Tat Gıda Information Security Policy

The purpose of the Information Security Policy is to define the requirements in order to ensure confidentiality, integrity and accessibility of the systems, information and assets operated by Tat Gıda. Information Security Policy is prepared taking into consideration the Communiqué Regarding the Management of Information Systems (Communiqué), VII-128.9 that was put into effect by the Capital Market Board for public companies, as well as other pertinent legislation, such as the Law on the Protection of Personal Data.

"Information Security Management System" is designed to protect the information assets from cyber attacks and to make sure that the security checks, i.e. policies, procedures, organization etc., are in place to ensure confidentiality, integrity and accessibility –whenever required- of the information.

Information Security Management System consists of two main parts: **strategic security** (process management) and **technical security** (operations). Strategic security includes security process management, especially including identification of the security strategy and creation of security policies. The strategy and policies are created in accordance with the company's goals and it is made sure that they are duly implemented. Technical security: security operations, especially including installation, management and monitoring of security systems fall within the scope of technical security. The policies determined to be within the scope of strategic security during technical security work must be implemented. Technical security work may be performed inside the Information Technologies Department as well as through outsourcing, provided that the necessary conditions are met.

The information assets owned are the most important values of Tat Gıda along with the means to produce, process and offer information. Tat Gıda needs considerable information as well as many information assets in order to fulfill its corporate functions. It is among the main goals of Tat Gıda to properly ensure confidentiality of such information and to make sure that it has the proper content and is accessible whenever needed.