Erdemoğlu Holding A.Ş.
Information Security Policy

Erdemoğlu Holding Anonim Şirketi ("**Erdemoğlu Holding**") has made information security one of the fundamental principles of its operations. In this context, as an institution aware of the necessity to systematically manage and protect the information assets of Erdemoğlu Holding and its stakeholders, our primary objective is to ensure the confidentiality, integrity, and availability of information by effectively managing the identified risks through risk management practices.

This aim is pursued through;

► Ensuring the confidentiality of all information that Erdemoğlu Holding and its subsidiaries/group companies are obliged to protect,

► Ensuring not only the confidentiality but also the integrity and availability of information assets,

► Protecting the information assets in both physical and electronic environments that affect the operations of Erdemoğlu Holding and its subsidiaries/group companies,

► Protecting against unauthorized access that could harm the confidentiality and integrity of information, and increasing the awareness and consciousness levels of Erdemoğlu Holding and its subsidiaries/group companies' employees regarding information security,

► Protecting information assets against all kinds of threats that may come from inside or outside,

► Ensuring access to information through designated authorities and business processes,

► Complying with legal requirements and contracts related to information security with our stakeholders,

► Maintaining and improving our business continuity,

► Maintaining effective internal and external communication within the scope of information security,

► Reducing information security-related risks by conducting risk assessment and risk monitoring activities related to the information assets of Erdemoğlu Holding and its subsidiaries/group companies,

► Ensuring the continuity of the risk management system,

► Aiming to conduct all our activities and sustainable growth in accordance with the Information Security Management System.

In this regard we declare and commit;

► Ensuring that all units and employees of the community act in accordance with the Information Security Management System Standard, as well as the requirements arising from or that may arise from legal practices and contracts,

► Periodically reviewing the objectives and targets set within this scope, and creating the necessary resources to achieve these objectives and targets,

► Supporting continuous improvement and development regarding the Information Security Management System, and increasing the awareness of all employees and stakeholders about all innovations, changes, and developments within this system framework.