# General Policy on the Internal Information System
# Complaints Channel

| | |
|---|---|
| **Document** | General Policy on the Internal Information System - Complaints Channel |
| **Description** | Definition of the functioning of the Internal Reporting System (Whistleblower Channel) |
| **Start date** | September 2024 |
| **Purpose** | Establish the rules governing the operation of the Internal Information System (Complaints Channel). |
| **Ranking** | Public document |

**Index**

1. PURPOSE, SCOPE AND GUIDING PRINCIPLES..... 3

1.1 Aim and purpose.....3
1.2. Scope and mandatory nature .....4
1.3. Legal regime .....5
1.4. Guiding principles.....6

2. REPORTING.....8

2.1 Means of submitting complaints .....8
2.2. Background information .....9
2.3. Incompatibility..... 10

3. DEFENCES AND OBLIGATIONS OF THE REPORTER AND THE REPORTED PERSON..... 10

4. ESSENTIAL PRINCIPLES OF THE SUBSEQUENT PROCEDURE FOR MANAGING THE INFORMATION RECEIVED. ..... 11

5. COMMUNICATION..... 12

5.1. Communication ..... 12
5.2. Interpretation..... 13
5.3. Training and awareness-raising.....13
5.4. Commitment of the addressees of the Policy .....13

6. HISTORICAL, APPROVAL, ENTRY INTO FORCE AND REFORM OF THE POLICY. EVIDENCES..... 13

6.1. History, adoption and entry into force.....13
6.2. Monitoring, continuous adaptation and reform of the Policy .....13
6.3. Custody of evidence .....14

7. PERSONAL DATA PROTECTION.....14

Annexes..... 14
Definitions.....16
Reception of the Internal Information System Policy.....17

## 1. PURPOSE, SCOPE AND GUIDING PRINCIPLES

### 1.1. Aim and purpose

The purpose of this Policy is to explain to all users of the TECNIC PROCESS EQUIPMENT MANUFACTURING SL (hereinafter, TECNIC) Internal Information System (hereinafter, IIS or Whistleblower Channel) how it works, how they can access it and what its functionalities are. That is, its general principles of operation, as well as those of defence of the informant and the reported person.

The Whistleblower Channel is the tool through which all TECNIC members, i.e. members of the governing body, managers, employees and third parties can inform the entity of the possible commission of criminal conduct and serious or very serious administrative infractions (these will be the informants or communicators).

The aforementioned third parties, i.e. those who must also be allowed to file a complaint, are participants and members of the Board of Directors, including non-executive members, freelancers, any person working for or under the supervision of contractors, subcontractors and suppliers; former employees, trainees, candidates in selection processes or in pre-contractual negotiation, volunteers and workers in training at the entity. However, it is hereby stated for the record that, without prejudice to the fact that TECNIC will contemplate all the guarantees contained in this Policy, the current regulations only establish protection measures for those persons who have or have had an employment or professional relationship with TECNIC and in relation to the matters set out in art. 1.2 (a and b) below.

It is the will of the Board of Directors to create a mechanism, among others, to guarantee compliance with the law and the effectiveness of the Code of Ethics and TECNIC's internal protocols, thus preventing them from becoming mere declarations of will and contemplating a policy of zero tolerance towards illegality.

Likewise, the use of this Channel may allow TECNIC to adapt its activity to the regulations in force, guarantee compliance with its internal regulations and reduce the risk of criminal or illicit conduct within TECNIC, protecting not only the entity but also its employees and representatives.

TECNIC's Board of Directors will be responsible for the implementation of the Whistleblowing Channel, after consultation with the legal representation of the employees, if it is so constituted. It will also be responsible for appointing, removing or dismissing the Head of the Internal Information System (hereinafter, the Head), who must be a person with sufficient training and knowledge to assume this responsibility (the System must guarantee that communications can be processed effectively). The person in charge may be a single person or a collegiate body (committee), and must be independent and autonomous with respect to the other members of the entity in the exercise of his or her functions and may not receive instructions of any kind in the exercise of his or her functions. In the case of appointing a collegiate body, depending on the content of the complaint that may be received, the person responsible for its internal investigation shall be appointed with each of them, without prejudice to the management function of the member of the collegiate body who shall assume the position of System Manager (delegate).
TECNIC will provide the personal and material means that may be necessary for the development of its mission. Once the person in charge has been appointed, in whatever

format, he/she shall be notified to the Independent Authority for the Protection of the Informant, which in Catalonia is the Anti-Fraud Office of Catalonia.

It shall be the responsibility of the Responsible Officer: to receive and process the reports that reach the Whistleblowing Channel, to comply with the provisions of this Policy and what is required of him/her according to the content of the Law, as well as to review compliance with the Procedure for the Management of Communications Received, respecting the rights and duties of the parties involved in the IMS. In general, to supervise the proper functioning of the Complaints Channel and its management system.

### 1.2. Scope and enforceability

**Objective scope of application: What can and cannot be reported through the Whistleblowing Channel:**

In the Whistleblowing Channel, complaints may be submitted that refer to actions or omissions that occur or have occurred in TECNIC's sphere of action and that constitute an infringement in a labour or professional context of a rule or principle that affects the entity and that meet the following characteristics. In any case, they may be reported:

a) Conduct constituting a criminal offence or a serious or very serious administrative offence, such as fraud, payment of an undue commission, non-payment of a tax or price fixing in a public tender;
b) Any act or omission of European Union law provided that:
    i. This concerns public procurement; financial services, products and markets and the prevention of money laundering and terrorist financing; product safety and conformity; transport safety; environmental protection; radiation protection and nuclear safety; food and feed safety, animal health and animal welfare; public health; consumer protection; protection of privacy and personal data; and security of networks and information systems.
    ii. Affects the financial interests of the European Union, or
    iii. It has an impact on the internal market, e.g. infringements of EU competition rules and state aid.

Incidents that are not included in this section, such as issues closely linked to Human Resources or personnel policies (e.g. holidays, remunerations, relations between employees, interpersonal conflicts, etc.), recommendations or suggestions not linked to regulatory compliance issues or to the provision of services by the entity will not be considered as incidents to be reported through the Whistleblower Channel.

In the event of doubt as to the nature of the event in question on the part of the reporter, and provided that the reporter is acting in good faith, the event may be reported without any problem. The Head will review its content and analyse its possible admissibility, which will be communicated to the whistleblower.

**Concerns**
In the case of concerns that the recipients of this Policy may have regarding regulatory compliance or the use of the Whistleblower Channel (e.g. how to interpret a regulation or

how to act in a specific case), they may address them to hhrr@tecnic.eu, without in any case being able to use this e-mail to communicate the complaint itself.

**Subjective scope of application: To whom is this Policy addressed?**
This Policy is addressed to all those who, in any way, provide employment or professional services to TECNIC, i.e. participants or members of the Board of Directors, management or supervision of the entity, including non-executive members, employees and regular external collaborators (as detailed in article 1.1), as well as to any person who may act on behalf or for the benefit of TECNIC without any geographical limitation whatsoever. The Policy shall also apply to (i) all of them, whether they have the status of informant, investigated/complainant or witness and (ii) to the Controller as the body responsible for receiving and/or processing the complaints that may be received through the Whistleblower Channel.

**Mandatory:**
Compliance with this is an employment or contractual obligation for all of them, and failure to comply with it may be subject to disciplinary sanctions in accordance with the provisions of the labour regulations governing where the entity carries out its functions (e.g. applicable Collective Bargaining Agreement), as well as the corresponding regulations or contractual document.

Any of the addressees of this Policy is obliged to report incidents of which they become aware through the means set out in the following chapter.

### 1.3. Legal regime

The organisation, use and operation of the Whistleblowing Channel shall be governed by this Policy, which shall be complemented by the General Procedure for the Management of Information Received. Likewise, any regulations that may be issued by the authorities or administrations in relation to the whistleblowing channels or other regulations that may regulate aspects relating thereto (e.g. laws regulating the protection of personal data or the prevention of money laundering and the financing of terrorism and, significantly, all those that regulate the protection of fundamental rights) shall be observed.

### 1.4. Guiding principles

This Policy responds, among other things, to the desire of TECNIC's Board of Directors to establish a commitment to zero tolerance towards crime, administrative infractions, illegal acts and respect for legality and good practices.
In line with the above, this set of rules governing the obligation to report incidents to the Controller and the procedure for managing them will always comply with the principles of *freedom, independence and impartiality, confidentiality, indemnity, protection and prohibition of reprisals, integration and trust*. In other words:

**a) Freedom**: This Policy and its procedures, as well as the Complaints Channel, shall be freely accessible to all persons to whom this Policy is addressed, as set out in point 2.

**b) Independence and impartiality:** The person in charge, as the body responsible for receiving and managing the complaints that may be made through the channel, shall act, in the performance of these functions, always in accordance with the principles of

independence and impartiality. Respecting, always and objectively, the observance of the rights and guarantees of all parties involved in the process.

**c) Confidentiality**: The information received through the whistleblowing channel will always be treated under strict confidentiality parameters. In other words, the Controller will never reveal (i) the name of the whistleblowers in good faith, nor any data or information from which their identity can be directly or indirectly deduced, (ii) the identity of any other person identified in the complaint during the investigation phase; (iii) the complaint itself received and will prevent any action aimed at discovering the above points.
Without prejudice to the foregoing, the Controller may transmit information related to the complaint in the following cases:

- To other TECNIC departments when this is essential for the proper conduct of the investigation, a circumstance that will be determined at the beginning of the investigation in order to identify the parties who will have access to information related to the complaint. Access to information may also be granted to other departments during the course of the investigation when this is necessary as the investigation progresses;
- To third parties when it is necessary to engage their services for the proper conduct of the investigation (e.g. lawyers, consultants, experts, private detectives, translators, etc.); a circumstance that may be determined during the course of the investigation process. In such cases, a confidentiality undertaking shall be requested from the third party;
- To the TECNIC governing body when deemed necessary given the possible seriousness of the facts;
- Where there is a legal obligation or court order to do so;
- To the Human Resources Department, once the investigation has been completed and an affirmative conclusion has been reached as to possible authorship and responsibility. This shall be done so that, if necessary, the corresponding sanctioning measure may be imposed on the person denounced and responsible. This Department may also have access when it is necessary to adopt precautionary measures for an employee under investigation in the initial phase of the procedure;
- To other TECNIC departments, once the investigation has been completed, in order to coordinate with them the implementation of improvement measures on TECNIC's processes that are recommended in the final report of conclusions.

In all of the above cases, a declaration of confidentiality must be requested and the identity of the persons concerned (meaning the informant) shall never be revealed when known, nor shall the report itself be provided. The obligations described in point 7 of this Policy regarding the protection of personal data shall also be taken into account.

The protection of the identity of the complainant may be waived in the following cases:

- When there are special circumstances that make it advisable to identify him/her, and provided that he/she has given his/her consent;
- At the express request of authorities or judicial bodies in the context of an investigation and, in particular, where it is necessary to safeguard the rights of defence of the persons complained of.
- In the event of such disclosure of the alerter's identity, the alerter shall be informed beforehand, except when this could compromise the investigation or the judicial

procedure or when this is prohibited by a legal regulation (e.g. the Money Laundering Prevention Act).
- In any case, this transfer of data will be made in compliance with the personal data protection legislation that may be applicable.

This protection of the confidentiality of the whistleblower's identity does not apply where the whistleblower intentionally discloses his or her identity in the context of a public disclosure. Nor does it apply where it is the reported subject who discloses his or her own identity in any context.

**d) Indemnity, protection and prohibition of retaliation:** No bona fide reporter may suffer any form of retaliation or attempted retaliation from TECNIC as a result of a report. TECNIC will also take special care to ensure that no bona fide whistleblower may suffer any negative consequences as a result of a report (e.g. suspension of employment, dismissal or removal from employment; demotion or denial of promotion, etc.).
TECNIC will ensure that no member of TECNIC takes any action that could lead to retaliation against the whistleblower. This guarantee shall also extend to any witnesses or third parties (including facilitators, understood as persons who can help the whistleblower to make the report and legal representatives of workers who can advise or support the whistleblower) and legal persons owned by the whistleblower who collaborate or are involved in the investigation of the reported event.

Good faith on the part of the sender shall be deemed to be lacking when the sender acts with awareness of the falsity of the facts communicated or acts with manifest disregard for the truth.

As evidence of this lack of good faith, the intention to take revenge, to harass the disclosed person, to damage his/her honour or to harm him/her at work or professionally shall be considered as evidence of this lack of good faith.

Irrespective of the criminal and civil liability that may arise from the above, the alerter in bad faith shall be disciplined or contractually sanctioned, where possible, in accordance with the applicable labour and contractual regulations. Facts communicated in error shall not be punishable, provided that there is good faith on the part of the alerter.

**e) Integration:** TECNIC will integrate the different complaint channels it may have into a single one for better management, without prejudice to the particularities to be observed by each one in its management.

**f) Trust:** TECNIC will generate trust in the use of the Channel by all its members in order to make the Channel as efficient as possible.

## 2. COMPLAINTS: How can I file a complaint?

### 2.1. Means of lodging complaints

The recipients of this Policy may make the complaints mentioned in point 1.2 above through the Complaints Channel platform that TECNIC has set up, i.e. through the platform accessible through this link: *https://co-resol.bcnresol.com/webclick*

If the informant so requests, he/she may also submit his/her communication by means of a face-to-face meeting with the Officer in Charge within a maximum of 7 days of his/her request.

In the case of communications made through face-to-face meetings, these must be documented, subject to the informant's consent, through a complete and accurate transcription of the conversation made by the person in charge of the SII.

In any event, the complainant shall be given the opportunity to review and, where necessary, amend or expand the transcription of the information.

In order to ensure the confidentiality of the channel, only the Responsible and the persons referred to in art. 7 (for example, the person to whom TECNIC entrusts the reception of the complaints for their subsequent processing by the Responsible) will have access to the content of the complaints submitted, being responsible for their management and processing. Likewise, the Complaints Channel platform will always be protected by a password that must be changed every 6 months and known only to the persons mentioned herein. These tools and any other tool that may be used to process complaints shall also include the necessary technical and security measures to guarantee the confidentiality of the Complaints Channel.

The above are all the internal means of TECNIC through which a complaint may be sent, and these should be the preferred means of communication. However, whistleblowers may also address their complaints to an external body: the Independent Authority for the Protection of Whistleblowers of Catalonia (Oficina Antifrau de Catalunya) or any other authority competent to receive complaints.

Communications made by means of self-denunciation, i.e. by means of reports in which the alerting subject denounces facts that affect his/her own person, will also be accepted. On these occasions, the reporting person shall have the dual status of both reporting and denounced, and his or her rights and obligations in this capacity shall be observed.

In the event that any person at TECNIC who is not the person in charge receives a complaint by any means, he/she must immediately forward it to the person in charge and keep the information received confidential. Failure to comply with this obligation may result in disciplinary sanctions.

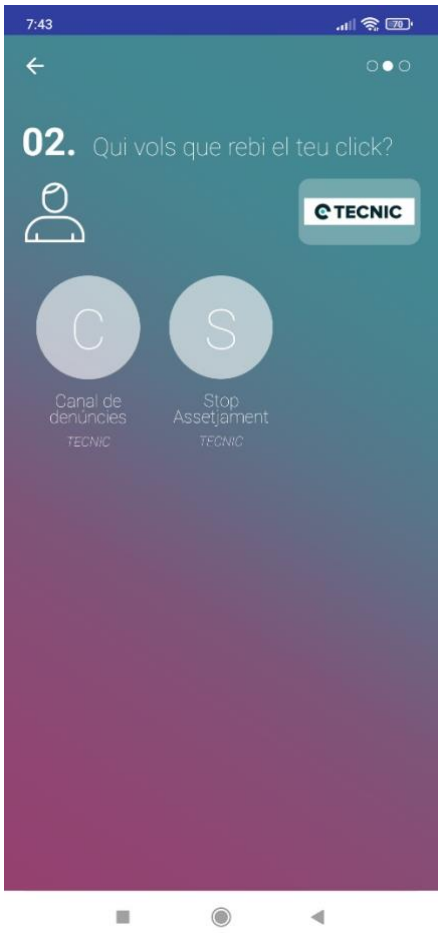
Likewise, any type of information that may be received from outside, such as, for example, from public administrations or judicial bodies, may be dealt with by means of this Policy and the General Procedure for the Management of Information Received. Likewise, the Controller may also submit to this Policy any facts detected in the normal course of its activity. In all these cases, the complaint received or facts detected will also be treated in accordance with the provisions of this Policy and the General Procedure for the Management of Information Received.

### 2.2. Basic information

Complaints submitted through the Complaints Channel should, as far as possible, contain the following minimum information:

- The fact, behaviour or irregularity reported, as well as the date on which it took place. No legal classification or legal assessment of the fact under investigation by the informant is required, although the informant must have reasonable grounds to believe that the reported fact is true;
- The reason why the occurrence is considered unusual or irregular;
- Identity of the persons responsible for the above if known (reports may also be accepted for unknown but identifiable subjects);
- Evidence that is available to prove that the act or irregularity has been committed (the provision of evidence by the reporting person is not obligatory, but it is recommended). Under no circumstances may evidence be obtained by violating fundamental rights or in an unlawful manner. In cases where this doubt may arise, the reporting person shall refrain from obtaining the evidence without prior consultation with the third party he/she deems appropriate;
- Identification of the complainant, although anonymous communications may also be accepted. In the event that an anonymous complaint is received through the complaints channel, the information received will be treated with the necessary precautions required for this type of communication and without this circumstance preventing the application of this Policy or the General Procedure for the Management of Information Received.
- Specification of whether the alerter or third parties are in a risk situation that needs to be urgently remedied or serious situations of possible immediate risk.

All of the above is requested on the platform's home screen, and the spaces provided for this purpose must be filled in. This is provided as an example:


Users can also access the instructions for using the Complaints Channel through the explanatory video that you will find at this link: https://youtu.be/ISVkuv-SuzU?si=RS_W58HyU1ZzVxju.

In any case, the reporting party is obliged to make the report truthfully, without misrepresenting the truth, and without prejudice to the fact that the information transmitted is only due to indications of an infringement of those mentioned in section 1.2. The use of bad faith in the Whistleblowing Channel, such as, for example, making false or unfounded reports, is prohibited and will be sanctioned by TECNIC whenever possible.

TECNIC's platform for submitting complaints guarantees the anonymity and confidential treatment of the information that may be received through it, insofar as it is managed by a third party outside TECNIC and only those expressly authorised to do so may access the information.

### 2.3. Incompatibility

In the event that the complaint directly or indirectly affects the IBS Officer, the complaint will be forwarded to the other members of the committee (the platform allows for the complaint to be addressed to a specific subject).

When this situation of incompatibility with the person in charge arises, the fact that he/she does not abstain from his/her duties will constitute a very serious breach of this Policy, with the consequent labour or contractual sanctions that may be imposed.

## 3. DEFENCE AND OBLIGATIONS OF THE INFORMANT AND THE REPORTED PERSON

TECNIC, through the Controller, will ensure that the whistleblower is protected in good faith and uses the Whistleblower Channel in accordance with the provisions of this Policy through the following principles of action:

a) You will treat as confidential your identity, the identity of the persons who may be mentioned in the communication you make and the facts that are exposed. This means that only those persons authorised to do so, and identified above, will be able to access the information relating to the report and will not be able to share it with any other third party.
b) It will treat anonymity in those cases where the communication is made in this way. That is, when the whistleblower makes the report anonymously, his or her identity will never be known, which is guaranteed by the platform that is maintained by a third party external to the entity.
c) Provide an interpreter or translated documentation when needed by the reporter to understand the scope of his/her rights and obligations as well as the use of the Whistleblower Channel.
d) It shall observe an absolute prohibition on receiving any form of retaliation, including threats of retaliation and attempted retaliation, for information that the whistleblower may provide for the investigation. That is, if the whistleblower in good faith receives any form of retaliation for his or her cooperation with the entity, the whistleblower in question shall be sanctioned immediately where possible. In the event that the informant understands that he/she is being the victim of retaliation, he/she must immediately inform the person in charge of the situation so that TECNIC can take the corresponding measures.
e) In general, it will receive support from TECNIC during the time the complaint is being handled, as well as with the procedures that may arise after the complaint has been filed, and will ensure that the provisions of the General Procedure for the Management of Information Received are respected.

At the same time, the reporting person should consider the following obligations in the use of the Whistleblower Channel:

a) Act in good faith.
b) Not to communicate facts that are false or manifestly contrary to the truth.
c) Provide as much detail as possible about the facts you report and cooperate with the investigation as far as possible.

d) As far as possible, follow up on the complaint you submit in order to be informed about its processing and to be able to answer any clarifications or requests for information that may be formulated.
e) Respect the confidentiality of the information provided and of the very existence of the complaint and its subsequent processing procedure.

TECNIC will also ensure the rights of the reported person, such as the right to honour, to the presumption of innocence, to not suffer prospective investigations and to have access to the facts attributed to him/her and to be heard about them. All of this is developed in the General Procedure for the Management of Information Received, which complements the content of this section.

The Controller shall ensure that the rights and obligations of the whistleblower and the reported person are respected throughout the handling of the report and with the consequences following the report, such as legal proceedings.

## 4. ESSENTIAL PRINCIPLES OF THE SUBSEQUENT PROCEDURE FOR MANAGING THE INFORMATION RECEIVED

When the person in charge receives a complaint, without prejudice to the provisions of the General Procedure for the Management of Information Received, he/she shall initiate the internal investigation phase of the reported facts, the essential principles governing the latter being the following:

a) Once the report has been received by any of the means established in this Policy and only by the persons authorised to do so, the Controller will send the informant, within a maximum period of 7 calendar days from the receipt of the report by the Controller or external third party where applicable, an acknowledgement of receipt; unless this could jeopardise the confidentiality of the communication.
b) If necessary, e.g. when the information received is insufficient, the Controller may ask the reporter for additional information on the reported facts during the course of any investigation that may be carried out.
c) It will study the facts contained in the complaint received and will, in the first place, carry out an analysis of its plausibility. That is, it will review whether or not the facts reported should be investigated, deciding whether to admit the complaint or to reject it. This will be notified to the informant;
d) In the event that the complaint passes the above plausibility filter, the Head will initiate an internal investigation in which he/she will carry out the investigative measures deemed necessary, such as, for example, an interview with the complainant (if not anonymous), with witnesses and with the subject of the complaint and/or the analysis of any documentation that may be necessary. In the event that there are reasonable grounds to believe that the facts reported or investigated are criminal in nature, a decision may be taken not to interview the subject of the complaint in order to safeguard his or her rights of defence.
e) During the conduct of any investigation it carries out, it shall at all times respect the rights and guarantees provided for in this Policy, in the General Procedure for the Management of Information Received and in the legal system, such as proportionality, impartiality, independence and the rights of defence, presumption of innocence, honour and contradiction of the parties affected by the investigation.

f) Finally, with the facts that have been analysed, he/she shall issue a conclusions report in which the facts observed are assessed and a conclusion is reached. Where appropriate, the Head may also include in his report a proposal for the adoption of measures to improve the entity's processes.
g) On the basis of the conclusions reached by the Head in his report, TECNIC will analyse, if necessary, the adoption of disciplinary or contractual measures or the exercise of legal actions.

## 5. COMMUNICATION

### 5.1. Communication

A copy of this Policy will be delivered, either by telematic means or on paper, to all those to whom it is addressed, so that all of them may be aware of their duties, rights and guarantees in relation to the use of the Whistleblowing Channel. In any case, easy and continuous access to this Policy shall be ensured to all its recipients. In the event that the recipients of this Policy do not speak Spanish, they shall be provided with a translation into a language they can understand. Evidence of having delivered this Policy to all its addressees shall be kept, without prejudice to its being understood as communicated to third parties outside the company via its website.

This Policy will also be published on TECNIC's homepage, in a separate and easily identifiable section for easier access.

### 5.2. Interpretation

In case of doubt about the interpretation of this Policy, queries will be sent to the Responsible via the e-mail address indicated above so that they can be resolved.

### 5.3. Training and awareness raising

TECNIC will also provide specific training on the use of the Whistleblowing Channel to all its members, which will be supported by this Policy and which must include, in any case, the following points:

- The existence of a Complaints Channel in the entity for the purposes described herein;
- How to use the Complaints Channel correctly and what the process is;
- Rights and duties of users of the Whistleblowing Channel;
- The obligation of the parties to whom this Policy is addressed to inform the entity of any of the facts described in section 1.2.

TECNIC will also provide specific training on the management of the Whistleblowing Channel to those responsible for receiving and processing complaints, in this case the person in charge of the Whistleblowing Channel and the management team. It must ensure that the person in charge is trained and qualified to manage the complaints channel.

TECNIC will keep evidence of any courses or other training or awareness-raising activities that may have been carried out for all users of the Whistleblowing Channel.

### 5.4. Commitment of those to whom the policy is addressed

All TECNIC's employees must be aware of the Policy, actively contribute to its respect and report any breaches of it that they become aware of, as well as any deficiencies they may observe in its content or development. TECNIC's management body will pay special attention to these duties.

## 6. HISTORICAL, APPROVAL, ENTRY INTO FORCE AND REFORM OF THE POLICY. EVIDENCE

### 6.1. History, approval and entry into force

Historical:

The following table shows the different versions of the Policy that have been drawn up, as well as the date and subsequent modifications that each version of the document may have undergone:

| VERSION | AUTHOR | DATE | CHANGES |
|---|---|---|---|
| 1.0 | External advisor | September 2024 | Initial version |
| 2.0 | To be determined | To be determined | To be determined |

Adoption and entry into force:

This Policy shall be approved by TECNIC's Board of Directors. The date of approval will be recorded in the minutes of the same. This date will be the date from which the document will enter into force in the entity.

### 6.2. Monitoring, continuous adjustment and reform of the Policy

Continuous monitoring and adaptation:

Periodic reviews of the content of the Policy will be established to guarantee its continuous adaptation to TECNIC's reality, legislative or jurisprudential changes, etc. Likewise, its use will be monitored and compliance with the Whistleblowing Channel system may be measured by means of indicators. All this in application of the principle of continuous improvement that governs TECNIC's processes.

Reform:

The Policy may be amended by the Board of Directors on its own initiative and/or at the proposal of any addressee of this Policy.

### 6.3. Custody of evidence

The person in charge will ensure the custody of all evidence that accredits the training, control, supervision and correction activities that have been carried out at TECNIC in accordance with the previous sections. This will be done in coordination with the corresponding personal data protection regulations for each of TECNIC's areas of activity.

## 7. PROTECTION OF PERSONAL DATA

In order to ensure compliance with personal data protection legislation and, in general, to prevent the improper use of information, TECNIC shall guarantee, in the management of the Internal Information System and with regard to both the informant and the reported person or third parties, that the processing of personal data arising from the application of this Policy shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016; by Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights; by Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties; and by Law 2/2023 of 20 February on the protection of persons who report regulatory offences and the fight against corruption; as well as by the provisions of the Procedure for the Management of Information Received on the protection of personal data.

**ANNEX I**

**Definitions:**

a) **Whistleblowing Channel: a** tool that TECNIC makes available to all its members to be able to report, securely, confidentially and/or anonymously, facts that may constitute a crime or a serious or very serious administrative offence.
b) **Reporting, alerting or communicating person:** a person who, either identified or anonymously, communicates to TECNIC any of the above facts in the reasonable belief that the information is true at the time of reporting. This person may be a member of the entity or a third party as described here. It should be borne in mind that Law 2/2023 of 20 February regulating the protection of persons who report regulatory infringements and the fight against corruption will only protect those who have an employment or professional relationship with TECNIC and who report an event constituting a criminal offence or a serious or very serious administrative offence. This is without prejudice to the protection that may be provided for the whistleblower in other bodies of law.
c) **Reported person:** person who is presumed to be the author and responsible for the reported facts. This person will also enjoy certain rights that will be developed in the General Procedure for the Management of Information Received and which are set out here.
d) **Head of the Internal Complaints System: a** single-person or collegiate body, appointed by TECNIC's Board of Directors, responsible for the management and processing of the Complaints Channel and subsequent internal investigations that may be carried out.
e) **Retaliation:** acts or omissions that are prohibited by law or that directly or indirectly result in unfavourable treatment that places the individuals concerned at a particular disadvantage compared to another in the employment or professional context, solely because of their status as whistleblowers, or because they have made a public disclosure. Such as, for example, dismissal, lack of internal promotion, job changes, etc.

**ANNEX II**

**Reception of the Internal Information System General Policy**

By signing this document, I certify that I have received, read and understood the General Policy of the Internal Information System. At the same time, I undertake to respect and comply with it.
I also understand that in the event that I fail to comply with its contents, this could lead to disciplinary action by TECNIC.
I also hereby agree to be updated on changes to the Policy and to read any future revisions that may be made to the Policy.

DATE:

NAME:

SIGNATURE: