Telekom Srbija

Excerpt from the Policy of the Information Security and Privacy Management System

The policy of the Information Security and Privacy Management System (hereinafter: ISMS and PIMS) established in accordance with the requirements of the current version of the ISO 27001 and ISO 27701 standards defines the basic principles for Telekom Srbija to:

- ensure confidentiality, integrity and availability of information,
- prevent the violation of personal data, the occurrence of security incidents and minimize their impact on business operations,
- establish general guidelines and principles related to information security and privacy,
- provide a framework for establishing ISMS and PIMS objectives.

The ISMS and PIMS Policy applies to all business processes within the scope of the established ISMS and PIMS, which relate to information or its processing.

Basic policy principles:

- ISMS and PIMS are an integral part of the Integrated Management System established by Telekom Srbija, which is regularly harmonized with the requirements of the current version of ISO 27001, ISO 27701 and other standards implemented by Telekom Srbija. The established system is continuously improved and supported by the necessary resources required to comply with the principles described in this policy.
- Telekom Srbija is committed to implementing and maintaining compliance with ISO standards related to information security and privacy regulations.
- ISMS and PIMS are implemented and maintained in compliance with the following principles:
  - the focus is on protecting information, especially personal data from destruction, loss, alteration, or unauthorized disclosure and access,
  - the approach to managing information security and privacy is based on risk management,
  - the expectations of users and other stakeholders are considered,
  - information security and privacy protection are present in all stages of the life cycle of information, products, and services,
  - information security and privacy requirements are an integral part of regulations, business processes and contractual obligations,
  - ISMS and PIMS regulations are documented, regularly updated and available to stakeholders responsible for their implementation,
  - organizational and technical protection measures are established considering the assessed risks, the level of technological development and the costs of implementation in order to ensure that they are adequate, appropriate and effective.
- The management of Telekom Srbija conducts on a precautionary and regular basis the assessment of risks to information security and privacy arising in the course of Telekom Srbija's operations. As part of risk management, informed decisions are made on accepting, reducing, avoiding, and transferring risks.
- ISMS and PIMS (implemented measures and established processes) are regularly checked and reviewed.

- Changes affecting the context of the established ISMS and PIMS are monitored and analysed. Based on these analyses and, if necessary, risk assessments, the appropriate measures are defined to improve the system.
- ISMS and PIMS are improved, taking into account the requirements of laws, standards, changes in technology, as well as new threats and vulnerabilities.
- Activities to improve awareness of information security and privacy are regularly carried out among employees, users, and stakeholders.