Telko Yazılım

INFORMATION SECURITY POLICY

The management of TELKO YAZILIM BİLİŞİM TELEKOM HİZMETLERİ TİCARET LİMİTED ŞİRKETİ (the "Company") recognizes the importance and need to develop and improve information security measures and tools in the context of evolving international laws and regulations on information and personal data protection, as well as in the context of customer expectations. Complying with information security requirements, as well as ensuring confidentiality of customers' personal data will create a competitive advantage for the Company, ensure its stability, compliance with legal, regulatory and contractual requirements, and enhance its image. To effectively implement information security and personal data protection processes, the Company has implemented an information security management system (hereinafter - ISMS) in accordance with the requirements of international standards ISO/IEC 27001:2013 and ISO/IEC 27701:2019.

1. GOALS AND OBJECTIVES

The purpose of information security is to maintain the stable functioning of the Company, protect the processes and assets belonging to the Company and its customers.

The goals of the Company in the field of information security:

- sustainable operation and development of the Company, ensuring continuity of services to customers
- maintaining the Company's status as a reliable solution provider for telecom operators and service providers in the eyes of potential customers, increasing its investment appeal;
- guaranteeing the security of processes and assets owned by the Company and its customers;
- compliance with legal and other regulatory requirements in the sphere of information security and personal data protection in all jurisdictions where the Company has a presence.

Tasks to be undertaken to achieve information security goals:

- ensuring compliance with international information and personal data protection laws, including the requirements of the European Union's General Data Protection Regulation (GDPR), as well as national information security standards and regulations;
- information security risks management;
- Application of various organizational and technical measures to ensure information security, use of advanced technologies to counter information security threats;
- Involvement of the Company's employees in the IS processes, increasing the level of responsibility, awareness, continuous training and obtaining feedback;
- Ensuring business continuity based on a set of organisational, methodological and technical measures aimed at minimising the consequences of the loss of information assets and uninterrupted provision of services to Clients;
- Regular assessment of ISMS with applicable internal and external requirements through internal audits, monitoring of ISMS processes efficiency, analysis by the Company's management;
- introduction of corrective actions in case of detection of deviations or inconsistencies in the work of the ISMS with internal and external requirements.

2. PRINCIPLES OF INFORMATION SECURITY MANAGEMENT

The Company's information security management is guided by the following basic principles.

- **Legality.** Protection of the Company's assets complies with the provisions and requirements of international and national laws and other regulations in force.
- **Systematicity.** A systematic approach to information security requirements means that all interrelated, interacting and changing over time elements, conditions and factors, which are essential for understanding and solving the information and personal data protection tasks, are taken into account.
- **Complexity.** Information security is ensured by an effective combination of organizational, methodological measures and software and hardware tools. Application of various means and technologies for protection of processes and assets reduces the probability of implementation of the most significant threats to information security.
- **Continuity of improvement.** Asset protection measures and tools are continuously improved in accordance with the results of information security management system performance analysis, taking into account the emergence of new methods and means of information security threats, and also taking into account the information security experience of other organizations.
- **Reasonable sufficiency and adequacy.** Software and hardware tools and organizational measures aimed at protecting assets are designed and implemented on the basis of regular risk assessment in such a way as not to result in a significant deterioration of the main functional characteristics and performance of the Company's information systems.
- **Personal responsibility.** Responsibility for asset security is assigned to each employee within the limits of his or her authority.
- **Control.** Assessment of information security system efficiency is an integral part of information security assurance work. In order to timely identify and suppress attempts to violate the established rules of asset security, the Company defined procedures for continuous control over the use of asset processing and protection systems, and the results of control are analyzed on a regular basis.

The Company's management sets a personal example of leadership and commitment regarding ISMS and promotes the involvement and active participation of the Company's personnel in information security processes.

The Company management assumes responsibility for compliance of the information security policy provisions with the stakeholders' requirements, communicating and explaining them to the Company employees and stakeholders, assigning responsibility for appropriate tasks to achieve these goals at all levels, as well as for their implementation, periodic review and revision.

The provisions of this Information Security Policy are binding on employees of all structural units of the Company, as well as employees of contractors, if it is provided by the contract.

Last update: August 23rd, 2022