PROCEDURE FOR MANAGING THE INTERNAL INFORMATION SYSTEM

Table of contents

1. PURPOSE

ENSA has implemented an Internal Reporting System with the aim of channelling and facilitating the submission, receipt, management and resolution of reports concerning alleged irregularities or breaches, and any violation of compliance obligations and the Code of Conduct, thereby fostering a compliance culture based on the principles and values of the ENSA Group.

The purpose of this document is to set out the necessary provisions for managing ENSA's internal reporting system in accordance with the requirements laid down in Law 2/2023 of 20 February, regulating the protection of persons reporting regulatory infringements and combating corruption.

Law 2/2023 transposes into Spanish law Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

2. SCOPE OF APPLICATION

2.1. Personal Scope

This Procedure applies to all staff working at ENSA, as well as to members of the organisation's governing body. It also applies to those who provide services on a regular basis, even if they are not part of the permanent workforce (through a contractor or on a work placement).

It shall also apply to those who report information on infringements obtained in the context of an employment relationship that has already ended, as well as to those whose employment relationship has not yet commenced, in cases where the information on infringements was obtained during the recruitment process.

Furthermore, the scope of application includes any natural or legal person who has obtained information on regulatory breaches in a professional context.

2.2. Material Scope

The following may be reported via the Internal Reporting System:

a. Breaches of European Union (EU) law, provided that they fall within the scope of the EU acts listed in the Annex to Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 and affect the EU's financial interests within the internal market.
b. Within the Spanish legal system, criminal offences, serious or very serious administrative offences, and breaches of labour law relating to health and safety at work.
c. Any other breaches set out in the ENSA Group's Code of Conduct, the Criminal Compliance and Anti-Bribery Policy, or its internal rules on Good Corporate Governance. The handling of reports relating to this type of breach not subject to Law 2/2023 shall be carried out in accordance with the general principles set out in the Internal Reporting System Policy.

3. MEASURES TO PROTECT AGAINST RETALIATION

3.1. CONDITIONS FOR ACCESS TO PROTECTION

The guiding principle of ENSA's Internal Reporting System Policy is the protection of the whistleblower. Consequently, individuals who report any of the regulatory breaches covered by the scope of Law 2/2023 shall be entitled to protection provided that the following circumstances apply:

- they have reasonable grounds to believe that the information in question is true at the time of reporting, even if they do not provide conclusive evidence, and
- the report has been made in accordance with the requirements set out in this Procedure.

In addition, the protection measures shall also apply, where appropriate, to:

a. The legal representatives of employees in the performance of their duties to advise and support the whistleblower.
b. Individuals who, within the organisation in which the whistleblower works, assist the whistleblower in the process.
c. Individuals who are related to the whistleblower and who may suffer reprisals, such as the whistleblower's colleagues or family members.

d. Legal entities for which the whistleblower works, or with which they have any other type of relationship in a work context, or in which they hold a significant stake. For these purposes, a stake in the capital or in the voting rights corresponding to shares or holdings is deemed to be significant when, by virtue of its proportion, it enables the person holding it to exert influence over the legal entity in which the stake is held.

However, the following persons are expressly excluded from the protection scheme:

a. Information contained in reports that have been deemed inadmissible.
b. Information relating to complaints about interpersonal conflicts or which affects only the whistleblower and the persons to whom the communication refers.
c. Information that is already fully available to the public or that constitutes mere rumours.

Furthermore, the Internal Reporting System may accept and handle reports concerning conduct which, whilst not constituting a criminal offence or a serious or very serious administrative offence, involves breaches of internal regulations or irregular practices (for example, breaches of the Code of Conduct or other corporate rules). However, such reports and the persons making them shall fall outside the scope of protection provided for in Law 2/2023 (in accordance with the provisions of Article 7.4 thereof), without prejudice to their processing in accordance with ENSA's internal regulations and procedures.

3.2. PROHIBITION OF RETALIATION

Acts constituting retaliation, including threats of retaliation and attempts at retaliation against persons who submit a report in accordance with the provisions of this Procedure, are expressly prohibited.

Retaliation is understood to mean any acts or omissions that are prohibited by Law 2/2023, or which, directly or indirectly, constitute unfavourable treatment that places those who suffer them at a particular disadvantage compared with others in the workplace or professional context, solely by virtue of their status as whistleblowers, provided that such acts or omissions occur whilst the investigation is ongoing and within two years of its conclusion.

Specifically, the following shall be considered acts of retaliation:

a. Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including the non-renewal or early termination of a fixed-term employment contract once the probationary period has been completed, or early termination or cancellation of contracts for goods or services; the imposition of any disciplinary measure; demotion or refusal of promotion; and any other substantial change to working conditions; and the failure to convert a fixed-term employment contract into a permanent one, where the worker had legitimate expectations that they would be offered permanent employment; unless such measures were taken in the normal exercise of managerial authority under labour legislation or the relevant regulations governing the status of public servants, on the basis of proven circumstances, facts or breaches, and unrelated to the submission of the communication.
b. Damages, including reputational damage, or financial loss, coercion, intimidation, harassment or ostracism.
c. Negative assessments or references regarding work or professional performance.
d. Inclusion on blacklists or the dissemination of information within a specific sector, which hinders or prevents access to employment or the awarding of contracts for works or services.
e. Refusal or revocation of a licence or permit.
f. Denial of training.
g. Discrimination, or unfavourable or unfair treatment.

In the event of retaliation, the Head of the Internal Reporting System must be informed immediately via the email address compliance@ensa.es.

In addition, the Head of the Internal Reporting System will periodically monitor the situation of the whistleblower and, where applicable, of those persons covered by the protection scheme.

If the Head of the Internal Reporting System finds that reprisals have been taken whilst the protection scheme is in force, in addition to any disciplinary measures and/or administrative sanctions that may apply, the necessary and available measures will be taken to restore the persons subjected to reprisals to the situation they were in prior to the harm suffered.

4. OBLIGATIONS IN RELATION TO THIS PROCEDURE

4.1. Obligations of ENSA staff

In general, all ENSA staff, including members of the organisation's governing body, must maintain the strictest confidentiality regarding:

a. The identity of the whistleblower.
b. The identity of the persons affected by the report.
c. The identity of any other persons mentioned in the report.
d. Any information reported via the internal reporting system.

In particular, those authorised to know the identity of the whistleblower shall ensure the confidentiality of that identity and that of any third party mentioned in the report.

Where a report is submitted via channels other than those set out in this Procedure, or to staff members not responsible for processing it, the recipient of the report must immediately forward it to the Internal Reporting System Manager (hereinafter 'the System Manager').

The System Manager may request the cooperation of ENSA staff in the investigation proceedings; within the applicable legal framework, such staff shall be obliged to:

a. Appear before the System Manager, should they be required to do so, and answer all questions put to them.
b. Respond to all requests for information or documentation made by the System Manager.
c. Maintain confidentiality regarding the existence of the investigation and its content.

Requests for cooperation must be complied with without delay and, in any event, within the time limits specified by the System Manager.

Furthermore, ENSA staff, including members of the organisation's governing body, must refrain from:

- Obstructing the submission of reports.
- Preventing, obstructing or delaying the follow-up to reports, including the provision of false or incomplete information or documentation if so requested.

- Taking any retaliatory action, including threats of retaliation and attempts at retaliation, against persons who submit a report or other persons covered by the scope of protection, in accordance with the provisions of section 3 of this Procedure.
- Disclosing information via the Internal Reporting System whilst knowing it to be false.

4.2. Obligations of non-ENSA staff

The obligations established for ENSA staff shall apply to non-ENSA staff who fall within the scope of this Procedure.

In both cases, a failure to cooperate with the System Manager may result in the case being closed.

5. CHANNELS FOR REPORTING BREACHES

On ENSA's corporate website (www.ensa.es), there is a link entitled 'Ethics Channel' which provides access to a platform provided by a specialist technology company. This platform is equipped with appropriate technical measures to guarantee the confidentiality and security of information, as well as anonymity when this method of reporting is chosen.

Once the report has been submitted, it will be automatically recorded on the platform, creating a case file to which all documentation relating to the report must be attached. Furthermore, a confidential channel will be established for exchanging messages with the whistleblower, regardless of whether the report was made by name or anonymously.

It is also possible, at the whistleblower's request, to report breaches of regulations through a face-to-face meeting with the System Manager; such a meeting may be requested via the following email address: compliance@ensa.es, and must take place within the following seven (7) days.

If the report is made via a face-to-face meeting, the System Manager will document it in one of the following ways, subject to the whistleblower's prior consent:

a. By recording the conversation in a secure, durable and accessible format, or
b. By means of a complete and accurate transcript of the conversation.

Without prejudice to the rights to which the whistleblower is entitled under data protection legislation, they will be given the opportunity to verify, correct and sign to confirm the transcript of the conversation.

In addition, the communication may be submitted via an external channel set up and managed by the Independent Whistleblower Protection Authority (AIPI), a public-law body operating at national level and linked to the Ministry of the Presidency, Justice and Relations with the Courts.

6. PROCEDURE FOR HANDLING REPORTS

The Compliance Committee is responsible for the Internal Reporting System; the Chair of the Compliance Committee is the individual to whom the powers to manage the Internal Reporting System and to process investigation files have been delegated.

In the event of a vacancy, absence or illness of this person, or where it is substantiated that they are in a situation of conflict of interest, the Head of the General Secretariat and of the Council and Sustainability will act as their substitute.

6.1. Receipt of reports

Any person deciding to make a report must provide, together with the report, as much information as possible regarding the facts reported, and must expressly include:

a. The nature of the informant’s relationship with ENSA, in accordance with section 2.1 of this Procedure.
b. The date or dates on which the reported events took place.
c. The person(s), if any, responsible for those events.
d. A complete and accurate description of the facts.
e. Documents, data and other sources of evidence or information which, where applicable, may facilitate the investigation of the facts.

Upon receipt of the information, within a period not exceeding seven calendar days following its receipt, an acknowledgement of receipt shall be sent to the whistleblower, unless this would jeopardise the confidentiality of the communication.

Once the information has been recorded, the System Manager must verify whether it sets out facts or conduct constituting a breach, irregularity or unlawful act under ENSA’s Good Governance System. To this end, the System Manager may, if deemed appropriate, request additional information from the whistleblower to clarify or supplement the details provided in the report, together with any documents or data deemed necessary to substantiate the existence of the irregular or unlawful conduct.

Once the initial assessment of the report has been carried out on the basis of its subject matter, the System Manager shall refer the report to the case handler, bearing in mind that:

a. Reports concerning workplace harassment, sexual harassment or harassment on the grounds of sex shall be referred to the Head of the People and Talent Division and shall be dealt with in accordance with the provisions of ENSA's Protocol on the Prevention of and Response to Harassment. If the final report concludes that the reported facts constitute harassment, that report must be forwarded to the Head of the General Secretariat and the Board of and Sustainability to proceed in accordance with the provisions of section 6.4. In all cases, the maximum time limit established in this Procedure for responding to the investigation will be observed.
b. Reports concerning data protection breaches shall be referred to the person responsible for coordinating the protection of personal data within the organisation, although they shall be processed in accordance with the provisions of the following sections. In the event of the vacancy, absence or illness of this person, or where it is alleged, with supporting evidence, that they are in a situation of conflict of interest, the Compliance Committee shall act as the case manager.
c. Communications concerning other matters shall be handled by the Compliance Committee, in accordance with the provisions of the following paragraphs.

In all cases, the Compliance Committee must ensure that the case is dealt with promptly.

6.2. ADMISSIBILITY OR INADMISSIBILITY PROCEDURE

Once this preliminary analysis has been carried out, the case manager shall decide:

a. To reject the report for consideration in any of the following cases:
   - Where the facts described lack any plausibility.
   - Where the facts described do not constitute an offence falling within the scope of this Procedure.
   - Where the report is manifestly unfounded because it does not meet the requirements set out in section 6.1 of this Procedure, or where there are

reasonable grounds to believe that the evidence was obtained through the commission of a criminal offence.

- Where the report does not contain new and significant information regarding infringements compared with a previous report in respect of which the relevant proceedings have been concluded, unless there are new circumstances justifying a different course of action.

In the event that the report is rejected, the System Manager shall ensure that the whistleblower suffers no adverse consequences as a result of having made the report.

b. To accept the report for processing, applying, where appropriate, the protection regime against possible reprisals in accordance with the terms set out in paragraph 3 of this Procedure.

In cases where reports are made by persons who do not fall within the scope of this Procedure, the report shall be rejected, without prejudice to any appropriate legal action that may be taken.

The decision to accept or reject the report for consideration shall be communicated to the whistleblower as soon as possible. The decision to reject the report for consideration shall be briefly justified.

6.3. INVESTIGATIVE PROCEDURES

The case manager shall carry out all investigative procedures deemed appropriate to verify the accuracy of the facts reported and shall record these in the case file. Some of the main procedures that may form part of the investigation are detailed below:

a. Conducting interviews with the whistleblower, with the individuals mentioned in the report or with ENSA staff, which must be properly documented.
b. Gathering all information or documentation deemed necessary from any of the organisation's departments.
c. Accessing the IT systems and devices that the organisation makes available to its employees for professional purposes (for example, laptops, email accounts, storage devices, etc.), within the limits set out in the applicable employment regulations and data protection legislation.

If necessary, the case manager may seek the necessary assistance from third parties outside the organisation to carry out the investigative procedures, which must, in all cases, comply with the principles set out in the Internal Reporting System Policy. Any recruitment procedures that need to be followed shall be carried out with the necessary speed to ensure that the investigation deadlines are met.

The person concerned by the information will be informed of the allegations against them, although this information will be provided at the time and in the manner deemed appropriate to ensure the successful completion of the investigation.

Under no circumstances will the identity of the whistleblower be disclosed to them, nor will they have access to the communication. Furthermore, they shall have the right to be heard at any time in order to present their version of events and to provide any evidence they deem appropriate and relevant. All of this shall be carried out with full respect for their right to honour, the presumption of innocence and the right to a defence, in accordance with the provisions of Law 2/2023. They shall also be informed of the possibility of appearing in the presence of a lawyer.

6.4. CONCLUSION OF THE PROCEEDINGS

Once the investigation has been completed, the case officer will issue a report containing a summary of the procedures carried out to verify the plausibility of the facts, an assessment of those procedures and the conclusions reached.

The case officer shall close the case in the following circumstances:

a. Where there are no facts that could constitute a regulatory infringement falling within the scope of this Procedure.
b. Where the investigations carried out do not provide sufficient evidence that the breach has been committed.
c. Where the established facts clearly do not constitute a regulatory infringement falling within the scope of this Procedure.
d. Where it has not been possible to identify the person or persons responsible.
e. Where it is concluded, at any time, that the infringement is time-barred.

However, should the investigation reveal any shortcomings that need to be rectified, a report setting out proposals for improvement will be drawn up and forwarded to the Presidency.

The informant and, where applicable, the person concerned will be notified that the case has been closed.

If the case manager considers that the investigations carried out provide sufficient evidence of a regulatory breach falling within the scope of this Procedure, they shall forward their report to the Head of the General Secretariat and the Council and Sustainability Department for a ruling on the legal classification of the facts.

Upon receipt of the legal report, if the facts could constitute a criminal offence, the Public Prosecutor's Office or the European Public Prosecutor's Office must be informed immediately should the facts affect the financial interests of the European Union, provided that no other fundamental rights are affected.

Furthermore, the case handler must propose appropriate preventive measures to mitigate the risk of a recurrence of the misconduct. Should the misconduct not have ceased, they must also draw up a proposal on how to remedy the situation.

In all cases where the case has not been closed, the reports from the case manager and the Head of the General Secretariat and the Council and Sustainability Department shall be forwarded to the Presidency for information.

Furthermore, should disciplinary measures be warranted against an employee of the organisation, the reports shall be forwarded to the relevant People and Talent Department so that it may, in the exercise of its powers, assess the possible measures to be adopted in accordance with labour regulations and the applicable internal procedures.

The Compliance Committee, in its capacity as the investigating body of the Internal Reporting System, may draw up the conclusions and, where appropriate, make any proposals it deems fit, though under no circumstances shall it be responsible for imposing disciplinary measures.

Once any disciplinary measures have been taken by the relevant People and Talent department, the Compliance Committee will be informed for the purposes of being kept apprised and monitoring the situation.

A brief summary of the investigation's findings shall be provided to the whistleblower and the person concerned.

The time limit for completing the proceedings and responding to the whistleblower shall not exceed three months from the date of receipt of the complete report or, where applicable, from the date on which any deficiencies that led to the report being deemed inadmissible have been rectified. This time limit may be extended, with justification, for a maximum of a further three months in particularly complex cases.

As a general rule, any necessary procedures shall take place on ENSA's premises during working hours from Monday to Friday.

The whistleblower and the person(s) referred to in the report may submit representations regarding the decisions taken by the case manager, who is authorised to review them if they consider there are grounds to do so.

7. CONFLICT OF INTEREST

The submission of a report that directly affects individuals who may be actively involved in its management and investigation – that is, one or more members of the Compliance Committee – shall result in their automatic exclusion from the entire investigation and analysis process until its resolution, in order to avoid any conflict of interest or incompatibility and thus ensure the objectivity and independence of the actions carried out by the Compliance Committee itself.

Members of the Compliance Committee shall be obliged to maintain the utmost confidentiality regarding the report. Furthermore, members involved in a conflict of interest shall be prohibited from having direct or indirect access to any information relating to the identity of the whistleblower or the progress of the ongoing investigation.

8. PROTECTION OF PERSONAL DATA

The processing of personal data arising from the application of this Procedure shall be governed by the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights, Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of preventing, detecting, investigating and prosecuting criminal offences and enforcing criminal sanctions, and in Title VI of Act 2/2023 of 20 February, regulating the protection of persons reporting regulatory infringements and combating corruption.

The data controller for the personal data processed within the Internal Information System is Equipos Nucleares S.A., S.M.E. (ENSA).

Personal data and any other information provided via the internal reporting system will be processed for the purpose of receiving reports of regulatory breaches, analysing their content and managing the relevant case file. The processing of personal data is based on compliance with a legal obligation, in accordance with Article 30 of Law 2/2023.

The identity of whistleblowers will be kept confidential at all times; it will not be disclosed to the persons to whom the reported facts relate or to third parties.

Data subjects may exercise their rights to object, access, rectification, erasure, restriction and data portability by sending an email to protecciondedatos@ensa.es or by post to Equipos Nucleares, S.A., S.M.E., Avda. Juan Carlos I, No. 8, 39600 Maliaño (Cantabria).

Should the person to whom the facts set out in the communication relate exercise their right to object, it will be presumed, unless there is evidence to the contrary, that there are compelling legitimate grounds justifying the processing of their personal data.

Access to the personal data contained in the Internal Reporting System shall be restricted, within the scope of their powers and duties, exclusively to:

a. The Compliance Committee, as the body responsible for the Internal Reporting System, and the person managing the relevant case file.
b. The Head of the General Secretariat and of the Board and Sustainability at ENSA, where disciplinary measures may need to be taken against an employee and where legal action may be required in relation to the facts set out in the report.
c. Any data processors who may be appointed.

The processing of data by other persons, or even its disclosure to third parties, shall be lawful where necessary for the adoption of corrective measures within the organisation or the handling of any disciplinary or criminal proceedings that may be applicable.

Under no circumstances shall personal data that is not necessary for the investigation of regulatory breaches falling within the scope of this Procedure be processed; such data shall, where appropriate, be deleted immediately. Likewise, any personal data that may have been disclosed and that relates to conduct not falling within that scope shall be deleted.

If the information received contains personal data falling within the special categories of data, it shall be deleted immediately, without being recorded or processed.

Data subject to processing shall be retained in the system only for the time strictly necessary to decide whether to initiate an investigation into the reported facts.

If it is established that the information provided, or part thereof, is untrue, it shall be deleted immediately upon becoming aware of this fact, unless such untruthfulness may constitute a criminal offence, in which case the information shall be retained for the time necessary whilst the legal proceedings are ongoing.

In any event, if three months have elapsed since the receipt of the report without any investigative proceedings having been initiated, the information must be deleted, unless the purpose of retaining it is to provide evidence of the system's operation. Reports that have not been acted upon may only be retained in anonymised form, and the blocking obligation set out in Article 32 of Organic Law 3/2018 of 5 December shall not apply.

Under no circumstances may personal data relating to the information received and to internal investigations be retained for a period exceeding ten years.

9. FAILURE TO COMPLY WITH THE PROCEDURE

In general, all ENSA staff, including members of the organisation's governing body, are required to comply with the provisions of this Procedure; disciplinary measures may be taken in the event of non-compliance.

Furthermore, Law 2/2023 establishes a system of penalties to which all natural and legal persons who commit any of the offences defined in that Law are subject. Where natural persons are responsible for the offences, the amount of the fines will range from 1,001 to 300,000 euros, depending on whether a minor, serious or very serious offence has been committed.

Within the state public sector, the Independent Whistleblower Protection Authority (A.I.P.I.) shall be responsible for applying the penalty regime.

The obligation to comply with this Procedure extends to persons outside ENSA who submit a report via the organisation's internal reporting system.

10. APPROVAL, ENTRY INTO FORCE AND DISSEMINATION

ENSA's Board of Directors is the body responsible for approving this Procedure, which came into force on the date of its approval and was published on ENSA's corporate website and on its intranet.

Notwithstanding the foregoing, this Procedure will be subject to ongoing review and, where necessary, updating, in order to bring it into line with any regulatory changes that may occur, as well as to incorporate any identified opportunities for improvement.

Following a proposal from the Compliance Committee and subject to the approval of the Management Committee, the update to this Procedure was approved by ENSA's Board of Directors on 25 June 2026.

The relevant management department will organise the necessary training initiatives to ensure the proper dissemination of this Procedure, the culture of compliance and the objectives of Act 2/2023.