INFORMATION SECURITY POLICY

HEXOD SECURITY S.L

1. INTRODUCTION

Hexod Security S.L., from now on Hexod, is a company dedicated to cybersecurity, specializing in analyzing and validating vulnerabilities for our clients.

The company seeks constant interaction with partners, clients, and suppliers, sharing knowledge and experience in cybersecurity to create secure work ecosystems that aim to achieve the highest levels of confidentiality, integrity, and availability, thereby ensuring information security.

2. OBJECTIVE

The purpose of this document is to establish the basic security guidelines and define the organization's commitment to comply with the security requirements that guarantee the security of the company's information systems.

This document also reflects the company's commitment to continuous improvement in terms of security, which will ultimately improve the security of the services offered and the organization's internal processes.

3. SCOPE

This policy is mandatory for all members of Hexod, both in their internal relationships and in their relationships with third parties.

This policy applies to all information used by Hexod in the development of its professional activities.

4. RESPONSIBILITIES

Hexod is committed to ensuring the security of all assets under its information security system, applying the necessary measures, by always being in compliance with the various applicable laws and regulations.

The responsibility for ensuring compliance with and updating of the security policy lies with the *Security Manager* who, together with the CEO as the person ultimately responsible, will be responsible for formulating the basic security principles and guidelines and ensuring compliance with this document and all actions, policies and procedures derived from it.

All persons in connection with Hexod are formally under the obligation to know and comply with this policy and other internal codes that may be established by the management, as well as to use it appropriately and comply with the controls and recommendations mentioned in this document.

5. DEFINITIONS

From the perspective of information security:

- **Confidentiality:** data and information systems are only accessible to authorized individuals.
- **Integrity:** data and information systems are not modified, lost, or destroyed without authorization.
- **Availability:** data and information systems are accessible to authorized parties when needed.

6. DESCRIPTION

a. MISSION AND GENERAL PRINCIPLES

Hexod's mission is to build customer confidence in cybersecurity by analyzing and validating vulnerabilities that could compromise the continuity of their business.

Hexod and its employees are guided by the following values:

- **Teamwork,** with the conviction that people working together can achieve anything.
- **Innovation,** betting on creativity, and change as essential elements for growth.
- **Quality and efficiency,** always seeking continuous improvement in the pursuit of excellence.
- **Constant communication with clients,** addressing and understanding their current needs, and providing specific solutions that ensure success.
- **Transparency** in all our actions, generating a positive impression among clients and suppliers, fostering a relationship of trust.

This policy, in line with the mission and values of the company, adheres to best security practices as outlined in the International Standard ISO/IEC 27001 and complies with current legislation regarding personal data protection and information security. In this regard, Hexod establishes specific policies, procedures, and protocols to manage each of the aspects and requirements mandated by the standard.

The secure handling and protection of information is a priority for Hexod due to its strategic nature and importance for business continuity. For this reason, this policy aims to preserve the three basic components of information security: confidentiality, integrity, and availability of information.

This policy is taken into consideration during all phases of the information lifecycle and the systems that house it.

b. MANAGEMENT COMMITMENTS

The management of Hexod, within the previously defined framework and aware of the importance of Information Security for providing quality service and achieving its business objectives, is committed to:

- ➢ **Continuously maintain and improve the Information Security Management System (ISMS) of the company,** providing all necessary resources to achieve the objectives established in line with what is stated in this policy.
- ➢ **Satisfy all stakeholder requirements regarding Information Security,** as well as legal and regulatory requirements and any others that Hexod subscribes to or implements within the organization.

- ➢ Focus Hexod's work on **achieving the established objectives**, which must be specific, measurable, achievable, realistic, and always oriented towards continuous improvement. These objectives will be measured and reviewed annually, and the necessary resources will be ensured for their achievement.
- ➢ **Adopt efficient management criteria to eliminate, minimize, transfer, or accept risks and opportunities in all organizational processes.** Risks will be considered in decision-making.
- ➢ Establish effective criteria and protocols to **anticipate potential information security failures**, taking into account the impact that a loss of confidentiality, integrity, or availability could cause.
- ➢ **Promote ongoing training and awareness** among the organization's personnel to enhance their contribution, while fostering their **creativity, innovation, and participation.**
- ➢ **Establish effective communication channels with stakeholders** to facilitate the smooth and secure exchange of information, allowing for the sharing of experiences and knowledge, and facilitating the creation of mutually beneficial synergies.
- ➢ **Provide the appropriate means** to ensure that this policy is communicated, understood, internalized, implemented, and followed by all individuals working in and for Hexod, both directly and indirectly.

7. APPROVAL AND REVIEW

This policy is subject to review during the annual audits conducted within the company. These audits, both internal and external, aim to assess compliance with the policies and to provide an objective evaluation of adherence to the agreed security standards.

In any case, at least once a year, the Information Security Committee will include among the topics to be discussed, the review, update, and proposed modifications of this policy. This policy, or any significant changes to it, must be communicated to the organization and brought to the attention of stakeholders. The Information Security Policy takes effect from the moment of its publication, following the approval of the CEO.

8. COMPLIANCE CONTROL

Any deviation or exception to this policy must be documented, justified, and formally accepted by the person responsible for the ISMS or their delegated representative.

In the event of verified non-compliance with any of the measures stipulated in this policy, management may take appropriate actions in line with human resources policies and current legislation to ensure compliance

A Coruña, 4th November, 2024

Roi Mallo,
CEO de Hexod