

# INFORMATION SECURITY POLICY



Customers and contracting partners of AXIOM PROVIS Int. (hereinafter referred to as "Company") fully trust that the confidentiality and security of their data are maintained in all areas.

Company management knows what a crucial role data plays in today's world of business and in both professional and private life. It is precisely for this reason that it continues to build and develop an information security management system in order for the company to protect its data assets and provide their customers and partners with an appropriate level of security.

To meet these expectations, the company **undertakes to implement the requests and to continue to develop the information security management system**. Furthermore, it sets forth the following policy as the framework for the company's stance on information security. This policy is an integral part of overall company management.

## Security Policy Goals

First and foremost, our goal is to ensure the confidentiality, integrity and availability of all our own data, as well as our customers' data in order to provide problem-free support for our business activities. Through this policy, we hereby declare to all business partners, employees, public and state administrators as well as the general public that our company is capable of **efficiently protecting information, tangible and intangible assets** that are ours as well as those entrusted to us under legislation valid in the Czech Republic and in the European Union, through international contracts and through other requests for the protection of information security.

## Information Security Standards and Principles

- ▲ To create and continue to improve the organizational structure, technical resources and other measures in order to create, implement and increase the efficiency of the information security management system in the company.
- ▲ To provide the availability of information at a time and place based on the needs of the company and its customers and to manage the integrity of this information for the duration of its entire life cycle.
- ▲ To educate its employees to ensure that they are fully informed and up-to-date regarding internal, legal and regulatory requirements in terms of information security.

- ▲ To maintain legislative, contractual and normative requirements for information security. To always ensure that security and compatibility are an integral part of all delivered and created company information products.
- ▲ To continue to evaluate access to asset management and to assess information risks, to establish an acceptable level for these risks and to apply adequate measures to provide the required level of information security.
- ▲ To continuously identify security incidents and to implement effective measures to continue to improve information security.
- ▲ To increase system efficiency for information security management through regular monitoring and reassessments.
- ▲ To prevent misuse and/or loss of information through the definition of responsibilities and the control of access to information and to areas, where information assets are found.
- ▲ To set up company processes to deal with security events and incidents, to eliminate outages and to provide resilient information systems while supporting the continuity of business activities.

Company management supports the information security management system and declares that it shall create appropriate conditions (material, human resources, organizational) to enable the implementation, maintenance and continuous improvement of the information security management system so that the goals and principles set forth in this policy are attained.

The information security management system policy and the related documents are binding for all employees with access to information regardless of their job title, position or role in the company.

In Zlín, January 1, 2019

  
**Petr Franěk**

výkonný ředitel  
AXIOM PROVIS Int.

