

It has been determined that all software used within the scope of PROTENG includes Technical Support, Software Development, Hardware and Maintenance Processes and all hardware and software related to them, all server system elements and end-user computers and all physical and electronic information assets within the institution, based on corporate business process management.

In this context, Proteng;

- To protect Proteng Müh.Danş.Tic. A.Ş.'s information assets against all kinds of threats that may arise internally or externally, knowingly or unknowingly, to ensure accessibility of information through business processes, to meet legal requirements, and to work towards continuous improvement.
- To ensure the continuity of the three basic elements of the Information Security Management System in all activities carried out:
- Confidentiality: Preventing unauthorized access to important information,
Integrity: Demonstrating that the accuracy and integrity of information are ensured,
Accessibility: Demonstrating that authorized persons can access information when necessary,
- To be concerned with the security of not only the data kept electronically but also all data in written, printed, oral and similar media.
- To raise awareness by providing Information Security Management training to all personnel,
- To report all existing or suspicious vulnerabilities in Information Security to the ISMS Management Representative and to ensure that they are investigated by the ISMS Management Representative,
- Preparing, maintaining and testing business continuity plans,
- To identify existing risks by conducting periodic assessments on Information Security; to review and follow up action plans as a result of the assessments,
- To prevent any disputes and conflicts of interest that may arise from contracts,
- Meeting business requirements for information accessibility and information systems.

Cenk Alkan
General Manager