WHISTLEBLOWER INTERNAL INFORMATION AND ADVOCACY SYSTEM POLICY

ARESBANK S.A.

HISTORY OF REVISIONS CARRIED OUT

VERSION	DATE	ELABORATE	APPROVED	REVISION
V.1	19/09/2023	Global Risk Control. Regulatory Compliance Area	Board of Directors	Approval of the Policy
V.2	24/05/2024	Global Risk Control. Regulatory Compliance Area	Board of Directors	Revising and Updating the Policy

INDEX

I. INTRODUCTION

The purpose of this Policy is to define the general principles that must govern the establishment and management of the Internal Information System of Aresbank, S.A. (hereinafter, "**Aresbank**"), as well as the defense of Informants.

With the approval of the Policy of the Internal Information System and defense of the Whistleblower (hereinafter, the "**Policy**"), Aresbank complies with the provisions of Law 2/2023, of February 20, 2023, regulating the protection of persons who report regulatory and anti-corruption violations, the purpose of which is to provide adequate protection against reprisals that may be suffered by individuals who report certain infractions regulations, as well as strengthening the culture of information, the integrity infrastructures of organizations and the promotion of the culture of information or communication as a mechanism to prevent and detect threats to the public interest.

Aresbank has approved this Policy with the aim of promoting its ethical culture of integrity and transparency through the establishment of an Internal Information System that allows detecting and acting on behaviours contrary to the applicable legislation, granting the necessary protection to Whistleblowers.

This Policy, as well as its successive amendments, will be duly publicized on Aresbank's Intranet and on its website, once approved by the Board of Directors, for the purpose of informing all affected persons.

II. APPLICABLE REGULATIONS

Currently, the regulations in force in Spain for the regulation of Whistleblowing Channels are as follows:

- 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.
- Law 2/2023, of 20 February, regulator for the Protection of Persons Reporting Regulatory Violations and Anti-Corruption.
- Circular 1/2011 of the Attorney General´s Office, of 1 June, on the criminal liability of legal persons in accordance with the reform of the Penal Code carried out by Organic Law number 5/2010.
- Circular 1/2016 of the Attorney General's Office, on the criminal liability of legal persons in accordance with the reform of the Penal Code carried out by Organic Law number 1/2015.
- Report 2007/128 on the creation of internal whistleblowing systems in companies and whistleblowing mechanisms, issued by the Spanish Data Protection Agency.
- Opinion 1/2006 on the application of European Union data protection rules to internal whistleblowing mechanisms in the field of accounting and internal audit controls, the fight against fraud and banking and financial crime, issued by the Article 29 Working Party of the Directive 95/46/CE in 2006.
- Art. 31 bis 5, section 4 of the Organic Law 10/1995, of 23 de November, of the Penal Code.
- Art. 24 Organic Law 3/2018 of 5 de December, of Personal Data Protection and Guarantee of Digital Rights.

- Royal Decree-Law 11/2018, of 31 August transposing directives on the protection of pension commitments to workers, prevention of money laundering and entry and residence requirements for third-country nationals and amending the Act 39/2015, of 1 October, of the Common Administrative Procedure of Public Administrations.

III. SCOPE OF APPLICATION

3.1. Subjective scope

This Policy applies to Aresbank, as well as to all directors, officers, employees or persons who have a relationship with the Bank, regardless of their functional or hierarchical position (hereinafter, the "**Staff**").

In addition, the scope of application of the System includes any natural or legal person who has had, has or may have a professional relationship, or within the framework of a professional context, with Aresbank (hereinafter, the "**Third Parties**").

3.2. Objective scope

In accordance with the provisions of the Internal Information and Protection System Whistleblower System Procedure (hereinafter, the "**Procedure**"), Staff and Third Parties may report knowledge or motivated suspicion of irregular conduct or conduct that may entail a breach of current legislation and Aresbank's internal regulations.

Specifically, Staff and Third Parties may report knowledge or motivated suspicion of irregular conduct in the following matters:

1. Any violation the principles set out in the Code of Conduct;
2. Violations of Aresbank's Criminal Risk Prevention or any internal ethics and compliance standards;
3. Facts or conducts that may have criminal significance;
4. Serious or very serious administrative offences.
5. Infringements of Labour Law on Occupational Safety and Health;
6. Any other type of irregularity that may imply liability for Aresbank;
7. Infringements of European Union law included in the material scope 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, and the Spanish Law transposing.

In addition, the Internal Information System can also be used to raise doubts or queries in this regard.

IV. MECHANISMS FOR REPORTING COMPLAINTS

Aresbank has multiple communication channels to promote a culture of communication as a basic element of the Internal Information System:

- **Whistleblowing Channel:** Online platform provided by a specialized technology company and accessible through the website https://aresbank.es/es/cumplimiento.html in the Compliance section, separate and easily accessible. The platform has measures in place to preserve the security and integrity of information and the processing of personal data. The

Whistleblowing Channel allows communications to be made orally or in writing, even anonymously. Communications relating to sexual and/or gender-based harassment may be reported through the Whistleblowing Channel.

- **Face-to-face meeting**: Through the Whistleblowing Channel, the Whistleblower may request a face-to-face meeting to verbally communicate the facts to be reported. In these cases, the communication will be recorded and you will be informed of the processing of your data in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- **Mail**: by post to Paseo de la Castellana, 257, 28046 MADRID (Spain) to the attention of the Chief Risk and Compliance Officer as Head of the Internal Information System (hereinafter, "**System Manager**") of the entity.

Aresbank has established an Information Management Procedure that establishes the necessary provisions to ensure that the Internal Information System, in general, and the internal channels, in particular, comply with the legally enforceable requirements.

Notwithstanding the foregoing, communications regarding moral, sexual and gender-based harassment shall be processed in accordance with the procedure established in the Protocol for the prevention of and action against sexual harassment and harassment based on sex. Likewise, for the reports made on customer transactions with indications of money laundering and terrorist financing, specifically for the reporting of suspicious transactions by an Aresbank employee, the procedure determined in the AML Manual will be followed.

In both cases, all the guarantees and rights set forth in this Policy and in the Internal Information System Procedure will be respected.

In the event that any information included within the objective scope of application of the System is communicated by means other than those provided for above, it will be ensured that its processing is in accordance with the provisions of this Policy.

- **External channels of information**

Whistleblowers also have the possibility of submitting their communications to the Independent Authority for the Protection of Whistleblowers, or to the corresponding regional authorities or bodies, and, where appropriate, to the institutions, bodies or agencies of the European Union, of the commission of any actions or omissions included in the scope of application of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory breaches and the fight against corruption.

Annex I of this Policy includes a list of the main competent authorities that have external reporting channels.

V. INTERNAL INFORMATION SYSTEM GUARANTEES

Aresbank undertakes to provide the following guarantees in the management of the information received through the Internal Information System:

- **Regulatory Compliance**

Ensure that communications are processed in a comprehensive and professional manner, in compliance with current legislation, applicable internal regulations and, in particular, data protection regulations.

- **Anonymity**

Any communication received through the Internal Information System may be anonymous, if the Informant so requires, regardless of whether it is submitted in writing or orally.

- **Confidentiality**

The System is designed, established and managed in a secure manner, in such a way as to guarantee at all times the confidentiality of the identity of the Informant and of any third party mentioned in the communication, as well as of the actions carried out in the management and processing of the same, as well as the protection of data. preventing access by unauthorized personnel.

Confidentiality will be guaranteed even when the communication is made through reporting channels other than those established or to staff members who are not data controllers.

In this sense, any person who receives the communication of information has the obligation to send it without delay to the System Manager.

Any breach of this obligation of confidentiality will be considered a very serious breach.

- **Secrecy**

Encourage the persons involved in the processing and investigation of communications to act with the utmost discretion regarding the facts they know by reason of their position or function.

- **Prohibition of Retaliation**

Aresbank prohibits any action or omission constituting retaliation against those who report in good faith facts or actions that are within the scope of application of this Policy, as well as against other persons who, in good faith, may participate in the investigation process.

- **Good Faith Communications**

Communications must always be made in good faith. The communication made maliciously, with a fraudulent or deceptive attitude, with the intention of harming another person, will determine the adoption of the corresponding legal or disciplinary measures.

In this regard, the prohibition of retaliation provided for in this paragraph shall not apply when the investigation concludes that the communication is false and that there has been bad faith.

- **Rights of Informant and the Data Subject**

During the investigation process of a complaint received in the Internal Information System, Aresbank will respect the fundamental rights of the persons affected in the process at all times.

In this regard, the investigation shall be governed at all times by respect for the presumption of innocence and the right to honour of the persons concerned.

Likewise, the right of the person affected by the communication to be informed of the actions and omissions attributed to him/her, and to be heard at any time, is recognized. In any case, such communication shall take place at the time and in the manner deemed appropriate to ensure the successful completion of the investigation.

This duty to inform the individual will not be applicable in cases where the communication refers to money laundering and terrorist financing in which, in accordance with the applicable sectoral legislation, the principle of prohibition of disclosure will apply.

- **Protection of Personal Data**

The data protection regime that is affected as a result of the management of the Internal Information System will be governed by the data protection regulations in force at any given time.

Access to the data will be limited to all personnel whose intervention is strictly necessary during the procedure and investigation

- **Independence and impartiality**

In the management of communications received through the Internal Information System, any person in whom there may be a conflict of interest must abstain. This guarantees the independence, impartiality and objectivity expected of such persons in the performance of their duties.

In this regard, the general principles of action in the event of a conflict of interest should be as follows:

- Refrain from deliberations and decision-making processes.
- Fefrain from access to confidential information.
- Transparency and Proactive Statement on Conflicts of Interest.
- Collaboration in the resolution of conflicts of interest.

For the management and resolution of conflicts of interest, the provisions of Aresbank's Bribery and Corruption Prevention Policy will be followed in all cases.

- **Transparency and accessibility**

Ensure that information about the Internal Information System and its regulation is transmitted in a clear and understandable manner, as well as the publicity and accessibility of the System.

- **Traceability and Security**

Integrate all the measures that are necessary to guarantee the integrity, monitoring and security of the information.

VI. RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM

The Board of Directors has appointed Aresbank's *Chief Risk and Compliance Officer* as System Manager, insofar as this position is a management position endowed with autonomy and independence with respect to the rest of the bank's bodies and does not receive instructions of any kind in its exercise.

On the other hand, the System Manager is equipped with all the personal and material resources to carry out his/her duties in the appropriate manner.

The main functions of the System Manager are as follows:

- Secure and Promote the proper functioning of the Internal Information System, including the proper management of the information received.
- Acting as an interlocutor, on behalf of Aresbank, with the Independent Whistleblower Protection Authority.
- Making the decision to outsource part of the management process to external experts when reasons of complexity, objectivity and the preservation of confidentiality and anonymity so advise.

Both the appointment and dismissal of the System Manager must be notified to the Independent Whistleblower Protection Authority, in accordance with the legally established procedure, specifying, in the case of termination, the reasons that have justified it.

VII. REVISION AND UPDATE OF THE POLICY

The Regulatory Compliance function is responsible for the periodic review of this document, as well as the internal regulations that develop it.

This Policy shall be reviewed and submitted to the Board of Directors for approval, where appropriate, at least every three years.

Apart from this three-year periodicity, Aresbank's regulatory compliance function will also review the content of the report and submit it to the Board of Directors for approval, after review by the Compliance Committee, whenever any of the following circumstances occur:

- Changes in the applicable regulation.
- Shortcomings identified in internal or external audits and other possible control processes.
- Approvals or modifications of internal policies and procedures that affect the content of this policy.
- Significant organizational changes affecting this Policy.

ANNEX I: MAIN EXTERNAL CHANNELS FOR COMMUNICATIONS SET OUT IN ARTICLE 2 OF LAW 2/2023

Public Authority	Access web address
Independent Whistleblower Protection Authority	In the process of creation
Bank of Spain	www.bde.es/wbe/es/para-ciudadano/gestiones/canal-de-denuncias-del-banco-de-espana/
Spanish Data Protection Agency	sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/tramitesCiudadano.jsf
National Securities Market Commission	www.cnmv.es/portal/whistleblowing/presentacion.aspx
Tax Agency	sede.agenciatributaria.gob.es/Sede/colaborar-agencia-tributaria/denuncias/denuncias-no-tributarias.html
Madrid	Municipal Anti-Fraud and Corruption Office (https://www.madrid.es/portales/munimadrid/es/Inicio/El-Ayuntamiento/Denuncias)
Catalonia	Anti-Fraud Office of Catalonia (Anonymous Complaint Mailbox | Anti-Fraud Office of Catalonia)
Basque Country	In the process of creation