ÜSTÜNBERK HOLDING

INFORMATION SECURITY POLICY

INFORMATION SECURITY SCOPE

This policy applies to all the units that utilize the Information Technologies network, third party users with access to the information system as well as service, software or hardware vendors that provide technical support to information systems.

Üstünberk Holding Information Security aims to establish the continuity of information systems with a view to protecting reputation, reliability, and information assets of Üstünberk Holding, and sustaining business activities with minimum interruption; enhance employee awareness on security and employee compliance with security requirements; ensure third parties comply with security requirements and up-to-date technical security controls are actively performed, and our company is managed with a risk-focused approach.

INFORMATION SECURITY GOALS;

- Make sure our Information Security Management System is documented, certified and continuously improved in a way to meet the ISO 27001 standard requirements,
- Act in accordance with our Corporate Vision and Mission,
- Reduce information security risks that threaten business continuity, and ensure business continuity,
- Protect the Holding's reputation from damages originating from information security and improve the group's reputation,
- Ensure confidentiality, integrity, and accessibility of the information stored physically and electronically, while fully complying with legal obligations, customer requirements, operational and contractual terms,
- Enhance awareness of the employees and users on Information Security in order to minimize information security risks, helping them acknowledge their responsibilities,
- Identify and evaluate security requirements for the electronic infrastructure, improve this infrastructure by keeping abreast of technological developments and establish business continuity,
- Achieving an acceptable level of security for external access,
- Define information security requirements for third parties, customers and suppliers and make sure they comply with the information security management system,
- Protect the confidentiality of critical customer and employee data as well as the information on our strategic goals, design, production, sales and supply with respect to our Products and Services,
- Manage operations by integrating them with other management systems in place with the intention of detecting Information Security violations and immediately intervening in these violations.