okto —
digital

okto—digital security policy

okto-digital s.r.o. is aware of the importance of the information systems it operates, the significance of the data processed in them, the value of the assets and technologies it uses for its activities and the obligation to protect the legitimate interests of its customers and all persons with whom it comes into contact.

For this reason, the Company has decided to implement and maintain an information security management system in accordance with the requirements of ISO/IEC 27001:2022. The Company has adopted and is committed to promoting and achieving the following strategic objectives and principles:

1. To manage information security in accordance with the requirements of ISO/IEC 27001, ISO/IEC 27002 and applicable Slovak and EU legislation.
2. To adopt and implement a Security Policy, the aim of which is to create the prerequisites for ensuring an adequate level of information security in all activities and functions of the company.
3. Protect the rights and interests of owners, customers, employees and business partners by implementing effective and efficient security mechanisms and measures.
4. Raise the security awareness of employees and systematically guide and motivate them to improve and comply with security principles at work.
5. Ensure the confidentiality, availability and integrity of personal data, trade secrets and other sensitive information assets of the Company, its customers and business partners in their processing.
6. Ensure the security, reliability and quality of the IS in operation by using modern information technologies and their gradual improvement and streamlining.
7. To create conditions for the safe location of individual IS components, depending on their importance, and to ensure their physical protection and protection against environmental influences.
8. Protect the company's reputation and ensure high ethical standards and quality of the services provided.
9. To ensure the reporting and resolution of security incidents with an emphasis on preventing their recurrence.
10. To improve the information security management system, to continuously improve its efficiency and integrity in line with new service delivery requirements and to create organisational conditions for ensuring IS security.

The security policy is company-wide. Compliance with the security policy is monitored by internal audits. Failure to comply with the rules and principles set out in the security policy and the security measures taken is considered a breach of work discipline.

Approved by Štefan Gembický, 29. 02. 2024