IURIS Corporate

Internal System Policy Information

VIARIUM INGENIERÍA, S.L.

viarium

POLICY ON THE INTERNAL INFORMATION SYSTEM	
Version number:	3
Date of approval:	NOVEMBER – 2024
Prepared by:	**IURIS CORPORATE, S.A.**
Approved by:	**VIARIUM INGENIERÍA, S.L.**
Status:	IN FORCE

VERSION CONTROL		
Date	**Document title**	**Version**
September 2020	Whistleblowing channel	1
May 2023	Whistleblowing policy	2
November 2024	Whistleblowing Policy	3

CONTENTS

1. Introduction 4

2. Material scope of application 4

3. Scope of application 5

4. Governance, Roles and Responsibilities 5

4.1. Management of the internal information system 5

4.2. Processing of communications 6

5. Formulation of communications 6

6. Key aspects relating to the whistleblowing channel 6

6.1. Rights of the whistleblower regarding communications made through the whistleblowing channel 7

6.1.1. Right to protection during the investigation 7

6.1.2. Prohibition of retaliation 7

6.1.3. Right to receive information 8

6.1.4. Availability of communication channels 8

6.1.5. Right to restriction of processing 8

6.1.6. Anonymity 8

6.1.7. Right to confidentiality 8

6.1.8. Right to erasure of personal data 9

6.2. Rights of the accused regarding communications made via the reporting channel 9

6.2.1. Right of defence and presumption of innocence 9

6.2.2. Right to be informed and to be heard 9

6.2.3. Right to confidentiality 9

7. Reporting of false or malicious complaints 10

8. Protection of the Whistleblower 10

8.1 Scope of protection 10

8.2 Information excluded from protection 11

9. Communication and dissemination 11

1. Introduction

The purpose of this internal reporting system policy is to set out the elements that ensure its proper configuration and to define the principles of confidentiality, whistleblower protection and processing established in Law 2/2023 of 20 February, regulating the protection of persons reporting regulatory breaches and combating corruption.

In this regard, **VIARIUM INGENIERÍA, S.L.,** hereinafter **VIARIUM**, has set up the email address canal.etico@viarium.es as the main internal reporting channel for receiving communications, without prejudice to other established channels. Notwithstanding the foregoing, it is emphasised that this channel has been implemented as a key and suitable tool for supervision, control and prevention in the field of ethical and regulatory compliance, with the aim of promoting a culture of transparency and ethics, free from corruption, fraud or administrative or criminal breaches, in accordance with the provisions of Law 2/2023 of 20 February "on the protection of whistleblowers", as well as the provisions, where applicable, of Article 31 bis of the Criminal Code regarding compliance, Circular 1/16 of the Attorney General's Office and the case law of the Supreme Court on the matter.

To this end, **VIARIUM** has established an Internal Reporting System (hereinafter also referred to as the "IRS"), which incorporates the Internal Reporting Channel (hereinafter also referred to as *the* "Channel"), providing a confidential and secure means as the preferred channel for reporting potential breaches or illegalities without fear of reprisals, as it has been designed and established in a secure manner.

VIARIUM's SII guarantees the confidentiality of the identity of whistleblowers and any third parties mentioned in the report, as well as the procedures involved in the handling and processing of reports, taking into account, in all cases, data protection regulations and preventing access by unauthorised personnel.

2. Scope of application

The infringements that may be the subject of a report must be limited to the following matters:

a) Any acts or omissions that may constitute infringements of European Union law, in accordance with the requirements set out in the regulations.

b) Acts or omissions that may constitute a serious or very serious criminal or administrative offence. In any event, this shall be understood to include all serious or very serious criminal or administrative offences that result in financial loss to the Treasury and the Social Security system.

c) Significant breaches, or well-founded indications that such breaches have occurred, of VIARIUM's internal regulations and the basic principles of the Code of Ethics, whether or not they entail any infringement of the matters set out in the preceding sections.

d) Queries regarding the internal regulations established within the Criminal Compliance System.

3. Scope of application

The internal reporting channel has been established for those who have obtained information regarding breaches in a work or professional context involving **VIARIUM**, including in all cases:

a) persons who are public servants or employees;

b) self-employed persons;

c) shareholders, stakeholders and members of our organisation's administrative, management or supervisory bodies, including non-executive members;

d) any person working for or under the supervision and direction of contractors, subcontractors and suppliers;

e) whistleblowers who publicly report or disclose information regarding breaches obtained in the context of an employment or statutory relationship that has already ended, volunteers, interns, trainees, regardless of whether they receive remuneration, and those whose employment relationship has not yet commenced, in cases where the information regarding breaches was obtained during the recruitment process or pre-contractual negotiations.

In accordance with the above, this Policy is binding and applicable to all members of VIARIUM, as well as to any entities in which VIARIUM holds a stake or exercises management control. Similarly, it shall also apply to members of other entities and organisations linked to VIARIUM through a controlling interest or for whose management VIARIUM is responsible.

4. Governance, Functions and Responsibilities

In accordance with Article 5 of Law 2/2023, the Board of Directors of VIARIUM INGENIERÍA, S.L. is responsible for implementing the Internal Reporting System at VIARIUM, following consultation with the workers' legal representatives.

In accordance with the provisions of Article 8(2) of Law 2/2023, the Board of Directors of VIARIUM has appointed the **Compliance Body** (OCN) and its **Support Team** as the Internal Reporting System Officer (hereinafter also **the SII Officer),** a body which has delegated the management of the internal reporting system and the handling of investigation files to the **OCN**. Furthermore, the Board of Directors is responsible for the dismissal or removal of the SII Officer.

The **SII Manager** shall carry out their duties independently and autonomously from the entity's other bodies or organisations, without receiving instructions of any kind and with access to all the necessary human and material resources to carry them out.

4.1. Management of the internal reporting system

Article 6 of Law 2/2023 establishes that *"The management of the internal reporting system may be carried out within the entity itself or by engaging an external third party, under the terms provided for in this law. For these purposes, the management of the System is considered to be the receipt of information*."

In accordance with the above, the management of the Internal Reporting Channel has been entrusted to the Compliance Body, which is responsible for receiving reports whilst ensuring the confidentiality of the information, its objective handling (for which it may seek specialist external advice), data protection and the secrecy of communications.

VIARIUM shall send the person making the report or communication an acknowledgement of receipt thereof within a maximum of seven (7) days of its receipt, unless the complainant expressly requests otherwise or the SII manager considers that such acknowledgement may compromise the protection of the complainant's identity or the confidentiality of the communication.

4.2. Processing of communications

All reports or communications will be answered and resolved as quickly as possible, in accordance with the legally established timeframes. Under no circumstances will information be disclosed to third parties, except where required by the authorities.

The SII Officer has access to specialist external advice **(IURIS CORPORATE, S.A.)** to ensure the proper conduct of their duties and the handling of investigation files.

Specifically, VIARIUM has a procedure for the management, handling, investigation and resolution of communications received.

5. Submission of reports

Reports shall be submitted electronically to the **email address** canal.etico@viarium.es, in accordance with the provisions of section 4 of VIARIUM's whistleblowing channel management protocol.

Although reports must be made in writing, the whistleblower may also request a face-to-face or online meeting with the external SII Manager within a maximum period of seven days. This meeting must take place at the SII Manager's premises or online. The SII Manager will draw up minutes of the meeting, either through an exact and complete transcript of the conversation, which will be made available for the attendees to sign, or through a recording, in which case the whistleblower will be notified and informed of how their data will be processed. Without prejudice to the rights to which they are entitled under data protection regulations, the whistleblower will be given the opportunity to check, correct and accept the transcript of the conversation by signing it.

6. Key aspects associated with the whistleblowing channel

The internal reporting channel is established as one of the cornerstones of the regulatory compliance and prevention system implemented at **VIARIUM** in accordance with the provisions of Article 31 Bis of the
CP, Circular 1/16 of the Attorney General's Office, Supreme Court case law on the matter, Law 2/2023 and EU Directive 2019/1937 on the matter. This channel has been established in accordance with the highest standards of diligence in this area and the corresponding safeguards:

- **Confidentiality and Anonymity**: The confidentiality of communications received through the Ethics Channel (as well as through other channels) is its cornerstone, guaranteeing, in all cases, the confidentiality of the identity of the person making the report and the information provided, of the persons concerned and of any third parties mentioned therein, except where required by the judicial authorities in accordance with the provisions of the law and with all the safeguards established therein. Should the recipient of the communication be a person other than those responsible for the Channel, they are obliged to maintain the confidentiality of the communication and forward it immediately to those responsible.
- **Data Protection**: The Channel and its management have been established in accordance with the principles of information protection and compliance with personal data protection measures, in accordance with the applicable regulations in this area.
- **Protection of the complainant/whistleblower** (see section 6.1).
- **Record-keeping:** The Channel maintains a register of communications/reports submitted to safeguard the processing, management and integrity of the information provided through this channel.
- **Protection of those affected by the communications** (see section 6.2).
- **Sanction:** If the investigation concludes with conclusive evidence that the facts under investigation are true and linked to irregular or unlawful conduct, the person reported may be subject to a sanction in accordance with the applicable regulations.
- **Professionalism and Experience**: The SII Officer draws on external advice from experts in regulatory compliance and criminal prevention to ensure the proper handling, management and analysis of communications and complaints, as well as to safeguard the rights of both the complainant and the person against whom the complaint is made in cases where the allegations are unfounded or made in bad faith.

6.1. Rights of the complainant regarding communications made through the reporting channel.

6.1.1. Right to protection during the investigation

VIARIUM guarantees the **whistleblower's** right to **protection** during the investigation; however, if the whistleblower makes the content of the report public, they may only avail themselves of protective measures if they have first reported the matter via the Internal Reporting System.

6.1.2. Prohibition of retaliation

VIARIUM guarantees that **it will not take any retaliatory action** against anyone who, in good faith and in accordance with legally established parameters, reports conduct or the appearance of conduct contrary to the law and/or internal regulations, nor will it incur any liability for doing so. Conversely, misuse of the Channel, consisting of the reporting of manifestly false facts or actions, may be grounds for disciplinary action in accordance with

VIARIUM's Disciplinary System. Similarly, failure to report conduct or the appearance of conduct that violates the law and/or internal regulations may be subject to disciplinary action in accordance with current legislation.

6.1.3. Right to receive information

The complainant shall be **informed**, in writing, **throughout the course of the complaint, of** the decisions taken during the investigation and, where applicable, the processing of the complaint, as well as the results and/or measures adopted following such proceedings, with reasons given.

6.1.4. Availability of reporting channels

The complainant may choose the channel for the complaint that they consider most appropriate, with preference given to **VIARIUM's** Internal Reporting Channel.

6.1.5. Right to restriction of processing

During the complaint process, **the complainant will not be asked for data that is not strictly necessary** to process the complaint and, subsequently, data that is not strictly necessary for the investigation may not be requested or retained.

The information provided may not be used for purposes other than the investigation.

Should a report contain information relating to trade or business secrets, or other information that could affect the commercial, economic, strategic or security interests of **VIARIUM** or any third parties involved, such information must be used only to the extent strictly necessary for the investigation of the report and may not be disclosed or shared for any other purpose.

Any data that is excessive or irrelevant to the investigation of a complaint, or that has been collected accidentally, shall be deleted immediately.

6.1.6. Anonymity

Should the whistleblower wish to remain **anonymous**, they shall not provide any personal data in this regard, regardless of the means of communication used, nor shall any data be obtained that would allow their identification. Notwithstanding the foregoing, in the case of anonymous reports, the whistleblower will be required to indicate which of the circumstances set out in this Policy entitles them to access the Communication Channel.

6.1.7. Right to confidentiality

The identity of the whistleblower shall remain **confidential** and may not be disclosed without their express consent to any person other than those authorised to receive and handle reports, with the exceptions[1] established by EU law or Spanish legislation in the context of investigations carried out by the authorities or in the course of legal proceedings. In such cases, the whistleblower will be notified before their identity is disclosed, unless such disclosure could jeopardise the investigation or legal proceedings.

[1] The identity of the complainant and any other information referred to in paragraph 3 of this Policy may only be disclosed where this constitutes a necessary and proportionate obligation imposed by Union or national law in the context of an investigation carried out by national authorities or in the context of legal proceedings, in particular to safeguard the right of defence of the data subject.

6.1.8. Right to erasure of personal data

Data subject to processing may be retained in the information system only for the time strictly necessary to decide whether to initiate an investigation into the reported facts.

If three months have elapsed since the receipt of the report without any investigative proceedings having been initiated, the data must be **deleted from the** reporting **system**, unless the purpose is to retain it as evidence of the functioning of the legal entity's model for the prevention of criminal offences or unless judicial proceedings or investigations by the competent authorities arise from it[2] . Reports that have not been acted upon may only be recorded in anonymised form.

6.2. Rights of the accused regarding reports made via the reporting channel

6.2.1. Right to defence and presumption of innocence

Throughout the reporting process, **VIARIUM** will guarantee the **rights of defence and the presumption of innocence** of those affected by the reports and will not impose any disciplinary or legal measures, as the case may be, until the veracity of the reported facts has been verified, the relevant evidence has been gathered, and it has been concluded that a criminal act has taken place or one contrary to the ethical principles and values established at **VIARIUM.**

The person against whom the complaint is made shall have the right to an investigation based on an **objective analysis** of the evidence gathered, ensuring an **effective and transparent investigation**.

6.2.2. Right to be informed and heard

In particular, the accused will **be informed of the investigation** being carried out so that they may exercise their right of defence, having **the right to be heard** at any time and to put forward any arguments they deem appropriate.

Such notification shall take place at a time and in a manner deemed appropriate to ensure the successful conclusion of the investigation. In cases where disclosure of information regarding the investigation process poses a significant risk to the ability to investigate effectively, notification to the accused may be delayed for as long as such a risk exists. The aim is to prevent the destruction or tampering of evidence by the accused.

6.2.3. Right to confidentiality

Information provided to the accused must be done in such a way as to protect the **confidentiality** of the complainant; their identity may not be disclosed without their express consent to any person other than staff authorised to receive and handle

[2] Second subparagraph of paragraph 4 of Article 24 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights.

complaints, with the exceptions[3] established by EU or Spanish law in the context of investigations carried out by the authorities or in the course of legal proceedings.

7. Reporting of false or malicious complaints

The **VIARIUM** Whistleblowing Channel must be used responsibly and appropriately.

Reporting false facts with a malicious and dishonest attitude constitutes a breach of the good faith that must govern working relationships within **VIARIUM**, and may result in disciplinary measures in accordance with the current Collective Agreement, as well as criminal and/or civil liability.

Furthermore, the whistleblower shall be deemed to be acting in bad faith whenever they are aware of the falsity of the facts, act with manifest disregard for the truth, act with the intention of seeking revenge or harming the person reported, or act with the intention of undermining the honour or professional, business or employment reputation of any person associated with **VIARIUM.**

If, following due analysis, it is concluded that the facts reported are manifestly false and that the report has been made with malicious intent and in bad faith:

(i) the report will be closed, documenting the reasons for closing the case, thereby concluding the investigation;

(ii) this circumstance will be referred to the person responsible for HR so that, in coordination with **VIARIUM's** SII Manager, disciplinary measures may be proposed in accordance with the current Collective Agreement; and

(iii) the proposed sanction shall be communicated in writing to the relevant **VIARIUM** manager, who shall decide on the disciplinary action to be taken against the complainant acting in bad faith.

8. Whistleblower Protection

8.1. Scope of protection

Persons who report breaches relating to the matters set out in **section 2** of this policy shall be entitled to protection provided that the following circumstances apply:

a) They have reasonable grounds to believe that the information in question is true at the time of reporting or disclosure and that said information falls within the material scope of application of the **VIARIUM** Whistleblowing Channel.

[3] The identity of the complainant and any other information referred to in paragraph 1 may only be disclosed where this constitutes a necessary and proportionate obligation imposed by Union or national law in the context of an investigation carried out by national authorities or in the course of judicial proceedings, in particular to safeguard the right of defence of the data subject.

b) The report or disclosure has been made in accordance with the requirements set out in this Policy.

c) It is not demonstrated that their report was made in bad faith.

8.2. Information excluded from protection

The following persons are expressly excluded from the protection provided for in this Policy:

a) Information previously reported via **VIARIUM** that has been deemed **inadmissible**.

b) Information relating to complaints about **interpersonal conflicts** or which affects only the whistleblower and the persons to whom the communication refers.

c) Information that is already fully **available** to the public or that constitutes **mere rumours**.

d) Information relating to **acts or omissions not covered by section 2 of this Policy**.

9. Communication and dissemination

In order for this policy, as well as the Channel, to fulfil the purposes for which it has been established, it is necessary to communicate and disseminate it so that any member of **VIARIUM** or its subsidiaries, as well as its suppliers, collaborators or external advisers and, in general, any person or company with a direct or indirect involvement with **VIARIUM** and/or acting on its behalf and for its benefit, has due knowledge of the internal reporting system. For this reason, and with the aim of ensuring proper communication and dissemination, **VIARIUM** will implement the relevant communication plan and provide access to this document to anyone who requests it.

Finally, this document is published on **VIARIUM's** corporate website so that anyone may consult it.