Azkoyen Group	SYSTEM POLICY	Code: VPSIS00009 Revision: 1.0

INFORMATION SECURITY POLICY

Management system: **ISO 27001 Information Security Management**	**Process:** P11 - Manage Information Technology	**Work centre:** **VPS**
Revised by: **Luis Villafranca Rodriguez** **10/11/2023**	**Approved by:** **Juanje Alberdi** **10/11/2023**	**Approved by:**

LIST OF AMENDMENTS	
Description of the amendment Revision	
1.0	Creation of the document

CONTENTS

1. INTRODUCTION

AZKOYEN's business processes depend to a large extent on the Information Systems and the Information that they store. The mission of the Security Policy is to establish the global Security guidelines for the organisation, as well as to protect the information assets.

These guidelines include the adoption of a series of organisational measures and rules that are set out in this document and further developed in their associated documents, the purpose of which is to protect AZKOYEN's information resources, and the information systems used for processing them, against internal or external, deliberate or accidental threats, in order to ensure compliance with the confidentiality, integrity, availability and legality of the information.

This Policy is based on best practice recommendations for ensuring Security in Information System Management (International Standards ISO 27001 and ISO 27002), as well as on current legislation applicable to this area.

2. AIM

The main objective in creating this Policy is to guarantee users access to information in the quantity and quality required for performing their duties, as well as to avoid serious losses of information and unauthorised access to it.

3. SCOPE

3.1. EMPLOYEES

Information Security is a joint effort. It requires the involvement and participation of all members of the organisation who work with Information Systems. Therefore, each employee must comply with the requirements of the Security Policy and its associated documentation. Employees who deliberately or negligently breach the Security Policy will be subject to disciplinary action as set out in the last chapter of this document.

3.2. INFORMATION SYSTEMS

This Policy affects all AZKOYEN VPS information assets, whether in digital or paper format, of a personal nature or not, and whether stored on personal computers or servers, smartphones, networks, applications, operating systems, or company processes that belong to and/or are managed by AZKOYEN. This Policy covers the aspects most directly related to the responsibilities of and proper use by personnel.

3.3. THIRD PARTIES

This Security Policy is extended to and must be understood and complied with by any external person connected to third parties who carry out any kind of processing of the information owned by AZKOYEN. Furthermore, this Policy and its associated procedures shall be compulsory for third party suppliers contracted to provide professional services in the areas deemed appropriate, in the event that they carry out any activity involving access to or processing of any system or information owned by AZKOYEN, and this shall be defined in the contract.

4. ROLES & RESPONSIBILITIES

4.1. USERS

Users must be aware of and apply the Security Policies, procedures, standards and apply current legislation. They must understand them and comply with them.

In general, anyone who generates information is responsible for its classification in accordance with the Company's instructions. Furthermore, anyone using information and/or information systems is obliged to manage them with the necessary care and to use them only for authorised tasks and in compliance with the regulations. This also applies to external personnel.

4.2. OWNERS

The ownership of information assets generally corresponds to the General Management, or Department heads, who must acquire, develop and maintain the Company's applications as support systems for decision-making and other activities of the Company.

The owners must specify the classification of their assets that is most appropriate to their critical value, availability and relative importance to the organisation. Their classification will indicate the level of risk and protection, as well as the level of access to that information or application.

4.3. ADMINISTRATORS

Administrators are Employees in charge of safeguarding the Company's own and third party information.

Each information system must have at least one authorised administrator as stated in the Security Document.

They are responsible for storing information, implementing access controls (to prevent unauthorised access) and running regular backups (to ensure the availability of critical information).

5. POLICY MAINTENANCE, APPROVAL AND REVIEW

The Information Security Manager is responsible for establishing and maintaining AZKOYEN's Security Policy, manuals and related procedures.

The General Management is responsible for approving and publishing the Policy, distributing it to all Employees and to all affected third parties, as well as reviewing and evaluating the Security Policy.

Any change or development that affects or could affect the content of this Security Policy will be recorded with a new signature on the approval document. In this way, the commitment to information security is specified and confirmed.

The validity and reasonableness of this Policy shall be reviewed regularly, and always within a period not exceeding one year, and any improvements, adaptations or amendments required by organisational, technical or regulatory changes shall be made as appropriate.

6. DISTRIBUTION OF THE POLICY

The Security Policy document shall be accessible to all internal personnel, shall be provided during induction to new employees and shall be distributed by e-mail every 12 months to all internal and external employees subcontracted by AZKOYEN who handle data and resources belonging to the company so that they are aware of the security rules in place.

Any substantial change to the document shall be distributed to all users through a formal notification, sent by e-mail or by internal communication, in a form accessible to them, by means of a communication format provided for this purpose.

7. SANCTIONS/DISCIPLINARY PROCEEDINGS

Any premeditated or negligent violation of the security policies and rules and which involves potential damage, incurred or not, to AZKOYEN, will be sanctioned in accordance with the mechanisms provided for in the Company Agreement and in the legal, contractual and corporate regulations in force.

All of the actions in which AZKOYEN's security is compromised and which are not foreseen in this Policy must be reviewed by the General Management and by the Security Manager in order to issue a ruling in accordance with the Company's criteria and the legislation in force.

Disciplinary actions in response to breaches of the Security Policy are the responsibility of Department Managers in conjunction with Administration and General Management.

8. INFORMATION SECURITY POLICY

Azkoyen's business processes depend to a large extent on the Information Systems and the Information they store. This Security Policy aims to establish global security guidelines to protect the corporate information assets.

These guidelines include the adoption of a series of organisational measures and the establishment of a set of rules aimed at dealing with threats - internal or external, deliberate or accidental - in order to ensure compliance with the principles of confidentiality, integrity, availability and legality of information.

This Policy is based on an information system management model that is in line with the implementation of the ISO/IEC 27001:2022 international standard, and integrated with ISO/IEC 9001: 2015 and ISO /IEC

45001, as well as in compliance with the legislation in force, especially in the field of personal data protection:

> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the General Data Protection Regulation (GDPR).
> Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (LOPD-GDD).

The Azkoyen VPS senior Management team is firmly committed to promoting and leading an integrated Information Management System, in which all users are aware that each one of them is a key factor in its security and must be guided by the following governing principles referred to above (confidentiality, integrity, availability and legality).