INFORMATION SECURITY POLICY

The main theme of the ISO/IEC 27001:2022 Information Security Management System in our organization, within the scope of "Information Security Activities in the Manufacturing Sector," is to demonstrate the management of information security in human, infrastructure, software, hardware, organizational information, information belonging to third parties, and financial resources. It aims to ensure risk management, measure the process performance of information security management, and regulate relationships with third parties regarding information security.

In line with this, our information security policy and procedures aim to:

- Manage information assets, determine the security values, needs, and risks of assets, and develop and implement controls for security risks.
- Define the framework set by methods for determining the values, security needs, vulnerabilities, and frequencies of threats to information assets.
- Define a framework for evaluating the effects of threats on the confidentiality, integrity, and accessibility of assets.
- Establish working principles for processing risks.
- Continuously monitor risks by reviewing technological expectations in the context of the scope of services provided.
- Comply with national or international regulations, legal and regulatory requirements, fulfill obligations arising from agreements, and meet information security requirements arising from corporate responsibilities to internal and external stakeholders.
- Reduce the impact of information security threats on service continuity and contribute to continuity.
- Have the competence to rapidly intervene in potential information security incidents and minimize their impact.
- Maintain and improve the level of information security over time with a cost-effective control infrastructure.
- Enhance corporate reputation and protect against adverse effects based on information security.
- Ensure the continuity of the Information Security Management System.

As top management, we commit to complying with the requirements specified in ISO/IEC 27001:2022 to achieve the defined information security objectives. We will allocate the necessary resources for the efficient operation of the "Information Security Management System", evaluate its effectiveness, and continually improve it.