



COMPLIANCE


INTERNAL INFORMATION SYSTEM POLICY

18.06.2024


CLUE TECH, S.A.
CLUE AEROSPACE, S.L.U.
CLUE TECHNOLOGIES, S.L.U.
Palmeras del Limonar, 31 Of.1
29016 Málaga Spain

+34 951 286 911
hello@clue.aero
www.clue.aero


ISSUED BY

Name	Date	Signature
Pablo Liñan Aller	17.06.24	

REVISED BY

Name	Date	Signature
Pilar Malpartida	17.06.24	

APPROVED BY

Name	Date	Signature
Ignacio Fernández Montes	18.06.24	

REVISION HISTORY

Rev	Description of Change	Author	Effective Date
1	First Issue	Pablo Liñan Aller	18.06.24

Table of Contents

1.INTRODUCTION.....	4
2.PURPOSE AND SCOPE.....	5
3.PRINCIPLES AND GUARANTEES OF THE INTERNAL INFORMATION SYSTEM .	6
3.1. Good faith and truthfulness.....	6
3.2. Collaboration duty	6
3.3. Confidentiality and collaboration.....	6
3.4. Absence of retaliations	7
3.5. Presumption of innocence and defense right	7
3.6. Impartiality	8
3.7. Personal data protection.....	8
4.INDIVIDUALS RESPONSIBLE FOR THE INTERNAL INFORMATION SYSTEM ..	10
5.THE WHISTLEBLOWING CHANNEL AS THE INTERNAL INFORMATION SYSTEM'S MAIN TOOL.....	11
5.1. Identification.....	11
5.2. Characteristics of the use of the Whistleblowing Channel	11
6.EXTERNAL CHANNEL	12
7.REPORTING OF INFORMATION	13
8.INFORMATION MANAGEMENT PROCEDURE	14
8.1. Acknowledgment of receipt.....	14
8.2. Admission process	14
8.3. Investigation phase	15
8.4. Preventive measures	15
8.5. Resolution and termination of the file	16
8.6. Communication to the public prosecution or other competent authority	17
9.INFORMATION REGISTER-BOOK.....	18
10....APPROVAL, PUBLICATION, MODIFICATION AND VALIDITY OF THIS POLICY	19
ANNEX I - DEFINITIONS	20
ANNEX II – INDIVIDUALS RESPONSIBLE FOR THE SYSTEM	21

1. Introduction

The Internal Information System is one of the main tools to ensure legal compliance and thus prevent the commission of crimes and administrative infractions within the national and European Union framework.

In this regard, the Internal Information System stands as one of the main pillars of the Group's commitment to the principles of regulatory compliance, ethics, and transparency.

On the other hand, the Whistleblowing Channel is configured as the main tool of the Internal Information System and as the preferred channel to report crimes or administrative infractions that may occur within the Group.

2. Purpose and scope

This Policy regulates and sets forth the general principles of the Internal Information System and constitutes the main guide for its use (including the use of the Whistleblowing Channel), defining also the guidelines, the action protocol, and the information management procedure. Likewise, the Policy aims to provide protection measures and guarantees for informants and to prohibit any type of retaliation against them.

This Policy applies, on the one hand, to all companies that form part of CLUE and, on the other hand, to the following individuals (who may use the Internal Information System provided they have obtained information about crimes or administrative infractions in a work or professional context):

- Partners, shareholders, directors, attorneys, executives, managers, and employees of CLUE, including interns or trainees.
- Third parties related to or interested in CLUE (stakeholders), including, without limitation, suppliers, customers, collaborators, job applicants, etc.

The material scope of application of the Internal Information System and, therefore, the protection granted by this Policy, is limited to information related to actions or omissions that may constitute: a) violations of European Union law included in article 2.a) of the Internal Information System Act; b) criminal offenses or serious or very serious administrative offenses; and c) violations of CLUE's Code of Ethics.

3. Principles and guarantees of the Internal Information System

3.1. GOOD FAITH AND TRUTHFULNESS

In accordance with the provisions of the Internal Information System Act, good faith must be observed in its use. Consequently, communications submitted through the Internal Information System (including the Whistleblowing Channel) should be based on a reasoned or reasonable belief that acts which may constitute the infractions covered by the material scope of this Policy have occurred or may occur.

In this regard, any information communicated through the Whistleblowing Channel (or any other means of the Internal Information System) must adhere to the principle of truthfulness. The submission of false, fraudulent, or misrepresented information is not protected. Similarly, communications should avoid being based solely on conjecture, suspicion, or rumors lacking any form of verification or basis.

However, the above paragraph should not be interpreted as requiring the submission of evidence or proof as an absolute prerequisite for using the Internal Information System. Protection extends to all individuals who have reasonable grounds to believe that the information is truthful at the time of communication or disclosure, even if conclusive evidence is not provided.

3.2. COLLABORATION DUTY

All individuals, whether natural persons or legal entities included within the scope defined in the previous section 2, have an obligation to report behaviors that may constitute infractions covered by the material scope of this Policy. It is noted that such reporting may be conducted through the Whistleblowing Channel, or any other means provided for by the Internal Information System Act (e.g., external channels).

3.3. CONFIDENTIALITY AND COLLABORATION

Secrecy and confidentiality of the informant's identity, the management of the Internal Information System, and any information contained in the communication (including the identity of the alleged offender and the acts and omissions attributed to them) are guaranteed at all times.

In this regard, only the Individuals Responsible for the System, which role is regulated in section 4 of this Policy and in the Internal Information System Act, may access the content of communications processed through the Whistleblowing Channel.

The identity of the informant will never be disclosed without their explicit consent, unless required by a competent judicial body or administrative authority, in which case the informant would be notified unless such notification could compromise the investigation or judicial procedure.

Additionally, **anonymous communications** are permitted on the Whistleblowing Channel when submitting the communication.

3.4. ABSENCE OF RETALIATIONS

The adoption, attempted adoption, or threat of any retaliations against informants (including those who have made a public disclosure in accordance with Title V of the Internal Information System Act) and third parties related to them (mentioned in Article 3.4. of the Internal Information System Act) is **strictly prohibited**, provided they have adhered to the provisions of the Internal Information System Act and this Policy. The definition of retaliation is referred to in Article 36 of the Internal Information System Act.

Any individual who believes they are subjected to any form of retaliation has the right to approach any of the Individuals Responsible for the System and request protection, information, advice, and assistance. Upon verification of the existence of any type of retaliation (including threats and attempts of retaliation) against these individuals, corrective or protective measures will be taken as necessary. Additionally, as stated in Article 36 of the Internal Information System Act, any person who believes they have not been protected by the Group against retaliations may seek protection from the competent authority.

3.5. PRESUMPTION OF INNOCENCE AND DEFENSE RIGHT

The presumption of innocence and the right to honor of individuals affected by communications processed through the Internal Information System are guaranteed.

Likewise, as stated in Article 39 of the Internal Information System Act, affected individuals have the right to defense and access to the case file (while always respecting the confidentiality of the informant's identity). Furthermore, confidentiality of the identities of affected individuals and the facts attributed to them is ensured.

3.6. IMPARTIALITY

Impartiality of the Individuals Responsible for the System is guaranteed. In the event that any Individual Responsible for the System receives a communication and is found to be in a conflict of interest, they will be recused by the other Individual Responsible for the System. The other Individual Responsible for the System, who is not in a conflict of interest, will then assume the responsibility for conducting the investigation and subsequent resolution.

Conflicts of Interest for the Individuals Responsible for the System is considered to exist in the following situations:

- I. Being the person affected by the communication.
- II. Having a family relationship or similar affective relationship with the person affected by the communication.
- III. Having a direct hierarchical dependency on the person affected by the communication.

In such cases, the conflicted Individual Responsible for the System will step aside, ensuring that the investigation and resolution process remains impartial and fair.

3.7. PERSONAL DATA PROTECTION

The protection of personal data included in any information submitted through the Internal Information System is ensured by adherence of any personal data processing to the applicable legislation and regulations.

It is noted that personal data provided through the Internal Information System will only be processed for the investigation, management, and resolution of communications, and to comply with legal obligations affecting the Group under the Internal Information System Act and other applicable regulations. In this regard, it is noted that the legal basis for processing personal data lies on the prevention of criminal and administrative offenses and compliance with current legislation.

Each company of the Group will be the data controller regarding the information received by the Internal Information System regarding acts within its scope. Nevertheless, the provided data will be collected, processed and stored by the parent company of the Group, Clue Tech, S.A., which will be considered as:

- (i) data controller regarding the information received by the Internal Information System regarding acts within the parent company's scope.

- (ii) data processor regarding the information received by the Internal Information System regarding acts within the affiliate's scope. This data processing will be regulated by the relevant data processor agreement, and it is based on CLUE's legitimate interest in centralizing administrative tasks in the parent company.

It is noted that personal data will only be retained for the necessary time to investigate received communications and resolve cases; however, as stipulated in the Internal Information System Act, they may be kept for the time necessary to provide evidence of compliance with applicable legislation.

Additionally, any false information will be immediately deleted, except if it may constitute a criminal offense, in which case the data will be retained for the duration of the criminal proceedings. Under no circumstances will personal data unnecessary for understanding and investigating offenses be processed, and if such data is inadvertently communicated, it will be promptly deleted. Furthermore, all personal data pertaining to behaviors outside the scope of this Policy will be deleted. Moreover, if the received information contains personal data classified as special categories of data, it will be promptly deleted without processing or recording.

Finally, it is noted that data subjects may exercise their rights of access, rectification, opposition, erasure, restriction of processing, non-automated processing, data portability, and withdrawal of consent by written communication to the email address privacy@clue.aero, specifying the right they wish to exercise and attaching a copy of their identity document for verification.

4. Individuals Responsible for the Internal Information System

The responsibility for the correct functioning of the Internal Information System will rest with two (2) executive officers of the Clue Group, who will exercise delegated functions independently of the governing body of Clue Group companies. In this regard, the individuals responsible for the Internal Information System (hereinafter referred to as the "**Individuals Responsible for the System**") are identified in **Annex II**.

The Individuals Responsible for the System will be primarily responsible for managing and ensuring the proper functioning of the Internal Information System. They will function as a collegiate body (for the purposes of Article 8 of the Internal Information System Act), and both individuals will be accountable for implementing and managing the information management procedure diligently. The Individuals Responsible for the System will carry out their roles independently, autonomously, and free from influence by any other body or person within the Group.

The Individuals Responsible for the System shall adopt resolutions unanimously, except in cases of Conflict of Interest, where the decision will be made by the Individual Responsible for the System who is not affected by the Conflict of Interest.

The appointment and/or removal of the Individuals Responsible for the System will be notified to the Independent Authority for the Protection of Informants (or competent regional authority) within ten (10) business days following the appointment or removal. Similarly, in the event of removal, the reasons justifying it must be notified.

The Individuals Responsible for the System will delegate the ordinary management powers to one of their individuals (the "**Delegate**").

5. The Whistleblowing Channel as the Internal Information System's main tool

5.1. IDENTIFICATION

The Whistleblowing Channel serves as the main vehicle for receiving communications at CLUE regarding behaviors covered by the material scope of this Policy. It is accessible to all individuals within the personal scope of this Policy through the CLUE website (<https://clue-tech.personiowhistleblowing.com>).

Any disclosure of information to CLUE regarding a potential infringement covered by the material scope of this Policy should preferably be carried out through the Whistleblowing Channel, specifically through the platform or link mentioned.

5.2. CHARACTERISTICS OF THE USE OF THE WHISTLEBLOWING CHANNEL

The Whistleblowing Channel has been developed with a focus on principles of security, confidentiality, and anonymity preservation, ensuring that only the Individuals Responsible for the System can access the information communicated through it.

It is noted that the use of the Whistleblowing Channel is limited to reporting alleged infringements mentioned in section 2 of this Policy, and it cannot be used for other purposes.

The informant has the right to communicate information through the Whistleblowing Channel in writing, as indicated by the Internal Information System Act. Similarly, the informant has the right to request a face-to-face meeting with one of the Individuals Responsible for the System to present information regarding any infringement covered by the material scope of this Policy. In such cases, the meeting must be held within seven (7) days following the request, unless it is not feasible due to reasons attributable to the informant. If a face-to-face meeting takes place, it will be recorded with the informant's prior consent, in accordance with the Internal Information System Act. In the absence of consent, the conversation with the informant must be transcribed, and the informant should sign and accept such transcription.

6. External channel

Any individual within the subjective scope of this Policy may also report the commission of any actions or omissions covered by the material scope of this Policy to the Andalusian Office against Fraud and Corruption (<https://buzon.antifraudeandalucia.es/#/>), either directly or after having communicated through the Whistleblowing Channel.

It is noted that the Whistleblowing Channel is the preferred vehicle for reporting any actions or omissions covered by the material scope of this Policy. However, individuals may choose, depending on circumstances, to report directly to the Andalusian Office against Fraud and Corruption.

This external reporting channel is governed by the Internal Information System Act and the website of the Andalusian Office against Fraud and Corruption, to which this Policy refers.

7. Reporting of information

The information provided must include a clear and detailed description of the infractions, and if possible, identify the perpetrator, as well as the place and the date on which they occurred. Additionally, the informant may indicate any clues and evidence available, and if there is documentary evidence, it can be submitted directly through the Whistleblowing Channel.

It is noted that despite not knowing the identity of the perpetrator, information relating to infractions covered by the material scope of this Policy can be provided through the Whistleblowing Channel. In such cases, the area or department within which the infraction occurred must be specified.

The informant has the option to include their identity or remain anonymous. If the identity is revealed, the informant may specify one or more preferred means of communication (such as address, email, etc.), thereby accepting that the Delegate or any other Individual Responsible for the System may communicate with them to request further information, clarifications, or meetings.

All data provided in the communication will be strictly confidential and processed in accordance with the personal data protection regulations, the provisions on the protection of personal data included in the Internal Information System Act and this Policy.

Upon receiving the communication, the informant will be provided with a unique code to access the Whistleblowing Channel and check the status of the matter. This unique code also allows the informant, if anonymity was requested, to provide new information without revealing their identity. For security reasons, the informant should securely retain the unique code as it cannot be recovered if lost or forgotten.

8. Information management procedure

8.1. ACKNOWLEDGMENT OF RECEIPT

The informant will receive an acknowledgment notification within seven (7) calendar days from the communication, unless doing so could jeopardize the confidentiality of the communication or if the informant has chosen to remain anonymous. However, in any case, an acknowledgment of receipt of the information will be issued and recorded in the Whistleblowing Channel. This allows the informant who has opted to remain anonymous to verify that the communication has been received by accessing the Whistleblowing Channel with the unique code provided.

8.2. ADMISSION PROCESS

Within fifteen (15) calendar days from the communication, the informant (provided they have indicated a means of communication) will be notified regarding the admission or rejection of the communication for processing. Otherwise, the action will be recorded in the Whistleblowing Channel, allowing the informant to check the processing status by accessing the Whistleblowing Channel with the unique code provided.

The decision on whether to admit or reject communications received through the Whistleblowing Channel will be the responsibility of the Individuals Responsible for the System. Communications may only be rejected for the following reasons:

- The reported facts lack credibility.
- The reported facts do not constitute an infringement covered by the material scope of this Policy.
- The communication was not made by a person within the subjective scope of this Policy.
- The communication is evidently unfounded.
- The communication concerns matters already investigated in previous proceedings, unless new and relevant information is provided or new factual or legal circumstances justify further investigation.

Unanimous decision by the Individuals Responsible for the System is required for rejecting communications. The informant will be notified (or the decision will be made available through the Whistleblowing Channel) regarding the rejection decision and the reasons justifying it.

If the communication relates to facts already under investigation in another ongoing case, its processing and investigation will be consolidated with the ongoing case.

8.3. INVESTIGATION PHASE

Once the communication has been admitted for processing, all relevant investigative measures will be carried out to verify the truthfulness of the facts or omissions reported in the communication.

The investigative measures must be proportional, necessary, and essential to fulfill their purpose. In this regard, only data and information strictly necessary to verify whether any of the infractions listed in section 2 of this Policy have been committed will be obtained and stored.

The informant (if they have reported through a preferred means of communication) will be given an opportunity to be heard, as well as any witnesses they wish to present who may have knowledge of the facts or omissions under investigation.

Likewise, the affected person by the communication will be given an opportunity to be heard; they will be informed of the alleged infractions included in the communication, from which point they may submit written allegations. The affected person may also provide any evidence they deem appropriate and relevant.

All evidence submitted by the parties will be included in the record. Statements from the parties and witnesses will be recorded in minutes and also included in the record, upon the specific party's or witness's signature. All this documentation will be stored in the Internal Information System, in strict compliance with confidentiality obligations.

The investigation phase shall not exceed two (2) months from the receipt of the communication, except in cases of special complexity that require an extension of the deadline, in which case the investigation phase may be extended up to four (4) months and fifteen (15) natural days from the receipt of the communication.

Once the investigation phase is completed, the Individuals Responsible for the System will prepare a report outlining the proposed course of action for concluding the initiated record and the proposal for sanctions or dismissal.

8.4. PREVENTIVE MEASURES

In accordance with the presumption of innocence and the other principles underlying this Policy (with emphasis on the principle of proportionality), the Individuals Responsible for the System may decide on the adoption of preventive measures aimed at avoiding or preventing the following risks:

- I. Commission of new infractions or continuation of the infringing conduct.
- II. Concealment or destruction of evidence.

8.5. RESOLUTION AND TERMINATION OF THE FILE

After analyzing the documentation of the file, the Individuals Responsible for the System will reach one of the following conclusions:

1. Archive the file, considering that the reported facts or omissions have not been proven or cannot be categorized under any infraction covered by the scope of this Policy.
2. Declare the existence of infractions and, if applicable, communicate the resolution of the file to the competent body to establish corrective measures and enforce disciplinary actions or sanctions.

Within a period of three (3) months from the receipt of the communication, the informant will be notified, or the information will be made available to them through the Whistleblowing Channel, regarding the actions taken to verify the truthfulness of the reported facts and the outcome of the investigation, as well as the resolution of the file. However, in cases of special complexity, this notification may be delayed up to six (6) months from the receipt of the communication.

In order to establish regulatory compliance and ethics as a culture within the Group, the Individuals Responsible for the System may adopt measures aimed at preventing possible recurrences of infractions, such as:

1. Enacting internal rules and corporate policies.
2. Providing specific training.
3. Establishing risk monitoring systems.

Any measures adopted will be carried out with strict adherence to the principle of confidentiality preservation established in the Internal Information System Act and this Policy.

8.6. COMMUNICATION TO THE PUBLIC PROSECUTION OR OTHER COMPETENT AUTHORITY

If the facts could potentially constitute a criminal offense, the received information concerning them will be promptly forwarded to the Public Prosecutor's Office. On the other hand, if the facts could affect the financial interests of the European Union, the information will be communicated to the European Public Prosecutor's Office.

9. Information register-book

There will be a register-book of communications received through the Whistleblowing Channel containing the following data:

- a) Date of receipt of the communication;
- b) Identification code;
- c) Actions taken;
- d) Resolution and measures adopted; and
- e) Closing date.

Confidentiality of the information contained in the register-book will be guaranteed at all times. As stipulated in the Internal Information System Act, access to the contents of the aforementioned register-book in whole or in part may only be granted upon reasoned request by the competent judicial authority, through a court order, within the framework of a judicial procedure and under its supervision.

Personal data related to the information received and internal investigations referred to in this section will only be retained for the period necessary and proportionate to comply with the Internal Information System Act and other applicable regulations. Under no circumstances shall data be retained for a period exceeding ten (10) years.

10. Approval, publication, modification and validity of this Policy

This Policy has been approved by the governing body of CLUE's parent company on **June 18, 2024**.

Any modification to this Policy must be approved by the governing board of the parent company of CLUE upon proposal by the Individuals Responsible for the System. In any case, reviews of this policy will be conducted biennially by the Responsible Parties of the System, who will propose modifications and updates, if necessary, to the board of directors of the parent company of CLUE.

This Policy will come into effect on its approval date and will remain in force indefinitely until any modification is adopted as provided in this clause.

Annex I - Definitions

“Internal Information System” shall refer to the set of tools, policies and procedures established in CLUE and aimed at implementing a system that ensures the secure receipt and effective handling of communications, as well as protection in favor of informants and related third parties.

“Whistleblowing Channel” shall refer to CLUE’s Internal Information Channel (the main tool of the Internal Information System understood as a channel for the receipt of information).

“CLUE” o **“Group”** shall jointly refer to Clue Tech, S.A., Clue Technologies, S.L.U. and Clue Aerospace, S.L.U.

“Internal Information System Act” shall refer to Law 2/2023 of 20 February on the protection of persons who report regulatory offences and the fight against corruption.

“Individuals Responsible for the System” shall refer to its definition included in Clause 4 of this Policy.

“Delegate” shall refer to its definition included in Clause 4 of this Policy.

Annex II – Individuals Responsible for the System

The governing body of CLUE's companies has appointed today, as Individuals Responsible for the System, the following persons:

- **Mr. Pilar Malpartida**, as head of talent & people.
- **Mr. Pablo Liñan Aller**, as chief of staff & head of legal, who will also exercise the Delegate's duties.



SIMPLE SOLUTIONS
TO BIG PROBLEMS

Grupo Clue
Palmeras del Limonar 31, Oficina 1
29016 - Málaga - Spain
hello@clue.aero
www.clue.aero

