Information Safety Policy

As Egis, our main objective through our Information Security Policy is to ensure the management of information security within people, infrastructure, equipment, customer information, corporate information, third-party information, and financial resources; to secure risk management; to measure the performance of information security management processes; and to regulate relationships with third parties regarding information security. In line with these objectives, our commitments are as follows:

- To manage information assets, identify their security values, requirements, and risks, and to develop and implement controls for identified security risks.
- To define the framework that will determine the methods for identifying the value, security requirements, vulnerabilities, threats, and frequency of threats to information assets.
- To define a framework for assessing the impact of threats on confidentiality, integrity, and availability of assets.
- To establish working principles for the treatment and management of risks.
- To continuously monitor risks within the scope of provided services, considering technological expectations.
- To comply with applicable national or international regulations, legal and legislative requirements, and obligations arising from agreements, and to meet information security requirements arising from corporate responsibilities towards internal and external stakeholders.
- To reduce the impact of information security threats on service continuity and contribute to operational continuity.
- To have the capability to respond quickly to potential information security incidents and implement measures to minimize their impact.
- To maintain and improve information security levels over time through a cost-effective control infrastructure.
- To provide all personnel with awareness, information, and training on the Information Security Management System (ISMS), policies, processes, etc., and to repeat this training at regular intervals.
- To continuously improve the system by considering ISMS practices, audits, and corrective action results.
- To implement the Information Security Management System in an integrated manner alongside other management systems within the organization.
- To carry out activities to understand and comply with the Personal Data Protection Law (KVKK).
- To enhance corporate reputation and protect the organization from negative impacts arising from information security issues.

Ozan KUMRAL
Director of Operation and Maintenance
17.09.2025