ZORLU

INFORMATION SECURITY POLICY

INFORMATION SECURITY POLICY

Zorlu Holding Information Security Management System (ISMS) has been established to protect the confidentiality, integrity, and availability of information by implementing asset and risk management processes, and to provide assurance to relevant parties that risks are properly managed.

Zorlu Holding operates its information security processes in compliance with TS ISO/IEC 27001:2022, the SPK Information Systems Management Regulation, the CBDDO Information and Communication Security Guide, the Energy Market Regulatory Authority (EPDK) Cyber Maturity Model, and PCI DSS standards. Zorlu Holding commits to utilizing the necessary resources across all group services to ensure the implementation and continuous improvement of the Information Security Management System.

This policy has been prepared by Zorlu Holding Senior Management and approved by the Board of Directors. The Technology and Digital Business Development Group Presidency is primarily responsible for ensuring compliance with the Information Security Policy and related policies.

The main objectives set to systematically manage information security are as follows:

- To ensure the confidentiality, integrity, and availability of corporate information assets and all entrusted information assets from relevant parties within the scope of the Information Security Management System,
- To assess risks related to the confidentiality, integrity, and availability of information and minimize the impact of these risks,
- To comply with all legal regulations related to information security and contracts made with third parties (business partners, customers, suppliers, etc.),
- To comply with all laws, regulations, and notifications applicable to Zorlu Holding,
- To adhere to all policies and procedures published within the management systems maintained by Zorlu Holding,
- To allocate necessary resources and plan training programs to improve employee competencies in order to meet the requirements of the Management System and operate it effectively,
- To prevent interruptions in critical business processes, and if not possible, to restore operations within the targeted recovery time,
- To plan awareness-raising and guiding activities to ensure the participation and compliance of all personnel and business partners with the management systems,
- To conduct regular reviews aimed at continuous improvement of the processes and activities used for the implementation of the Management System,
- To prepare policies and procedures related to mandatory information security controls, review compliance with these policies and procedures, and conduct controls for their development and improvement,
- To ensure that all working methods and principles are compatible and balanced with information security processes.
- Information Security and Cybersecurity risks and threats are continuously monitored, and detected incidents are responded to quickly and effectively, demonstrating a comprehensive management model.

Zorlu Holding Information Security Policies and Procedures are applicable and mandatory for all personnel who use company information and/or business systems, whether full-time or part-time, contractual or permanent, regardless of their geographic location or business unit. Third-party service providers who do not fall under these classifications are also required to adhere to the general principles of this policy and information security procedures, as well as other security responsibilities they are obligated to comply with.