

## INFORMATION SECURITY POLICY

Via application of this policy Angst Pfister Advanced Technical Solutions A.Ş. Upper Management commits and declares to fulfill the following basic principles that are the requirements of the accountability, continuity and sustainability of the services within the scope of the Information Security Management System in order to provide the continuity of the work processes that are realized with a vision of being a manufacturer, design partner and solution provider for both Vibration Prevention and impermeability products in the global market.

The unauthorized usage, modification, disposition and damaging of the information assets with or without intent shall be prevented.

The information taken from the customers shall be protected against unauthorized access in line with the basic principles of information security.

The information of the customers collected for work purposes shall be used only for those purposes and shall never be shared with third parties.

The necessary resources shall be provided in order to perform the requirements regarding the customers with infrastructure, process and personnel appropriate to the requirements of the legal legislation .

The confidentiality of the corporate and personal information or without considering the ownership of the third parties the produced and/or used information within the information security scope of the Angst Pfister Advanced Technical Solutions A.Ş. will be kept under guarantee.

Access control will be provided in accordance with the “need to know” principle and the information shall be protected against unauthorized access.

Via the design, application and continuity of the Information Security Management System risks will be reduced to acceptable levels .

The information will be protected under any circumstances independent of the usage forms like electronic communication of the information, sharing with third parties, usage for research purposes, and storage in physical and electronic media .

Information assets shall be defined with their confidentiality levels and their secrecy and integrity will be provided by having employees to apply confidentiality precautions .

The requirements identified by the R.T laws, regulations, circulars, customer contracts and the legal legislations work demands will be met and working in accordance with these.

In order to protect from the effects of the grand disasters and operation errors, the work continuity management of the services provided to customers shall be applied and a work continuity management plan will be established. The sustainability of the work continuity plan will be provided and tested.

The information security awareness of the personnel shall be raised and trainings that will encourage them to contribute to the operation of the system will be provided regularly to the organization employees and new entries .

All actual and suspected violations of information security shall be reported and measures to prevent repetition will be taken.

REV. NO : 00

ISSUE DATE : 23.08.2016

ERAY ULUGÜL

GENERAL MANAGER

[SIGNATURE]