INTERNAL REPORTING SYSTEM MANAGEMENT PROCEDURE

PREPARED BY	REVIEWED BY	APPROVED BY	APPROVED BY
Audit and Control Directorate Elena Diez Martínez Director of Audit and Control	**General Secretariat and Board of Directors** José Antonio Benedicto Iruiñ General Secretary and Secretary of the Board of Directors	**Steering Committee** José Antonio Benedicto Iruiñ Secretary of the Steering Committee	**Board of Directors** José Antonio Benedicto Iruiñ Secretary of the Board of Directors

Revision	Date	Motive
0	09.06.2023	Initial edition. Compliance with Law 2/2023 of 20 February (Protection of whistleblowers)

TABLE OF CONTENTS

1. PURPOSE 3
2. SCOPE OF APPLICATION 3
2.1 Subjective Scope 3
2.2 Objective Scope 3
3. MEASURES TO PROTECT AGAINST RETALIATION 4
3.1 Conditions for Access to Protection 4
3.2 Prohibition of Retaliation 5
3.3 Support Measures 6
4. OBLIGATIONS OF ENSA STAFF 7
5. INITIATING A REPORT 8
6. REPORTING MANAGEMENT PROCEDURE 8
6.1 Reporting Receipt 9
6.2 Acceptance or Non-acceptance Procedure 10
6.3 Investigation Proceedings 11
6.4 Completion of the Proceedings 11
7. CONFLICT OF INTEREST 13
8. PROTECTION OF PERSONAL DATA 13
9. NON-COMPLIANCE WITH THE PROCEDURE 15
10. APPROVAL, ENTRY INTO FORCE AND DISSEMINATION 15

1. PURPOSE

ENSA has implemented its Internal Reporting System with the purpose of channelling and facilitating the submission, receipt, management and resolution of any reports of alleged irregularities or breaches as well as any violation of compliance obligations and the Code of Conduct, in order to foster an environment of compliance based on ENSA Group's principles and values.

The purpose of this document is to establish the provisions necessary to manage ENSA's Internal Reporting System in accordance with the requirements set out in Law 2/2023 of 20 February, regulating the protection of individuals who report regulatory infringements and oppose corruption.

2. SCOPE OF APPLICATION

2.1 Subjective Scope

This procedure shall apply to whistleblowers who are employees of ENSA or interested parties, and who have received information about policies on offences in an employment or professional context, to include:

a) individuals who have the status of employees of the company.
b) self-employed individuals providing services to the company.
c) shareholders, individuals belonging to the administrative, management or supervisory body of the company, including non-executive members.
d) any individual working for or under the supervision and direction of contractors, subcontractors or suppliers.

It shall also apply to individuals who report on breaches obtained in the framework of an employment or statutory relationship that has already ended, volunteers, trainees, trainee workers (whether or not they receive remuneration), and those whose employment relationship has not yet started, in cases where the information on breaches was obtained during the recruitment process or pre-contractual negotiation.

2.2 Objective Scope

The Internal Reporting System may be used to report:

a) any act or omission which may constitute an infringement of European Union law provided that

1. they fall within the scope of the European Union acts listed in the Annex to Directive (EU) 2019/1937 of the European Parliament or of the Council of 23 October 2019 on the protection of individuals reporting breaches of EU law, regardless of their qualification by the internal legal system;

2. they 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

3. they affect the internal market, as referred to in Article 26(2) of the TFEU, including infringements of EU competition rules and aid granted by states, as well as infringements relating to the internal market in connection with acts that infringe corporate tax rules or practices aimed at obtaining a tax advantage that distorts the object or purpose of the legislation applicable to corporate taxation.

b) actions or omissions that could constitute a serious or very serious criminal or administrative offence. All serious or very serious criminal or administrative offences involving financial loss for the Public Treasury or Social Security shall be understood to be included.

c) any actions or omissions that may constitute breaches of ENSA Group's Code of Conduct, Criminal and Anti-Bribery Compliance Policy or its internal rules of Good Corporate Governance.

3. MEASURES TO PROTECT AGAINST RETALIATION

3. 1 Conditions for Access to Protection

The guiding principle of ENSA's Internal Reporting System Policy is whistleblower protection. Accordingly, all individuals who report a breach of the regulations provided for in the scope of application of this procedure shall be entitled to protection provided that:

- they have reasonable grounds to believe that the information provided is true at the time of the report, regardless of a potential lack of 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 the employees in the exercise of their functions of advising and supporting the whistleblower.
b) natural individuals who, within the organisation in which the whistleblower provides services, assist the whistleblower in the process.

c) natural individuals related to the whistleblower who may suffer retaliation, such as colleagues or family members of the whistleblower.
d) legal individuals with whom the whistleblower has any type of professional relations or significant shareholding, which is defined as a holding of capital, share, voting rights, or other participation deemed to be significant when, by virtue of its proportion, enables the holder to have an influence on the stakes of the whistleblower.

Individuals reporting the following are expressly excluded from the protection regime:

a) Information contained in reports that have not been accepted for processing.
b) Information relating to complaints about interpersonal disputes or concerning only the whistleblower and the individuals to whom the report relates.
c) Information which is already fully available to the public or which constitutes mere hearsay.

3. 2 Prohibition of Retaliation

Acts constituting retaliation, including threats of retaliation and attempts to retaliate against individuals submitting a report under this Procedure are expressly prohibited.

Retaliation signifies any acts or omissions which are prohibited by Law 2/2023, or which, directly or indirectly, involve unfavourable treatment that places the individuals suffering them at a particular professional disadvantage compared to another individual solely due to their status as whistleblowers, provided that such acts or omissions occur during the investigative proceedings and within two years of their completion.

Retaliation shall be deemed to take the form of:

a) 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 a permanent one, where the employee had legitimate expectations that he/she would be offered a permanent job; unless these measures were carried out as part of the regular exercise of managerial authority under the relevant labour or public employee statute legislation, due to circumstances, facts or breaches that are provable and unrelated to the submission of the report.

b) damages, including reputational damage, economic loss, coercion, intimidation, harassment or ostracism.
c) negative evaluation or professional references.
d) blacklisting or disseminating information in a particular sectoral area, which hinders or prevents access to employment or the contracting of works or services.
e) refusal or revocation of a licence or permit.
f) refusal of training.
g) discrimination, unfavourable or unfair treatment.

In the event of retaliation, immediately report the case via email to: canaletico@ensa.es in order to alert the Compliance Committee, which operates as the Internal Reporting System Manager. This committee shall diligently monitor the situation of the whistleblower and, where appropriate, of those individuals included in the protection regime.

If the System Manager finds that retaliation has been taken during the period of protection, in addition to the disciplinary measures and/or administrative sanctions that may be applicable, the necessary and available measures shall be taken to restore the retaliated individual to the situation prior to the harm suffered.

3. 3 Support Measures

ENSA shall provide its own support and assistance measures, without prejudice to those adopted by the Independent Whistleblower Protection Authority (A.A.I.), to individuals who report or disclose breaches referred to in paragraph 2 through the internal reporting channels outlined in this procedure, via the following support measures:

a) Comprehensive and independent information and advice from the company on the procedures and remedies available, protection against retaliation and preservation of the rights of the individuals concerned.
b) Adequate support with any relevant authority involved in the protection against retaliation, including certification of eligibility for protection under this act.
c) Legal assistance in criminal proceedings and in cross-border civil proceedings in accordance with local law.
d) Financial and psychological support, on an exceptional basis, if declared necessary by the Independent Whistleblower Protection Authority (A.A.I), following an assessment of the circumstances stemming from the submission of the report.

4. OBLIGATIONS OF ENSA STAFF

All ENSA staff, including individuals belonging to the entity's administrative body, must maintain complete confidentiality regarding:

a) the identity of the whistleblower.
b) the identity of the individuals affected by the report.
c) the identity of any other individuals mentioned in the report.
d) any type of information reported through the Internal Reporting System.

The individuals entitled by law to know the identity of the whistleblower shall serve as the guarantor of confidentiality in all aspects of the report, including the identities of the author and any third party mentioned in the report.

Where the report is sent by means other than those set out in this procedure or to members of staff not responsible for its processing, the recipient of the report shall immediately forward it to the individual in charge of the System (hereinafter "the System Manager").

The Internal Reporting System Manager may request ENSA staff to collaborate in the investigation, who shall have, within the applicable legal framework, the obligation to:

a) appear before the System Manager, in the event that they are required to do so, answering all questions they are asked.

b) respond to all appropriate requests for information or documentation requested by the System Manager.

c) Maintain confidentiality about the existence of the investigation and its contents.

The request for cooperation must be executed without delay within the deadlines set by the Internal Reporting System Manager.

ENSA staff, including individuals belonging to the entity's administrative body, shall refrain from:

- obstructing the submission of reports.
- preventing, complicating or delaying the follow-up on reports, by means including, but not limited to, providing false or incomplete information or documentation if requested.
- engaging in any retaliation, including threats of retaliation and attempts of retaliation, against individuals submitting a report or other individuals falling within the scope of protection, as set out in paragraph 3 of this procedure.

- communicating information known to be false through the Internal Reporting System.

The obligations established for ENSA staff apply to non-ENSA staff who are included in the scope of application of this procedure.

Failure to cooperate with the reporting System Manager may result in the file being closed.

5. INITIATING A REPORT

On ENSA's corporate website (www.ensa.es) there is a link labelled Ethical Channel that permits access to a platform provided by a specialised technology company. This platform has appropriate technical measures in place to guarantee the confidentiality and security of the information, as well as anonymity.

Upon submitting a report, a log will be registered on the platform automatically and a file will be generated, to which all the documentation related to the report must be attached.

Regulatory breaches can be reported via a face-to-face meeting with the Internal Reporting System Manager, at the request of the whistleblower via email submission to canaletico@ensa.es.

In the event of communication via a face-to-face meeting, the internal reporting System Manager shall receive the consent of the whistleblower to document in one of the following formats:

(a) a recording of the conversation in a secure, durable and accessible format; or
b) a complete and accurate transcript of the conversation. In this case, the System Manager shall be assisted by the individual in charge of the General Secretariat and of the Board.

Without prejudice to the rights of the whistleblower and in accordance with data protection regulations, the whistleblower shall be given the opportunity to verify, rectify and agree by signature to the transcription of the conversation.

The report may be addressed to an external channel developed and managed by the Independent Whistleblower Protection Authority (A.A.I.), a public law entity at the state level linked to the Ministry of Justice.

6. REPORTING MANAGEMENT PROCEDURE

The Compliance Committee is responsible for the Internal Reporting System, and the individual in charge of the Audit and Control Directorate is the natural individual to whom the Board of Directors has delegated the management of the Internal Reporting System. A

subcommittee of the Compliance Committee created for this purpose shall be responsible for the management and processing of the investigation files of the reports received.

In the event of vacancy, absence or illness of this individual, or when it is alleged that he/she is in a situation of conflict of interest, the General Secretary and Secretary of the Board shall act as a substitute.

6.1 Reporting receipt

All individuals who submit a report shall provide all possible information on the facts reported including the following requirements:

a) The nature of the professional association between the whistleblower and ENSA, in accordance with section 2.1 of this procedure.
b) The date(s) on which the reported event(s) occurred.
c) The person(s), if any, responsible for such acts.
d) A full and accurate description of the facts.
e) Documents, data and other evidence that may aid the investigation.

Upon receipt of the report, acknowledgement must be given within seven calendar days of receipt, unless doing so would jeopardise the confidentiality of the report.

After recording the report, the System Manager shall determine if the case constitutes a breach, irregularity or unlawfulness of ENSA's Good Governance System. Additional information may be requested from the whistleblower if deemed necessary to clarify or complete the report.

Following the initial assessment of the report, the management of the file may be further guided by the following:

a) Reports on the basis of workplace, sexual or gender-based harassment shall be referred to the People and Human Talent Area and shall be processed in accordance with the provisions of ENSA's Protocol for the Prevention of and Action Against Harassment. If the final report concludes that the facts reported constitute harassment, the report shall be sent to the individual in charge of the General Secretariat and the Board in order to proceed in accordance with the provisions of section 6.4. The maximum time limit established in this procedure for responding to the investigation proceedings shall be respected. In the event of the vacancy, absence or illness of this individual, or in cases of a justified allegation of conflict of interest, the director responsible for the compliance area shall act as the manager of the file.

b) Reports relating to data protection breaches shall be referred to the individual responsible for coordinating the entity's personal data protection and processed in accordance with the provisions of the subsequent sections. In the event of vacancy, absence or illness of this individual, or when there is a justified allegation of a conflict of interest, the director responsible for the compliance area shall act as the manager of the file.

c) Reports on other matters shall be managed by the delegated subcommittee in accordance with the subsequent sections.

In all cases, the System Manager shall ensure that the file is dealt with expeditiously.

6.2 Acceptance or Non-acceptance Procedure

Following this preliminary analysis, the System Manager shall select one of the following actions:

a) Not to accept the report for processing, due to any of the following circumstances:

- The facts reported lack credibility or do not constitute a breach, irregularity or unlawfulness of ENSA's Corporate Governance System.
- The facts reported do not constitute an infringement of the law within the scope of application of this procedure.
- The report is deemed to be unsubstantiated due to the absence of requirements outlined in section 6.1 of this procedure or if there are reasonable grounds to believe that the evidence was obtained through an offence.
- The report does not contain significant new information on infringements that have already been outlined in a previously processed unless there are recent circumstances that justify a different follow-up.

b) To accept the report for processing, with the consequencing system of protection against possible retaliation as outlined in the terms of section 3 of this procedure.

c) To immediately forward the report to the Public Prosecutor's Office in the event of a possible criminal offence.

In the case of reports made by individuals who are not included in the subjective scope of this procedure, the report shall be rejected without prejudice to the appropriate legal action to be taken.

The decision of acceptance or non-acceptance shall be communicated to the whistleblower as soon as possible. The reasons for the non-acceptance shall be stated succinctly.

6.3 Investigation proceedings

The investigation proceedings must make every effort to verify the plausibility of the facts reported and all details must be recorded in the file. The following are some but not all of the key proceedings that may shape the investigation:

a) Interviews with the whistleblower, individuals mentioned in the report or with ENSA staff, all of which shall be properly documented.
b) Information or documentation it deemed necessary from any of the entity's directorates.
c) Access to computer systems and devices that the entity makes available to its employees for business purposes (e.g. laptops, e-mail accounts, storage devices, etc.), within the limits set out in the applicable labour and data protection regulations.

If necessary, the System Manager may be provided with the necessary assistance to carry out the investigative proceedings, which shall respect the principles set out in the Internal Reporting System Policy. The recruitment procedures to be followed shall be carried out as expeditiously as necessary to meet the deadlines of the investigation.

It must be ensured that the individual involved in the report is made aware of the report and facts as summarised, though this information shall be provided at such time and in such format as is considered appropriate to ensure the proper conduct of the investigation. In no case shall the identity of the whistleblower be communicated to the individuals concerned, nor shall access to the report be given. Affected parties have the right to be heard at any time in order to present their version of the facts and provide any evidence they deem appropriate and relevant, always with full presumption of innocence. Affected parties shall be informed of the possibility of being aided by a lawyer.

6.4 Completion of the proceedings

Upon completion of the investigation, the System Manager shall issue a report containing a summary of the facts reported, the actions carried out in order to verify the plausibility of the facts, the assessment of the proceedings, the evidence supporting them, and the conclusions reached in the investigation.

The written report of the conclusions reached shall be submitted to the Compliance Committee, which will take one of the following decisions:

a) To close the file in the following cases:

- Absence of the facts that could constitute a regulatory infringement as outlined in this procedure.
- Lack of proof that an offence has been committed.
- Proven facts that do not manifestly constitute an infringement of the rules falling within the scope of this procedure.
- Inability to identify the person(s) responsible.
- Conclusion that, at any time, the infringement is beyond the statute of limitations.

The whistleblower and, where appropriate, the individual(s) concerned shall be notified of the closure of the file.

b) If the resolution of the Compliance Committee concludes that the individual concerned or any other individuals involved at ENSA are responsible for the conditions or conduct reported, the resolution shall be passed on to the Steering Committee to proceed with appropriate measures.

c) If the Compliance Committee considers that the proceedings carried out sufficiently accredit the commission of a regulatory infringement included in the scope of application of this procedure, it shall forward the report to the individual in charge of the General Secretariat and of the Board so that he/she may rule on the legal classification of the facts.

d) Upon receipt of the legal report, if the facts could be criminal in nature, the Public Prosecutor's Office or the European Public Prosecutor's Office shall be informed immediately if the facts affect the financial interests of the European Union.

In all cases in which the file has not been closed, the reports of the System Manager and of the individual in charge of the General Secretariat and of the Board shall be sent to the Chair of the Board of Directors for information.

If disciplinary measures will be taken against an employee of the entity, the reports are to be forwarded to the competent Directorate for People and Human Talent.

The decisions taken will be summarised to the whistleblower and to the individual concerned.

The period for finalising the proceedings and providing a response to the whistleblower may not exceed three months from the receipt of the complete report or, where applicable, from the compliance with requirements received after non-acceptance of the report. This period may be extended by up to a maximum of three additional months in cases of particular complexity.

7. CONFLICT OF INTEREST

The submission of a report that directly affects individuals who may actively participate in the management and investigation of the same, i.e. one or several members of the Compliance Committee, shall be automatically excluded throughout the investigation and analysis process until its resolution, in order to avoid any type of conflict of interest and incompatibility and to guarantee the objectivity and independence of the actions carried out by the Compliance Committee itself.

Excluded members of the Compliance Committee shall be obliged to maintain the utmost confidentiality of the report, with direct or indirect access to any information on the identity of the whistleblower and the ongoing investigation process is prohibited.

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 Guarantee of Digital Rights, 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 in Title VI of Law 2/2023 of 20 February, regulating the protection of individuals who report regulatory offences and the fight against corruption.

Equipos Nucleares S.A., S.M.E. (ENSA) is responsible for the processing of personal data processed in the Internal Reporting System.

Personal data and other information provided through the Internal Reporting System shall be processed for the purpose of receiving notifications of regulatory infringements, analysing their content and managing the corresponding file. The processing of personal data is based on the fulfilment of a legal obligation, in accordance with Article 30 of Law 2/2023.

The identity of whistleblowers shall be kept confidential to prevent communication both to involved parties and third parties.

The interested parties shall be able to exercise their rights of opposition, access, rectification, suppression, limitation and portability by sending an e-mail to protecciondedatos@ensa.es or by post to Equipos Nucleares, S.A., S.M.E., Avda. Juan Carlos I, nº 8, 39600 Maliaño (Cantabria).

In the event that an individual referenced in the report exercises the right of opposition, it shall be presumed that, in the absence of proof to the contrary, there are compelling grounds that legitimise the processing of his or her personal data.

Access to personal data contained in the Internal Reporting System shall be limited, within the scope of their competencies and functions, exclusively to:

a) The Internal Reporting System Manager and whoever manages the corresponding file.
b) ENSA's People and Human Resources Directorate, only when disciplinary measures may be taken against an employee.
c) The individual in charge of the General Secretariat and of the Board of ENSA, should legal action be taken in relation to the facts described in the report.
d) The individuals in charge of processing that may be appointed.

The processing of the data by other individuals and communication to third parties is lawful where the adoption of corrective measures in the entity or the processing of the sanctioning or criminal proceedings is required.

Under no circumstances shall personal data be processed if they are not necessary for the knowledge and investigation of the regulatory infringements included in the scope of application of this procedure, and, where appropriate, they shall be deleted immediately.

Any personal data that may have been communicated in relation to conduct that does not fall within this scope shall also be deleted.

In the case the submitted report contains personal data included in the special categories of data, it shall be deleted immediately, without being recorded or processed.

The data processed shall be kept in the system only for the time required to decide whether to initiate an investigation into the facts reported.

If it is established that the information provided or any aspect of it is not truthful, it shall be immediately deleted upon confirmation of the facts, unless this lack of truthfulness may constitute a criminal offence, in which case the information shall be kept for the time necessary during the legal proceedings.

When three months have elapsed since the receipt of the report and no investigation has been initiated, the report shall be deleted, unless the purpose of the storage is to leave evidence of the functioning of the system. Reports that have not been processed may only be recorded in anonymised form, without the obligation to block provided for in Article 32 of Organic Law 3/2018, of 5 December, being applicable.

In no case shall personal data relating to information received and internal investigations be kept for a period of more than ten years.

9. NON-COMPLIANCE WITH THE PROCEDURE

All ENSA personnel, including individuals belonging to the entity's administrative body, are obliged to comply with the provisions of this procedure, and disciplinary measures may be taken in the event of non-compliance.

Non-compliance with this Procedure may result in fines of up to 1,000,000 euros for the organisation, and up to 300,000 euros in the case of individuals, as established in articles 63 and 65 of Law 2/2023, with an active commitment to compliance with all aspects of the Internal Reporting System required by all participants.

The obligation to comply with this Procedure extends to individuals outside ENSA who make a report through ENSA's Internal Reporting System.

10. APPROVAL, ENTRY INTO FORCE AND DISSEMINATION

The Steering Committee and the Board of Directors of Equipos Nucleares, S.A., S.M.E. (ENSA) are the competent bodies for the approval of this procedure.

This procedure is effective from the moment of its approval and shall be published on ENSA's corporate website, as well as on the intranet.

The People and Human Talent Directorate shall provide training on this policy and the procedure, with the purpose of facilitating and promoting usage and complying with Law 2/2023.