

ISO27001 Information Security Management Systems Policy

With the purpose of Creating Fulfilling Moments and Creating a Better Future, JTI Tütün Ürünleri Sanayi A.S. Information Security employs the principles of ensuring the permanency of information systems, increasing the level of awareness of the employees and ensuring their compliance with the security requirements in order to maintain JTI's reputation and reliability, protect its information assets and maintain its basic and system support activities with the least possible interruption of service at all times in order to become #1 International Tobacco Company by volume by 2030.

In order to realize and continuously improve this principle on which information security is essential, we are committed to.

- Develop an Information Security Culture based on Our Way; «Start With Us», «Make it Count», «Welcome Challenge», and «Shape Tomorrow, Today » to Bring our Human Best
- To ensure the optimal protection of all information assets, information, and support business systems, to provide secure access to the information assets of itself and its stakeholders, to protect the confidentiality, integrity, and availability of personal and corporate information as data controller and data processor,
- Minimize the serious effects that may occur on the integrity and reputation of JTI business activities in the event of loss, corruption, or theft of information and support business systems,
- Make sure that JTI Employees are aware of the Information Security principles to enable them to proactively manage the impact of the events related to these principles and to ensure business continuity and the minimization of damage,
- Validate the risk management principle for all information assets of JTI and ensure that these assets, support business systems, networks, and other facilities are protected from internal or external, intentional, or accidental threats,
- The scope, content, and application of Information Security standards should be sufficient to address the risk level faced by JTI; ensure compliance with legal, regulatory, policy, and best practice requirements,
- Evaluate continuous improvement opportunities and conduct studies to keep the Information Security Management System alive.

JTI Information Security policies are applicable to all employees who use the information or business systems of JTI, whether they are working full-time or part-time, on permanent or temporary contracts, regardless of their location or function. It is imperative that all individuals, such as third-party service providers and their support personnel, who do not fall within these classifications but need to access JTI's information adhere to the general principles of this policy, along with the other security liabilities and obligations they must fulfill.

All practices mentioned in our policy are the priority of the company management and are under the responsibility of all company employees. Our policy is accessible to all stakeholders and is reviewed annually by management.

Bahadır SAYIN

Information Technologies
Business Solutions Manager

Wojciech ODZIMEK

Cluster Operations Lead