

INFORMATION SECURITY POLICY


The nature of ExaByte d.o.o. business requires the exchange of information both internally and externally with customers, partners, and other business stakeholders. To maintain business continuity, the company takes measures to protect information assets from internal and external, intentional, or accidental threats to confidentiality, integrity, and availability of information. Bearing this in mind, the company management formulates the principles of Information Security Policy as well as framework for information security objectives:

- Ensure the confidentiality of information and protect it from unauthorised access and misuse,
- Maintain the integrity of information to ensure its lasting accuracy and applicability,
- Make information and information systems available to interested parties in accordance with business needs,
- Build relationships and maintain communication with interested parties by understanding their context and needs and expectations of interested parties,
- Regularly carry out the identification, analysis, and assessment of information security risks,
- Plan and take actions based on the results of the regular information security risk assessment,
- Ensure information security awareness, education, and training for employees and other interested parties,
- Apply information security measures to ensure compliance with legal, regulatory, and contractual requirements, as well as other information security requirements,
- Ensure appropriate controls and continuous improvement by planning and achieving measurable objectives and monitoring the performance of the system and applied information security measures,
- Investigate and analyse security incidents and take appropriate actions to address the causes,
- Investigate and analyse security vulnerabilities and threats and take appropriate actions to address the causes of threats and reduce risks,
- Develop, maintain, and test recovery plans in order to prevent potential consequences of security incidents and to preserve business continuity if the incident occurs.

In order to meet these obligations and ensure the appropriate level of controls necessary to demonstrate compliance with the adopted processes, our policy is to maintain a functional and effective information security management system that is established, maintained, and improved in accordance with the requirements of the international ISO/IEC 27001:2022 standard.

The CEO is responsible for communicating and making available the Information Security Policy to all employees and other interested parties.

Varaždin, 27.05.2024.



Bernard Toplak, CEO