

Information Security Policy

Information Security Management System of Bakioğlu Holding Group Companies is based on the following fundamental principles;

Reliability (Confidentiality): Preventing the availability or accessibility of information to unauthorized individuals, entities, or other operating systems

Integrity: Maintaining the integrity and accuracy of the assets

Accessibility: Ensuring access and availability upon the request of an authorized person

- Establishing, developing and ensuring the sustainability and continuous improvement of the management system required to identify, assess and implement controls related to the security requirements, risks, vulnerabilities and opportunities with respect to our business strategy and information security processes,
- Ensuring full compliance with legal, operational and contractual requirements, and securing the confidentiality, integrity, and availability of all information stored in physical and electronic media,
- Ensuring full compliance with all legal requirements regarding customs legislation,
- Establishing working principles for handling risks, as well as developing and implementing controls for security risks. Continuously reviewing the technological expectations and developments to monitor risks,
- Mitigating the impact of information security risks on the business continuity and ensuring the business continuity,
- Possessing the competency to rapidly respond to potential information security incidents and mitigating the impact thereof,
- Minimizing information security risks, raising the awareness of users and employees regarding information security, and ensuring that they are well aware of their responsibilities,
- Assessing information security performance and the effectiveness of the information security management system against defined objectives,
- Ensuring the protection of the personal data,
- Establishing and evaluating the security requirements of the electronic infrastructure serviced, improving it by adapting to technological developments, and ensuring the service continuity,
- Ensuring that external service providers fulfill the requirements and necessities required by the information security system,
- Providing an acceptable level of security for accessing the system externally,
- Defining the information security requirements of third parties, customers, and suppliers, and ensuring their compliance with the information security management system,
- Safeguarding and enhancing the Holding's reputation in case of information security-based adverse impacts,
- Establishing the information security standards for group companies, auditing them at regular intervals, and ensuring the compliance.
- Assessing the potential impacts of climate change on information security and implementing the required measures to mitigate these impacts.