This policy covers all units using the institution's Information Technologies infrastructure, users who access information systems as third parties, and service, software or hardware providers who provide technical support to information systems.

Information Security aims to ensure the continuity of Information Systems in order to protect the company's reputation, reliability, information assets, to continue business activities with the least possible interruption, to increase the awareness of employees and their compliance with security requirements, to ensure compliance with third parties and to actively implement up-to-date technical security controls, and our company is managed from a risk perspective.

OUR GOALS;

- To ensure that our Information Security Management System is documented, documented and continuously improved in a way that meets the requirements of the ISO 27001 standard,
- Acting towards the Vision and Mission of the Company
- To reduce the impact of information security risks on business continuity and to ensure business continuity,
- To reduce the impact of climate change and ensure sustainability,
- To protect and improve the company's reputation from negative effects based on information security,
- Ensuring confidentiality, integrity and accessibility of all information stored physically and electronically by ensuring full compliance with legal requirements, customer requirements, operational and contractual terms.
- To increase the awareness of users and employees about information security and to make them aware of their responsibilities in order to minimize Information Security risks,
- To determine and evaluate the security requirements of the electronic infrastructure served, to develop by following technological developments and to ensure service continuity,
- To provide an acceptable level of security for accessing the system from outside the company,
- Defining the information security requirements of third parties, customers and suppliers and ensuring their compliance with the information security management system,
- Protecting the confidentiality of critical data such as strategic goals, design, production, sales, supply sources, customer and employee information regarding our Products and Services,
- To manage our activities in an integrated manner with other management systems we implement, in order to detect situations that violate Information Security in a timely manner and to intervene immediately.