INFORMATION SECURITY POLICY

The purpose of Erkurt Holding Information Security Policy is to ensure the continuity of all business processes and information related to their activities, especially the production processes of Erkurt Holding and group companies serving the automotive and white goods industries, to prevent information security violations by reducing the effect of potential threats to information and to keep the risk of damage to a minimum level.

The compliance of the Information Security Management System with the ISO / IEC 27001 standard within the holding and group companies includes all information assets within Erkurt Holding and group companies. Employees at all locations, internal and external suppliers and contractors are obliged to work in accordance with the procedures related to this policy.

As the Board of Directors, we undertake to act on the development and continuous improvement of the Information Security Management System in order to meet the needs and expectations of our customers and to create a complete customer satisfaction, to ensure that the applications to be made for the legal and applicable conditions of the relevant parties are defined end-to-end within all processes and that they can be monitored digitally by committing to compliance.

Based on this purpose, our priorities, and targets for the purpose of protecting the information assets of Erkurt Holding and group companies against internal and external, intentional or unintentional threats are:

- To ensure data integrity, accessibility, and confidentiality by protecting the reliability and corporate reputation of the company,
- To provide training to all our employees to improve their technical and behavioural competences to increase awareness of information security,
- Defining information assets and business processes and ensuring the systematic management of risk assessments regarding them and enabling continuous improvement,
- To comply with all legal regulations and contracts regarding information security,
- To ensure that the contracts made with our customers, business partners, suppliers, non-governmental organizations, public institutions, and organizations comply with the relevant legislation,
- To ensure that the basic and supportive business activities of the institution continue with the least interruption and to implement the emergency action plan in extraordinary situations,
- Protecting corporate applications, data, communication network and equipment against loss, unauthorized use, and abuse,
- To ensure that all users are fully aware of the Information Security Policy and related supporting procedures and instructions,
- When there is a breach of information security, to ensure the information security urgently by implementing actions to the determinate, report, and record of the violation in question.