

IMPROVIT has adopted the *Information Security Policy* and is committed to the effective implementation and provision of resources for the improvement of the Information Security Management System (ISMS).

- The Information Security Policy aims to ensure:
 - Continuous protection of information against unauthorized access.
 - Continuously ensuring the confidentiality of IMPROVIT's information, clients and partners.
 - Continuously maintaining the integrity of IMPROVIT's information, clients and partners.
 - Continuous assurance of the availability of information and business transactions.
 - Monitoring and compliance with the legislative, regulatory and contractual requirements concerning IMPROVIT.
 - The *Business Continuity Plan* is maintained and tested for its effectiveness.
 - Adequate training of the IMPROVIT employees in information security issues.
 - Confirmed or suspected information security breaches are reported to the Information Security Officer and System Manager and are thoroughly investigated and dealt with in time and effectively.
- Appropriate procedures and individual security policies are in place to support the policy, including technical and organizational measures of protection.
- Compliance with the legislation and requirements of ISO 27001:2022 is ensured and with the ongoing monitoring of the implementation of the ISMS.
- The Systems Manager is responsible for maintaining the Information Security Policy and for providing support and advice in its implementation.
- IMPROVIT's top management is responsible for the implementation of the *Information Security Policy* as well as for ensuring the compliance of the supervised personnel.
- Compliance with the *Information Security Policy* is mandatory for all parties that have been or are cooperating with IMPROVIT.

Any violations of the *Information Security Policy* are subject to disciplinary actions. The decision depends on the nature and impact of the violation.

For IMPROVIT

07/11/2022

Version: 1.0