Information Security Guideline

Version: 1.0
Date: 01.04.2026

Content

Statement by the Management

In this information security policy, the management board of IKARUS Security GmbH (hereinafter referred to as "IKARUS") defines the objectives and strategies that serve as a foundation for all decisions and actions related to information security within the company.

The purpose is to implement uniform standards and processes for information security in the interest of the company, customers, employees, and other interested parties.

The information security policy is derived from and harmonized with the overall corporate strategy. It is essential for achieving corporate goals and executing the corporate strategy.

This policy enters into force on April 1, 2026, and is binding for all IKARUS employees.

Scope of Application

The information security management system covers all office premises of IKARUS Security GmbH as well as IKARUS data centers at service providers in Europe.

The regulations apply to all IKARUS employees and all organizational units at the locations mentioned, regardless of the nature of their employment relationship and their hierarchical position.

It covers all services used by IKARUS and addresses all processes and projects for the processing, transfer, storage, archiving, and deletion of information, regardless of its form (electronic, written, or verbal).

Information Security Policy

In an increasingly networked and digitized world, protecting sensitive data and systems is crucial to ensuring confidentiality, integrity, and availability. We recognize the ever-growing threat to information security and are committed to continuously implementing, reviewing, and improving appropriate security measures to meet our obligations to our stakeholders.

This information security policy defines the principles, objectives, and measures for ensuring the security of information within our organization. It serve as a basis on which we build a culture of information security that is firmly anchored in our daily work processes.

It serves as a guideline for all employees, contractors, and partner companies and sets out expectations, responsibilities, and procedures for handling information. By complying with this policy, we not only help protect our own data and systems, but also the privacy and security of our customers, partners, and other stakeholders.

Personal Responsibility

A prerequisite for achieving information security objectives is the conscientious and careful handling of data, information, and information-processing systems by all IKARUS employees and all third parties involved in these processes. Managers at all levels serve as role models and are obliged to communicate and implement all defined measures to ensure information security within their areas of responsibility. Each individual employee contributes to the successful implementation of information security through their personal commitment.

By operating an information security management system in accordance with the state of the art, IKARUS ensures that information security objectives are consistently pursued.

A Chief Information Security Officer, reporting directly to senior management, ensures that the maturity level is continuously improved.

Information Security Objectives

The fundamental objectives of information security are to ensure the availability, integrity, and confidentiality of all systems and information.

The maturity level of information security is increased by achieving the following information security objectives:

- Availability: Ensure that systems and information are available at all times to authorized users or other interested parties and are not affected by failures or attacks.
- Integrity: Ensuring the accuracy, completeness, and reliability of information by protecting it from unauthorized modification, manipulation, or destruction.
- Confidentiality: Ensuring that information can only be viewed or used by authorized persons or entities and is protected from unauthorized access.
- Authenticity: Verification of the identity of users, systems, or data; verification of the authenticity of sources to ensure that they are genuine and trustworthy.
- Non-repudiation: Ensuring that an action or transaction cannot be denied or disputed after it has taken place by logging all relevant activities and making them verifiable.
- Attributability: Ability to attribute actions, events, or transactions to a specific person or entity in order to ensure accountability.
- Data protection: Protection of personal data against unauthorized processing, disclosure, or misuse in accordance with applicable data protection laws and guidelines.
- Compliance: Adherence to legal, regulatory, and contractual requirements relating to information security, as well as internal guidelines and standards.
- Resilience: Ability of systems to defend themselves against threats, attacks, natural disasters, or other disruptions and maintain their functionality.
- Risk minimization: Identification, assessment, and reduction of security risks through appropriate security measures and controls to minimize potential damage or loss.

General Information

Classification

The information security policy is a high-level document describing our general approach to information security. Processes, procedures, and measures are described in other documents, which together form the information security management system.

Risks of Non-Compliance

Failure to comply with guidelines may result in damage to IKARUS. Depending on the nature of the violation, the employees concerned may be held accountable both disciplinarily and legally.

Contact Point

The Chief Information Security Officer (ciso@ikarus.at) is available to answer questions and provide support regarding information security.