Guideline for the

Guarantee of Information Security

of

medavis GmbH

Bannwaldallee 60

76185 Karlsruhe
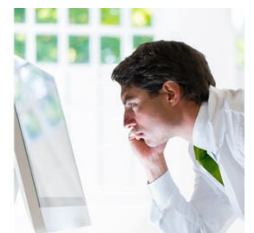
Germany

V1.0

Content

The Importance of Information Security

The automated processing of data and information plays a key role in the fulfilment of our company's tasks. All essential processes are significantly supported by information and communication technology (IuK technology).

Due to the increased dependence on modern information and communication technology, the risk of impairment of information infrastructures and their components (IT infrastructure) through deliberate attacks from inside and outside, negligent actions, ignorance or potential failure of the technology has increased significantly, both qualitatively and quantitatively.

A lack of information security can lead to disruptions in the performance of tasks, as well as violate the legitimate interests of the persons concerned.

Against this background, an appropriate level of information security in business processes must be organized.

This guideline does not regulate any technical details; these are dealt with separately.

Achieving Information Security

Information Security refers to a state in which the risks to the security objectives of confidentiality, integrity and availability of information and information technology are reduced to an acceptable level through appropriate measures. In addition to the security of IT systems and the data stored in them, information security also includes the security of data and information that is not electronically processed and stored.

Meaning of the terms:

− **Confidentiality**: Confidential data, information and programs must be protected against unauthorized access and unauthorized disclosure. The objects of protection include the stored or transported message contents, detailed information about the communication process (who, when, how long, with whom, etc.) and data about the sending and receiving process.

− **Integrity**: The term integrity refers to information, data, and the entire IT system. Integrity of information means its completeness and correctness. Completeness means that all parts of the information are available. Information is correct if it reflects the described facts without distortion. On the other hand, the term integrity also refers to IT systems since the integrity of information and data can only be ensured if they are processed and transmitted properly.

− **Availability**: The functions of the hardware and software in the system and network area as well as necessary information are available to the user at the right time and the right place.

In order to achieve these goals, medavis GmbH has installed an Information Security Management System in accordance with ISO 27001. medavis management and employees undertake to comply with the rules, procedures, requirements, and specifications established within this framework and to continuously improve the information security management system.

The security measures must be in an economically justifiable relation to the potential damage that can be caused by security incidents. For this purpose, information security risks are assessed

according to the damage at occurrence and probability and security measures are defined if necessary.

For the implementation of the necessary and appropriate security measures, the necessary resources (personnel, material, and investment means) are provided.

Scope of Application

The guideline always applies when IT systems are planned, introduced, or operated. The guideline applies throughout the company.

The guideline and the resulting regulations and measures must be regarded and complied with by all employees.

This guideline has been issued and approved by the medavis management.

Karlsruhe, 29.01.2020

Geschäftsführung medavis GmbH: Jörg Dittrich   Elmar Kußmaul