Internal Information System Policy

Approved by the Board of Directors of

CELSA STEEL S.A. on 28 January 2025

Important information about this document	
Identification of the Policy	*Internal Information System Policy*
Global or national implementation policy	Global
Rules it replaces	Whistleblower Protection Policy
Rules it repeals	None
Related standards	*Incoming communications management procedure*
Business unit or function concerned	All business units and functions of the *CELSA* Group
Staff concerned	All *Organisational Members and Business Partners,* as appropriate
Mainly responsible for its monitoring	*Ethics Committee*
Date of approval	28/01/2025
Date of last update	
Date of implementation	28/01/2025

INDEX

1. Definitions 4

2. Purpose of CELSA's Internal Information System Policy 7

3. Communication channels 8

4. Scope of application 10

5. Principles and safeguards of the Internal Information System 11

6. Protection of the parties involved in a *complaint* 14

6.1 Scope of protection 14

6.2. Protection and support measures 14

6.2.1. Protection and support measures for *whistleblowers* and *affected persons* 14

6.2.2. Measures for the protection of *Defendants* 14

6.3. Activation of protection 15

7. Fraudulent or bad faith *allegations* 16

8. Roles and responsibilities 17

8.1. Ethics Committee 17

8.2. Board of Directors 17

8.3. Steering Committee 17

Annex I 18

Annex II 20

1. Definitions

The definitions of those concepts that are frequently used in this document are listed below (quoted in *italics*):

- ***CELSA / Organisation***: for the purposes of the *Criminal Prevention Model,* it will refer to the company CELSA STEEL, S.A. and to the rest of the entities that make up the *Criminal Control Perimeter,* listed in Annex I of the *Criminal Compliance Policy*.
- ***Criminal control perimeter:*** includes the entities adhering to *CELSA*'s *Criminal Prevention Model*, listed in Annex I of the *Criminal Compliance Policy*.
- ***Board of Directors:*** *CELSA*'s governing body, to the extent that it has primary responsibility and authority for activities, governance and policies, and to which *CELSA*'s *Management Committee* reports and is accountable.
- ***Management Committee:*** a group of members within *CELSA,* with management and control functions within the *organisation* at the highest level
- ***Audit and Control Committee****: a* permanent body made up of several members of the *Board of Directors*, of an informative and consultative nature, without executive functions, with full powers of information, advice and proposal within its scope of action, which is responsible, among other duties, for supervising *the Criminal Prevention Model*.
- ***Members of the Organisation***: members of the *Board of Directors*, members of the *Management Committee*, employees, workers or temporary employees or employees under a collaboration agreement and all other persons under the hierarchical subordination of any of the above.
- ***Business partners:*** any legal or natural person, other than *Members of the Organisation,* with whom the *Organisation* has or plans to establish some kind of business relationship. By way of example, but not limitation, this includes installation companies, agents or commission agents, suppliers, external advisors, *joint ventures*, customers and, in general, natural or legal persons contracted by *CELSA* to deliver goods or provide services.
- ***Third party:*** a natural or legal person or body independent of the *Organisation*.
- ***Criminal Prevention Model***: an organisational and management system for the prevention of crime, whose objective is the prevention, detection and management of *criminal risks*, and whose essential basis is represented in the *Criminal Compliance Policy* and in the *Crime Prevention and Response Manual*.
- ***Ethics Committee:*** *CELSA*'s internal collegiate body with autonomous powers of initiative and control, which is entrusted, among other tasks, with the responsibility of supervising the operation and observance of the *Criminal Prevention Model.* The existence of this body responds to the requirements established in Spanish criminal law (article 31 bis of the

Spanish Criminal Code) regarding the supervision of the *Criminal Prevention Model*. Likewise, the *Ethics Committee* performs the role of Head of the Internal Information System.

- ***Procedure for the management of communications received by CELSA:*** document that establishes the necessary mechanisms for the early communication and management of any *infringement*, as well as the necessary procedures for the internal processing of *queries*, and the internal processing and investigation of *complaints* or any known circumstance that should be investigated.
- ***Internal Information System:*** measures adopted in accordance with Law 2/2023 for the management of communications relating to *infringements* of the regulations referred to in this text. The *Internal Information System* has a *System Manager in charge of* the management and diligent processing of the *Communications* received, in accordance with the provisions of *CELSA's Procedure for the Management of Communications Received.*
- ***Communication:*** a statement of a question about the scope, interpretation or compliance with the regulations applicable to *CELSA.* Depending on its content, a communication may consist of a Query or a Report.
- ***Consultation:*** communication by which any *Member of the Organisation* requests a clarification, response or opinion on the scope, interpretation or compliance with the regulations applicable to *CELSA.*
- ***Whistleblowing***: communication regarding a possible *breach* (active or omissive behaviour) of the regulations applicable to *CELSA,* understood as the set of ethical and compliance commitments voluntarily assumed by the *Organisation*, as well as the current legislation applicable to it at any given time.
- ***Infringements:*** behaviour, whether active or inaction, that involves a breach of the regulations applicable to the *Organisation,* including any breach of European regulations and/or serious or very serious criminal, administrative or labour-related offences relating to health and safety at work, established in the Spanish legal system, as well as breaches of internal regulations, including the *Code of Ethical Conduct*, that occur within the *Organisation* or in which the *Organisation* may be involved. An Infringement, depending on its seriousness, may range from a mere formal breach of a requirement included in an internal rule, to the commission of acts constituting a crime potentially attributable to the *Organisation.*
- ***Informant***: a natural or legal person who anonymously or by name files a *Complaint*. The figure of the *informant* includes:
    - *Members of the Organisation*: includes employees whose employment relationship is in force, has ended or has not yet begun, shareholders and members of the *Board of Directors*, paid and unpaid volunteers and trainees.

- *Business partners*, as well as any person working under their supervision and direction: Subjects or legal entities external to the *Organisation*, with which the Organisation has or plans to establish a business relationship, as well as any person working under the supervision and direction of these.
- *Third parties* and other individuals, e.g. trade unions.
- Any person, natural or legal, with a present or future fit in the above contexts.

- ***Affected persons*****:** this figure includes, among others, the following:
  - Witnesses, or other persons involved in the Query *or Report*.
  - Researchers.
  - Family members, trade union representatives, and other persons supporting the Whistleblower.
  - Those from which information is obtained that led to the filing of a Report.
- ***Reported***: natural or legal person(s) linked to the reported *Infringements*, as perpetrators, participants or even accessories. They may be identified in the *Communication* or be specified throughout the process of its management.
- ***Retaliation*****:** any action or omission, whether attempted, threatened or actual, direct or indirect, which may result in harm or disadvantage to the *Whistleblower* or other *Affected Persons*, in the employment or professional sphere, solely because of their status in relation to the Report or because they have performed a public disclosure.
- ***Independent Whistleblower Protection Authority (IPA): an*** independent administrative authority, as a public law entity at state level, which will act in the fulfilment of its main function of protecting *whistleblowers.* Its other functions include the management of its own external channel, the processing of sanctioning procedures and the imposition of sanctions, among others.

2. Purpose of CELSA's Internal Information System Policy

The purpose *of* this *CELSA Internal Information System Policy,* approved by its *Board of Directors*, is to specify the criteria for the use and management of the different communication channels existing in *CELSA* through which *Members of the Organisation*, *Business Partners* and *Third Parties* may submit *Queries* and/or *Complaints* about potential *Infractions* that may arise within the *Organisation* in the course of its activities.

This document details the different channels that can be used for this purpose, ranging from a simple report to the hierarchical manager -who must communicate it to the *Ethics Committee* - to communication through the channels provided by *CELSA.*

All *CELSA Members* have the obligation to report individual or collective behaviours or circumstances that occur in the context of their activities in *CELSA* and that may involve a breach of the content of this text or the other documents that make up the *Criminal Prevention Model* of *the Organisation*, regardless of whether such behaviours have been ordered or requested by a superior.

The purpose of this *Policy*, which sets out the obligation and use of *CELSA'*s *Internal Reporting System*, is to provide advice, certainty and protection to anyone with knowledge of potential *Breaches*. *CELSA* wishes to emphasise that, in any event, *Retaliation* against a Bona Fide *Whistleblower* for making a Query and/or Report is strictly prohibited.

3. Communication channels

Different internal channels are made available to *Members of the Organisation*, *Business Partners* and *Third Parties* so that they can submit any type of *Communication* related to possible *Infringements*.

In particular, the following channels of **written** communication exist:

- The *Ethics Channel* will be available at the following link: https://celsa.integrityline.com/, accessible from the *Organisation's* employee portal and on *CELSA*'s corporate website.
- By Email: comite.etico@gcelsa.com
- By post to the following address for the attention of *the Ethics Committee*:

  C/Ferralla, 12, Pol.Ind. San Vicente,
  08755 Castellbisbal (Barcelona) Spain

It will also be possible to perform a **verbal** *Communication* (in case of Reports or Queries made by *Members of the Organisation*) through the following means:

- By telephone:
  Spain +34 910477636.
  France +33187212291.
  Poland +48221523361.

  The Reporting Party must enter the Access PIN code 9097, corresponding to CELSA, after initiating the call, and may choose to communicate in the official language of the place from which the communication is performed, in English, or in Spanish.
- By means of a face-to-face meeting with the *Compliance Manager* or any other member of the *Ethics Committee*, within seven (7) days of the request. This communication will be previously informed and will be transcribed and the whistleblower will be informed of the processing of his/her data in accordance with the legislation in force.
- Line manager or a member of *CELSA's management,* who should forward the information to the *Ethics Committee*

Verbal communications, including those performed through a face-to-face meeting, by telephone or by voice messaging system, will be documented, subject to the *Informant*'s consent, , and the Informant will be informed of the processing of his or her data in accordance with the provisions on personal data protection.

Regardless of the means of communication used, the *Reporting Person* will receive a six-digit code (Case ID) that must be retained in order to access the secure communication channel through the *Ethical Channel*.

The official channel for receiving information on the status of the *Report* or contacting the *Whistleblower* will be the *Ethics Channel*.

CELSA encourages all *Members of the Organisation* or subjects who suspect or know of *CELSA-related breaches* to use these internal channels to make their *Communications* to *CELSA*.

Any *Consultation* or *Complaint* will be handled by the *Ethics Committee* under the terms developed in this *Policy* and in the *Procedure for handling communications received.*

Furthermore, the *Organisation* informs any potential *Whistleblower* that it also has external channels of information available to the competent authorities and, where appropriate, to the institutions, bodies, organs or agencies of the European Union, such as, among others:

- In antitrust matters: Complaint of prohibited conduct | CNMC
- In the area of tax offences: Tax Agency: Complaints
- In case it is related to subsidies or fraud involving European funds: Anti-fraud mailbox - Complaints channel of the Recovery and Resilience Mechanism - Recovery, Transformation and Resilience Plan Government of Spain (planderecuperacion.gob.es).
- National Anti-Fraud Coordination Service: IGAE:Servicio Nacional de Coordinación Antifraude (hacienda.gob.es)
- Oficina Antifrau de Catalunya: Complaints to the Anti-Fraud Office of Catalonia
- As well as any other competent local authority where CELSA operates.

CELSA also informs potential *whistleblowers* of the existence of a public body called the *Independent Whistleblower Protection Authority*, to which they can also turn.

Most convenient, however, is the use of the internal channels mentioned above as the preferred channel of communication.

Persons who file a Report must collaborate with the *Ethics Committee* in the analysis and investigation phase when required to do so. Likewise, they must maintain due confidentiality regarding the collaboration provided and the facts brought to *CELSA*'s attention. This obligation is also assumed by *CELSA*.

4. Scope of application

This *Policy* is of mandatory application in the *Organisation*. *Policy* applies to the members of the *Board of Directors,* the *Audit and Control Committee*, the *Management Committee* and all professionals who make up *CELSA*, regardless of the companies to which they belong, their place of residence or the place where their activities are carried out.

The *Policy* is also applicable to *CELSA*'s contractors, subcontractors and suppliers, as well as to those persons linked to *CELSA* by a statutory framework, voluntary work, internships, training or who have obtained the information in the context of a selection process or pre-contractual negotiation or an employment relationship that has already ended.

The *Whistleblower* protection measures provided for in this *Policy* shall also apply (i) to the natural persons who assist the *Whistleblower* in the whistleblowing process in the employment context; (ii) to the natural persons related to the *Whistleblower* who may suffer *Retaliation* in the employment context (i.(iii) legal persons related within the meaning of article 3.4.c) of Law 2/2023 of 20 February 23, regulating the protection of persons who report regulatory infringements and the fight against corruption.

Members of the Organisation shall comply with its contents, irrespective of their position and role. Thus, the scope of this *Policy* covers all *Queries* and *Complaints* that may be raised by any *Member of the Organisation*, *Business Partner* and *Third Party*.

It also binds those persons who, even if they are not *Members of the Organisation*, are aware of the existence of any *Infringement* in their professional relationship with *CELSA*.

The material scope of application is set out in **Annex I** of this *Policy*.

5. Principles and safeguards of the Internal Information System

With regard to *Communications* performed by *Members of the Organisation*, *Business Partners* and *Third Parties, CELSA* guarantees the absence of *Retaliation*, discrimination or sanctions for those communications performed in good faith or for those actions aimed at avoiding participation in illicit actions.

In any case, the management of the *Internal Information System* shall always be guided by the following three general principles:

- **Principle of trust and confidentiality:** *CELSA* will handle any reported *Infringement* in an appropriate, serious and objective manner. Likewise, it will manage them in an efficient and transparent manner, avoiding, in any case, infringing the principle of impartiality, as well as independence and autonomy.

  The identity of the *Reporting Person* and the *Reporter*, as well as of any other *Interested Person* in the *Complaint*, is kept confidential.

  Any person entitled to participate in the file, including its investigation, must maintain the confidentiality of the information received or known. They may not, therefore, disseminate to third parties the information known in the exercise of their functions, in particular that relating to personal data.

  The exception to the previous paragraph concerns the need to share information with the persons involved in the case on a *need-to-know* basis in cases where it is strictly necessary and legitimate.

- **Principle of objectivity**: not only the facts and circumstances that establish or aggravate the responsibility of the *Defendant*, but also those that exempt, extinguish or mitigate it will be investigated.

  Investigators must ensure that they are impartial and objective during the course of the investigation and that they have no personal ties to the suspected persons or any interest in the final outcome.

- **Principle of impartiality:** the handling of *Complaints* and any subsequent investigations shall be performed by appointing persons who have no connection with the activities or business affected. Likewise, care shall be taken to ensure that they do not have any relationship with the persons affected, other than strictly professional. It is understood that there is a relationship that transcends the professional if *CELSA* is aware of the existence of a relationship of friendship or personal relationship that exceeds the professional relationship, which may violate the required impartiality.

  Therefore, the treatment of facts and persons shall be performed in a neutral and objective manner.

In addition and during the practical management of *Communications*, attention will also be paid to the following principles:

- **Principle of adequacy and sufficiency:** *CELSA* will assign to the resolution of the case all the means deemed adequate and sufficient to comply with the purposes of the investigation, given the circumstances of the case, so that there is traceability of the deliberation process adopted by the *Organisation*, and it may be able to justify the measure to any *Third Party*.

- **Principle of subsidiarity or ultima ratio**: if a less harmful channel of communication can be used, *CELSA* will resort to the least invasive option given the circumstances of the case.

  Notwithstanding the above, *CELSA* may, subject to the relevant legal safeguards, take immediate and interim measures until such time as the matter in question is properly resolved. Once the proceedings have been completed, the measures may be continued or discontinued.

- **Principle of presumption of innocence:** any *Reported Person* has the right to be treated as innocent until, where appropriate, the commission of an *Infringement* is established and a sanction is imposed.

- **Principle of compliance with applicable regulations:** all the goodness of the corporate strategy would be undermined if the methods used were unlawful. *CELSA* is committed to respecting the rights of *Affected Persons* to be heard and to provide information to those affected. Persons complained of facts that may be under investigation have the right to file it.

- **Protection of Bona Fide *Informants*:** *CELSA* safeguards the guarantees of *Informants*. As a general principle, their identity will not be disclosed beyond the persons responsible for the reception and follow-up of cases, without the explicit and unequivocal consent of the *whistleblower*.

- **Prohibition of *Retaliation*:** *CELSA* does not tolerate any *retaliation* - by action or omission, regardless of whether it is generated in the workplace or in the workforce - against anyone who, in good faith, reports facts that could constitute a *Breach* in accordance with the provisions of this *Policy*, guaranteeing the necessary protection and support from the time of filing the *Complaint* until two years after the end of the investigation.

  However, once the two-year period has elapsed, the *whistleblower* may request protection from the *Independent Authority for the Protection of Whistleblowers*, which may, exceptionally and with justification, extend the period of protection, after hearing the persons or bodies that may be affected.

  This protection applies equally to the *Respondent* and to any other *Person affected by* the *Complaint* process, such as a family member or a supportive partner.

- **Principle of proportionality**: this principle responds to the need for the sanction to be adjusted to the seriousness of the facts, preventing it from being an arbitrary or disproportionate measure. For this purpose, the following principles shall be considered:
    - Adequacy: sanctions must be appropriate to the purpose they justify.
    - Sufficiency: sanctions must be sufficient for their intended purpose.
    - Due process: everyone has the right to be heard and to assert their legitimate claims against those in charge of the investigation.

CELSA will not discriminate against any person on the basis of the *Complaint*. Nor will CELSA take any retaliatory or intimidatory action against them.

Violations of the above principles shall be investigated and, where appropriate, sanctions shall be adopted in accordance with current legislation, including the adoption of provisional measures while the disciplinary proceedings are pending. Such measures may include the removal of persons from the workplace, or any other measure deemed appropriate in view of the circumstances.

All protection measures are conditional on the *Whistleblower*'s good faith, understood as the conviction that the communication of the facts of which he/she is aware are truthful. In this sense, *CELSA* will not consider that *Whistleblowers* have infringed any restriction on the acquisition, access or disclosure of information of the *Organisation*, and will not incur any liability of any kind provided that:

- act in good faith;
- and that the access or acquisition of information provided does not in itself constitute a criminal off*ence*.

The protection guaranteed by this procedure extends to the Affected *persons*, among others, to co-workers, family members, witnesses or third parties who intervene for the best resolution of the case, who shall also be required to observe the duty of confidentiality, where appropriate.

6. Protection of the parties involved in a report

The *Organisation* will provide protection and support to both the bona fide *Whistleblower* and the *Affected* Persons against the possible harm that they may suffer as a result of reporting possible *Breaches* of which they have become aware, under the terms contemplated in section 5.2.1 of this *Policy*.

6.1 Scope of protection

The protection of *Whistleblowers* and *Affected Persons* shall extend to all *Retaliation* against them.

Some examples of possible *Retaliation* are attached as **Annex II** to this *Policy*.

6.2. Protection and support measures

6.2.1. Protection and Support Measures for the *Informant* and *Affected Persons*

Protection shall involve taking reasonable steps to prevent harm to, and compromise the confidentiality of, the *Informant* or the *Persons concerned.*

For its part, support will involve encouraging and reassuring the *Reporting Person* or *Persons concerned* about the value of reporting *Breaches* and taking steps to assist their welfare.

On the other hand, if *CELSA* becomes aware that *Retaliation* is taking or has taken place, it will take reasonable steps to stop and address it.

CELSA also informs *whistleblowers* of the existence of additional support measures provided for by current legislation and which will be provided by the *Independent Whistleblower Protection Authority*. Specifically, the following are foreseen:

- Full information and advice on the remedies available against *Retaliation.*
- Effective assistance by the competent authorities.
- Legal assistance in criminal proceedings and cross-border civil proceedings.
- Financial and psychological support if deemed necessary by the *Independent Whistleblower Protection Authority.*

6.2.2. Measures for the protection of the *Complainants*

CELSA also provides for various protection measures for the *Respondents*. In this regard, it will ensure that:

- Maintain the confidentiality of the identity of the *Respondents*, as well as the commitment to protect it throughout the procedure.
- To prevent the *Respondent* from being exposed to reputational damage or other negative consequences during the course of investigations.

- Guarantee the rights of defence of the *Respondent*, including the right to be heard at any time, as well as the possibility to file it and to provide the evidence he/she deems relevant to defend him/herself.
- Allow the *Respondent* to have access to the file in order to be aware of the actions or omissions attributed to him/her and to be informed of the processing of his/her data protection rights.
- Adopt additional remedial measures, in the event that no evidence of violations is obtained, if deemed appropriate by the Organisation.

6.3. Activation of the protection

The protection and support provided to the *Whistleblower*, other *Affected Persons* and *Respondents* will be triggered and start as soon as an *Enquiry* or *Complaint* is received, and will continue during and after the conclusion of the investigation process, and even thereafter for a maximum period of two years from the end of the investigation of the *Breach*.

Once the two-year period has elapsed, an extension may be requested from the *Independent Whistleblower Protection Authority* which, exceptionally and with justification, may extend the period of protection, after hearing the persons or bodies that may be affected.

7. Fraudulent or bad faith *allegations*

The protection and support provided by the *Organisation* will be subject to the *Whistleblower* having made the *Complaint* in good faith.

The *Reporting Person* must have reasonable grounds to believe, in light of the circumstances and the information available to him/her, that the facts he/she reports are true. In this sense, good faith entails reporting with at least reasonable grounds to believe that the information about possible *infringements* reported was true at the time of reporting.

Those who deliberately and knowingly communicate incorrect or misleading information will not be supported and protected by the *Organisation*. In addition, *CELSA* will consider each individual case for the purpose of imposing proportionate disciplinary measures against *Members of the Organisation* or commercial measures against *Business Partners* and *Third Parties* who make a Bad Faith *Disclosure*.

8. Roles and responsibilities

8.1. Ethics Committee

CELSA's Board of Directors has designated the *Ethics Committee* as "*Responsible for the Internal Reporting System*", which is unique for all *CELSA* companies.

The roles and responsibilities of the *Ethics Committee* in relation to *Enquiries* and *Complaints* are described in *CELSA's Incoming Communications Management Procedure.*

8.2. Board of Directors

The roles and responsibilities of the *Board of Directors* in relation to *Enquiries* and *Complaints* received are as follows:

- Formally approve this *Policy*, as well as any modifications or updates that may be necessary to maintain its validity and effectiveness.
- The Board of Directors is responsible for adopting the relevant decisions regarding the *Complaints* on facts that may generate criminal liability for *CELSA*, once it has received, through the *Audit and Control Committee*, the report on the conclusions of the investigation, prepared by the *Ethics Committee*.
- The *Board of Directors* shall inform, through the *Audit and Control Committee*, the *Ethics Committee* of the actions agreed or ratified, so that they are duly documented and recorded. Among others, it shall order disciplinary measures that are legitimate and proportionate to the facts reported, and in the event of affecting *Members of the Organisation*, through the *Ethics Committee* it shall inform the corresponding area for their appropriate execution within the applicable labour framework.

8.3. Steering Committee

The roles and responsibilities of the *Steering Committee* in relation to *Enquiries* and *Complaints* received are as follows:

- The *Management Committee* will be responsible for adopting the relevant decisions with regard to *Complaints* about facts related to serious or very serious administrative infringements, infringements in matters of safety at work and any other infringement of the legal system applicable to *CELSA* and the rest of the internal regulations of the *Organisation*, once it has received the report on the conclusions of the investigation drawn up by *the Ethics Committee*.
- The *Management Committee* shall inform the *Ethics Committee* of the agreed actions, so that they are duly documented and recorded. Among others, it shall order disciplinary measures that are legitimate and proportionate to the facts reported, and in the event of affecting *Members of the Organisation*, it shall inform the corresponding area for their appropriate execution within the applicable labour framework.

Annex I

Material scope of application

Consultations and *Complaints* that are performed on non-compliances, materialised or potential, through the internal channel:

- Breaches of the *Code of Ethical Conduct and Professional Conduct* or *CELSA*'s internal regulations, as well as of any external rules, legislation or regulation applicable in each country or territory, including, in particular, breaches of criminal law and antitrust regulations, due to their particular seriousness and the specific commitment that *CELSA* has undertaken with respect to their observance and compliance.
- Infringements of European Union law, provided that:
  - They fall within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937, irrespective of their qualification under national law;
  - affect the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU); or
  - have an impact on the internal market, as referred to in Article 26(2) TFEU, including infringements of EU competition rules and aid granted by States, as well as infringements relating to the internal market in relation to acts in breach of corporate tax rules or practices aimed at obtaining a tax advantage that would defeat the object or purpose of the legislation applicable to corporate taxation.
- Actions or omissions that may constitute a serious or very serious criminal or administrative offence. In any case, all serious or very serious criminal or administrative offences involving financial loss to the Public Treasury and Social Security shall be understood to be covered. This protection shall not exclude the application of the rules relating to criminal proceedings, including investigation proceedings.
- Queries and doubts about the *Code of Ethical Conduct* or *CELSA*'s internal regulations, which may include, but are not limited to, issues related to:
  - Interpretation of ethical principles and values set out in the *Code*.
  - Practical application of the standards of professional conduct in specific situations related to the *Code* or any *CELSA Policy*.
  - Gift and hospitality policy issues and their practical interpretation in *CELSA*.
  - Conflicts of interest and how to manage them in accordance with *CELSA*'s Conflict of Interest Management Policy.
  - Identification of behaviour that could contravene the principles set out in the Code or in *CELSA*'s internal regulations.

The protection provided in this *Policy* for *Members of the Organisation* who report breaches of labour law in the field of occupational safety and health is without prejudice to the protection provided by their specific regulations.

Annex II

Requirements for access to protection measures and examples of *retaliation*

Persons who report or disclose violations under this *Policy* are entitled to protection under the following circumstances:

- They have reasonable grounds to believe that the information is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and that the information is within the scope of this *Policy*,
- The communication or disclosure has been performed in accordance with the requirements of this *Policy*.

Persons who communicate or disclose information are expressly excluded from the protection provided for in the Whistleblower Protection Act:

- Information contained in communications that have been rejected by any internal information channel when the facts reported lack all plausibility, do not constitute an infringement of the legal system included in the scope of application of this law, and when the communication is manifestly unfounded.
- Information linked to complaints about interpersonal conflicts or which concern only the informant and the persons to whom the communication or disclosure relates and which do not have criminal implications.
- Information which is already fully available to the public or which constitutes mere hearsay.
- Information relating to actions or omissions not covered by this regulation.

The following is an example of *Retaliation*, which is prohibited in all cases by the *Organisation*:

- 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, or early termination or cancellation of contracts for goods or services, imposition of any disciplinary measure, demotion or denial of promotion and any other substantial modification of working conditions and failure to convert a temporary employment contract into an open-ended one, among others.
- Damage, including reputational damage, or economic loss, coercion, intimidation, harassment or ostracism.
- Negative evaluation or references regarding work or professional performance.
- Inclusion on blacklists or dissemination of information in a given sectoral area, which hinder or prevent access to employment or the contracting of works or services.
- Refusal or revocation of a licence or permit.
- Refusal of training.
- Discrimination, or unfavourable or unfair treatment.