

INFORMATION SECURITY POLICY

As Kale Baęlantı Teknolojileri, our aim is to ensure the security and business continuity of information related to all existing and to be created activities within the scope of the Information Security Management System with minimum interruption, to ensure the confidentiality of all information belonging to the Company and third parties that it is obliged to protect, to prevent or minimize the effects of security breaches related to information security and to minimize business losses to the lowest possible level.

From this point of view, our goal is;

- To protect our Company's information assets against all kinds of threats that may come from inside or outside, to ensure accessibility to information as required by business processes, and to meet legal and regulatory requirements,
- To ensure the continuity of the confidentiality, integrity and accessibility of information, which are the three basic elements of the Information Security Management System in all the activities we carry out, to identify and evaluate the Risks related to them, and to implement the necessary controls for all assets above the acceptable level,
- To raise awareness by providing Information Security Management trainings to all our employees,
- Prepare and maintain business continuity plans and carry out drills,
- To identify existing risks by making periodic assessments on Information Security, to review and follow up action plans as a result of the assessments,
- We are subject to national, international or sectoral regulations, legal and related legislation
- To identify existing risks by making periodic assessments on Information Security, to review and follow up action plans as a result of the assessments,
- To fulfill the requirements of legal and relevant legislation with national, international or sectoral regulations to which we are subject, to meet the obligations arising from agreements, to ensure information security requirements arising from corporate responsibilities towards internal and external stakeholders,- To ensure that innovations, changes and developments within the framework of the Information Security Management System are announced in a way to ensure the awareness of all employees and stakeholders,- To prevent any disputes and conflicts of interest that may arise from contracts,- All actual or suspected vulnerabilities that threaten Information Security,
- To report to the ISMS Team and to ensure that it is investigated by the ISMS Team.

Özkan Keskin
General Manager
03.07.2024