INFORMATION SECURITY POLICY

STRATEGY AND GOALS

This policy defines the basic objectives, principles, and scope of Information security management system (ISMS) in RT-RK. ISMS is based on ISO 27001 standard and encompasses. all procedures, instructions, and controls, aiming to protect confidentiality, integrity, and availability of information assets used in the company, including outsourced or entrusted assets from external entities.
Main ISMS objectives are:

- To protect all information assets of RT-RK, its partners or clients, against any security threats - internal or external, intentional, or accidental.
- To minimize business losses by preventing or reducing the risks.
- To ensure business continuity.
- To provide a framework reviewing ISMS in order to improve information security.

BASIC PRINCIPLES AND SCOPE

The basic principles of the information security policy are:

- Commitment of the management through delegating powers regarding information security and raising employees' awareness of their roles and responsibilities related to information security.
- Enforcement of ISMS through efficient application of appropriate procedures, instructions, and specifically designed control measures.
- Information and other information assets are protected in a way that is adequate to security risk.
- Protection of the interests of internal and external users, clients, business partners, and other interested parties, including their personal data.

The scope of application includes all the activities related to the management of information security:

- Application to all business processes and information assets of RT-RK .
- Maintaining Registry of information assets and classification of information confidentiality.
- Identification, analysis and assessment of risk regarding information security, as a prerequisite for risk mitigation plans.
- Providing compliance with statutory, regulatory, and contractual requirements.
- Application of security controls during project management and development or modification of IT products and services.
- Providing security and continuity of IT resources outsourced from suppliers and recovery of information and system in case of catastrophic events.
- Managing information security incidents.
- Regular information security trainings for employees and regular audit and evaluation of the ISMS.

AWARENESS AND RESPONSIBILITIES

CISO is responsible for implementation, monitoring, and constant improvement of information security. All managers and process owners are responsible for the application of information security policy and control measures in their business processes and for monitoring its application by employees.
All employees are responsible for preserving security - confidentiality, integrity, and availability of information during its collecting, processing, storing or transfer. Employees and subcontractors must apply control measures to minimize risks to information security. Information security policy and other ISMS documents are available on the Intranet website to all users responsible for its application.

19.01.2024.

GENERAL MANAGER