Azkoyen Group

Information Security Policy

December 20, 2024

Information Security Policy Context

In today's digital era, companies increasingly rely on technology and information systems to carry out their daily operations. This reliance has transformed how businesses manage their processes, interact with customers, and compete in the market. Information has become a strategic asset that must be protected to ensure regulatory compliance, business continuity, and maintain stakeholder trust.

Similarly, digital transformation has led companies to adopt advanced technologies that improve operational efficiency, personalize customer experience, and enable data-driven decision-making. However, it has also increased the likelihood of attacks and risks associated with information security.

In addition, regulations impose strict requirements on how companies must manage and protect personal information regarding data protection. Failure to comply with these regulations can result in significant economic, personal, and commercial penalties, as well as reputational damage.

In short, information security is essential for the success and sustainability of companies in today's digital environment, protecting information assets, strengthening stakeholder trust, ensuring regulatory compliance, and providing a solid foundation for innovation and growth.

Information Security Policy

This document contains Azkoyen's Information Security Policy (hereinafter, the "Policy"), whose main objective is to protect all corporate information assets against threats—whether internal or external, deliberate or accidental—while ensuring the guiding principles of:

- **Confidentiality**: protecting information against unauthorized access and ensuring that only authorized individuals, entities, or processes can access it. This is the fundamental principle for safeguarding privacy and data security.

- **Integrity**: ensuring the accuracy of information and its processing methods. This principle ensures that data is not improperly altered, whether by error or malicious actions, keeping information consistent and reliable throughout its lifecycle.

- **Availability**: ensuring that information systems are available for use by authorized users when needed. This principle ensures that information assets are accessible at the right time and place, enabling business continuity.

- **Legality**: complying with all applicable laws, regulations, and standards, with special attention to the fundamental right to informational self-determination or personal data protection. This principle ensures that Azkoyen operates within the established legal framework.

This Policy is created under a continuous improvement management model and is based on the applicable legislation in each case, as well as the private international standards ISO 27001 and ISO 27002 (regardless of whether each entity within Azkoyen obtains the corresponding certification) and complementary good practice recommendations.

Azkoyen is firmly committed to promoting and leading an information management system in which all users are aware that each of them is a key factor in its security, and that information security depends on a joint effort. Consequently, all users must be familiar with and comply with this Policy, guided by the above principles.

This Policy is developed and supplemented through, among others, the following documents, which set out procedures, instructions, formats, and specific measures at different levels regarding information security:

- Communication plan for the information security management system
- Legal compliance control
- Change management
- Privacy by design and by default analysis
- Data protection impact assessment procedure
- Asset management
- Password management policy
- Logical access control
- IT user management procedure
- Information security objectives
- Information security roles, responsibilities, and authorities
- Human resources-related security
- Corporate information system user manual

This Policy is a corporate policy and applies to all Azkoyen companies.

Scope

Internal users

All personnel employed by any of the companies within the Azkoyen Group.

External users

This Policy also applies to any external entity or person authorized to perform any type of processing on Azkoyen's information assets. This includes individuals and companies providing outsourced services of any kind, whenever the execution of such services involves or may involve access to any system or information owned by or under the responsibility of Azkoyen.

Information systems

This Policy applies to all Azkoyen information assets, regardless of the type of medium—digital, analog, or paper; whether or not the content includes personal data; whether the information is hosted on professional or personally used equipment or devices (such as laptops, smartphones, tablets, etc.) or on servers, platforms, networks, applications, operating systems; and regardless of whether such assets are administered by outsourcing companies.

Furthermore, for security purposes, this Policy also applies to information assets that, while owned by others, are administered by Azkoyen.

Roles and Responsibilities

Information system users

All users, both internal and external, must be aware of and comply with the Policy, as well as follow the procedures, measures, provisions, and specific obligations contained in the associated documentation that apply to them based on their assigned functions.

Risk owners

The risk owners of each of the companies within the Azkoyen Group are those individuals who have the authority to manage the risks associated with the assets and the responsibility to report to the Senior Management of each of those companies (the "Risk Owners"). For this purpose, the Risk Owners classify the assets in line with their critical value, availability, and relative importance to Azkoyen. Their classification determines the level of risk and protection, as well as the level of access to such information or application.

Within each Azkoyen company, the Risk Owners are the individuals assigned in the procedures and instructions, as well as those legally designated, the Area Managers, the Directors, and Senior Management, in that order.

The specific allocation of roles and responsibilities, as well as the security control mechanisms for information security in each of Azkoyen's divisions, will be developed through the corresponding internal regulations.

Approval and Review of the Policy. Relationship with Other Policies

Azkoyen's Board of Directors approves this Policy and, through its **Board Sustainability Committee** , ensures the development and implementation of this Policy, its strategies, and the plans arising from it.

Likewise, the Sustainability Committee (made up of executives from different areas and belonging to all business segments of the Azkoyen Group), the General Managements, and the Human Resources Department, in accordance with this Policy, promote and implement strategies, plans, programs, and initiatives, assign responsibilities at different levels of the organization, involve all employees, and support the Committee in its activities.

To ensure communication, transparency, accountability, and compliance with information security objectives, Azkoyen has control bodies that continuously monitor, measure, and evaluate the company's performance and progress toward its objectives, as set out in the Sustainability Policy.

An ordinary review of this Policy is carried out annually to adapt it to organizational, technical, or regulatory changes. However, extraordinary reviews may be carried out whenever necessary.

In addition, as an identification and evaluation mechanism, Azkoyen annually updates its Risk Management model (risk map) with the help of an external advisor. This identifies, categorizes, and prioritizes risks (including cyber risks and business information security risks) to establish mitigation actions for the most relevant ones and an audit plan for those actions.

This Policy and its supporting documents are related to and complemented by the following internal Azkoyen regulations:

- Sustainability Policy
- Internal Information System and Whistleblower Protection Policy and Procedure
- Whistleblowing Channel Privacy Policy
- Risk Management and Control Policy
- Compliance Manual
- Code of Conduct

This Policy was approved by Azkoyen's Board of Directors, exercising its authority to approve and update corporate policies, on December 20, 2024, and entered into force upon its approval.

In the event of non-compliance with the obligations set forth in this Policy, the employee may be sanctioned in accordance with the applicable regulations and collective bargaining agreements.

Publication of the Information Security Policy

This Policy is public and is permanently published in its updated version on the corporate website www.azkoyen.com. It may also be included in the user manual or similar documents provided to individuals joining any of the Azkoyen Group companies upon hiring.

Contracts with external service providers that involve or may involve access to Azkoyen's assets will include a reference to the commitment to comply with this Policy and to its availability on the website www.azkoyen.com.

Without prejudice to the publication of the updated version on the aforementioned website, any substantial change to this Policy will be communicated to all users—internal and external—through the communication channel(s) in place (for example, email, webinar, etc.).