Information security guideline

Content

The importance of information security and the significance of information technology at evasys GmbH

evasys GmbH offers its customers software solutions and accompanying services in the areas of consulting, training and hosting with a focus on use in surveys, audits and quality management. Our customers include many public institutions for whom information security is a particular concern in addition to their basic corporate responsibility due to their public role model function. In addition to our corporate responsibility to protect the information assets of our customers, service providers, suppliers, partners and our own company, this customer requirement is not only important to evasys GmbH, but we expressly support it. Both evasys GmbH and its interested parties therefore consider information security to be a primary objective. Consequently, a decisive factor for business reputation, risk minimization and conformity with legal requirements is ensuring an appropriately high level of security for the information in need of protection and the processes and systems that support it.

Due to our software solutions, the information assets to be protected include, in particular, our customers' data, which is collected in our software and stored and processed via the infrastructure provided. The primary assets to be protected are therefore the protection of the software developed and provided by us and the hosting of the systems used by our customers.

In order to achieve an appropriately high level of security, a primary goal is secure information technology that guarantees high availability and the technological protection of digital systems and data. This goal of high availability as well as the confidentiality and integrity of IT systems and data plays a leading role in the implementation of the security strategy applied at evasys GmbH and therefore receives special attention and depth of regulation.

Other security objectives of information security extend beyond information technology and include

- personal and physical safety,
- the handling of security incidents,
- business continuity management and
- compliance with specifications.

To implement the security objectives and to ensure and maintain the required level of security, evasys GmbH operates and continuously develops an information security management system (ISMS). This ISMS of evasys GmbH is based on the principles of the international standard ISO/IEC 27001 and the recommended measures of the associated series of standards. This reflects the high standards of evasys GmbH with regard to the implementation of information security measures and is guaranteed by an annual external audit.

Effective implementation of information security is of central importance to evasys GmbH and is promoted by a corporate culture in which the importance of information security is understood and implemented in all areas and at all hierarchical levels. All employees are actively involved in securing information in their respective areas of responsibility. Employees are continuously sensitized and trained to create an awareness of security risks and sensitize

them to the importance of secure handling of information. This commitment and awareness enables us to guarantee the confidentiality, availability and integrity of information in the long term.

This guideline forms the foundation for all activities and measures in the area of information security at evasys GmbH. It binds all employees, including managers and staff, and is therefore binding for the entire company. In order to achieve the information security objectives, a security organization has been introduced and an information security officer has been appointed.

As part of the mandate of this information security guideline, the security organization of evasys GmbH has established processes for controlling, monitoring and improving information security and, as a result, has issued risk-oriented security instructions. The security organization continuously monitors and improves their implementation and effectiveness. The Information Security Officer reports directly to the management level. Enforcement is periodically reviewed by the management and violations are pursued and sanctioned.

Scope of Application

The information security guideline applies to evasys GmbH and evasys labs Kft.

Objectives and principles of information security at evasys GmbH

The objectives and principles are set out below as a framework for the further development of the regulations at evasys GmbH. The focus here is on ensuring the confidentiality, integrity and availability of information. In addition, the fundamental principles in the context of information security are defined, including compliance with regulations, segregation of duties, ownership, minimization of rights and services, traceability, responsiveness and appropriate documentation.

Goals of information security

Information security refers to the protection of information with the aim of maintaining business operations and minimizing business risks. As described at the beginning, the establishment and maintenance of our ISMS is aimed at safeguarding the confidentiality, integrity and availability of information. We therefore define the following objectives for the information security management system:

Confidentiality: The confidentiality of evasys GmbH information must be maintained by ensuring that sensitive data is protected from access or disclosure by unauthorized persons.

Integrity: The integrity of evasys GmbH's information must be ensured so that it is always correct and complete and thus meets the requirements and expectations of employees,

customers and cooperation partners.

Availability: The information of evasys GmbH should be accessible and usable at all times and reliably for authorized persons in order to carry out business processes smoothly and efficiently.

Other properties such as authenticity, accountability, non-repudiation and reliability, which could be mentioned in ISO/IEC 27001, are largely covered by maintaining confidentiality, integrity and availability and are therefore not defined separately in this guideline.

Principles in the context of information security

The following principles are to be adhered to appropriately, taking into account technical, economic or administrative framework conditions.

Compliance with legal, external, contractual and internal regulations: Information security regulations must be identified and implemented through appropriate measures.

Separation of functions: Critical functions in business processes that may not be performed by the same person or organizational unit must be separated. This is done by separating functions and responsibilities organizationally and supporting this separation technically as far as possible and reasonable.

Ownership: Information, assets and IT systems and applications are assigned to owners. They are responsible for controlling the creation, development, use, maintenance and security of their organizational assets.

Minimum rights: Access and access to information, systems and applications is restricted to the necessary group of people. Authorizations are to be developed on a risk basis. Each user is only granted access authorization for the information required to perform the tasks assigned to him or her.

Minimum services: The users (persons, technical users or other IT systems) of resources are only provided with the services that they actually need. When using information technology, this means that only the functionality that is actually required is available.

Traceability and verifiability: All activities and events relevant to information security should be traceable to the required extent. Records of information security-relevant events must not be untraceably alterable.

Reaction: When information security incidents occur, they must be reported to the risk management board, which must then react. By recognizing threats in good time and reacting appropriately, a negative impact on information security in the business processes can be prevented or reduced to an acceptable level while taking risk aspects into account.

Appropriate documentation: The level of detail in the documentation must always be such that an expert third party who is not involved in the company can understand the planned activities within a reasonable period of time.

Organization of the ISMS

Responsibility for information security

Overall, the management is responsible for the appropriate implementation of information security in the company and supports the planned allocation of the necessary technical, financial and human resources for information security. Information security is firmly integrated into the structures, hierarchies and work processes of evasys GmbH. An information security officer has been appointed. The information security officer reports directly to the management.

The information security officer and the IT administrators are provided with sufficient financial and time resources by the management in order to receive regular training and information and to achieve the defined information security objectives.

Owner of information, processes and IT systems / applications

Risk assessments are used to determine the protection requirements for key information assets in the business processes. The owner makes decisions about access rights to its information, taking into account technical restrictions and administrative aspects as well as the development and implementation of cost-effective solutions.

Implementation of the ISMS

Legal, contractual, organizational, technical, personnel and infrastructural risks to information security are identified on the basis of a comprehensible risk assessment in order to prevent the occurrence of a risk and the resulting damage.

Information security is achieved by implementing suitable measures. Measures can be: documented decisions in the form of guidelines, directives and instructions or processes, procedures, organizational structures and technical software and hardware functions.

The Measures must be introduced, implemented, monitored, checked for effectiveness and, if necessary, improved in an appropriate and risk-oriented manner. This is to ensure that the specific security objectives of evasys GmbH are met. The implementation and effectiveness checks must be documented appropriately.

Violations: Violations of information security regulations must be reported to the respective line manager or the risk management board. Conduct that jeopardizes the security of information or IT systems and applications may be subject to disciplinary action or penalties under employment law.

In order to limit or prevent damage, security incidents must be responded to quickly and consistently. The aim is to maintain critical business processes and restore the availability of information and failed systems within a defined, tolerable period of time. Emergency measures are defined as part of the emergency and crisis management regulations.

Training, further education and awareness-raising measures The information security measures for handling information and processing information technology are indispensable for achieving the objectives of information security and preventively safeguarding business operations. All employees must be regularly and appropriately sensitized to the risks involved in handling information and processing information technology. To this end, evasys GmbH provides training programs tailored to the target group. The evasys GmbH ISMS team facilitates participation in training measures and ensures this.

Effectiveness test of the ISMS

The ISMS is regularly - but at least annually - reviewed for appropriateness, up-to-dateness and effectiveness and evaluated by the management. The management levels support the constant maintenance of the security level. Employees are encouraged to report possible improvements or weaknesses to their line manager or the risk management board.

The required and targeted security level is ensured by continuously checking that the ISMS regulations are up-to-date and appropriate and that they are complied with. Deviations are analyzed with the aim of improving the security situation and keeping it constantly up to date.

Duty to cooperate

Managers and employees

All managers and employees of evasys GmbH ensure information security through their responsible actions and comply with the laws, regulations, guidelines, rules, instructions and contractual obligations relevant to information security.

Every manager is responsible for ensuring that the employees in their area of responsibility implement information security in accordance with the applicable regulations.

Employees are obliged to implement the information security measures in their area of responsibility and to comply with the rules. They are supported in this by recurring awareness-raising courses and training sessions.

The management supports continuous improvements in the level of security and encourages all employees and users of the IT infrastructure to report potential areas for improvement or weaknesses to the relevant departments.

Suppliers and service providers

evasys GmbH must define risk-oriented security requirements for suppliers or service providers who provide services for evasys GmbH.

Implementation of the guideline

evasys GmbH implements the information security requirements based on this guideline. Furthermore, the guideline is regularly reviewed for appropriateness and adapted if necessary.

Come into effect

The management has implemented and published this information security guideline as part of the corporate policy.