ALANTRA

WHISTLE-BLOWING POLICY

OF THE ALANTRA GROUP

Last update	26/02/2025
Updated by	Risk and Compliance Department
Approved by	Board of Directors

ALANTRA

1. OBJECTIVE

This document sets out the Whistle-blowing Policy developed by the Alantra Group to comply with the provisions of current regulations. Legal and regulatory requirements demand that the Alantra Group and its companies establish an internal information system through which employees, directors, related third parties, shareholders and suppliers of Alantra, among others, can report legal violations or violations of internal policies and procedures, such as irregularities of a financial and accounting nature, breaches of the Internal Code of Conduct, the General Code of Ethics and Conduct and activities related to money laundering or market abuse.

This policy and its related procedures comply with the Securities Market Act, article 197, as well as with the recommendations issued by the CNMV regarding internal control over financial reporting in listed companies and Act 2/2023 of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption (hereinafter, the "**Whistleblower Protection Act**") based on the transposition of 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.

The objectives of the Whistle-blowing Policy (the "**Policy**") reflect Alantra's commitment to conduct its business in accordance with the highest standards of professionalism and ethics in a compliant environment. Integrity in our business behaviour and in our management of systems is crucial to the success of Alantra's business and to the fulfilment of our professional responsibilities.

The Policy for Reporting Violations reflects Alantra's commitment to ensure that all matters relating to potential violations of laws, rules, regulations or internal policies and procedures, and reported in good faith, are handled appropriately and corrected as appropriate.

2. SUBJECTIVE SCOPE OF APPLICATION

The Whistle-blowing Policy set out in this document shall apply to the parent company of the Alantra Group (hereinafter "**Alantra"** or the "**Group"**), to all subsidiaries in which control is exercised[1] and to its employees and trainees (hereinafter the "**Bound Persons"**).

This Policy establishes a channel and protocol for the reporting of potential breaches of law and Alantra's policies committed by Bound Persons. However, persons who can potentially report a violation include not only Covered Persons, but also related third parties, who can report potential violations of the law of Alantra's policies under the terms of this policy:

- Ex - employees;
- Volunteers;
- Persons participating in selection processes;
- Agents;
- Shareholders, participants and persons belonging to the administrative, management or supervisory body of Alantra, including non-executive members;

[1] Pursuant to Article 42 of the Commercial Code.

- Suppliers and those other persons established by the Whistleblower Protection Act.

These persons, together with the Bound Persons, are defined as "**Reporting Parties**", "**Reporting Persons**" or "**Informants"**.

Limitations on the subjective scope of application of this Policy are imposed by the applicable legal framework.

The Risk and Control Committee (hereinafter, **"R&CC"** or "**Risk & Control Committee"**) is the body responsible for defining this Policy and submitting it to the Board of Directors for approval. The R&CC is also responsible for ensuring that it is reviewed, updated or amended.

The R&CC is also responsible for keeping the Whistle-blowing Policy accessible to Reporting Parties at all times via Alantra's website or equivalent electronic means.

For the purposes of this Policy, a report (hereinafter "**Whistleblowing"** or "**Communication"**) shall mean any notification of a breach made by a Reporting Person, when:

- The Reporting Party expresses the will to report or communicate said breaches. Therefore, Reporting shall not be understood to mean any information to which a Reporting Party may have access, when there is no express desire on the part of the Reporting Party to report it; and

- The subject of the complaint corresponds to the type of breaches listed in article 2.1 of the Whistleblower Protection Act or to the internal procedures and policies of the Group and its companies.

3. INTERNAL INFORMATION SYSTEMS

3.1. Responsible for the internal information system

The person responsible for the system shall be the head of the Group's Risk and Compliance Department (hereinafter, the "**CRO**") and his appointment, removal or dismissal shall be notified to the Independent Whistleblower Protection Authority within ten working days of the approval of the Policy.

3.2. Internal information channels

Alantra will at all times maintain internal reporting channels in place to enable written and/or verbal communications to be made to report any potential breaches to the CRO. Communication to the CRO may be made through:

- Breaches notification e-mail channel, whistleblowing@alantra.com.

- By telephone (+34917458565)

- Postal mail to the following address: Álvaro Fernández Herrero; Alantra Partners S.A. C/ José Ortega y Gasset 29; Madrid 28006, Spain.

- Face-to-face meeting.

Oral communications, including those made through a face-to-face meeting, by telephone or by voice messaging system, shall be documented in one of the following ways, subject to the consent of the Reporting Party:

- By recording the conversation in a secure, durable and accessible format;

- Through a complete and accurate transcript of the conversation made by the staff responsible for dealing with it.

If the subject of the Communication is the CRO itself, the Communication should be addressed directly to one of the following members of the Risk and Compliance department:

- By telephone:

    - Roberto Jiménez Fernández (+44 (0) 757 841 8532)

    - Jacobo González Arrojo (+34917458484)

- Postal mail to the following address:

    - Roberto Jiménez Fernández: 77 Queen Victoria St London London London EC4V 4AY UK

    - Jacobo González Arrojo: Alantra Partners S.A. C/ José Ortega y Gasset 29; Madrid, Spain.

- Face-to-face meeting.

Any non-compliance reported in good faith by the Reporting Persons shall be duly investigated, and the confidentiality of all reports shall be guaranteed. As far as possible, the allegedly irregular facts, reference dates, names and positions of those involved, that is to say, all information that can be provided for the purposes of verifying and verifying the accuracy of the same, and the reality of the facts that are reported, shall be indicated.

The notification channel must be communicated to all Bound Persons both at the start of the relationship and on a regular basis.

3.3. Protective measures

Alantra guarantees bona fide Reporting Persons, as well as persons collaborating with the investigation, that under no circumstances will their actions entail harmful consequences or reprisals, respecting their rights at all times, and implementing the following protection measures:

- Prohibition of retaliation: suspension from work, dismissal, economic damage or loss, coercion, harassment, negative evaluation, blacklisting or cancellation of licences or permits.

- Support measures: comprehensive information or counselling on the protection and rights of the complainant, effective assistance in their protection and financial and psychological support.

- Protection measures for persons under investigation: presumption of innocence, right of defence, access to the file, confidentiality.

- Leniency programmes: exemption of the complainant who has participated in the commission of the offence from liability for the administrative sanction that would apply under certain circumstances.

All reports of breaches will be treated with complete confidentiality. Such confidentiality extends not only to the Reporting Persons but also to the alleged offenders.

3.4. Matters susceptible to reporting.

By way of illustration only, the following is a description of possible breaches that could be considered as such for the purposes of this Policy:

a) Any violation of existing legislation;

b) Breach the Internal Code of Conduct on matters related to Alantra's securities market and the Group's internal policies and procedures, as well as the regulations on Personal Data Protection, according to the terms established by law and in Alantra's internal policies, including the policies and procedures that are particular to the different companies belonging to the Group;

c) Breach of the Alantra Group's General Code of Ethics and Conduct;

d) Violation of employment obligations;

e) Fraudulent or disloyal conduct in job-related tasks and the illicit appropriation or theft of the assets of Alantra, peers or clients. In addition, the performance of any of the foregoing offences by any other person within the premises of Alantra;

f) Violation of confidentiality undertakings.

g) Regular drunkenness or drug addiction.

h) Breach of Alantra rules with the aim of concealing, falsifying or covering up the real situation and nature of the financial statements or risk exposures. For more information in this respect, please consult the internal control over financial reporting (ICFR) procedures.

i) Abuse of authority by bosses.

j) Any crime and other conduct against sexual freedom and moral integrity at work, in particular sexual harassment and harassment based on sex, including those committed in the digital environment;

k) Offensive conduct, whether verbal or physical, vis-a-vis persons who work at Alantra or their household members.

l) Workplace harassment.

4. COMMUNICATIONS MANAGEMENT PROCEDURE

All notifications of Communications will be treated with complete confidentiality. Such confidentiality extends not only to the Reporting Persons but also to the alleged offenders.

4.1. Process:

1. The CRO shall confirm to the Reporting Person in writing within a maximum of 7 calendar days (unless this could breach the confidentiality of the Communication), by the means that affords it greater protection, receipt of the notification of the breach. This notification does not imply the admission of the same, which shall be based on the provision of objective facts and clear breach of the internal procedures and policies or of the law in force.

   In case the Communication has been made to a Bound Persons other than the Staff responsible for the internal reporting system (section 3 of this Policy), the recipient shall be obliged to immediately forward to the System Responsible the notification and ensure the confidentiality of the Communication and the Informant. The CRO shall inform the Reporting Person of the receipt.

2. The CRO shall conduct all necessary inquiries and investigations, safeguarding the confidentiality of the Reporting Person at all times.

   In the event that the CRO considers that there is sufficient and objective evidence of the possible commission of an breach or a criminal offence, it shall admit the notification of the breach for processing. This circumstance, as well as, where appropriate, the non-admission of the Communication, shall be notified to the Reporting Party within a period not exceeding 10 working days (in the event that additional information has been requested from the Reporting Party, this period shall be extended by 5 days) following notification of receipt of the breach.

   Within this period of 10 working days, the CRO may request the Reporting Party to proceed, within a period of 5 working days, to rectify any possible defects in the Communication, or to clarify or complete the Communication by providing such documentation and/or data as may be necessary to accredit the irregular conduct reported. In the event that the Reporting Party fails to make the required correction, the Communication may be filed.

3. Likewise, the CRO shall inform the accused, within 10 working days from the admission for processing of the notification of the breach, of the fact of having been the subject of a Communication, as well as of the nature of the notified facts, his or her right to be heard, the presumption of innocence, honour and his or her rights in matters of data protection. The defendant, by virtue of his or her right to defence, may provide any information and objective evidence he or she deems appropriate for this purpose. However, at no time may the identity of the Reporting Party be disclosed.

4. The duration of the investigation shall not exceed two months from the receipt of the Communication. Only in exceptional circumstances which, due to the complexity of the case, require further analysis, the CRO may request an extension of the time limit from the CACR or its chairperson, in which case the time limit may be extended by up to a maximum of two additional months.

5. Within the framework of the right of the Reporting Party to be informed of the actions or omissions attributed to it and the right to be heard at any time, the CRO shall inform it periodically of the status of the breach notification, and in any case of the sending of the report (with the conclusions of the investigation and the proposed measures to be taken) to the CACR, after a maximum of 10 working days have elapsed.

6. The CRO shall prepare a report to the CACR within the maximum time limit set for the investigation, informing it of the notifications received and the outcome of the investigations carried out. It shall also propose to the CACR the measures to be taken and, where appropriate, the notification to the supervisor or competent authorities of the notification received, as well as the outcome of the investigations carried out.

   Accordingly, the CACR, on the basis of a report from the CRO or, where appropriate, the R&CC, will be the body responsible for proposing the measures to be taken in relation to the Communications received, within one month of the completion of the investigation. During this period, the CACR may additionally initiate further proceedings and collect additional evidence, extending the deadline for a decision by one month.

7. The decisions of the CACR shall be recorded in the meeting minutes of the relevant meeting and the secretary shall, where appropriate, notify the board of the directors of the companies concerned of the decisions taken so that these bodies may notify and, where appropriate, implement the measures approved to the respondent.

8. The CRO may escalate notifications of breaches directly to the Alantra Board of Directors if for any reason the CACR is unable to meet within a reasonable period of time or in the event that the seriousness of the reported facts requires immediate action.

9. In cases where the decision taken by the CACR requires notification to the Supervisor or Competent Authorities, the CRO shall be required to give effect to such notification.

4.2. Communication with the Reporting Party.

The CRO will be responsible for notifying the Reporting Parties of the outcome of the decision taken, as well as the reasons for the decision. Except in exceptional circumstances, the response period is a maximum of 3 months from the receipt of the notification. Notwithstanding the above, if the proceedings require a longer period, this may be extended to 6 months.

The CRO shall notify the Reporting Party of its right to approach the competent authorities (identifying the external channels to do so), if the resolution adopted does not include such a report, as well as in the event that the Reporting Party does not agree with the resolution adopted.

4.3. Information to the defendant.

The accused shall be informed by the board of directors of the company to which he belongs, or by a representative thereof, of the decision taken and, where appropriate, of the measures to be implemented, within a maximum of 10 working days from the adoption of the decision.

The companies concerned and their boards of directors shall be required to confirm to the CACR that the measures have been implemented. The CACR may delegate Alantra's Risk and Control Committee to monitor compliance with the resolutions adopted.

4.4. Compliance with data protection law.

The registration of Communications and reports received under this Policy shall at all times comply with the requirements of the Personal Data Protection Regulations.

Both the Informant and the defendant may, at any time, exercise their right of access, rectification, erasure, objection, restriction of processing and data portability with regard to the information contained in the said register. This right is limited to their own data. The informant may not therefore have access to the data of the data subject, nor may the latter have access to the data of the former.

All the information contained in this file will be considered to be of a high level of security as established by the European Data Protection Regulation for the purposes of safeguarding the confidentiality of the same and the conservation of the data.

The personal data processed in the register shall be deleted no later than 90 days after the end of the investigation if the facts have not been proven. In the event of legal action, the data shall be retained for as long as it is necessary for Alantra to exercise its rights in court or to protect the rights of the Reporting Person vis-à-vis other employees or his or her employer.

In no case will data be kept for a period longer than 10 years.

5. REGISTER OF COMMUNICATIONS.

The CRO shall be responsible for maintaining and keeping a record of all Communications received and the internal investigations to which they give rise, guaranteeing, in all cases, the confidentiality of the persons involved. To this end, the register shall only be accessible by the CRO and the competent judicial authority if so required, in accordance with the legislation in force.

The register shall include at least the details of the Reporting Parties and the respondent, the date of the notification, the assessment or analysis carried out, as well as the decision taken and the date on which it was taken.

6. POLICY UPDATES

6.1. Duties and responsibilities.

The following functions have a particular role to play in the development and operation of this Policy:

a) Risk and Control Committee: The Group Risk and Control Committee is responsible for reviewing the content of this Policy at least every two years and incorporating possible changes in legislation or in Alantra's internal policies.

b) Chief Risk Officer: As Group Risk and Compliance Officer, he is responsible for analysing all breaches notifications received, confirming receipt of the notification to the Reporting Parties, as well as notifying them of the resolutions adopted. He is also responsible for notifying the CACR or the Board of Directors of Alantra of the nature of the same for the adoption, where appropriate, of any necessary measures.

c) CACR: This body is responsible for approving the resolution of all notifications received as well as proposing any amendments it deems appropriate or necessary to the Whistle-Blowing Policy to the Board of Directors for approval .

d) Employees: All employees, representatives and directors of the Alantra Group companies covered by this Policy are responsible for compliance with this Policy.

6.2. Compliance.

The provisions of this Policy are mandatory. Any deviation from these guidelines should be escalated to the CRO.

Failure to comply with this Policy may result in disciplinary action, including dismissal of those who fail to comply.

Inappropriate use of this procedure, by reporting false breaches in bad faith, may also lead to such disciplinary measures.

7. DISTRIBUTION OF THE WHISTLEBLOWING POLICY.

The Risk and Compliance Department undertakes to disseminate the Whistle-blowing Policy to all Bound Persons.

Such dissemination shall include, as a minimum, information on the existence of the whistleblowing channel provided for in the Whistle-Blowing Policy, the ways in which it can be addressed, and guarantee confidentiality during the reporting process as well as in the eventual investigation process.