

## EBEBEK MAĞAZACILIK ANONİM ŞİRKETİ INFORMATION SECURITY POLICY

EBEBEK Mağazacılık A.Ş. operates as a leading company in its sector in collaboration with its barents, employees, suppliers, and partners, and is committed to taking all necessary measures to safeguard information security.

- In accordance with the Personal Data Protection Law, we process the data of employees, barents, and third parties in compliance with the technical and administrative measures set forth in the “Personal Data Security” guideline, as well as other legal obligations and regulations.
- We ensure the security of personal data and store such data in secure environments that are properly maintained.
- We organize awareness trainings and information activities for employees and third parties, when necessary, to strengthen information security.
- We publish this policy and share it transparently with all stakeholders, keeping them informed on this matter.
- We identify risks that may compromise the confidentiality, integrity, and accessibility of personal data and information assets, evaluate these risks based on their impact and likelihood, and take appropriate measures to mitigate them.
- To ensure the continuity of operations and workflows, uninterrupted accessibility of information assets is essential. In case of an unexpected interruption, we implement measures and conduct activities to reactivate operations within a specified period, supported by emergency and disaster recovery scenarios.
- Our Information Security Policy enters into force with the approval of the Board of Directors and is carried out under the responsibility of the Information Security Management Systems (ISMS) Board. The policy is reviewed at least once a year and updated or improved when necessary.
- This policy covers the protection of electronic information assets obtained from our commercial activities and related logistics, storage, accounting, finance, quality assurance, procurement, human resources, administrative affairs, legal, sales, marketing, internal audit, and information technology processes, as well as the lawful processing, storage, protection, confidentiality, and integrity of personal data retained within our company.