PUBLIC

Clue

# Security Policy

CD-120

10.07.2023

**CONTACT**

CLUE
Palmeras del Limonar, 31
29016 Málaga Spain

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

# Revision History

| Rev. | Amendment | Description | Author | Date |
|---|---|---|---|---|
| #01 | 00 | First Issue | Carlos Cañero | 02.06.2023 |
| #01 | 01 | Added ISO/IEC 27001 reference | Carlos Cañero | 10.07.2023 |

# Table of Contents



# Tables

*This section has been left blank intentionally.*

# Figures

*This section has been left blank intentionally.*

# 1. Security Policy

Our security policy outlines the key items protected within the organization; It starts with the correct development of the Clue processes, which depend, in part, on Information Technology (IT) systems being adequately protected. This reliable protection allows Clue to better perceive its interests, to efficiently carry out its obligations in information security by facing the possible risks and accepting those that, based on the available information, are understandable, mitigated, controlled, and treated when necessary.

This Security Policy identifies the rules and procedures for all individuals who access and use Clue's assets and resources. In turn, this policy seeks to convey our organizational culture in which the rules and procedures are governed by focusing on our employees' information and work.

The purpose of information security at Clue is to minimize the risk of damage by preventing security incidents, as well as to reduce their potential impact where it is unavoidable. To achieve this, we have developed a Security Management methodology that allows us to regularly analyze the degree of exposure of our important assets to those threats that may take advantage of certain vulnerabilities and introduce adverse impacts to the activities of our personnel or to the important processes of our organization.

For this reason, Clue's Security Policy takes into account how people in the organization actually use and share information among themselves and with the public.

This Security Policy aims to preserve the confidentiality, integrity, and availability of the systems and information used by the Clue members and is based on the following main principles:

- Confidentiality, which involves the protection of Clue assets from unauthorized entities. Protecting the confidentiality of information related to clients and development plans.
- Integrity, which ensures that the modification of assets is handled in a specific and authorized manner.
- Availability; which is a system state where authorized users have continuous access to those assets.
- Compliance: with the rules governing the industry to which the organization belongs.
- To understand and address operational and strategic information security risks so that they remain at acceptable levels for the organization.
- Publicly accessible web services and internal networks meet the required availability specifications.
- Understanding and meeting the needs of all stakeholders.
- All members of the staff are duly informed and responsible for information security as it is a factor of great relevance in their work.
- Information security risks are always monitored; this leads to take relevant measures when changes that involve an unacceptable level of risk occur.
- Situations that may expose the organization to the violation of laws and legal norms will not be tolerated.
- Our Security Policy plays an important role in the decisions made by the top management to support the continuity of good productivity and innovation and seeks to facilitate our organization and staff to fulfill their mission and objectives.
- The organization's Senior Management expresses without any doubt, its total commitment with the continuous system improvement and with its final purpose, which should be none other than to comply with the information security requirements of the system's stakeholders.
- The policies and procedures contained in the Information Security Management System compliance with the ISO/IEC 27001.

The Security Team advises the Management Team and provides specialized support tasks to all staff members and ensures that information security status reports are available and that each staff member is responsible for maintaining information security within their work-related activities.The functions and responsibilities of the Security Team are described in the Organization Chart.

The organization counts on the collaboration of all employees by applying the proposed security policies and directives.Compliance with this policy and the information security policy is mandatory for all the members of the organization.

**Signed by**

**Electronic Signatures**

Signatures
2023-07-10 16:24:25
Carlos Cañero Fernández signed with meaning **Authorship**

2023-07-10 16:24:46
Begoña Montoro signed with meaning **Review**

2023-07-10 16:25:49
Juan Francisco Pérez signed with meaning **Review**

2023-07-17 13:00:37
Ignacio Fernández Montes signed with meaning **Approval**


SIMPLE SOLUTIONS

TO BIG PROBLEMS

Clue

Palmeras del Limonar 31

29016 - Málaga - Spain

hello@clue-technologies.com

clue.aero