

AIRTFICIAL | Anti-Corruption Policy

Approved by the Board of Directors on 6th September 2023



Anti-Corruption Policy

Reference	A_POC-08
Title of the Standard	Anti-Corruption Policy
Summary of the Standard	The company's commitment to transparency and the fight against corruption through responsible and ethical conduct in its work and relations with third parties.
Scope	Airtificial Group
Category	Policy
Responsible	
Date of approval	6 September 2023
Approved by	Airtificial Board of Directors
Affects	Not applicable
Version	0



Content

1	Introduction	3
2	Fraud definition.....	3
3	Policy addressees. Roles and responsibility for the prevention and detection of fraud	3
4	Processes.....	4
4.1	Higher-risk businesses or activities	4
4.2	Geographical areas of highest risk.....	4
4.3	Acceptance and supplier relations	4
4.4	Invitations and gifts.....	5
4.5	Donations.....	5
4.6	Hospitality.....	5
4.7	Expenditure Control	5
4.8	Employee and Third Party Travel	5
4.9	Business partners.....	6
4.10	Mergers or acquisitions.....	6
4.11	Recruitment	6
4.12	Employee registration.....	6
5	Reporting of unethical or illegal actions or conduct	6
6	Dissemination of the Compliance Policy and anti-fraud Best Practices	6
7	Applicable legislation	7

1 Introduction

This policy is the result of the constant review and improvement process implemented in Airtificial Group in relation to regulatory compliance and aims to adopt a proactive, structured and targeted approach to managing the risk of fraud. The aim is to adopt proactive and proportionate anti-fraud measures that offer a satisfactory cost-effectiveness ratio. Airtificial Group is committed to establishing a specific policy and processes with the objective of establishing zero tolerance to fraud, starting with the adoption of an appropriate attitude from the most senior positions.

Robust and effective systems of controls can significantly reduce the risk of fraud; however, such systems cannot completely eliminate the risk of fraud occurring or going undetected. For this reason, systems must also ensure that fraud detection procedures are in place and that appropriate action is taken when potential fraud is detected.

This guidance is intended as a "step-by-step" guide to address any fraud that may still exist after other good financial management measures have been effectively put in place.

International standards such as the American FOREIGN CORRUPT PRACTICE ACT (FCPA), the British BRIBERY ACT, as well as the anti-corruption principles contained in TRANSPARENCY INTERNATIONAL have been taken into account in the development of this policy.

2 Fraud definition

Fraud may be defined as an act or acts of deception, breach of trust or knowing inaccuracy, such as the intentional misrepresentation of financial or other statements, by persons inside or outside the organisation, intended to prepare or produce damage or harm of a material nature, such as the misappropriation of assets or the obtaining of financial or other benefits.

In other words, fraud is an action contrary to truth and rectitude, which harms the person against whom it is committed.

This policy covers different offences that can lead to fraud such as fraud, bribery, bribery, influence peddling or corruption (public or private), all of which are regulated in articles 251, 399, 427, 430 and 455 of the Penal Code, respectively.

3 Policy addressees. Roles and responsibility for the prevention and detection of fraud

The roles and responsibility for fraud prevention and detection are described below:

- a) The company's senior management is the body responsible for defining the Anti-Corruption Policy and for promoting a culture of compliance and ethical behaviour within the company, communicating the importance and responsibility of all directors, employees and collaborators in the process of prevention and detection of fraud events, guaranteeing the necessary resources to ensure compliance with the objectives of the policy.
- b) The Chief Compliance Officer (CCO) is responsible for analysing the complaints reported through the whistleblowing channel, guaranteeing the confidentiality and security of the information and reporting to the Audit Committee, in order to determine the corrective, preventive or disciplinary actions to be proposed to the Board of Directors.
- c) The Audit Committee is also responsible for assessing the effectiveness of and compliance with the Anti-Corruption Policy through review and monitoring mechanisms, as well as managing and supporting the implementation of any necessary updates.
- d) The managers of each company and each area are responsible for knowing and understanding the Anti-Corruption Policy, the actions that may constitute fraud, for implementing the controls they are responsible for, reporting suspicious incidents and co-operating with any resulting investigations.
- e) Employees are equally responsible and must refrain from acts which, in contravention of the policy developed here, may directly or indirectly benefit the company.

4 Processes

Identification of activities, processes and businesses that present or increase the risk of fraud.

4.1 Higher-risk businesses or activities

The following activities, processes and businesses have been identified as posing a higher risk of fraud:

- 1.- Relations with Administrations;
- 2.- Purchase and sale of public and/or private companies;
- 3.- Obtaining Municipal and Sectoral Permits;
- 4.- Acceptance and maintenance of suppliers with a risk profile;
- 5.- Acceptance and maintenance of customers with a risk profile;
- 6.- Invitations and gifts to third parties;
- 7.- Donations;
- 8.- Sponsorship;
- 9.- Employee travel;
- 10.- Registration of employees;

4.2 Geographical areas of highest risk

High-risk areas are considered to be those places within Spain or abroad, including free trade zones and port areas, as well as certain regions where there is public knowledge of a higher potential risk of fraud-related offences.

4.3 Acceptance and supplier relations

The Supplier Acceptance Procedure should incorporate the following matters whenever applicable:

- 1.- In those cases where there are reasons to justify it, the criminal record certificate of the partners or last owners of the supplier could be requested;

- 2.- Verify suspicious situations in relation to the supplier, such as prices of products or services well below the market price;

- 3.- Obtain corruption risk information from the supplier's country of origin if the supplier is foreign (e.g. Transparency International indexes, or blacklisting);

- 4.- Check free public databases to which the company may have access that contain names of persons and organisations convicted or prosecuted for offences under the laws;

- 5.- Prepare and maintain a database with the suppliers whose evaluation has been rejected due to their links or risk related to the aforementioned crimes, in order to avoid re-evaluating them (Single Register of Suppliers per company);

- 6.- When a potentially hazardous supplier is identified in terms of risk, it shall be reported immediately;

- 7.- Before entering into business relations with a supplier, a document shall be used in which the supplier expressly declares its commitment to this policy. In such a document, the service provider or supplier shall state at least the following:

- a) The supplier/service provider declares to comply with all applicable laws, rules, regulations and requirements in the delivery of the product or the provision of services.
- b) The supplier/service provider declares that it is not part of its business practices, nor is it part of its business to provide payments or other benefits to a public employee, domestic or foreign, to perform actions or omissions for its own or the company's benefit.
- c) Declare that it has controls in place to prevent fraud crime. If this is not the case, the company shall make available to the supplier or service provider a copy of the Code of Conduct or Code of Ethics and its corresponding Crime Prevention Manual.

The respective contracts shall include clauses regulating the possibility of terminating the contractual relationship in the event of non-compliance with the provisions of the preceding paragraphs.

4.4 Invitations and gifts

As a general company policy, it is expressly forbidden to give gifts or extend invitations to potential public sector clients or their employees, or to officials of any public institution, or foreign public officials who, by virtue of their duties, are or may be required to

- I. interacting with the company,
- II. decide, directly or indirectly, on company business.

In the case of invitations received by a manager from a third party or a public official, whether national or foreign, the Chief Compliance Officer must be informed immediately and may only be accepted with the prior authorisation of the latter. Such notification shall not be necessary in the case of mere courtesy or in the case of invitations or gifts that do not exceed ONE HUNDRED AND FIFTY (150.00) euros.

In those cases in which the Chief Compliance Officer decides not to accept the gift or gift, it will be returned within a maximum period of five days, and the person involved must accredit the effective return of the gift or gift.

4.5 Donations

The following obligations are an integral part of any procedure governing donations:

- 1.- Establish the chain of authorisation for donations;

Ensure that the entity receiving the donation has the proper accreditations (legal validity, constitution, legal representatives, etc.);

- 3.- Identify the work that the institution receiving the donation carries out in society;

- 4.- Establish the purpose of the donation and the use of the resources donated by the company;

- 5.- Check free public databases to which the company has access that contain names of individuals and organisations convicted or prosecuted for crimes.

4.6 Hospitality

A record should be kept with the necessary physical evidence of payments made for the organisation of events, which should include an identification of the recipient or beneficiary of the event and the purpose of the benefit.

The holding of any event shall require the express authorisation of the Chief Compliance Officer, to whom the necessary information must be provided regarding the amount and destination of the intended event, as well as a list of the persons, natural or legal, to be invited.

4.7 Expenditure Control

The Operational Procedures on expenditure in the different workplaces will have built-in cash control for the detection of:

- 1.- Unusual expenses;
- 2.- Excessive quantities of a single good or service;
- 3.- Payments made to the same service provider.

The company's funds shall be used only to cover minor expenses related to the normal and usual operation of the management concerned (mobilisation, office supplies and other minor expenses duly justified).

These funds may not be used for invitations to public officials or for other purposes than those indicated in the preceding paragraph. Representation expenses shall not be subject to approval as long as they do not exceed the amount determined in section 4.4 above.

4.8 Employee and Third Party Travel

It is prohibited to finance travel for public employees or members of private companies with company funds or on behalf of the company.

The list of expenses allowed as travel expenses (taxi, public transport, private car rental, parking, tolls, hotel, restaurants, etc.) and the list of non-reimbursable expenses (fines of any kind, personal medication expenses, first class flights without the corresponding authorisation, hotel services, personal aesthetics, maintenance and repair services for the private vehicle, etc.) shall be determined.

4.9 Business partners

The Due Diligence process carried out on potential business partners of the company, whether for the purposes of a strategic alliance or joint venture, will not only consider commercial and financial aspects, but will also analyse all the information necessary to detect a possible link between the external company and any of the requirements established in Article 31 bis of the Criminal Code.

4.10 Mergers or acquisitions

The due diligence process must necessarily include an analysis of all the information that can be gathered on the involvement of the company to be acquired, or with which a merger is being sought, in any of the offences determined by criminal legislation or implementing regulations.

4.11 Recruitment

The company will at all times maintain a strict selection and recruitment procedure for both permanent and temporary positions.

The company shall refrain from recruiting persons with special connections to those public employees with whom it is necessary to come into contact in the course of the company's business.

This procedure includes a check of their employment and financial background for potential links to fraud offences within the legal framework regulating access to personal data of job applicants.

All employees (fixed-term contracts, permanent contracts, etc.) of the company must sign an employment contract in which they specifically commit themselves to strict compliance with the Crime Prevention Policy.

4.12 Employee registration

The company shall maintain a register of its employees and collaborators which shall contain at least the following information:

- 1.- Curriculum Vitae;
- 2.- Copy of the Identity Card;
- 3.- Declaration of having taken cognizance of and commitment to comply with the Code of Conduct, the Crime Prevention Manual and the other documents in which the Prevention Model is contained;
- 4.- Sanctions for non-compliance with internal rules.

5 Reporting of unethical or illegal actions or conduct

All company employees are encouraged to report or bring to the attention of the Whistleblower Channel any unethical and/or illegal action or conduct, through the channels established for this purpose, particularly through the Whistleblower Channel or the Internal Reporting System.

The company will not tolerate behaviour contrary to that set out in this policy, and failure to comply with this policy may result in disciplinary sanctions as set out in current legislation, including those of a more serious nature.

6 Dissemination of the Compliance Policy and anti-fraud Best Practices

The Governing Body is responsible for ensuring that the Airtificial Group complies with the laws and regulations applicable to it, respects the uses and good practices of the sectors and territories where it operates and observes the principles of social responsibility that it has voluntarily assumed.

Under the aforementioned, the Governing Body, through its officers and senior management, shall promote the monitoring by those in charge of anti-fraud principles and good practices, as well as any others of the same nature that may be incorporated in the future.

7 Applicable legislation

Convention on Combating Bribery of Foreign Public Officials in Foreign Public Transactions

International Trade Agreements adopted by the Organisation for Economic Co-operation and Development (OECD).

United Nations Convention against Corruption - in force since December 2005.

Inter-American Convention Against Corruption adopted by the Organization of American States

African Union Convention on Preventing and Combating Corruption - In force since August 2006.