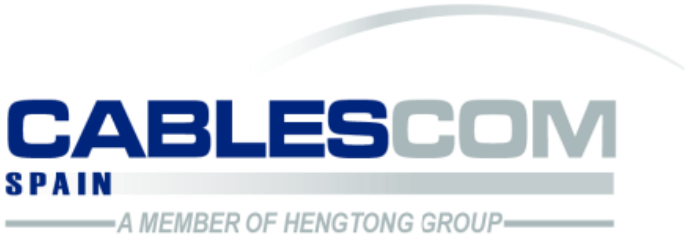

INTERNAL REPORTING SYSTEM POLICY

OF CABLES DE COMUNICACIONES DE ZARAGOZA, S.L.

JULY 2023

Contents

1. OBJECTIVE OF THE INTERNAL REPORTING SYSTEM POLICY

The company CABLES DE COMUNICACIONES DE ZARAGOZA, S.L. (hereinafter, "**CABLESCOM**" or the "**Company**"), in accordance with the provisions of Spanish Act 2/2023, of 20 February, on the protection of persons reporting regulatory breaches and the fight against corruption [*Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*] (the "Whistleblower Protection Act"), has implemented an internal reporting system that any member of the Company or any third party outside the Company who knows of or suspects a regulatory breach committed by a member of the Company or by third parties in contact with it within the framework of their employment or professional activities can report it internally, either anonymously or identifying themselves.

The internal reporting system may also be used to send CABLESCOM any queries related to the scope, compliance and interpretation of the regulations applicable to CABLESCOM.

CABLESCOM embraces all the principles included in the Whistleblowing Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law and in the Whistleblower Protection Act and, to emphasize that commitment, it approves this *Internal Reporting System Policy*, the provisions of which are complementary to those contained in *Procedure for Managing, Investigating and Responding to Reports Received through the Internal Reporting System* ("MIR Procedure").

The purpose of this Policy is to establish the general principles of CABLESCOM's internal reporting system, the rights of whistleblowers, and the procedure that regulates how the internal reporting system officer may be informed of the facts relating to the matters referred to in the following section on material scope of application.

2. MATERIAL SCOPE

This Policy protects individuals who report, through any of the procedures envisaged in it:

1. Actions or omissions that may constitute a **breach of EU law** as defined by the Whistleblower Protection Act.

2. Actions or omissions that may constitute a **serious or very serious criminal or administrative offense.** In any case, any serious or very serious criminal or administrative offenses that involve a financial loss for the Public Treasury and Social Security will be considered included.

In addition, the internal reporting system may also be used to report issues relating to the following matters, although in these cases neither the whistleblower nor the report will enjoy the protection granted in the Whistleblower Protection Act and in this Policy:

3. Report any actions or omissions that may constitute a **breach of internal regulations** of the Company — which do not constitute a breach of EU law or a serious or very serious criminal or administrative offense —.

4. Submit **any queries** related to the scope, compliance and interpretation of the applicable regulations CABLESCOM.

Therefore, any reports strictly related to labor issues or human resources policies (career development, remuneration, holidays, for example) or related to professional performance are **excluded** from the material scope of the internal reporting system. In those cases, the matter will be referred, if applicable, to the Human Resources Department.

The process of notifying reports through the internal reporting system must not be used to report **events that pose an immediate threat to life or property.** When emergency assistance is required, the situation must be reported to the emergency services.

3. PERSONS AFFECTED

This Policy extends, in addition to the directors, officers and employees of CABLESCOM, to other employees such as volunteers, interns, workers in training, candidates in the selection process, workers who have concluded their employment or business relationship and workers' representatives, as well as to any person working for or under the supervision and direction of contractors, subcontractors and suppliers, and to the shareholders of CABLESCOM.

The protection measures envisaged in this Policy shall also apply, where applicable: (i) to individuals who, within the organisation in which the reporting person provides services, assist the reporting person in the process; (ii) to individuals who are related to the reporting person and who may suffer retaliation, such as co-workers or family members of the reporting person; and (iii) to legal entities, for whom the reporting person works or with whom the reporting person has any other relationship in an employment context or in which the reporting person has a significant shareholding.

In addition, CABLESCOM's internal reporting system may also be used by CABLESCOM's customers who have knowledge or suspicion of a regulatory breach, and will be subject to the level of protection that the Whistleblower Protection Act expressly provides in relation thereto.

4. OBLIGATION TO REPORT BREACHES

Any member of CABLESCOM or a non-member third party who has relationships with the Company within the framework of its professional activity (in the terms set out in section 3 of this Policy), who is aware of any breach committed by any other member in an

employment or professional context, must immediately communicate it through any of the channels established for this purpose, without fear of being subject to any type of reprisals (in the case of those who are part of CABLESCOM this constitutes an obligation).

5. INTERNAL REPORTING SYSTEM OFFICER

The Board of Directors has appointed a collective body to manage the system, comprising:

- Qiang Wang, General Managing
- Isabel Banzo Vinué, Human Resources Director.
- Antonio Jesús Bernal Franco, Financial Director.
- Judit Gracia Leal, Human Resources.

All of them offer adequate guarantees of independence, confidentiality, data protection and secrecy of communications.

This body has decided to delegate to Judit Gracia Leal the specific authority to manage the internal reporting system and to process whistleblowing procedures.

6. INTERNAL REPORTING CHANNEL

CABLESCOM has set up an integrated internal reporting channel via the e-mail address provided for this purpose: buzon.comunicaciones@cablescom.com

Additionally, the whistleblower may request the person responsible for the system to hold a face-to-face meeting to submit the communication verbally, which must be held within a maximum period of seven days from the request. The meeting must be duly documented in one of the following ways:

- By means of a recording of the conversation in a secure, durable and accessible format –prior warning to the informant that the communication will be recorded, informing him/her of the processing of his/her data in accordance with the provisions of the regulations in force; or

- by means of a complete and accurate transcription of the conversation by the staff responsible for processing it. In addition, the whistleblower will be offered the opportunity to check, rectify and accept the transcription of the conversation by signing it.

Whistleblowers may also file reports **anonymously** or **identifying themselves.**

Any reports made must contain, as far as possible, the following aspects:

i. **First name and surname** of the person(s) to whom the facts and/or conduct being reported are attributed.

ii. **Date** of the facts and **maximum information** available on them.

iii. **Eventual documents** or other means of evidence within its reach that can prove the reality of the facts or conduct reported.

Beyond the above, any formal communication by a judicial body or a public authority will be considered a valid means of taking note of a breach.

In the event of a **conflict of interest**, i.e., the person affected by the report is one of the members of the system management body, the whistleblower may direct the report to the attention of any of the other members of the system management body or the Compliance Department, which will then assume, provisionally and for the sole purposes of managing this breach, the functions of the system officer. The same will apply when the system officer cannot address a specific matter, in which case they will be removed from all the processes in relation to it.

7. EXTERNAL WHISTLEBLOWER AND PUBLIC DISCLOSURE CHANNEL

Although the internal reporting channel is the preferred channel for reporting actions and omissions constituting a breach of EU rights or a serious or very serious criminal or administrative offense, any individual may go directly to the external whistleblower channel created by the Independent Whistleblower Protection Authority, and the competent regional authority, if applicable.

Furthermore, public disclosure of information on actions or omissions established within the scope of the Whistleblower Protection Act —i.e. actions and omissions constituting breach of EU rights or a serious or very serious criminal or administrative offense— will also entail protection of the whistleblower, if they have first communicated through internal or external channels, or directly by external channels, and appropriate measures have not been taken within the established period, and the requirements established in the following section are also met.

8. WHISTLEBLOWER PROTECTION

Within CABLESCOM, persons who report or disclose offenses **enjoy all the protection rights** envisaged in this Policy and in *MIR Procedure*, if:

1. They have reasonable grounds to believe that the information they communicate to CABLESCOM is true at the time of the report, and that this information falls within the material scope of the Policy.

2. They have submitted the report or disclosure in accordance with the requirements envisaged for this purpose by CABLESCOM and this Policy.

Persons who have reported or publicly disclosed information on actions or omissions referred to in the Whistleblower Protection Act anonymously, but who have subsequently been identified and meet the conditions envisaged in this section, will be entitled to protection as provided in this Policy.

Persons reporting to the relevant EU institutions or bodies on infringements within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019 will be entitled to protection under the Whistleblower Protection Act and this Policy.

On the contrary, persons who report or disclose the following **will not enjoy the protection** envisaged in this Policy and in the MIR Procedure:

1. Information contained in reports that have not been admitted for any of the following reasons:

    a. Where the events described are untrue.

    b. Where the facts outlined do not constitute an infringement of the legal system within the scope of the Whistleblower Protection Act or the material scope of this Policy.

    c. When the report is clearly unfounded or there are, in the opinion of the system officer, reasonable grounds to believe that it was obtained by committing an offense. In the latter case, in addition to not being admitted, a detailed list of the events considered to constitute an offense will be sent to the Public Prosecutors Office.

    d. When the report does not contain new and significant information on breaches subject to a previous report in respect of which the corresponding procedures have been concluded, unless new factual or legal circumstances arise that justify a different approach. In these cases, the system officer will notify the decision providing reasoning.

2. Information relating to claims for interpersonal conflicts or concerning only the whistleblower and the persons to whom the report or disclosure relates.

3. Information that is already fully available to the public or that constitutes a mere rumor.

4. Information relating to actions or omissions not included in the material scope of this Policy.

Non-admission of the report filed through the appropriate channels established will be communicated to the whistleblower within five business days, unless the report is anonymous or the whistleblower has waived receiving communications relating to the procedure.

9. PROHIBITION OF REPRISALS

CABLESCOM will take the necessary measures to prohibit any act constituting reprisals, including threats of reprisals and attempted reprisals, against the persons submitting a report regarding actions or omissions included in the material scope of this Policy.

Reprisals refers to any actions or omissions that are prohibited by law or that, directly or indirectly, entail unfavorable treatment that places the people who suffer them at a particular disadvantage compared with another in the employment or professional context, solely due to their status as whistleblowers, or because they have made a public disclosure.

For the purposes of this Policy, the following are considered reprisals:

1. 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 probation period has elapsed.

2. Early termination or cancellation of agreements for goods or services.

3. Imposition of any disciplinary measure, demotion or denial of promotions, and any other material modification of working conditions.

4. Failure to convert a temporary employment contract into an open-ended one, if the worker had legitimate expectations that they would be offered permanent work.

5. Harm, including reputational damage, economic losses, coercion, bullying, harassment, and ostracism.

6. Negative assessments or references regarding their work or professional performance.

7. Inclusion in blacklists or dissemination of information in a given sector that impedes or hinders access to employment or the contracting of works or services.

8. Denial or cancellation of a license or permit.

9. Refusal of training.

10. Discrimination, or unfavorable or unfair treatment.

The measures included in paragraphs 1 to 4 above will not be considered reprisals when they are performed exercising management authority as normal under the employment or regulatory legislation governing the relevant civil servants statute, due to circumstances, events or proven infringements, and note related to the submission of the report.

Furthermore, it is recorded that any person whose rights are harmed due to their report or disclosure after two years have elapsed may request the protection of the competent authority that, exceptionally and on a justified basis, may extend the protection period, following a hearing of the persons or bodies concerned (the denial of that extension of the protection period must be reasoned).

In addition, the whistleblowers may access, as applicable, the following support measures to be provided by the Independent Whistleblower Protection Authority and/or competent regional body.

10. MEASURES TO PROTECT AGAINST REPRISALS

CABLESCOM will take the necessary measures to ensure that whistleblowers are protected against reprisals. The main protection measures envisaged in both the Whistleblowing Directive and the Whistleblower Protection Act, to which CABLESCOM adheres and agrees to facilitate its effective application:

1. Any person who provides information on the actions or omissions referred to in points 1 and 2 of section 2 of this Policy or who makes a public disclosure in accordance with the Whistleblower Protection Act will not be considered to have infringed any restriction on disclosure of information and will not be held liable in any way in relation to that communication or public disclosure, if they have reasonable grounds to believe that the communication or public disclosure of that information was necessary to disclose an action or omission under this Policy. This measure will not affect criminal liability.

   The preceding paragraph extends to the disclosure of information made by workers' representatives, even if they are subject to legal obligations of secrecy or to the non-disclosure of confidential information. This is without prejudice to the specific rules on protection applicable under labor law.

2. The whistleblower will not be liable for the acquisition or access to the information that is reported or publicly disclosed, provided that such acquisition or access does not constitute an offense.

3. Any other potential liability of whistleblowers arising from actions or omissions that are not related to communication or public disclosure or that are not necessary to

disclose a breach under the Whistleblower Protection Act will be enforceable in accordance with the applicable law.

4. In proceedings before a court or other authority relating to the harm suffered by the whistleblowers, once the whistleblower has reasonably demonstrated that they have reported or made a public disclosure in accordance with the Whistleblower Protection Act and that they have suffered harm, the loss will be presumed to have occurred as a reprisal for who report breaches or for making a public disclosure. In those cases, it will be for the person who took the damaging measure to prove that that measure was based on duly justified grounds not connected with the communication or public disclosure.

5. In court proceedings, including proceedings relating to libel, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of business secrets, or to claims for compensation based on labor or statutory law, the persons filing a report in accordance with this Policy and the Whistleblower Protection Act will not be held liable in any way as a result of communications or public disclosure protected by that Act. Those persons will have the right to plead in their defense in the framework of those court proceedings that they have reported or made a public disclosure, provided that they have reasonable grounds to believe that the communication or disclosure was necessary to disclose a breach under the Whistleblower Protection Act.

11. PROTECTION MEASURES FOR PEOPLE TO WHOM THE REPORT RELATES

CABLESCOM will ensure that the persons to whom the report relates are heard within the framework of the internal investigation, are entitled to the presumption of innocence, the right to a defense and the right of access to the procedure in accordance with the Whistleblower Protection Act.

Likewise, the identity of the person to whom the report of breach relates will be protected and treated confidentially, as will the facts reported, in the same way as the identity of the whistleblower themselves, always with the limits and exceptions necessary to ensure the proper completion of the investigation, or any communication to the competent authorities.

12. SANCTIONS

The sanctions that may be imposed in each case shall be those provided for in the Workers' Statute, in the applicable Collective Bargaining Agreement or in the applicable labour legislation and shall be graduated according to the seriousness of the acts committed, and may take into consideration circumstances such as the damage caused, the victims'

circumstances, if any, etc. Additional measures may also be taken in addition to disciplinary measures, including appropriate complaints or the reporting of the facts to the appropriate administrative, police or judicial authorities.

In addition to possible labour disciplinary offences and sanctions, the Independent Whistleblower Protection Authority may impose fines of up to 300,000 euros for conduct such as the following:

1. Prevent or attempt to prevent reports or thwart or attempt to thwart their follow-up.

2. Take reprisal measures against whistleblowers.

3. Promote abusive procedures against whistleblowers.

4. Breach their duty to maintain confidentiality as regards the identity of the whistleblower or the persons involved in the report, and their duty of secrecy as regards any information related to the report filed.

5. Communicate or publicly disclose information knowing that it is false.

13. CONFIDENTIALITY

Despite the other sections of this Policy, CABLESCOM guarantees the confidentiality of the identity of the whistleblower and any third party referred to in the report and of the actions performed in the management and processing of the report, and the protection of data, preventing access by unauthorized personnel.

Accordingly, access to the data relating to the report is limited to those members specifically authorized by CABLESCOM to receive, monitor or resolve the reports received, and the third parties (for example, a judicial authority, the Public Prosecutors Office or the competent administrative authority) when it constitutes a necessary and proportionate obligation imposed by applicable regulations, in the context of an investigation performed by national authorities or within the framework of court proceedings, and, in particular, when the disclosure seeks to safeguard the right of defense of the person concerned.

In any case, except in the cases envisaged, CABLESCOM guarantees that no unauthorized person knows the identity of the whistleblower or any other information that may help to directly or indirectly infer their identity. Specifically, CABLESCOM guarantees that the person to whom the events described refer will in no case be informed of the identity of the whistleblower or, as applicable, of the person who made the disclosure.

CABLESCOM will also take care to ensure the confidentiality of the data and facts provided when the report is sent through whistleblower channels other than those established or to personnel not responsible for processing it. As part of this, CABLESCOM has adequately

trained its staff in this area and has warned about breaches of the duty of confidentiality and also the establishment of the obligation of the recipient of the report to send it to the system officer immediately.

In compliance with the above, CABLESCOM has implemented technical and organizational measures in the internal channel to preserve the identity and ensure the confidentiality of the data corresponding to the persons concerned and any third party mentioned in the information provided, particularly the identity of the whistleblower if they have identified themselves.

In relation to the persons affected by the report, CABLESCOM guarantees that, during the processing of the procedure, the persons affected by the report will be entitled to the same protection established for the whistleblowers, preserving their identity and ensuring the confidentiality of the facts and data of the procedure.

In turn, those who receive public disclosures have the same obligations described above, and under no circumstances will they obtain data that allow the whistleblower to be identified and they must have adequate technical and organizational measures.

Disclosures made under this section will be subject to the safeguards established in the applicable regulations and, in particular, the whistleblower will be informed before disclosing its identity, unless that information could compromise the investigation or court proceedings. When the competent authority notifies the whistleblower, it will send a letter explaining the reasons for the disclosure of the confidential data in question.

In any case, CABLESCOM will ensure that the competent authorities that receive information on breaches that includes trade secrets do not use or disclose them for purposes beyond what is necessary to correctly monitor the actions.

14. DATA PROTECTION

The personal data processed under this Policy and the *MIR Procedure*, including the exchange or transfer of personal data with the competent authorities, will be processed by CABLES DE COMUNICACIONES DE ZARAGOZA, S.L., with registered office at CALLE D (POLIGONO INDUSTRIAL MALPICA), 83, 50016 ZARAGOZA, as data controller in accordance with personal data protection regulations.

CABLESCOM has appointed a Data Protection Officer who can be contacted through dpo@cablescom.com.
The personal data provided through the internal system will be processed to receive and analyze the actions or omissions reported and, where applicable, decide whether to initiate an investigation into the facts reported. In addition, some information may be processed to provide evidence of the system's operation. In the latter case, CABLESCOM guarantees that the information stored as evidence will be anonymized.

If information is received that is not necessary to process and investigate the actions or omissions referred to in section 2 of the Policy, the data controller will immediately erase it. Furthermore, any personal data that may have been communicated and that relate to conduct that does not fall within the scope of the Whistleblower Protection Act and this Policy, and any information or part of it that is proven to be false will also be deleted, unless that lack of veracity may constitute a criminal offense.

The data controller will process the personal data provided by the whistleblower in compliance with a legal obligation, specifically, in compliance with the Whistleblower Protection Act. In addition, in the case of verbal reports, the whistleblower's consent to document that report, including in the case of face-to-face meetings, telephone calls or voice messages. In turn, the processing of sensitive data may be performed by the data controller for reasons of substantial public interest in accordance with Article 9(2)(g) of Regulation (EU) 2016/679.

The personal data collected through the internal channel will be stored in accordance with applicable law. Specifically, these data will be stored exclusively for the time necessary to decide on the appropriateness of initiating an investigation into reported facts, which, in any case, may not be for more than three months from receipt of the report. However, if it is necessary to process the personal data for longer to continue the investigation or, where applicable, because it is considered necessary to initiate the appropriate legal actions, the data will be stored, in an environment other than the internal channel, as necessary for CABLESCOM to conclude the investigation or to exercise the corresponding actions.

To comply with the purposes described above, the data controller may facilitate access to the personal data to:

(i) Third-party service providers, such as external advisers and collaborators who provide support in the management or, where applicable, investigation of reports received through the internal channel.

(ii) The relevant areas or departments for processing the report and, where applicable, investigating and adopting possible measures as regards the reported conduct, where necessary.

(iii) The personal data may also be transferred to the courts, the Public Prosecutor's Office, and the competent public authorities as a result of the investigation that may be initiated.

In connection with the above, on certain occasions, CABLESCOM may transfer the data provided to third countries located outside the European Economic Area (in particular, the group's parent company) for matters related to the existing employment relationship between the parties. In these cases, CABLESCOM has adopted the necessary measures to send the information anonymized and/or previously authorized, to provide appropriate protection to personal data.

If the data subject has any doubts or would like to obtain more information about the international transfer of his/her data, he/she can contact CABLESCOM at the following address dpo@cablescom.com

Moreover, the data subject is informed that, under the conditions established in the applicable regulations, it may exercise the rights recognized in the data protection regulations by sending, to the attention of the Data Protection Officer, a letter to the registered office or an email to the following address: dpo@cablescom.com

However, CABLESCOM informs that, if the person to whom the events described to in the report pertain or to whom the disclosure refers exercises the right of objection, it will be presumed that, unless there is evidence to the contrary, there are compelling legitimate grounds for processing their personal data.

Without affecting the rights corresponding to the whistleblower, in accordance with data protection regulations, if the report has been sent verbally, CABLESCOM offers the opportunity to verify, rectify and accept by signing the transcription of the conversation through the following address: dpo@cablescom.com.

Data subjects may also lodge a complaint with the Spanish Data Protection Agency (www.aepd.es).

The system officer will periodically review the proper functioning of the internal reporting system and the provisions of this Policy.

15. BASIC PRINCIPLES OF THE MIR PROCEDURE

The MIR Procedure is governed by the following principles, which shall be observed during the handling of any case:

- **Confidentiality**: The MIR procedure shall guarantee the confidentiality of the identity of the whistleblower, of any third party mentioned in the report and of the data relating to the incident reported, except for communication to the judicial authority, the Public Prosecutor's Office or the competent administrative authority in the context of a criminal, disciplinary or disciplinary investigation.

- **Impartiality:** The internal reporting system officer must be bound by the principle of impartiality in all cases, treating all communications in the same way, independently of the persons involved and avoiding any kind of conflict of interest.

- **Independence of the internal reporting system officer**: The person in charge of the system shall enjoy full independence and autonomy to agree the practice of the proceedings that she deems necessary to clarify the facts reported, pursuing in all cases the search for the truth.

- **Documentation:** Each communication will give rise to a file, in which the person responsible for the system will include detailed documentation of the entire investigation procedure.

- **Good faith:** The provisions of the MIR Procedure and this Policy shall be interpreted in accordance with the principles and requirements of good faith.

16. RECORD OF REPORTS

CABLESCOM will keep a record of all reports and queries it receives through the internal reporting system, collected in a "record book," complying at all times with the confidentiality requirements established, and for the time strictly necessary and proportionate to comply with EU legal and regulatory requirements.

APPENDIX I. APPROVAL AND AMENDMENTS

Version number	1
Party responsible	System manager
Date of first approval	June 2023