Senior Management Commitment

Pisano Senior Management undertakes to fulfill the requirements for the realization, operation, monitoring, review, maintenance and improvement of information security, and the fulfillment of applicable legal requirements and ISO / IEC 27001 standard.

Pisano adopts the following principles regarding information security management;

- Pisano values ensuring the safety of its activities regarding the products and services it offers to its customers and stakeholders.
- All business processes are aimed to be integrated, compatible and balanced with each other. Integrated and dynamic business strategy requires the security and continuity of information assets.
- Pisano adopts as a principle to take precautions against risks that may threaten the confidentiality, integrity and accessibility of its products and services that provide value to its customers and stakeholders.
- Intended outcomes of information security in line with this policy and the purpose of the organization are determined and continuous improvement opportunities are evaluated by measuring compliance at regular intervals.

Information Security Policy

Information security is possible by ensuring the confidentiality, integrity and accessibility of information assets.

- The necessity of confidentiality, that the information is accessible only by authorized people,
- Integrity requirement, ensuring the completeness and accuracy of information assets, protecting them from unauthorized changes,
- Accessibility requirement implies that information assets are available to authorized users when needed.

Information assets are properly classified in Pisano. The assets are valued and the value of the assets is calculated to develop an appropriate level of control.

Pisano creates principles that regulate its own corporate functioning in order to ensure information security. Determining the Information Security Policy, defining security roles and making all relevant updates are carried out with the support of the Senior Management and the coordination of all business units. Pisano may seek the opinions of internal and external experts when necessary.

Information Security Objectives

Pisano aims to carry out information security studies for the following purposes without compromising the principles mentioned above;

- Information Security Management System (ISMS) is planned, implemented and developed in line with the internationally accepted ISO / IEC 27001: 2013 Information Security Management System standard requirements,
- Necessary studies are carried out to comply with the relevant laws and regulations,
- Necessary actions for internal audit, management review, corrective actions and identifying risks and opportunities required for continuous improvement of ISMS are provided by the management and the teams that the management gives responsibility for information security,

- All roles and responsibilities related to information security are determined and authorizations are made by the management,
- The resources are provided by the management to carry out the necessary work within the framework of the information security management system,
- Together with its stakeholders, material and moral losses that may adversely affect the competitive advantage of the organization are prevented,
- The scope of Information Security Management System is decided by determining information assets, evaluating the information security expectations of related parties such as customers, suppliers and business partners, analyzing legal and contractual obligations, if any, and determined by the management in line with business strategies,
- An asset inventory is created in order to classify information assets and evaluate the confidentiality, integrity and accessibility of these assets,
- To manage information security risks, risk assessment, risk analysis and risk processing studies are carried out, necessary measures are developed and studies are carried out to prevent possible risks,
- Information security objectives in line with this policy and the purpose of the organization are determined, compliance is measured at regular intervals and opportunities for continuous improvement are evaluated,
- Confidentiality of personal information of employee is ensured,
- Customer information is prevented from being accessed by unauthorized people,
- Data integrity is ensured,
- Information security is provided at the supplier,
- Continuous development and protection of operational know-how is ensured,
- End user awareness of information security and this awareness are continuously increased,
- By managing information security effectively, possible damages arising from information security are minimized,
- Necessary studies are carried out to reduce the possibility of experiencing an information security violation, and if it occurs, a coordinated response is provided,
- Necessary arrangements are made to prevent interruptions in critical business processes, in case it cannot be exceeded, it is ensured that it can be operated again within the targeted recovery period,
- Confidentiality, integrity and accessibility of our customers' information assets are ensured within the scope of the Information Security Management System. Continuity of critical business processes related to the customer is ensured,
- Continuous improvement of the Information Security Management System is ensured,
- In human resources management, processes where rules are determined in terms of ensuring security before, during and after employment are established,
- It is ensured that necessary measures are taken to ensure security in internal working areas such as safe working areas, office areas, warehouses and around the institution,
- In order to conduct supplier relations safely; procedures are established for reviewing the procurement services and managing the changes that occur. Security requirements are determined especially in agreements with information technology suppliers that express information security risks.