



MAGYAR TELEKOM'S INFORMATION SECURITY POLICY

Magyar Telekom Group, as a market leading IT and telecommunications service provider and system integrator, takes complex efforts to ensure the Group's security and operates an information security management system based on international standards to maintain its leading position.

Scope of application:

The scope of the ISO 27001 compliant Information Security Management System of Magyar Telekom Group and Magyar Telekom Plc.

- is defined based on information security impacts identified in the external and internal environment of the organization,
- the information security requirements of Stakeholders, and
- the relationship between the above listed services and stakeholder activities.

Accordingly, Magyar Telekom Plc's information security management system, in compliance with ISO 27001 standard, covers the protection of the confidentiality and integrity of customer and confidential information as well as the maintenance of the availability of the information and the information management systems at a level that allows the operation of processes and the provision of services in an economical manner.

Basic objectives:

Our objective is to consciously manage human, technological, natural, and national security risks that threaten Magyar Telekom Group's activities and to preserve the value and business value of the Group's tangible, intellectual and information assets.

We are committed to achieving our goals, therefore:

- Lawfulness is the basis of all our activities. We, the employees of Magyar Telekom, fulfil our legal obligations to guarantee security.
- Fair conduct is a basic pillar of our corporate culture. Our senior managers set an example for the employees in complying with ethical principles. We act against bad faith activities and fraud.
- We prevent unauthorized access to and misuse of personal data of our customers and employees.
- We earn our customers' trust with reliable products and services.
- As a proactive approach, we regularly assess and manage the security risks that arise in our day-to-day business and make conscious decisions to prevent or reduce their impact.
- Our security measures are designed to ensure that they are sustainable, cost effective and leverage the available synergies.
- We respect the rights of individuals affected by security measures, freedom of expression and the media. Security measures restricting these rights may only be taken within the applicable legal boundaries, while respecting the principle of proportionality.
- We protect our financial assets and trade secrets through technical systems, technology, organization, control and awareness procedures and measures to ensure the success of our business.
- Access is always limited to the specific information and data that the recipient is authorized to know and that is strictly necessary for the performance of his or her work. The granting of access rights is immediate, limited and is reviewed regularly.



- We integrate security requirements into our business processes to help the development, marketing and sale of reliable products and services in the long term. In development and other major projects, security is a key factor in all circumstances.
- We monitor international security standards and apply them both in the Information Security Directive and in our internal policies based on the Directive.

We declare that the objectives set out in this security policy will be fully met in the interests of our shareholders, our customers, and the developing info-communications society.

Budapest, 03.21.2024.

Tibor Rékasi
Chief Executive Officer