Azkoyen Group	**SYSTEM POLICY**	*Code*: IS Policy (EN) *Version*: 1.0

INFORMATION SECURITY POLICY

Management System: Integrated	*Process:* P01 - Develop Vision and Strategy	*Work Centre:* Azkoyen Group
Reviewed by: David Armendariz Mancho *09/09/2024*	*Approved by:* Juanje Alberdi *09/09/2024*	*Approved by:*

The Azkoyen Group's ("Azkoyen") business processes largely depend on the information systems associated with such processes. Therefore, an Information Security Policy must be defined, which establishes the **essential and common guidelines** for all entities of the Azkoyen Group.

INFORMATION SECURITY POLICY

This document contains **Azkoyen's Security Information Policy** (the "Policy"), which aims to protect all corporate information resources against internal or external threats, whether deliberate or accidental, guaranteeing compliance with the governing principles of **confidentiality, integrity, availability and lawfulness, with special attention to the fundamental right of control of the company's own information or the protection of personal data**.

This Policy is based on a management model that focuses on continuous improvement and on the compliance with the current applicable laws, as well as with the private international standards ISO 27001 and ISO 27002 (regardless of whether each entity of the Azkoyen Group is certified or not), while observing all of the complementary and recommended best practices.

The Azkoyen Group has a firm commitment to promoting and leading an integrating information system, in which all users are aware of the fact that each and every one of them are key to ensuring the system's security and that information security must be regarded as a joint effort. As a consequence, all users must be familiar with and observe this Policy, and guide their actions according to the governing principles mentioned above.

This Policy is developed by means of approving the different associated documents, which are used to establish specific procedures and measures.

SCOPE

Internal Users

All staff with a labour relationship with any of Azkoyen's entities are required to be familiar with and comply with the Information Security Policy and with the specific obligations derived from the associated documents that may apply, based on their roles.

External Users

This Policy applies to all entities or external staff authorised to handle and process Azkoyen's information assets. This includes the staff and service outsourcing companies of any type, provided that the execution of these services involves or may involve access to any system or information owned or filed under the responsibility of Azkoyen.

Information Systems

The scope of this Policy includes all of Azkoyen's information assets, regardless of the format, whether digital, analogue or hard copies; whether the content includes personal data or not; whether the information is hosted in personal devices or computers (such as laptop computers, smartphones, tablets, etc.) or on servers, platforms, networks, applications, operating systems;

and also regardless of whether such assets are administrated by service outsourcing companies or not.

Likewise, this Policy also applies to the information assets owned by third parties but administrated by Azkoyen for the purpose of guaranteeing their security.

ROLES & RESPONSIBILITIES

Users of the Information Systems

All users must be familiar with and observe the Policy at all times, and comply with its procedures, measures and provisions, which are included in the corresponding documents and which apply according to their role.

Risk Owners

The Risk Owners of all entities that are part of Azkoyen refer to the people with the authority to manage the risks corresponding to the assets and who are accountable to the Senior Management of each entity. Therefore, the Risk Owners will classify the assets with a coherent approach and according to their critical value, availability and relative importance to the company. They will be classified according to the risk and protection levels and to the level of access to the associated information or application.

Each entity of the Azkoyen Group will have its own risk owners, which will be the Area Managers, Directors and Senior Management.

MAINTENANCE, APPROVAL AND REVISION OF THE POLICY

The Managing Directors of the Azkoyen Group’s Divisions are responsible for approving this Policy.

The Policy is reviewed once a year in an ordinary revision process to adapt it to the corresponding organisational, technical or regulatory changes. However, extraordinary revisions may be carried out if needed.

Any change or update that affects or may affect the content must be previously approved and recorded to ensure proper traceability.

PUBLISHING AND DISTRIBUTING THE INFORMATION SECURITY POLICY

This Policy is public and the latest version is published on the corporate website, www.azkoyen.com, without prejudice to being included in user manuals or any other similar document handed over as part of the onboarding materials to any person hired by the companies of the Azkoyen Group.

The agreements signed with external auxiliary service providers that require or are associated with access to Azkoyen’s assets will include reference to the commitment to observe this Policy, which will be posted on www.azkoyen.com.

Without prejudice to publishing the latest version on its website, any substantial change to this Policy must be notified to all users (internal and external) through the corresponding communication channel(s) (for example, via email, in a webinar, etc.).