AIRTIFICIAL

Internal **Information** System Policy

Approved by the Board of Directors on 13 June 2024

Internal Information System Policy - ENGLISH

Reference	A_POC-02
Title of the Standard	Internal Information System Policy
Summary of the Standard	The purpose of this Policy is to detail the scope of application of the IIS Internal Information System, its general principles and the guarantees offered in terms of the protection of both whistleblowers and the persons concerned.
Scope	Airtificial Group
Category	Policy
Responsible	Compliance Manager
Date of approval	13 June 2024
Approved by	Board of Directors
Affects	Not applicable
Version	0

Content

1 Introduction

Airtificial Intelligence Structures, S.A. (hereinafter, "Airtificial" or the Company) and all its subsidiaries (hereinafter, together with Airtificial, "Airtificial Group" or "Group") in accordance with the provisions of its Code of Ethics, is committed to achieving high levels of ethics and transparency in order to provide security to our customers, employees, shareholders, business partners and society as a whole.

This Policy reflects the principles and principles set out in 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, as well as the provisions of Law 2/2023 of 20 February on the protection of persons who report regulatory breaches and the fight against corruption.

In this regard, the Group maintains an Internal Information System (hereinafter IIS), which allows any person to report a breach of the applicable external or internal regulations, including its Code of Ethics, occurring within the Group and in the course of its ordinary business.

The IIS also channels any doubts about the interpretation of our Code of Ethics and internal regulations that may arise.

This Internal Information System Policy ("Policy") aims to detail the scope of application of the IIS, its general principles and the safeguards provided for the protection of both whistleblowers and the persons concerned.

2 Scope of application

This Policy is applicable to all members of the governing bodies, managers and employees of the companies that make up the Airtificial Group.

Additionally, any external person, natural or legal, who has had, has or may have a relationship or interest in Airtificial Group, is also encouraged to use the IIS in the cases regulated in this Policy, as a formal mechanism and independently of other means of communication made available.

3 Communications

Through the IIS, queries about the interpretation of the Code of Ethics and internal regulations can be communicated, as well as suspicions about irregularities taking place within the GroupIn particular, they may be the subject of information, complaints orreports:

- Any violation of national or European law, policies or procedures in force.
- Any action or omission committed by any means against our key stakeholders: employees, customers, shareholders, business partners, suppliers, as well as any attempt to conceal it.
- Any conduct that contravenes the ethical standards implemented in the company: reprehensible or dishonest ethical conduct by employees of the company, as well as any omission, situation or action that may involve a conflict of interest.
- All those actions and omissions detected, serious or very serious, which are not included in any of the previous sections and which violate any administrative procedure.

Consequently, any behaviour observed that violates the laws or administrative rules, the Code of Ethics, any internal regulations, or other mandatory rules such as protocols and policies implemented in Airtificial Group may be reported or denounced through the IIS.

Thewhistleblower, in addition to reporting any of the aforementioned infringements through the IIS, may contact or report them to the competent judicial or administrative authorities, the Independent Authority for the Protection of Whistleblowers (A.A.I), and/or, where appropriate, before the institutions, bodies or agencies of the European Union, among others: the National Anti-Fraud Coordination Service (hacienda.gob.es), the Anti-Fraud Office of Catalonia, the Andalusian Office against Fraud and Corruption (antifraudeandalucia.es), and the Agency for the Prevention and Fight against Fraud and Corruption of the Valencian Community (Antifraucv).

The information, complaint or report may be made in writing, verbally or by telephone, or by any electronic means addressed to any of the following addresses:

- Chief Compliance Officer Airtificial

  Calle General Díaz Porlier, number 49. 28001 Madrid
- Email address: Whistleblowing Channel - Airtificial
- Telephone number: 911 211 700 and the call may be recorded, subject to prior warning to the complainant.

In the event that any information is received and the identity or contact details of the whistleblower are known, the whistleblower will be notified of the receipt of the communication, complaint or report within seven (7) calendar days of its receipt.

In any case, the Reporting Party will be offered the possibility of providing his or her contact details in order to inform him or her about the processing of the mandatory procedure. Regardless of the means of communication used, the Reporting Party may designate a preferred means of communication to receive information on the status of his or her Complaint or to contact him or her to request additional information and/or clarification. The Reporting Person shall also be given the opportunity to verify, rectify and accept the transcript of verbal communications by signing it.

Communications may be submitted, upon request by thewhistleblower, by means of a face-to-face meeting with the Responsible for the IIS within a maximum period of (7) seven days. In this case, the Responsible of the IIS will previously inform the whistleblower that this verbal communication will be recorded, or transcribed, as well as of the processing of his/her data in accordance with the provisions of the Data Protection regulations.

Thus, in those cases in which the communication, complaint or denunciation is made verbally, it will be transcribed to the effect that:

- can be documented,
- may be known to the person concerned.

In the event that the reporter or whistleblower has documents or witnesses to the situation or infringement, he/she should indicate this so that those responsible can have access to them.

The language of the complaint should be simple and clear, explaining the reasons for the complaint so that it can be understood by all those involved.

The complaint may be anonymous or contain the details of the complainant and must identify the extent of the irregular conduct or infringement and, where appropriate, the person who is alleged to have committed it.

If possible, indicate the place or body before which the situation occurred or the possible infringement was committed and the date of commission.

Additional information may be requested from the reporter in order to clarify or specify the content of the information provided.

4 Internal communication channels

In addition to the Whistleblowing Channel - Airtificial, Airtificial Group has the following e-mail box:

Shareholder services: **investor.relations@airtificial.com**

5 Internal Information System Manager

The IIS and the Whistleblowing Channel are managed by Airtificial Group's Chief Compliance Officer (CCO), whose appointment will be communicated to the Independent Authority for the Protection of the whistleblower (A.I.I) who will sign the corresponding contract for the processing of information with the Airtificial Group. This person will also be in charge of the instruction of the information, complaints or reportsreceived through the IIS and to keep the due confidentiality of all the information known through the same.

6 Internal Information System Assurances

The procedure relating to the reports, complaints or information is governed by principles such as anonymity (if the whistleblower so wishes), independence, confidentiality, data protection, secrecy of communications, prohibition of retaliations. Likewise, the presumption of innocence of the person concerned shall be respected in all cases.

It will be classified as a very serious infringement as regards the possible breach of the guarantee of confidentiality when the communication is sent through channels of complaint other than those established or to members of staff not responsible for its processing, who will have been trained in this matter and warned of the obligation of the recipient of the communication to immediately forward it to the IIS Officer.

7 Protective Measures. Prohibition of retaliations

In relation to protection measures, the Airtificial Group establishes that Whistleblowers are entitled to protection when the following circumstances are present:

- who have reasonable grounds to believe that the information referred to is true at the time of communication or disclosure, even if they do not provide conclusive evidence, and the said information falls within the application of this Law,
- that the communication or disclosure has been made in accordance with the requirements of this Law.

Protection shall involve taking reasonable measures to prevent harm and protect the confidentiality of the whistleblower or persons associated with the whistleblower, such as witnesses or family members, among others.

These measures may be of a psychological, financial, legal or reputational nature.

- . In addition, support is provided to encourage the whistleblower about the value of reporting non-compliance and taking steps to help the whistleblower well-being.

AIRTIFICIAL also informs whistleblowers of the existence of additional support measures provided for by current legislation and which will be provided by the Independent Whistleblower Protection Authority. Specifically, the following are envisaged:

> Full information and advice on available remedies for retaliations

> Effective assistance by the competent authorities.

> Legal assistance in criminal proceedings and cross-border civil proceedings.

> Financial and psychological support if deemed necessary by the Independent Whistleblower Protection Authority.

Airtificial Group strongly encourages all managers, employees, suppliers and customers to report, communicate or disclose all activities or behaviours that may violate the law, the Code of Ethics or the company's policies, asserting that, in no case, the exercise of this power will involve any retaliation for the complainant or family members, so that it will not affect their employment or professional relationship, will not cause economic or reputational damage, will not be included in any list or register, nor will it affect their personal situation.

No person who makes a good faith report of wrongdoing shall be subject to retaliation (including threats or attempts of retaliation). Retaliation shall mean any acts or omissions that are prohibited by law, or that directly or indirectly result in unfavourable treatment that places the individuals concerned at a disadvantage compared to another in the employment or professional context, solely because they have made a report through the IIS.

The persons who are protected against possible retaliations are all those who have professional or employment ties with entities in both the public and private sectors, those who have already terminated their professional relationship, volunteers, trainees or trainees in training, persons who participate in selection processes. Protection is also extended to persons who provide assistance to whistleblowers, persons in their entourage who may suffer retaliation, as well as legal persons owned by the whistleblower, among others.

During the processing of the case, the reported person has the right to the presumption of innocence, to exercise his/her defence and to the same protection established for whistleblowers, preserving his/her identity and guaranteeing the confidentiality of the facts and data of the procedure.

To this end, a brief account of the facts investigated will be communicated to the person in question so that he/she can prepare his/her defence, provide evidence and make any allegations he/she considers necessary. Communications must be handled with the utmost respect for the defendant's honour and presumption of innocence. In the event that the communication is false, the defendant has the right to have this recorded in the register of communications. Under no circumstances will the whistleblower's personal data be disclosed to the reported person.

Finally, we must emphasize that Airtificial Group will not tolerate the abuse of this effective tool through fraudulent use. Thus, the company will sanction any whistleblower who files complaints or makes communications or disclosures that are manifestly false or reckless.

8 Communications Management

A copy of the information, complaint or report obtained will be provided:

> to the whistleblower for ratification, in case it was not submitted by an anonymous person, and to

> all members of the Audit and Sustainability Committee for their knowledge and follow-up.

Upon receipt of the information, complaint or denunciation, the opening of the file shall be ordered and, within seven (7) days, it shall be transferred to the person involved so that he/she is aware of the facts, the opening of the file, as well as its instructor. The informant's identity shall be kept confidential.

This notification could be delayed up to a maximum of three (3) months in those cases where it is considered by the company's management that it would jeopardise the investigation and/or the accreditation of the facts reported.

In the event that the CCO considers that the alleged facts may constitute a criminal offence, it shall immediately inform the Public Prosecutor's Office or the European Public Prosecutor's Office, when the alleged facts affect the financial interests of the European Union, after notifying the Audit and Sustainability Committee.

The documentation obtained from the informant shall be delivered to the affected party in person, accrediting its delivery by means of a handwritten signature (receipt), or by any communication that allows accreditation of its dispatch and receipt, so that he/she may make the corresponding allegations in due time. At the same time, with

absolute respect for the presumption of innocence, the informant will be informed of the requirements for processing the procedure so that he/she is aware of his/her rights, obligations and deadlines, giving him/her the opportunity to explain his/her version.

The person concerned may be heard at any time during the proceedings at his or her request. Failure by the person concerned to cooperate may in no case be considered as an admission of the facts complained of.

The allegations of the person concerned must be submitted to the CCO within ten (10) days of the actual delivery of the documentation provided by the informant.

During the period specified in the preceding paragraph, those responsible for processing the information, complaint or denunciation shall examine the documents and other means of proof, in order to verify the possible veracity of the facts related in the denunciation.

Once the period of ten (10) days indicated above has elapsed, the affected parties shall be given a further period of ten (10) days in which to submit such evidence as they consider relevant, useful and necessary to support their allegations or retentions.

Once the means of proof have been established, they shall be taken within a period of twenty (20) days with the appearance of the persons concerned.

Subsequently, within ten (10) days of the aforementioned hearing, the parties involved may file a written statement of conclusions explaining the extent to which they consider the evidence has been taken.

Once the procedure has been completed, the CCO shall submit the outcome of the findings to the Audit and Sustainability Committee. The latter, having heard the opinion of the CCO, shall draw up a reasoned proposal for a resolution, which it shall submit to the Board of Directors.

The final decision shall be notified in writing to the Informant and to the person concerned.

The procedure may not take longer than three months, except in cases of particular complexity. In this case, the procedure may be extended for an additional three (3) months.

The possible sanction shall become final when it is imposed by the relevant body, unless it is challenged in a court of law.

Airtificial Group will carry out the necessary actions to maintain at all times the most absolute confidentiality with respect to all data that may have access to the sanctioning procedure.

The information, complaint or denunciation shall be stored and recorded on optical, magnetic or electronic supports that guarantee its integrity, the correct reading of the data, the impossibility of manipulation and its adequate conservation and location. The internal investigations carried out shall be kept in the same format.

The Airtificial Group has a book-register of the Whistleblowing Channel, maintained by the Head of the IIS, where the communications received, the admission or filing of the same and/or the result of the investigation, among other points related to the investigation, guaranteeing, in all cases, the confidentiality requirements established in the Whistleblower Protection Act.

The data obtained will only be kept for the time strictly necessary, and will be deleted within the periods established in articles 26.2, 32.3 and 32.4 of Law 2/2023. Under no circumstances may they be kept for a period of more than ten years.

As long as the custody of the aforementioned documents is maintained, they shall be limited under the terms determined in the Data Protection Act.

9 Approval, Monitoring and Updating of the Policy

This Policy has been approved by the Board of Directors of the Company.

This Policy shall be reviewed and updated as necessary to adapt it to the legal, social, economic or environmental reality at any given time. Any modification of this Policy shall require the approval of the Board of Directors.