POLICY ON THE INTERNAL INFORMATION SYSTEM

VIARIUM INGENIERÍA, S.L.

POLICY ON THE INTERNAL INFORMATION SYSTEM	
Version number:	4
Date of approval:	OCTOBER – 2026
Produced by:	**IURIS CORPORATE, S.A.**
Approved by:	Management Body of 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
October 2026	Internal Information System Policy	4

CONTENTS

1. Introduction 5

2. Material scope of application 5

3. Personal scope of application 6

4. Governance, Roles and Responsibilities 7

4.1. Management of the internal information system 7

4.2. Processing of communications 8

5. Drafting of communications 8

6. Key aspects relating to the whistleblowing channel 9

6.1. Rights of the whistleblower regarding communications made via the Internal Reporting Channel 10

6.1.1. Right to protection during the investigation 10

6.1.2. Prohibition of reprisals 10

6.1.3. Right to receive information 10

6.1.5. Right to restriction of processing 11

6.1.6. Anonymity 11

6.1.7. Right to confidentiality 12

6.1.8. Right to erasure personal data 12

6.2. Rights of the accused regarding communications made via the Internal Information Channel 12

6.2.1. Right to a fair trial and presumption of innocence 12

6.2.2. The right to be informed and to be heard 13

6.2.3. Right to confidentiality 13

7. Communications not accepted 14

8. Reporting false or malicious complaints 15

9. Whistleblower Protection 16

9.1 Personal scope of protection 16

9.2. Information excluded from protection 16

10. Communication and dissemination 16

1. Introduction

The purpose of this internal reporting system policy is to set out the elements that ensure its proper implementation and to define the principles of confidentiality, whistleblower protection and the handling of reports, as laid down in Law 2/2023 of 20 February, which regulates the protection of persons reporting breaches of regulations and the fight against corruption.

In this regard, **VIARIUM INGENIERÍA, S.L.,** hereinafter **'VIARIUM,'** has set up the website https://viarium.factorial.es/complaints as the main internal information channel for receiving communications, without prejudice to other established channels. Notwithstanding the foregoing, it is emphasized that this channel has been implemented as a key and appropriate 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 illegal acts without fear of reprisals, as it has been designed and set up securely.

VIARIUM's Whistleblowing Scheme guarantees the confidentiality of the identity of whistleblowers and any third parties mentioned in the report, as well as the procedures conducted in the management and processing of reports, whilst at all times complying with data protection regulations and preventing access by unauthorized personnel.

2. Material scope of application

The infringements that may be reported must be limited to the following areas:

a) Any acts or omissions that may constitute infringements of European Union law, in accordance with the requirements laid down in the relevant legislation.

b) Acts or omissions that may constitute a serious or profoundly serious criminal or administrative offence. In any event, this should be understood to include all serious or profoundly 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 these entail a breach of the matters set out in the preceding sections.

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

3. Personal scope of application

The internal reporting channel has been set up for anyone who has obtained information about breaches in a work or professional context involving **VIARIUM**, including in all cases:

a) people who are civil servants or employees;

b) self-employed people;

c) shareholders, partners and people belonging to the administrative, management or supervisory bodies of our organization, 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 on infringements obtained in the course of an employment or statutory relationship that has already ended, volunteers, interns and trainees, regardless of whether or not they receive remuneration, and those whose employment relationship has not yet commenced, in cases where the information on infringements was obtained during the recruitment process or pre-contractual negotiations.

In accordance with the foregoing, this Policy is binding and applicable to all members of **VIARIUM**, as well as, where applicable, to entities under its control that adhere to **VIARIUM**'s Criminal Compliance System. Similarly, it shall also

be binding on members of other entities and organizations linked to **VIARIUM** through a relationship of control or for whose management **VIARIUM** is responsible.

4. Governance, Roles and Responsibilities

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

In accordance with the provisions of Article 8(2) of Law 2/2023, **VIARIUM**'s Governing Body has appointed the Compliance Body **(OCN)** as the Head of the Internal Information System (hereinafter also referred to as the **'SII Head'**). The SII Officer has delegated the management of the internal reporting system and the handling of investigation files to the Director of Internal Management, a member of the **NCO**. Furthermore, the Governing Body is responsible for the dismissal or removal of the SII Officer.

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

4.1. Management of the internal information system

Article 6 of Law 2/2023 states that *"The management of the internal reporting system may be conducted within the organization itself or by engaging an external third party, in accordance with the provisions of this Law. For these purposes, the management of the system is deemed to include the receipt of information."*

In accordance with the above, the management of the Internal Information Channel falls to the Director of Internal Management, as a member of the SII Officer to whom management powers have been delegated (hereinafter also referred to as the SII Manager), who is responsible for receiving communications whilst ensuring the confidentiality of the information, its objective handling, data protection and the secrecy of communications.

IURIS CORPORATE, S.A., as a specialist external member of the SII Controller, provides technical and legal support in the management of the System and maintains the register of communications, in accordance with the guarantees

of independence, confidentiality, data protection and secrecy of communications required by Law 2/2023 of 20 February. For these purposes, it shall be regarded as a data processor in accordance with legislation on the protection of personal data.

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

4.2. Processing communications

All reports or enquiries will be answered and resolved as quickly as possible, whilst complying with the legally established time limits. Under no circumstances will information be disclosed to third parties, except where required to do so by the authorities.

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

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

5. Drafting of communications

Communications must be submitted electronically via **the website** https://viarium.factorial.es/complaints,, in accordance with the provisions of section 3 of the **VIARIUM** Internal Information System management protocol.

Whilst communications shall be in writing, the informant may also request a face-to-face or online meeting with the SII manager within a maximum period of seven days. This meeting must take place at **VIARIUM's** registered office or online, and the SII case handler will draw up minutes of the meeting, either by means of an exact and complete transcript of the conversation, which will be made available for the attendees to sign, or by means of 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 the informant is entitled under data protection legislation, the informant will be given the opportunity to verify, rectify and accept the transcript of the conversation by signing it.

6. Key aspects relating to 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 Criminal Code, Circular 1/16 of the Attorney General's Office, the relevant case law of the Supreme Court, Law 2/2023 and EU Directive 2019/1937 on the matter. This channel has been designed to meet the highest standards of diligence in this area and includes the corresponding safeguards:

- **Confidentiality and Anonymity**: Confidentiality is the cornerstone of communications received via the Ethics Channel (as well as through other channels), ensuring, in all cases, that the identity of the person making the report and the information provided, as well as that of the individuals concerned and any third parties mentioned therein, remains confidential, except where required by the judicial authorities in accordance with the provisions of the law and subject to all the safeguards set out therein. Should the recipient of the report be someone other than those responsible for the Ethics Channel, they are obliged to maintain the confidentiality of the report and forward it immediately to those responsible. In any event, where an anonymous report is made via the web link provided by **VIARIUM**, in accordance with the provisions of section 5 of this policy, the tool will enable communication with the anonymous whistleblower to be maintained using the tracking code or credentials provided at the time the report is submitted, which the whistleblower must retain and check periodically.
- **Data Protection:** The Channel and its management have been organized in accordance with the principles of data protection and compliance with personal data protection measures, in line with the relevant legislation in this area.
- **Protection of whistleblowers** (see section 6.1).
- **Registration:** The Channel maintains a register of communications and complaints received to ensure that the information provided through this channel is processed, managed and protected from tampering in an independent manner.

- **Protection of those affected by communications** (see section 6.2).
- **Penalty:** If, in the conclusion of the investigation, it is conclusively established that the facts under investigation are true and are linked to irregular or unlawful conduct, the person against whom the complaint has been made may be subject to disciplinary action in accordance with the applicable regulations.
- **Professionalism and experience:** The SII Compliance Officer draws on external advice from professionals specializing in regulatory compliance and the prevention of criminal offences, to ensure the appropriate 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 whistleblower regarding communications made via the Internal Reporting Channel

6.1.1. Right to protection during the investigation

VIARIUM guarantees the right to **whistleblower protection throughout** the investigation; however, if the whistleblower makes the contents of the report public, they will only be entitled to protective measures if they first lodged a report via the Internal Reporting System.

6.1.2. Prohibition of reprisals

VIARIUM guarantees that it will not take any **retaliatory action against** anyone who, in good faith and in accordance with the legally established criteria, reports conduct or the appearance of conduct that contravenes the law and/or internal regulations, nor will it incur any liability for such reporting. This protection shall also extend to the whistleblower's relatives, subject to the limits set out in the applicable regulations.

6.1.3. Right to receive information

The complainant shall be informed, in writing, throughout the course of the complaint-handling process, of the decisions taken during the investigation and, where applicable, the processing of the complaint, as well as the outcomes and/or measures adopted following that procedure, together with a statement of the reasons therefor.

6.1.4. Availability of communication channels

The complainant may choose the channel for lodging the complaint that they consider most appropriate, and may, if they wish, use the **VIARIUM** Internal Reporting Channel.

6.1.5. Right to restriction of processing

During the process of lodging a complaint, the complainant will not be asked to provide any information other than that which is strictly necessary to process the complaint; subsequently, no information other than that which is strictly necessary for the investigation may be requested or retained.

The information provided may not be used for any purpose other than research.

Should a complaint contain information relating to trade or commercial secrets, or any 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 complaint and must 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 inadvertently, will be deleted immediately.

6.1.6. Anonymity

Should the person making the report 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 enable their identification. Notwithstanding the foregoing, in the case of

anonymous reports, the informant will be required to indicate which of the circumstances set out in this Policy entitles them to access the Internal Reporting 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 authorized to receive and handle reports, subject to the exceptions laid down 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 jeopardize the investigation or legal proceedings.

6.1.8. Right to erasure personal data

Data subject to processing may be retained in the information system only for as long as it is strictly necessary to decide whether to launch an investigation into the reported facts.

If, three months after receipt of the report, no investigative proceedings have been initiated, the report must be deleted from the reporting system, unless the purpose is to retain it as evidence of the functioning of the legal person's model for the prevention of criminal offences, or unless it gives rise to legal proceedings or investigations by the competent authorities. Reports that have not been acted upon may only be retained in anonymized form.

6.2. Rights of the accused regarding communications made via the Internal Information Channel

6.2.1. Right to a fair trial and presumption of innocence

Throughout the life cycle of the complaint, **VIARIUM** will guarantee the rights of defense and the presumption of innocence of those affected by

the reports and will not impose any disciplinary or, where applicable, legal measures until the veracity of the alleged facts has been verified, the relevant evidence has been gathered, and it has been established that a criminal offence has been committed or that conduct contrary to the ethical principles and values established at **VIARIUM** has taken place.

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

6.2.2. The right to be informed and to be heard

In particular, the accused will be informed of the investigation currently underway so that they may exercise their right of defense, having the right to be heard at any time and to put forward any arguments they deem appropriate.

Such notification shall be made at a time and in a manner deemed appropriate to ensure the successful completion of the investigation. In cases where disclosure of information relating to the investigation poses a significant risk to the ability to investigate effectively, notification to the person against whom the complaint is made may be delayed for as long as that risk persists. The aim is to prevent the destruction or tampering with of evidence by the person against whom the complaint is made.

6.2.3. Right to confidentiality

The information provided to the person against whom the complaint has been made must be disclosed in such a way as to protect the confidentiality of the complainant; the complainant's identity may not be disclosed without their express consent to any person other than those authorized to receive and handle complaints, subject to the exceptions laid down by EU or Spanish law in the context of investigations carried out by the authorities or in the course of legal proceedings.

7. Communications not accepted

Reports submitted via the Internal Reporting Channel may be rejected in the following cases:

- When reporting incidents or behavior that fall outside the scope of **VIARIUM**'s internal reporting channel.
- Where it is unfounded, it does not constitute a material and/or serious breach of **VIARIUM**'s internal regulations or is not supported by evidence or reasonable grounds.
- When it is general in nature and does not refer to specific, verifiable facts or data.
- Where it is repetitive, manifestly false or malicious, or carried out in circumvention of the law or in bad faith.
- When referring to incidents where the investigation has been concluded.
- When referring to matters under police or judicial investigation.
- For any other reason that the SII Manager may specify, providing a reasoned and substantiated explanation.

8. Reporting false or malicious complaints

VIARIUM's Internal Reporting Channel must be used responsibly and appropriately.

The communication of false information, with a malicious and dishonest intent, constitutes a breach of the principle of good faith that must underpin 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 that the facts are false, act with blatant disregard for the truth, act with the intention of taking revenge or causing harm to the person against whom the complaint is made, or act with the intention of undermining the honor or the professional, occupational or business reputation of any person associated with **VIARIUM.**

If, following a thorough investigation, it is concluded that the allegations are manifestly false and that the complaint was made maliciously and in bad faith:

(i) The complaint shall be closed, with the reasons for closing the case being documented, thereby bringing the investigation to an end;

(ii) This matter shall be referred to the person in charge of HR so that, in consultation with **VIARIUM**'s IT Manager, disciplinary measures may be proposed in accordance with the current Collective Agreement; and

(iii) The proposed sanction shall be notified in writing to the relevant body within **VIARIUM**, which shall decide on the disciplinary action to be taken against the complainant acting in bad faith.

Similarly, failure to report any conduct or apparent conduct that breaches the law and/or internal regulations may result in disciplinary action in accordance with current legislation.

9. Whistleblower Protection

9.1 Personal scope of protection

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

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

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

(c) That it is not shown that the communication was made in bad faith.

9.2. Information excluded from protection

The following people are expressly excluded from the protection provided for in this Policy: those who disclose:

a) Information previously communicated via **VIARIUM** which has been rejected.

b) Information relating to complaints about interpersonal conflicts or which concern only the person making the report and the individuals referred to in the report.

c) Information that is already fully available to the public or that amounts to mere rumors.

Information relating to acts or omissions not covered by paragraph 2 of this Policy or relating to those covered by paragraph 7 thereof.

10. Communication and dissemination

In order for this policy, as well as the Reporting Channel, to fulfil the purposes for which it has been established, it is necessary to communicate and publicize it so that any member of **VIARIUM** or its subsidiaries, as well as its suppliers, partners 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 a proper understanding of the internal

reporting system. For this reason, and with the aim of ensuring proper communication and dissemination, **VIARIUM** will draw up 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 can view it.