

INFORMATION SECURITY POLICY

BİRTECH INFORMATION TECHNOLOGIES is committed to protecting the confidentiality, integrity, and availability of all physical and electronic information assets across the organization in order to safeguard the institution's competitive strength, profitability, legal compliance, produced and developed assets, and commercial reputation.

To ensure that information—our most valuable asset—is protected accurately, appropriately, and in a timely manner, our organization has adopted and implemented the principles defined in the ISO 27001 Information Security Management Standard.

In order to protect the organization's existence, service continuity, and reputation within the sector, the following principles are implemented:

The confidentiality, integrity, and availability requirements of the company's information assets are determined by considering legal requirements, contractual obligations, corporate strategies, and the needs and expectations of relevant stakeholders, and appropriate protection measures are applied accordingly.

Information assets are used in alignment with management strategies and organizational objectives.

Corporate and customer information is protected through confidentiality agreements established with employees, business partners, customers, and third parties.

Internal and external risks that threaten information security are systematically identified, measured, evaluated, and managed to minimize potential impacts.

Awareness of information security is ensured among all relevant internal and external parties.

Security violations are recorded, reviewed, and corrective actions are taken to prevent recurrence.

Physical and technical security policies and rules are defined and implemented based on risk assessments.

Information security policies are reviewed and updated in accordance with changes in legislation, technology, or stakeholder requirements.

Business continuity plans and exercises are carried out to ensure secure access to critical information in extraordinary situations.

The requirements of the Information Security Management System are effectively implemented across all processes, regularly reviewed, and continuously improved.

Sincerely,

Serap Birekul (G.M.)

