



MAIN PRINCIPLES OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

We continuously develop and improve the established Information Security Management System (ISMS).



We handle information with due care and protect it accordingly.



We report and communicate information security vulnerabilities.



We educate ourselves on information security and promote awareness among employees and all external stakeholders.



Ljubljana, September 2026

INFORMATION SECURITY POLICY

At Kolektor Etra, we recognize information as a critical business asset. Accordingly, we have established an Information Security Management System (ISMS) to ensure the confidentiality, integrity, and availability of information. The ISMS is fully integrated into the company's overarching management framework.

CORE OBJECTIVES

- Protect information against unauthorized access, disclosure, alteration, or loss.
- Ensure compliance with applicable laws, regulations, contractual obligations, and the requirements of customers and other relevant stakeholders in the areas of information security and personal data protection.
- Promote information security awareness and provide appropriate training.
- Identify, assess, and mitigate information security risks.
- Ensure information security when working with external contractors and manage risks across the entire supply chain.
- Reduce the likelihood of security incidents through appropriate preventive measures.
- Ensure business continuity and incident recovery.
- Minimize business impact through effective detection of security incidents and mitigation of their consequences.

RESPONSIBILITY OF MANAGEMENT

To ensure effective information security management, as well as the continual improvement of the ISMS, company management ensures:

- establishment, implementation and continual development of the ISMS,
- achievement and monitoring of information security objectives,
- compliance with applicable legal, regulatory, and contractual requirements involving all relevant stakeholders in the areas of information security and personal data protection,
- clearly defined responsibilities and authorisations for tasks within the ISMS,
- the necessary financial, human, and other resources required for the implementation and operation of the ISMS,
- timely communication to employees and other relevant stakeholders regarding information security events.

RESPONSIBILITY OF EMPLOYEES

Each employee is personally responsible for:

- consistently complying with the ISMS Manual and ISMS Policy,
- protecting the company's information and information assets through careful and responsible handling and by preventing unauthorized access, disclosure, alteration, or loss of information,
- using information systems, access rights and authentication means exclusively for authorized business purposes, and safeguarding user accounts, passwords, and other authentication credentials,
- promptly reporting identified information security events, vulnerabilities, and risks,
- participating in information security training and awareness activities.

Information Security Policy is being periodically reviewed and updated when needed.

Peter Novak
director

Dejan Velikanje
director

dr. Tomaž Kmecl
director