Reporting Policy

Procedure for the referral and management of complaints regarding potential breaches of legal regulations and the Code of Conduct.

1. Introduction

This Reporting Policy or Procedure for Using the Whistleblower Channel was created in accordance with the guidelines set out in Section 301 of the Sarbanes-Oxley Act, initially adopted in 2004 with the initial purpose of managing the reception, custody and processing of complaints, in a confidential and anonymous manner, of information in good faith, about conduct contrary to the company's policies.

As a procedure subject to constant review, in accordance with the provisions of Law 2/2023 of February 20 regulating the protection of persons who report regulatory violations and the fight against corruption, the governing bodies of the Cox group have approved this updated version.

2. Code of Conduct

The Company's Code of Conduct (including the parent company and its subsidiaries), available on the corporate website and intranet, requires each and every employee of the Company, whether directors, officers or employees, regardless of location, position and company in which they provide their services, to comply with the principles of professional and ethical conduct both at a business and personal level in the performance of their duties and responsibilities. It is the responsibility and obligation of all of the above to comply with the Code and to report any potential breaches in accordance with this Reporting Procedure.

3. Internal Information System

The Internal Information System is the set of channels through which the company enables the communication of alleged or potential legal violations that may have been committed by any member (employee, operator, directors and administrators) of the company, together with the policies and procedures that regulate this process. It is integrated into the Common Management Systems of the group and consequently affects all subsidiary companies and all employees.

There is an Information System Manager, responsible for handling communications, maintaining contact with the reporting person, carrying out the relevant investigation procedure and preparing a report to the Resolution and Execution Body, which will be responsible for its assessment and taking appropriate measures.

The designated Responsible Party is a collegiate body, made up of the Director of Internal Audit and the Director of Compliance, with shared responsibility, delegating ordinary operations to the former.

The principles governing the Internal Information System are as follows:

- Accessibility : The Channel is public, secure, confidential and easily accessible to users.

- Good Faith : It is assumed that the informant acts in good faith and that his or her communication is based on facts or indications that can be reasonably and well-foundedly proven to indicate that conduct not permitted by legal regulations and the Company's Code of Conduct has been carried out. Any person who makes a complaint regarding a breach or alleged breach of the Code, or in relation to any current legal regulation, must be acting in good faith and have reasonable grounds to confirm that the information provided is true.

- Whistleblower Protection : guaranteed in all cases and for any communication, regardless of its content and format, including the confidentiality of the sender's data, the process and the absence of retaliation.

- Confidentiality : the identity and content of the communication will be considered confidential information and may not be revealed or disclosed without the consent of the informant.

- Presumption of innocence and right of defence: the right of defence will be preserved, providing clear and sufficient information to the person potentially involved in the reported facts, allowing them to know them and help in the investigation under the principle of their presumption of innocence.

- Impartiality and objectivity : the communication will be processed by the System Manager who can perform his/her function without bias, independently and autonomously.

- Transparency : the Internal Information System acts as a tool to guarantee transparency and fosters the trust of its stakeholders in the organization.

- Conflict of interest : if any person participating in the research process may be implicated or conditioned in their performance, they will abstain from participating in said process and will be replaced by a person of similar status who can perform the function with all guarantees. The collegiate nature of the body of the System Manager guarantees this condition a priori.

- Prohibition of retaliation : This Procedure aims to encourage and promote employees to report potential breaches of current regulations. Consequently, and for its own good, the company guarantees that no retaliation of any kind,

direct or indirect, labor, economic, etc., will be taken against those persons who exercise their right to information in good faith.

- Manifestly false complaints will be dealt with ex officio in a new file, under the same principles of this Procedure and will be considered a serious disciplinary offence.

- However, this measure may be suspended in those cases in which it is clear that the complainant is not an employee of the company or has filed a legal complaint, claim or similar claim against the company or any of its employees in any of the areas of jurisdiction: criminal, civil or labor, prior to his/her complaint under this procedure.

- Likewise, this guarantee may not be invoked in the event that the company has filed, prior to receiving the complaint, a lawsuit or legal claim of any kind against the employee.

4. Scope of Application

Through the Internal Information System, information can be obtained about any of the areas of activity, departments and centres of all companies belonging to the group.

In compliance with the provisions of Law 2/2023, the informant may make his/her communication in the following ways:

A) Confidential Communication

This is a communication in which the user provides his or her personal data. This information will be handled only by the personnel in charge of managing the information, guaranteeing the confidentiality of all communications and data transferred. Communications of information and research will be carried out through the email or telephone number provided, facilitating this process. The conversation may be recorded or transcribed confidentially.

The notification may be:

- Written: in written format, with the possibility of adding audio files, images or videos that are deemed appropriate and always having been obtained and justified in a lawful manner.

- Verbal: communication via voice note, in which the reasons and any relevant facts are orally detailed, or by calling the telephone number provided for this purpose or, failing that, the System Manager, during working hours to convey the communication, request information, or arrange an in-person appointment.

In Person: It is possible to arrange a face-to-face meeting with the Information System Manager where the communication can be made in person. This meeting will be held within 7 working days following the communication.

B) Anonymous Communication

This is a communication in which it is decided not to provide any personal data regarding the identity of the informant. No personal or contact data is provided and no computer data that allows identification or tracking will be kept. The data sent and the files provided will be encrypted, eliminating all information that allows identification. If technically this is not possible, the related files will be protected with a password, which will only be available to those responsible for the System.

It can also be:

- Written: in written format, with the possibility of adding audio files, images or videos obtained legally and with justification. The data sent is encrypted and the metadata of the files is deleted, making any type of tracking and identification impossible and completely anonymising the communication.

- Verbal: voice note (preferably distorted to make voice recognition impossible, choosing this option on the device. In this case, it will be impossible to carry out communication in person.

Communications should preferably be in Spanish or English and should be addressed to the email address (canal_denuncias@grupocox.com) or in a sealed envelope to the Director of Internal Audit and/or the Director of Compliance.

5. Users and informants

The following legally designated persons may carry out communications:

- Employees of any company in the group.

- Any person who works for or under the supervision or direction (contractors, subcontractors, suppliers, etc.) of any group company.

- Shareholders, participants and members of the management, administration or supervisory body of the company, including non-executive members.

- People whose employment relationship has already ended.

- People on scholarship or people employed during a training period.

- Persons whose employment relationship has not yet begun, in those cases in which information on violations has been obtained during the selection process or pre-contractual negotiation.

Taking into account the configuration as a group of companies under a Common Management System, the persons indicated in the list above may make communications about any of the companies that form part of the group.

External Whistleblower channel: the company has made available to interested third parties (customers, suppliers and other interest groups) an external channel through which they can report any alleged irregularities. The communication channel is located on the group's website (www.grupocox.com).

6. Content material

The material scope of the notifications, complaints or information provided by a user may refer, among others, to the possible or alleged commission of any conduct not permitted in the Code of Conduct, in the Criminal Prevention Policy and in internal procedures, and must include the evidence, indications or explanations on which the communication is based, including:

- Actions contrary to the company's Code of Conduct.
- Human Rights

Collusive practices (anti-competition)

- Practices relating to corruption, money laundering or terrorist financing.
- Accounting or financial information.
- Fraud (alteration of media, forgery, simulation, etc.).
- Conflict of interest and related-party transactions, in accordance with the specific provisions of the ad hoc Protocol.
- Environment
- Disclosure of confidential information, Privacy and Data Protection
- Any type of harassment, discrimination or inequality (race, nationality, colour, sex, gender or condition, disability, religion, etc.), including especially in the digital sphere, in accordance with what is specifically regulated in the ad hoc Protocol.

In accordance with the provisions of Organic Law 10/2022 of September 6, on the comprehensive guarantee of sexual freedom, and article 48 of Organic Law 3/2007 of March 22, for the effective equality of women and men, any conduct by action or omission, personal or collaborative, direct or indirect, by any physical or digital means, that violates sexual freedom and moral integrity at work, especially sexual or gender-based harassment, with any kind of violence, threat, harassment, coercion, express or tacit, temporary or recurrent, or discriminatory based on the foregoing, regardless of sex, gender, racial or ethnic origin, nationality, religion or beliefs, health, age, condition, orientation or identity, disability, marital status, migration, administrative situation or other of a similar intrinsic nature, is expressly included in this protocol.

In accordance with the provisions of Law 4/2023 of February 28, for the real and effective equality of trans people and to guarantee the rights of LGTBI people, and with its same terminology, any conduct by action or omission, personal or collaborative, direct or indirect, by any physical or digital means, that violates the freedom of choice of gender and / or sexual and its corresponding manifestation and moral integrity at work, especially harassment, with any kind of violence, threat, coercion, express or tacit, temporary or recurrent, or discriminatory due to the above, by direct or indirect discrimination, multiple or intersectional, by association or by error, is expressly included in this protocol.

7. Internal Information System Management Procedure

The Director of Internal Audit will notify the sender of an acknowledgement of receipt of the notification received (or of the meeting held) with a copy to the Director of Compliance.

The Administrative Body, or where appropriate, the Audit Committee, is responsible for investigating complaints, and appropriate corrective and disciplinary measures will be adopted based on the investigation carried out. In carrying out any investigation, the Director of Internal Audit is, by delegation, responsible for keeping a written record of all reported complaints that are in the investigation and resolution phase, as well as the allegations received.

a.Processing

All communications received, regardless of their format, subject matter or affected company, will be analyzed by the Controller independently, guaranteeing in all cases the confidentiality of the reporting person.

At this first stage, before classifying the communication, the System Manager will check whether there is a conflict of interest derived from its content. In such case, he will inform the Joint Manager and the Resolution Body so that he can abstain and be relieved by a suitable person who can perform the function guaranteeing the principles on which the Internal Information System is based.

Subsequently, the report will be assigned an identification code that will be incorporated into the System's management system. At the same time, the communication will be classified based on the affected company and subject matter. It may also be classified based on its importance and processing status, updated as the process progresses.

The following will be considered of greater relevance:

- Situations that give rise to criminal liability of the company or its directors, in addition to those crimes related to bribery and corruption;

- Situations in which there may be a risk of non-compliance with current legislation;
- Situations that, if revealed, could cause damage to the image or reputation;
- Situations that affect the continuity of the business and operation of the organization;
- Materiality;
- Number of people, locations or departments potentially affected;

Communications related to situations of discrimination or harassment of any kind (religious, racial, sexual, disability or gender or condition) will belong to group 1 in all cases.

The initial assessment may be modified as the investigation progresses, documenting and associating its justification and motivation with the file.

b. Preliminary analysis

Once the communication has been received and classified, the System Manager will determine whether or not it should be processed, assessing whether it meets the minimum requirements for this. This will be considered based on the viability of the information provided and the sufficiency of information to verify the facts. In any case, the decision will be documented and justified.
If the information affects more than one company, it will be processed jointly, carrying out the coordination activities that are considered appropriate.

c. Research

Once the communication has been processed, the System Manager will proceed to investigate, verify and analyse the facts. He may request the collaboration of the personnel, areas and departments that are considered necessary to clarify the situation. This procedure will be carried out in all cases under the principle of presumption of innocence.

d. Closure and Resolution.

Following the conclusion of the investigation phase , the System Manager will prepare a Closing Report which will provide sufficient information on the entire communication process, up to its conclusion. This Report will be forwarded to the Resolution Body for its assessment, which will be reflected in a Final Report. This Final Report may, based on the Resolution Body's assessment:
- Archive the case if the existence of the infringement is considered unproven.
- Consider the existence of an infringement to be proven, referring it to the Resolution Body, which, after analyzing the report, will make the decision on the case and carry out the appropriate actions, informing the affected Area and, in the event of disciplinary measures, the Human Resources Area, with the Resolution Body itself being able to execute its resolution.

e. Conservation of information

Every procedure, from the receipt of the communication, will have a maximum response period of three months, within which the phases detailed above will be carried out. Only in cases of extreme complexity, and with proof of this, may this period be extended for three more months. All phases of the procedure, as well as this Policy as a whole, will follow the provisions of Law 2/2023, of February 20. The information and file of the communication will be kept in accordance with the applicable legal requirements, following in all cases the precepts relating to the processing of personal data. It will be sent, if required by public administrations, courts and tribunals in the terms established by law, only within the limitation period of the actions that may be carried out as a result of the communication.

f. Protection of the whistleblower

The Internal Information System is governed by the principles of confidentiality, respect and legality. Based on this, any person who exercises his or her right to internal communication in good faith and in a proper manner will enjoy the protection established by current legislation.

The Internal Information System is designed to allow any informant who prefers to remain anonymous to do so, guaranteeing this. If the informant prefers to provide his or her identity, his or her anonymity will also be guaranteed, with no reference to his or her identity or data that could be identifying. If the informant's data becomes known for reasons beyond the proper processing of the System, the System Manager will inform the Compliance Director and the Human Resources Director, in order to carry out an analysis and continuous monitoring to maintain the employee's job stability.

Any action taken against a whistleblower that could be understood as a threat, discrimination, retaliation or coercion for speaking out will be considered a labor violation, in addition to any possible crimes that it could entail.

8. Advertising

The Management Body will promote and ensure the proper dissemination and knowledge of this Policy and the Internal Information System, without prejudice to the obligation of employees to know and act in accordance with legal and internal regulations in the performance of their work activity and functions.

9. Entry into force

This Policy comes into force upon its approval by the Board of Directors.

10. Contact Information

Web/Intranet:

www.grupocox.com
Email:
canal_denuncia@grupocox.com

Director of Internal Audit
Mr. Andres Fernandez Romero
andres.fernandez@grupocox.com
Palmas Altas Campus
Solar Energy Street 1 Building D - 3rd Floor
41014 Seville (Spain)

Chief Compliance Officer
Mr. Miguel Angel Jimenez-Velasco Mazario
majimenez@grupocox.com
Palmas Altas Campus
Solar Energy Street 1 Building D - 3rd Floor
41014 Seville (Spain)

11 Approval, validity, interpretation

This document enters into force upon approval by the Board of Directors and will remain in force until updated, revised or repealed. The current version, revised in September, 29th 2024, is the current one, approved by the Board on November, 21st 2024..

This policy must be kept up to date and may be reviewed annually, and on an extraordinary basis, whenever there are changes in the strategic objectives or applicable legislation, with the Compliance Director submitting a proposal for modification to the Appointments and Remuneration Committee, and from there to the Board of Directors.

Cox ABG Group, SA COX Group		
Policy	• Whistleblower Channel Proc	
Responsible	• Board of Directors	
Area	• Corporate – Regulatory Compliance	
Version	Date / Approval	Changes
1	September 29, 2024 / Nov 21, 2024	majv/afr