

## Procedure for Reporting Wrongdoing and Irregularities

Whistleblowing is a corporate compliance tool (internal control mechanism) through which employees or third parties (such as suppliers or customers) of a company can confidentially and securely report any wrongdoing they encounter in the course of their activities.

The "Whistleblower" is an individual who reports illegal or fraudulent activities within a public or private organization. The Whistleblower is often an employee but can also be a third party, such as a supplier or a customer.

Whistleblowing, therefore, is the practice of reporting violations of laws or regulations, crimes, cases of corruption or fraud, as well as situations that pose a risk to public health and safety.

The Whistleblowing Policy of Aesys S.p.A. encourages and protects employees, collaborators, suppliers, customers, and all its stakeholders (i.e., all parties with a business relationship with the Company), providing a preferential channel for reporting any act or omission carried out by anyone within Aesys S.p.A., in dealings with or on behalf of the company, that constitutes or may constitute a violation, or an inducement to violate laws and/or regulations, principles set out in Aesys S.p.A.'s Organizational, Management, and Control Model, as well as its Code of Ethics, which may directly or indirectly cause economic, financial, or reputational harm to Aesys S.p.A.

In light of the aforementioned regulatory provisions, Aesys S.p.A., already equipped with an Organizational, Management, and Control Model pursuant to Legislative Decree 231/2001 (also referred to as "Model 231"), has adjusted this Model and reviewed its reporting system, aligning the existing reporting system with new regulatory requirements.

To facilitate the submission and management of reports, Aesys S.p.A. has implemented a dedicated digital platform.

### 1. REGULATORY SOURCE AND NATURE OF THE INSTITUTION

Law No. 179/2017, titled "Provisions for the protection of individuals who report crimes or irregularities they become aware of within a public or private employment relationship," introduced amendments to Article 6 of Legislative Decree 231/2001. This law mandates the implementation of guarantees and protections for individuals who report misconduct relevant under Legislative Decree 231/2001 or incidents or behaviors that violate the Organizational, Management, and Control Model adopted by Aesys S.p.A. (hereinafter also referred to as "Aesys" or "the Company").

Legislative Decree No. 24/2023, implementing European Directive No. 1937/2019 (effective as of March 30, 2023, with full effect from July 15, 2023), consolidates into a single regulatory text the entire framework for reporting channels and the protections afforded to whistleblowers in both the public and private sectors. This results in a comprehensive and uniform regulation aimed at enhancing whistleblower protection, thereby incentivizing individuals to report illegal activities within the limits and in the manner specified by the decree.

### 2. PURPOSE OF THE DOCUMENT

This document aims to regulate the process of managing reports in a way that ensures the confidentiality of the Whistleblower's identity. The Company is committed to protecting those who, in good faith, have made a report from any intimidation or retaliation. Likewise, the Company reserves the right to implement measures under the corporate disciplinary system—as well as consider appropriate legal protection actions—against

Rev. 4 ottobre 2024 Pag.1 di 5

the Whistleblower in cases of reports made in bad faith and/or that are proven to contain slanderous or defamatory content.

### 3. WHO CAN REPORT

Anyone can make a report, particularly:

- **Company Personnel:** permanent and temporary employees, agency workers, and members of the administrative and control bodies;
- **Third Parties:** individuals who, in various capacities, have or intend to have work, collaboration, or business relationships with the Company.

The confidentiality of the Whistleblower's identity is ensured at all stages of the reporting and management process.

### 4. WHAT TO REPORT

Reports should concern events (of any nature, including mere omissions), that have already occurred or are highly likely to occur, related to Aesys Personnel and that may constitute wrongdoing, irregularities, or conduct in violation of:

- The Organizational, Management, and Control Model pursuant to Legislative Decree No. 231/2001 and the procedures implementing it;
- The Aesys Code of Ethics;
- Any (even suspected) violations of EU law by or within Aesys, including but not limited to:
  - Accounting, internal accounting controls, or auditing matters
  - Money laundering or terrorist financing
  - Financing clients who violate human rights or commit environmental crimes
  - Market manipulation
  - Insider trading
  - Confidentiality or privacy breaches
  - Theft
  - Fraud
  - Extortion or corruption
  - Verbal and/or physical violence and harassment
- Any conduct that could harm or damage the Company, even if only its image or reputation.

To ensure an effective investigation, the Whistleblower should report matters of which they have direct knowledge, providing all available information as clearly and comprehensively as possible, and include relevant and necessary details to allow appropriate and timely verification of the facts.

Reports should include, where possible:

1. A detailed description of the reported facts, indicating known circumstances (manner, time, and place) and how the information was acquired;
2. Identifying information of the Reported Person(s), to the extent known, or elements that may assist in their identification;
3. If available, supporting documents that may confirm the validity of the report, as well as identifying details of the Whistleblower (e.g., name and contact information) in cases where anonymity has not been chosen.

Communications, complaints, claims, or requests not related to the topics defined above are excluded. Reports should not concern personal grievances.

## 5. EXECUTION OF THE INVESTIGATION PHASE: REPORTING METHODS AND RECIPIENTS

Aesys provides its employees and stakeholders with a digital reporting channel via a dedicated platform, allowing everyone the opportunity to report any actual or suspected irregularities they may become aware of.

The digital platform is accessible via a link (<https://aesys.openblow.it/#/>) on the company website <https://www.aesys.com>. Once logged in, users can submit their report by simply filling out the predefined form. The digital platform offers maximum protection to safeguard the identity of the Whistleblower:

- Protects the identity of the Whistleblower and does not allow its disclosure without their explicit consent;
- Protects the identity of the reported individual;
- Maintains confidentiality of information in all contexts following the report;
- Enables digital management of reports by the company functions responsible for receiving and verifying them.

Reports are handled transparently through a predefined process. The entire process ensures protection for whistleblowers from direct or indirect pressure and discrimination by those responsible for verifying the reports, and it also allows whistleblowers to track the progress of the investigation.

Reports concerning alleged violations are forwarded to the Head of Crime Prevention (for convenience, hereafter "HCP"), a collegial body currently composed of the General Director, the HR Manager, and Aesys S.p.A.'s in-house Legal Department.

The HCP conducts an initial review and analysis of the received report to assess its admissibility and validity. Once the admissibility of the report is confirmed as relevant to whistleblowing topics, the HCP initiates an internal investigation into the reported facts and conduct. If the report pertains to matters unrelated to whistleblowing topics or is evidently unfounded, the HCP will dismiss the report and inform the Whistleblower accordingly.

The management and verification of the reported circumstances are conducted with impartiality and confidentiality, performing any deemed necessary actions, including interviewing the Whistleblower and any other individuals who may have information on the reported facts. To this end, the HCP may seek support and cooperation from relevant

company departments and, when necessary, external oversight bodies (Supervisory Body, Board of Statutory Auditors).

The HCP's preliminary assessment involves an impartial evaluation of the existence of the issues reported, consistent with the legal requirement for a "review and analysis" activity rather than a determination of actual events.

If, following the review, the HCP identifies grounds for the validity of the report, depending on the nature of the violation, it will immediately notify the relevant internal bodies according to their respective competencies. If necessary, it will report the facts to the competent judicial authorities, indicating that the report was submitted by an individual whose confidentiality is protected under Article 54-bis of Legislative Decree 165 of 2001. Should the judicial or accounting authority later request the identity of the Whistleblower, the HCP will provide this information after notifying the Whistleblower.

The traceability of the report management process is ensured through the electronic platform in use. To guarantee the management and traceability of conducted activities, the HCP ensures the preservation of reports and all related supporting documentation for five years from receipt, taking care to store the Whistleblower's identifying information separately from all other data.

### 6. WHISTLEBLOWER PROTECTIONS

Except in cases where liability may arise due to slander or defamation under criminal law or Article 2043 of the Civil Code, and in cases where anonymity cannot be maintained by law (e.g., criminal, tax, or administrative investigations, inspections by regulatory bodies), the Whistleblower's identity is protected in all contexts following the report. Therefore, except for the above exceptions, the Whistleblower's identity cannot be disclosed without their express consent.

The HCP ensures the utmost confidentiality of the Whistleblower's identity, meaning not only their name but also all elements of the report, including any attached documentation, to the extent that disclosure might, even indirectly, reveal the Whistleblower's identity. These elements are treated with the highest caution, starting with redaction of information in cases where, for investigative purposes, others must be informed.

In disciplinary proceedings, the Whistleblower's identity may be revealed to the disciplinary authority and the reported individual only when:

- 1) The Whistleblower gives their express consent;
- 2) The disciplinary charge is based, in whole or in part, on the report, and knowledge of the Whistleblower's identity is absolutely essential for the defense of the accused. In this case, Aesys cannot proceed with the disciplinary process if the Whistleblower does not expressly consent to the disclosure of their identity.

No form of retaliation or discriminatory measure, direct or indirect, affecting work conditions is allowed or tolerated against an employee who submits a report under this procedure for reasons directly or indirectly related to the report.

Aesys reserves the right to take appropriate action against anyone who engages in, or threatens to engage in, acts of retaliation against those who have made reports in accordance with this Policy.

**7. WHISTLEBLOWER RESPONSIBILITIES**

This procedure does not affect the criminal and disciplinary liability of the Whistleblower in the event of slanderous or defamatory reporting under criminal law and Article 2043 of the Civil Code. Additionally, any forms of abuse of this policy, such as reports that are manifestly opportunistic and/or made solely to damage the reported individual or other parties, as well as any other instances of improper use or intentional exploitation of the institution subject to this procedure, will also result in liability in disciplinary proceedings and other relevant forums.

**8. PRIVACY**

All personal data will be processed in accordance with applicable laws, as detailed in the Privacy Notice.