information about violations in a work or professional context, including in all cases:

- Employees, including those whose employment or professional relationship has already ended.
- Self-employed individuals.
- Volunteers.
- Interns.
- Job applicants.
- Partners, shareholders.
- Members of the board of directors.
- Anyone working under the supervision of contractors, subcontractors, or suppliers.

Likewise, the following shall also enjoy the protection established by this Policy, in accordance with the aforementioned Law 2/2023:

- the legal representatives of employees in the exercise of their functions of advising and supporting the whistleblower,
- individuals who, within the organization where the whistleblower provides services, assist the whistleblower in the process,
- individuals related to the whistleblower who may suffer retaliation, such as the whistleblower's coworkers or family members, and
- legal entities for which the whistleblower works, with which they have any other type of relationship in a work context, or in which they hold a significant stake. For these purposes, a stake in the capital or in the voting rights corresponding to shares or equity interests is considered significant when, due to its proportion, it allows the person holding it to exert influence over the legal entity in which the stake is held.

5. GENERAL PRINCIPLES AND GUARANTEES

5.1 Integration of Internal Channels

The reporting channel that forms part of the SERCOTEL Group's Internal Reporting System will be available and accessible to all employees or any third party, regardless of their relationship with the Group, as a comprehensive and preferred[1]channel for reporting information.

5.2 Confidentiality and Anonymity

The SERCOTEL Group guarantees both the confidentiality and anonymity (if desired) of the whistleblower and any other third party who is or may be mentioned and/or involved in the report, in the actions taken as a result of it, and in its processing, without the need to obtain data that would allow for their identification. In this regard, data protection is guaranteed, preventing access by unauthorized personnel.

[1] The safeguards set forth in this section shall be respected and apply even if the report is submitted through reporting channels other than those established for that purpose, or to staff members not responsible for processing it.

Accordingly, any proceedings conducted with third parties or other bodies, areas, or departments of the SERCOTEL Group must be carried out while maintaining the anonymity of the WHISTLEBLOWER and the SUBJECT OF THE INVESTIGATION, as well as the grounds for the report.

The Group guarantees that the identity of the whistleblower may only be disclosed to the Judicial Authority, the Public Prosecutor's Office, or the competent administrative authority within the framework of a criminal, disciplinary, or sanctioning investigation.

All those who, for various reasons, participate in tasks supporting the investigation of a specific incident must sign a Confidentiality Agreement to that effect.

In cases where the receipt of reports is managed by an external provider, it is always verified that the provider offers adequate guarantees regarding respect for independence, confidentiality, data protection, and the secrecy of communications.

In cases where a communication is sent through internal channels other than those established by Grupo SERCOTEL or is addressed to staff members not responsible for its processing, the organization guarantees the maintenance of the confidentiality described above. To this end, it has the Periodic Compliance Training Plan that Grupo SERCOTEL has implemented, which states (in accordance with the requirement of Article 9.2.g of Law 2/2023) that failure to comply constitutes a very serious violation of the Law and, furthermore, that the recipient of the communication must immediately forward it to the System Manager.

5.3 Presumption of Innocence and Honor

At all times, Grupo SERCOTEL guarantees the presumption of innocence and respect for the honor of all persons affected by a report.

Individuals affected by a report shall have the right to be informed of the actions or omissions attributed to them, as well as to be heard during the course of the investigation, without under any circumstances being informed of the identity of the informant.

Grupo SERCOTEL guarantees to individuals affected by the report: the right to the presumption of innocence, the right to a defense, and the right to access the case file under the terms set forth in Law 2/2023, as well as the same protection established for whistleblowers, preserving their identity and ensuring the confidentiality of the facts and details of the proceedings.

5.4 Access to External Channels and Public Disclosure

Whistleblowers may submit their reports through the external channel of the Anti-Fraud Office of Catalonia or to the relevant authorities or bodies in other autonomous communities, either directly or after first reporting through the corresponding internal channel of the SERCOTEL Group (compliance@sercotel.com , postal mail, or forms on the intranet or website).

Likewise, whistleblowers or informants are given the option to make a public disclosure through channels outside the organization.

Public disclosure consists of making information regarding the facts reported through this Reporting System available to the public.

In this context, for the protection provided by Law 2/2023 to extend to individuals who make public disclosures, the following conditions must be met:

a) The report must have first been submitted through internal and external channels, or directly through external channels, without appropriate measures having been taken within the established timeframe.
b) Have reasonable grounds to believe that either the violation may pose an imminent or clear danger to the public interest, particularly in an emergency situation, or that there is a risk of irreversible harm, including a threat to a person's physical safety; or, in the case of reporting through an external reporting channel, there is a risk of retaliation or it is unlikely that the information will be effectively addressed due to the particular circumstances of the case, such as the concealment or destruction of evidence, collusion between an authority and the perpetrator of the violation, or the authority's involvement in the violation.

5.5 Prohibition of Retaliation

SERCOTEL expressly prohibits acts constituting retaliation, including threats of retaliation and attempts at retaliation against individuals who file a report.

Retaliation is defined as any act or omission that is prohibited by law, or that, directly or indirectly, constitutes unfavorable treatment that places the individuals subjected to it at a particular disadvantage compared to others in the workplace or professional context, solely because of their status as whistleblowers or because they have made a public disclosure.

For the purposes of Law 2/2023, and by way of example, Article 36 of said law establishes that retaliation is considered to be that which takes the form of:

a) Suspension of the employment contract, dismissal, or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the probationary period has been completed, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion, or denial of promotions, and any other substantial modification of working conditions, as well as the failure to convert a temporary employment contract into a permanent one, in the event that the employee had legitimate expectations that they would be offered permanent employment; unless such measures are carried out within the regular exercise of managerial authority under labor law or regulations governing the status of public employees, due to proven circumstances, facts, or violations, and unrelated to the submission of the communication.

b) Damages, including reputational harm, or financial losses, coercion, intimidation, harassment, or ostracism.

c) Negative evaluations or references regarding work or professional performance.

d) Inclusion on blacklists or the dissemination of information within a specific sector, which hinders or prevents access to employment or the contracting of works or services.

e) Denial or revocation of a license or permit.

f) Denial of training.

g) Discrimination, or unfavorable or unfair treatment.

Any person whose rights have been infringed upon as a result of their communication or disclosure may, after a period of two years has elapsed, request protection from the competent authority, which, in exceptional and justified cases, may extend the protection period, following a hearing of the persons or bodies that may be affected. Any refusal to extend the protection period must be justified.

5.6 Support Measures

In accordance with the rules established by Law 2/2023, SERCOTEL makes available to the whistleblower or informant the appropriate support measures that, following an assessment of the circumstances, are deemed necessary. For example:

a) Information and advice on available procedures and remedies, protection against retaliation, and the rights of the affected person.

b) Legal advice.
c) Psychological support.

All of this is provided regardless of any assistance that may be available under Law 1/1996 of January 10 on free legal aid for representation and defense in legal proceedings arising from the submission of the report or public disclosure.

5.7 Protective Measures Against Retaliation: Disclaimer

Persons who report or disclose violations set forth in Section 3 of this document shall be entitled to protection provided that the following circumstances apply:

a) they have reasonable grounds to believe that the information in question is true at the time of the report or disclosure, even if they do not provide conclusive evidence, and that said information falls within the scope of Law 2/2023.

b) the communication or disclosure was made in accordance with the requirements set forth in Law 2/2023.

The following persons are expressly excluded from the protection provided by this law:

a) Information contained in communications that have been rejected by an internal reporting channel or for any of the reasons set forth in Article 18.2.a) of Law 2/2023.

b) Information related to complaints about interpersonal conflicts or that affects only the whistleblower and the individuals named in the report or disclosure.

c) Information that is already fully available to the public or that constitutes mere rumors.

d) Information referring to acts or omissions not covered by Section 3 of this document.

Persons who communicate information in accordance with this Policy shall not be deemed to have violated any restriction on the disclosure of information nor shall they incur any liability in connection with such disclosure, provided that they had reasonable grounds to believe that such communication or, where applicable, public disclosure, was necessary to reveal an act or omission under this Policy.

Informants shall not be held liable for obtaining or accessing information that is publicly communicated or disclosed, provided that such obtaining or accessing does not constitute a crime.

5.8 Personal Data Protection

The SERCOTEL Group undertakes to process the data contained in the communication in strict compliance with legislation on the protection of personal data and whistleblowers, ensuring at all times that there will be no retaliation.

The processing of personal data resulting from the application of Law 2/2023, on which this Policy is based, shall be governed by the provisions of Title VI of said Law, by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, Organic Law 3/2018 of December 5 on the Protection of Personal Data and the Guarantee of Digital Rights, and Organic Law 7/2021 of May 26 on the protection of personal data processed for the purposes of preventing, detecting, investigating, and prosecuting criminal offenses and enforcing criminal sanctions.

Personal data whose relevance to the processing of specific information is not apparent will not be collected; if collected accidentally, it will be deleted without undue delay.

6. COMMITMENTS TO COMPLIANCE

All individuals associated with the SERCOTEL Group must be familiar with the ethical and responsible principles, as well as with all the provisions and obligations contained in the various control measures (Internal Information System Policy, Criminal Compliance Policy, Code of Conduct, Confidentiality Policy, Data Protection Policy, Anti-Corruption, Anti-Fraud, and Anti-Bribery Policy, Harassment Policy, etc.) adopted by the organization, and are obligated to comply with them, as well as to preserve its integrity and reputation.

This Policy, together with the Code of Conduct and the other internal protocols, policies, and guidelines implemented by the Group, forms the cornerstone of the organization's compliance culture. For this reason, this Policy is mandatory for all individuals associated with the SERCOTEL Group, as well as for business partners, requiring not only compliance with applicable laws but also loyalty to the organization's ethical and responsible values and principles.

To facilitate awareness of this Policy and ensure compliance, it is made available to all Group members via the Intranet and to interested third parties through the organization's external communication channels (https://www.sercotelhoteles.com/es/compliance).

7. SANCTIONING SYSTEM

Any action that may constitute a limitation on the rights and guarantees of whistleblowers, or on their confidentiality and anonymity, or a breach of the duty of confidentiality regarding the information received and the data contained therein, may constitute a serious or very serious violation for non-compliance with the provisions of Law 2/2023 of February 20, regulating the protection of persons who report regulatory violations and the fight against corruption.

8. RESPONSIBILITY AND SUPERVISION

The SERCOTEL Compliance Committee is the governing body responsible for the Group's Internal Reporting System; it is tasked with ensuring its proper functioning and will be accountable for the prompt processing of the information received. Furthermore, this collegiate body delegates to one (1) of its members the powers to manage the system and process investigation files (Appendix 1 of this document).

The COMPLIANCE COMMITTEE enjoys independence and autonomy in the performance of its duties and was duly appointed by the Board of Directors of SAGATU ASOCIADOS COMERCIAL HOTELERA, S.L.U., the Group's parent company, with such appointment being communicated to the Anti-Fraud Office of Catalonia in the manner and within the timeframe established by law.

This Policy will be reviewed and/or amended by the COMPLIANCE COMMITTEE, which may outsource the service to specialized professionals:

1. Whenever relevant changes occur in the organization, in the control structure, or in the entity's operations that so warrant.
2. Whenever legal changes make it advisable to do so.
3. Whenever significant violations of its provisions come to light that likewise warrant such action.

This Policy will be reviewed at least once every two years, even if none of the circumstances described above occur.

9. APPROVAL

This Internal Information System Policy has been approved by the Board of Directors of Sagatu Asociados Comercial Hotelera, S.L.U. and may be amended to improve confidentiality and the effectiveness of the management of communications.

10. APPENDICES

Appendix 1) Compliance Committee and System Officer:

MEMBERS OF THE COMPLIANCE COMMITTEE AND OFFICER RESPONSIBLE FOR THE INTERNAL REPORTING SYSTEM
POSITION
Legal Department, Member of the Compliance Committee
Finance Department, Member of the Compliance Committee
Human Resources Department, Member of the Compliance Committee
CEO, Chairman of the Sercotel Group, and Member of the Compliance Committee; Compliance Officer and Designated Representative to the SII

11. VERSION HISTORY

Version	Date	Approved by	Reason for Change
Original V.	09/09/2021	Compliance Committee	
V.1	07/19/2023	Compliance Committee and Board of Directors of Sagatu Asociados Comercial Hotelera, S.L.U.	Adaptation to Law 2/2023
V.2	10/04/2023	Compliance Committee	Change of Registered Office
V.2	12/16/2024	Compliance Committee	Text Review
V.2	01/29/2025	Board of Directors of Sagatu Asociados Comercial Hotelera, S.L.U.	Text review