



Information security policy

The nature of the business of Perpetuum Mobile d.o.o. requires the exchange of information both internally and with external customers, partners, and other business stakeholders. To maintain the continuity of our operations, it is important to take measures to protect information assets from all internal and external, intentional or accidental threats to the confidentiality, integrity, and availability of information. With this in mind, the management of Perpetuum Mobile d.o.o. formulates the principles of the information security policy:


- Ensure the confidentiality of information and protect it from unauthorized access and misuse,
- Maintain the integrity of information to ensure its lasting accuracy and applicability,
- Make information and information systems available to stakeholders in accordance with business needs,
- Build relationships and maintain communication with business stakeholders with an understanding of our own context and the needs and expectations of stakeholders,
- Regularly carry out identification, analysis, and assessment of information security risks at planned intervals
- Base decisions and actions on the results of regular information security risk assessments,
- Through education and training, ensure employee awareness and capability for information security,
- Ensure compliance with legal, regulatory, and contractual requirements, as well as other information security requirements we have committed to, through applied information security measures,
- With measurable objectives and monitoring the effectiveness of the system and applied information security measures, ensure adequate control and continuous improvement,
- Timely report threats to information security to the persons responsible for managing information security,
- Monitor and analyze security vulnerabilities and threats and initiate appropriate actions to address causes and reduce risks,
- Monitor and analyze security incidents and initiate appropriate actions to eliminate causes of threats and reduce risks,
- Develop, maintain, and test plans for recovery from the consequences of security incidents and for business continuity.

In order to fulfill these obligations and ensure an adequate level of control necessary to demonstrate compliance with 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 standard ISO 27001:2022.

The Chief Executive Officer of Perpetuum Mobile d.o.o. is responsible for communicating the Information Security Policy to all persons working for or on behalf of Perpetuum Mobile d.o.o. and for making it available to relevant interested parties.

In Zagreb, 10.06.2025.



Blerim Sela, Chief Executive Officer