

INFORMATION SECURITY MANAGEMENT POLICY

Management and employees of UAB „WESTOIL“ follow the requirements of the ISO 27001 standard in their daily activities, implementing which they strive to avoid incidents that could harm the organization's reputation and are committed to:

- Ensure the protection of the organization's information and information technology.
- Ensure information security in accordance with operational requirements and relevant laws.
- Achieve and maintain adequate protection of the organization's assets.
- Prevent unauthorized physical and remote access, loss and interference with the organization's activities and information contained in information systems.
- Ensure that information security incident management is consistent and effective.
- Prevent loss, damage, theft or defects of assets and interruptions to the organization's activities.
- Ensure the accurate and secure operation of information processing facilities.
- Maintain the integrity and readiness of information and information processing facilities.
- Ensure that security is an integral part of information systems.
- Maintain an information security management system that ensures compliance with the requirements of LST ISO/IEC 27001:2022.
- Ensure compliance of the system with the organization's security policies and standards.
- Conduct periodic risk assessments to determine the need for further action.
- Strive for continuous improvement in information security management.

To achieve these goals, UAB “WESTOIL” has implemented an integrated management system that meets the requirements of ISO standards. UAB “WESTOIL” Information Security Management Policy is reviewed annually and, if necessary, updated to remain relevant. This policy is available to interested parties, and employees are familiar with it and must follow it in their activities.

CEO

Jurij Miruta

31.12.2024