



# ISMS Policy (Information Security Management System)

## Management Statement

The management of BMT Medical Technology s.r.o. (hereinafter referred to as BMT) declares the principles of information security. This policy is binding for all employees of the company to whom the information security management system applies and cooperating organizations.

The intention of BMT management is to maintain adequate protection of information assets in accordance with the laws and other legal regulations of the Czech Republic and the EU, even in cases where responsibility for information processing has been transferred to cooperating organizations.

## Information Security Objectives

Our goal is to ensure the confidentiality, integrity and availability of all our own and customer data to ensure the smooth running of our business activities and to ensure the operation of critical information infrastructure. To enforce this policy, the company has implemented and developed an information security management system according to ISO/IEC 27001.

### We commit to:

- comply with and fulfill legislative regulations in the field of information security and cybersecurity,
- ensure the availability of information at the time and place according to the needs of the company, but only to those who need it for their work activities, thereby maintaining the confidentiality of information according to the specified categories - public, internal, confidential, personal,
- manage the integrity and lifecycle of information from the moment of its creation, transmission, use to disposal,
- educate and develop our employees, suppliers and partners in the field of information security and cybersecurity,
- violation of information and cyber security rules is considered a gross violation of internal regulations and contractual relations.

### In relation to suppliers, we undertake to:

- ensure the protection of the organization's assets to which suppliers have access,
- agree with suppliers and properly document information security requirements to reduce risks associated with suppliers access to the organization's assets,
- establish and agree on relevant information security requirements with each supplier who may access, process, store or provide elements of the organization's information or critical information infrastructure,
- include in agreements with suppliers requirements for information security and cybersecurity risks associated with the supply chain of information and communication technology services and products,
- maintain the agreed level of information security and service delivery in accordance with supplier agreements.

### Furthermore:

- the company regularly monitors and reviews the delivery of services by suppliers,
- changes in the provision of services by suppliers, including changes in the maintenance and improvement of existing policies, procedures and information security measures, are managed with regard to the criticality of the information, systems and processes of the organization that are part of these changes, and with regard to repeated risk assessments.

## Commitment to meet applicable requirements

With this policy, we declare to all business partners, employees and owners, public and state administration and the general public the ability of the entire company to effectively protect information, elements of critical infrastructure, tangible and intangible assets owned and entrusted to us in accordance with legislative requirements with the valid legislation of the Czech Republic and the European Union, international treaties and other requirements for the protection of information security.

## Commitment to continuous improvement

### We commit to:

- determining the security measures taken based on the principle of assessing the severity of the assessed risks, their impacts and the economic cost of the measures,
- increasing the effectiveness of our information security management system through regular monitoring, risk reassessment, and management of security events and incidents through corrective and preventive measures