

# VICINAY

## Corporate Policy of the Internal Information System



- EMP
- ANA
- BRA
- DEF
- IDE
- CUS
- STR
- PLA
- TES
- SOL
- DAT
- PHO
- BRA
- DEV



INDEX

1. Introduction .....5

2. Objective .....6

3. Scope .....7

    3.1. Material scope of application .....7

    3.2. Personal scope of application .....7

4. General principles of action .....9

5. Internal information system manager and staff with access to information ..... 10

|         |                          |                    |
|---------|--------------------------|--------------------|
| G_00_03 | Version                  | Version 1          |
|         | Date of approval         | 12-12-2023         |
|         | Approval authority       | Board of Directors |
|         | Date of entry into force | 12-12-2023         |

| Version   | Date       | Responsible                   | Reason                                                                      |
|-----------|------------|-------------------------------|-----------------------------------------------------------------------------|
| Version 1 | 12-12-2023 | Regulatory Compliance Officer | Entry into force of the Corporate Policy of the Internal Information System |

This document was approved by the Board of Directors of VICINAY S.A on 12 December 2023, the date on which it becomes effective.



## 1. INTRODUCTION

1. The citizen collaboration is a key element in the Spanish rule of law, as it is not only manifested in the correct fulfillment of personal obligations but also in the collective commitment to the proper functioning of public and private institutions. Citizen collaboration is also considered a duty of every citizen when witnessing the commission of a crime.
2. Furthermore, in certain areas, such as finance or competition defense, specific tools have been implemented to allow citizens to provide supervisory bodies with useful information about irregular or illegal activities. There are also cases where civic actions have helped initiate investigations that resulted in the imposition of corresponding criminal penalties for irregular or corrupt behaviours.
3. It is important to emphasize that the legal system must protect individuals who report violations of the legal order within a professional relationship, as these civic behaviors have sometimes resulted in painful consequences for those who have reported such corrupt practices and other infractions. Therefore, it is essential to instill in society the awareness that those who break the law should be pursued, and violations should not be tolerated or silenced.
4. Vicinay S.A. and its dependent entities (hereinafter, also VICINAY or the Group) **have implemented and launched an Internal Information System, which is configured as one of the key and suitable elements for supervision, control, and prevention in the field of regulatory compliance.**

## 2. OBJECTIVE

1. The objective of this policy is **to outline the general principles** governing the Internal Information and Whistleblower Protection System (hereinafter, the System) defined at VICINAY and to publicize it with the aim of contributing to the collective commitment to the proper functioning of public and private institutions.
2. VICINAY **ensures adequate protection** for whistleblowers against possible reprisals they may face. It strengthens the culture of information and the integrity infrastructure of the entity, **fostering a culture of information** as a mechanism to prevent and detect threats to the public interest through the implementation of this System.



## 3. SCOPE

### 3.1. Material scope of application

1. The Scheme applies to any communication made by a reporting person which involves an act or omission that may constitute **a serious or very serious criminal or administrative offence** or which may constitute an infringement of European Union law provided that:
  - a. Enter within the scope of the acts of the European Union listed in the Annex to Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019;
  - b. Affect the financial interests of the European Union; or
  - c. Impact on the internal market.
2. That said, in the event that information is communicated outside this material scope of application, VICINAY reserves the right to pursue its investigation, but the informant may not be covered by retaliation protection measures.

### 3.2. Personal scope of application

1. The System applies to reporters who have obtained information about an offence in **an employment or professional context**, including in any case:
  - a. persons having the status of employed persons;
  - b. shareholders, participants and persons belonging to the administrative, management or supervisory body of VICINAY, including non-executive members;
  - c. any person working for or under the supervision and direction of contractors, subcontractors and suppliers;
2. It shall also apply to informants who report information on an infringement obtained in the framework of an employment or statutory relationship that has already ended, trainees, trainees in training, whether or not they receive remuneration, as well as to those whose employment relationship has not yet started, in cases where the information on infringements was obtained during the recruitment process or pre-contractual negotiation.
3. The measures for the protection of the whistleblower shall also apply, where appropriate, specifically to the legal representatives of the employees in the exercise of their functions of advising and supporting the whistleblower and to any natural or legal person in or assisting the whistleblower or related to the whistleblower who may suffer retaliation, such as colleagues or relatives of the whistleblower.



#### 4. GENERAL PRINCIPLES OF ACTION

VICINAY has implemented an internal information system based on the following general principles of action:

1. Act, at all times, under the protection of the **legislation in force** and within the framework established by the Code of Ethics, and in compliance with VICINAY's internal regulations. In particular, all the requirements set out in Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption, shall be complied with.
2. **Integrating** and coordinating the different internal information **channels** that may be established within the entity.
3. To have a procedure for **managing** information received.
4. Generate an environment of **transparency and accessibility** to both internal and external channels to favour the reporting of possible infringements by those persons included in the personal scope of application. Even the submission and subsequent processing of anonymous communications will be allowed.
5. Be **independent** and autonomous, appearing distinct from the internal information systems of other entities.
6. Guarantee the **confidentiality** of the information communicated, even through non-standard channels, and of the actions carried out in its management and processing, as well as the secrecy of communications.
7. Comply with the requirements established in the **regulations on personal data protection**.
8. Implement appropriate **awareness-raising and training programmes** specific to the persons involved in accessing the data subject to communication and generic for the rest of the organisation.
9. **Investigate and sanction** irregular acts and conduct in a fair, non-discriminatory and proportionate manner in accordance with the disciplinary regime. This would include false or bad faith reporting.
10. Promote an **environment and culture** that guarantees the effectiveness and appropriateness of its functioning in order to be able to know about a possible irregularity in the first place and not leave room for impunity against the whistleblower.
11. Design a **person responsible for the System**, avoiding possible situations of conflict of interest by assigning him/her the necessary financial, human and technical resources.
12. Establish **guarantees** for the protection of whistleblowers, prohibiting reprisals against whistleblowers and full access to support measures.
13. Guarantee the **right of the persons concerned** to be informed and to be heard at any time.
14. Respect the **presumption of innocence** and the honour of the persons concerned.
15. Refer the information to the **Public Prosecutor's Office** immediately when the facts could be indicative of a criminal offence. In the event that the facts affect the financial interests of the European Union, it shall be referred to the European Public Prosecutor's Office.

## 5. INTERNAL INFORMATION SYSTEM MANAGER AND STAFF WITH ACCESS TO INFORMATION

1. The Governing Body of the Group Entities has designated the Regulatory Compliance Committee as the **System Manager**.
2. The Head shall perform his or her duties independently and autonomously from the rest of the Group's bodies.
3. The Responsible Party shall be responsible for the diligent processing of information received through internal information channels.
4. Access to personal data contained in the Internal Training System shall be limited, within the scope of its competences and tasks, exclusively to:
  - a. The System Manager.
  - b. Regulatory Compliance Officer.
  - c. The human resources manager, only when disciplinary measures may be taken against an employee.
  - d. The person in charge of the legal services of the entity.
  - e. The persons in charge of processing that may be appointed.
  - f. The data protection officer.
5. That said, the processing of the data by other persons, or even their communication to third parties, shall be lawful when necessary for the adoption of corrective measures in the entity or the processing of the sanctioning or criminal proceedings that, where appropriate, may be applicable.

Vicinay, S.A.

Plaza Sagrado Corazón, 4 - Planta A  
E-48011 Bilbao

Email: [info@vicinay.com](mailto:info@vicinay.com)  
[www.vicinay.com](http://www.vicinay.com)

