INFORMATION-QUALITY SECURITY MANAGEMENT SYSTEM POLICY BGYS.PLT.00

As the top management of **KLİNİKYA TEKNOLOJİ ANONİM ŞİRKETİ**;

In **KLİNİKYA TEKNOLOJİ ANONİM ŞİRKETİ** Services**; ISO / IEC 27001: 2017 Information Security Management**

The main theme of the systems established in the **ISMS** standard is to demonstrate that information security management is provided within human, infrastructure, software, hardware, customer information, organizational information, all business and transactions, third party information and financial resources, to ensure quality and risk management, to measure information-quality security management process performance and to regulate relations with third parties on issues related to quality-information security and customer satisfaction.

In this direction, the purpose ***of our ISMS Policy*** is:

❖ To protect **the** information assets of **KLİNİKYA TEKNOLOJİ ANONİM ŞİRKETİ** against all kinds of threats that may occur from inside or outside, knowingly or unknowingly, to ensure accessibility to information as required by business processes, to meet the requirements of legal legislation, to work towards continuous improvement,

❖ To ensure the continuity of the three basic elements of the Information Security Management System in all activities carried out.

Confidentiality: Preventing unauthorized access to sensitive information,

Integrity: Demonstrating that the accuracy and integrity of information is ensured,

Accessibility: Demonstrating that authorized persons can access information when necessary,

Leadership and Commitment: Senior management of our company leads the establishment and implementation of ISMS and provides high level participation in ISMS practices.

❖ To take care of the security of not only the data kept electronically, but also all data in written, printed, verbal and similar media.

❖ To raise awareness by providing Information Security Management trainings to all personnel.

❖ To report to the ISMS Team all vulnerabilities in Information Security that actually exist or raise suspicion and to ensure that they are investigated by the ISMS Team.

❖ Prepare, maintain and test business continuity plans.

❖ To identify existing risks by making periodic assessments on Information Security. As a result of the assessments, to review and follow up action plans.

❖ To prevent any disputes and conflicts of interest that may arise from contracts.

❖ It meets business requirements for information accessibility and information systems.

We are committed.

GENERAL MANAGER