TERMS OF USE OF IREC'S INTERNAL INFORMATION CHANNEL

Welcome to the Internal Information Channel of the Fundació Institut de Recerca en Energia de Catalunya (IREC). Before continuing, we ask you to carefully read the following conditions, which regulate the responsible use of this channel.

For more details on how the channel works, we recommend that you consult the General Procedure of the Internal Information System, the Information on Personal Data Protection and the Questions and answers document. Your collaboration is critical to maintaining the highest standards of integrity.

1. Purpose and acceptance

This document establishes the conditions that regulate the use of the Internal Information Channel (hereinafter, "the Channel") of the Fundació Institut de Recerca en Energia de Catalunya (IREC). The submission of a communication through this Channel implies the full and unreserved acceptance of these conditions.

2. Purpose of the Channel

IREC's Internal Information Channel is the official, confidential and secure channel that we make available to you so that you can communicate, confidentially or anonymously, and with full guarantees, actions or omissions that may constitute serious or very serious criminal, administrative or very serious infringements or serious infringements of IREC's internal regulations of which you are aware in your employment or professional relationship with IREC, in accordance with the provisions of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption (hereinafter, Law 2/2023).

It works through an external and secure online platform, designed to protect your identity at all times and guarantee your anonymity, if you so wish, the confidentiality of the communication and the protection of your personal data, those of the people allegedly involved, and the information you share.

3. Modes of communication

You can choose to submit an identified or anonymous communication.

- **Communication identifying you**: if you decide to provide your contact details, IREC guarantees maximum confidentiality regarding your identity, in accordance with the provisions of Law 2/2023. Your details will allow us, if necessary, to request additional information from you to clarify the facts and, if you agree, to keep you informed about the status of your communication.

- **Anonymous communication**: You have the right to submit your communication completely anonymously. IREC guarantees that your identity will be protected throughout the process. To ensure effective anonymity, we recommend that you follow the technical indications detailed in the document "Questions and answers on IREC's internal information channel".

In the event that it is not an anonymous complaint, we will ask you for the minimum identification data in order to be able to request more information regarding the facts, if necessary, to report on the progress of the procedure (if the complainant accepts) and/or to arrange a personal interview with the person who holds the position of System Manager, member of the collegiate body Responsible for the Information System with delegated executive powers to carry out the preliminary analysis of the facts reported, the decision on whether or not to admit them for processing and, if so, the instruction of the corresponding investigation file

4. Management of anonymous communications and acknowledgment of receipt

IREC guarantees the possibility of submitting communications anonymously, ensuring the protection of the identity of the reporting person throughout the process.

If you submit a communication anonymously or through a medium that, by its nature (such as postal mail), does not allow a secure acknowledgment of receipt or could compromise the confidentiality of the information, IREC may omit to send such acknowledgment of receipt and subsequent communications. This measure is adopted in strict compliance with Article 9.2 c) of Law 2/2023, which provides that an acknowledgement of receipt will be sent "unless this may jeopardise the confidentiality of the information", so that it prioritises safeguarding the confidentiality of the information and protecting the identity of the informant over communication formalities.

If you wish to receive further communications while remaining anonymous, you can provide a secure email address (created for this sole purpose that does not contain your identifying data). In this case, you will receive the acknowledgement of receipt and subsequent communications at that address.

5. Obligations of the reporting person

By using this Channel to submit a communication of information, you agree to:

- Act in good faith: make your communication with the conviction that you have reasonable grounds to believe that the facts and information you present are true at the time of the communication, even if you do not provide conclusive evidence and even in cases where it is concluded that no infringement has occurred. The protection offered by the law protects those who report in good faith.

- Provide truthful and detailed information: describe the facts as clearly and completely as possible, providing the indications or evidence or evidence that you have to facilitate their verification. To this end, the communication must contain:

    - A brief title of the subject/communication.
    - Indication of the relationship of the respondent with IREC.
    - The indication of the IREC departments associated with the communication (optional information).
    - Indication of the category (to be selected) in which the reported facts best fit.
    - Place where the events occurred (optional information).
    - Date or period of occurrence (optional information).
    - A clear, chronological and as detailed description as possible of the actions or omissions that are reported that can be verified or verifiable directly or through investigation.
    - Indication of whether there are witnesses who can corroborate the facts (optional information).
    - Identification of witnesses and their relationship with IREC (optional information).
    - Identification of the persons and/or entities allegedly involved and their relationship with IREC (optional information).
    - Any documentation, file or evidence that supports the communication or, failing that, the indicia on which it is based.
    - Indication of how the informant became aware of the facts reported.
    - Indication of whether the information communicated has been previously forwarded to other bodies or authorities (optional information).
    - Indication of which bodies or authorities the information communicated has been previously sent (optional information).
    - Indication of whether the respondent wishes to request a meeting with the System Manager (System Manager).
    - Indication of the name and surname (optional information).
    - Indication of a telephone number (optional information).
    - Indication, where appropriate, of a secure e-mail address for the purpose of communications (optional information).
    - Only in the case of having marked the category: query, complaint or suggestion. Brief indication of the reason and what issue or issue you want to be resolved.
    - Solving a CAPTCHA.
    - Information on personal data protection.

- Making responsible use of the Channel: the communication of false information knowingly of its falsity or with manifest disregard for the truth by natural persons constitutes a very serious infringement according to Law 2/2023, which could be sanctioned by the

Independent Authority for the Protection of Whistleblowers with an administrative penalty of 30,001 to 300,000 euros. In accordance with current regulations, it may give rise to the demand for civil, criminal and administrative liability. If the reporting person belongs to IREC, he or she may be subject to the corresponding disciplinary measures.

6. IREC commitments and guarantees

IREC, in its firm commitment to transparency, ethics and the protection of people who report regulatory violations, assumes the following fundamental guarantees in the management of its Internal Information System and undertakes to:

- **Confidentiality and identity protection**

IREC guarantees the utmost confidentiality of your identity as a reporting person, of the affected persons and of any third party mentioned in the communication. The identity of the reporting person will not be disclosed to the affected persons or to third parties, except in the following exceptional cases:

- When the informant gives his or her free, voluntary and express consent to do so.
- When it is a strictly necessary communication imposed by a legal obligation in the context of a judicial investigation, the Public Prosecutor's Office or a competent administrative authority. In this case, the reporting person shall be informed in advance of such disclosure before it occurs, unless the competent authority considers that such prior communication could seriously jeopardise the success of the investigation.

- **Protection from retaliation**

IREC is committed to protecting the whistleblower against any type of retaliation, threat or attempted retaliation that they may suffer for having reported in good faith about regulatory violations. This protection extends from the moment of communication and throughout the process.

- **Diligent communication management and restricted access**

All communications received will be handled with the utmost diligence, objectivity and impartiality, respecting at all times the presumption of innocence and the right to honour of the people affected.

Only the System Manager and designated IREC support staff for the management of the Internal Channel can access communications and related information. These personnel are subject to a strict duty of confidentiality and professional secrecy, which persists even after their relationship with IREC is terminated. Access is governed by strict role-based access control and the "need to know" principle that covers:

- The full content of the communication.
- The identity of the reporting person, the affected persons and any third party mentioned.
- All documentation and information generated or collected during the investigation.

Failure to comply with this duty constitutes a very serious infringement, in accordance with the provisions of Law 2/2023.

- **Technical security measures for the protection of anonymity and information**

The protection of the whistleblower, the identity of all the people involved and the information processed, from the receipt of the communication to its resolution is our top priority. For this reason, IREC's Internal Information Channel is managed through a technological platform of a specialized external provider that acts as a data processor under a strict confidentiality contract with IREC. This platform complies with the highest standards of security and confidentiality, and is certified by the National Security Scheme (ENS) in the high category and ISO 27001.

The Internal Channel is designed to protect the anonymity of the whistleblower and not to store information that has not been explicitly provided, with the following measures:

- End-to-end encryption. All communication information and attachments you send travel encrypted from your device to IREC's authorized managers, ensuring that only authorized personnel to manage the communication can access it. This prevents anyone outside the process, not even the technical staff of the secure channel provider, from accessing the information.
- Metadata removal. The Channel automatically removes the metadata of the files you attach (such as author, creation date, etc.) before it is received by IREC's authorized managers.
- No IP tracking. The system does not log or store your IP address or any other identifier on your device.
- Voice anonymization. If you make a verbal communication, the Channel allows you to automatically distort your voice so that it cannot be recognized.
- Tracking cookies are not used and no information that you have not explicitly provided is stored.

7. Criteria for inadmissibility

The following will not be admitted for processing through this procedure:

- The respondent has no employment or professional relationship with IREC.
- When the facts lack all plausibility.
- Communications that refer to actions or omissions that do not fall within the scope of Law 2/2023 or the System.
- The communication is unintelligible or describes facts that are manifestly unfounded.
- Information for which there are reasonable indications that it has been obtained through the commission of a crime (for example, by illegally accessing confidential or sensitive data committing a crime of discovery and disclosure of secrets). In these cases, in addition to the inadmissibility, IREC must send the Public Prosecutor's Office a detailed account of the facts that are considered to constitute a crime.
- Information related to complaints about interpersonal conflicts or that affect only the reporting person and the people to whom the communication refers (not the IREC) or labor or contractual claims that do not involve a serious or very serious regulatory infraction. For these situations, IREC has other specific channels.

- Information that is already fully available to the public or communication that is substantially identical to a previous one already processed and resolved without providing facts, data, evidence or other additional, new and significant information, unless it provides new and relevant information or new circumstances have arisen that justify its revision that justify a new investigation.
- Communications that are based on mere rumours, personal opinions or when the information is excessively generic without referring to a specific fact, or is not supported by sufficient indications or specific facts to allow a reasonable verification of the information to be carried out to initiate an investigation.
- The facts have already been reported to the security forces, the courts or the Public Prosecutor's Office.
- This is information contained in communications that have already been previously rejected by the Internal Information Channel.
- Communications that, in themselves, violate the dignity of people or violate fundamental rights such as honour, privacy or one's own image, without prejudice to the responsibilities that may arise.
- Communications in respect of which there are reasonable indications that they have been made in bad faith (with knowledge of their falsity), will not only be inadmissible, but could give rise to the responsibilities provided for by law.

8. Communications with a different purpose

This channel is the preferred channel for persons who know the facts in the context of an employment or professional relationship with IREC with respect to the purposes described in paragraph 2. If communications are received on matters that, without constituting serious or very serious infringements, correspond to other areas (labour or salary claims related to Human Resources, workplace harassment, equality, etc.), these will be analysed and, where appropriate, referred to IREC's internal committees or procedures provided for their proper management, remaining outside the specific scope of protection of Law 2/2023.

The Internal Information System does not replace IREC's internal protocols for prevention and action in the event of harassment at work, sexual harassment or harassment based on sex at work resulting from collective bargaining under the Workers' Statute.

9. Concurrence with judicial proceedings or those of the Public Prosecutor's Office

IREC does not exercise the functions of judicial authority, Public Prosecutor's Office or judicial police. If the reported facts are already being investigated by these authorities, or if they initiate proceedings subsequently, IREC will suspend its proceedings, provide all the information at its disposal to the competent authority and provide the necessary support.

10. Exclusion of liability

IREC is not responsible for the incorrect use of the Channel by the informant, nor for the content or veracity of the information communicated when it is proven to be false or malicious. The responsibility for the information provided lies exclusively with the reporting person if he or she acts in bad faith.

11. Protection of personal data

The processing of the personal data you provide through the Internal Information Channel will be governed by the provisions of Regulation (EU) 2016/679 (GDPR), Organic Law 3/2018 (LOPDGDD) and Law 2/2023.

- Purpose: your data will be processed for the exclusive purpose of receiving, managing and investigating the communications presented through the Internal Information System, as well as to comply with the legal obligations arising from this.
- Legal basis: the processing is legitimised in compliance with a legal obligation applicable to the data controller, in accordance with the provisions of Law 2/2023.
- Rights: you can exercise your rights of access, rectification, deletion, limitation of processing and opposition, although the exercise of some of these rights may be limited to guarantee the confidentiality and success of the research.

You can obtain complete and detailed information on the processing of your personal data, by consulting the document "Information on personal data protection" of the Internal Information System.