

INFORMATION SECURITY POLICY

In line with our vision to become a leader by contributing more to our customers' success than our competitors in the business segments we serve, we consider "information" as a strategic corporate asset that must be protected in all environments and formats. Aligned with our corporate goals and strategies, we are committed to safeguarding information



at levels appropriate to the nature of our business and to ensuring its continual improvement. Within this framework, we aim to:

- Ensure the confidentiality of information by granting access only to authorized individuals,
- Maintain the integrity of information by protecting it against unauthorized alterations and ensuring its accuracy,
- Guarantee the availability of information by keeping it accessible and uninterrupted when needed.

Within the scope of our Information Security Management System, established and operated in accordance with the ISO/IEC 27001:2022 standard:

- We systematically assess, prioritize, and mitigate information security risks and strive for continuous improvement,
- We fully comply with all legal obligations and Borusan Group principles,
- We promote information security awareness among our employees, suppliers, and business partners, supporting their adherence to our policies,
- We manage information security breaches in a transparent, ethical, and systematic manner,
- We make decisions and take actions based on objective, reliable, and up-to-date information, making the most of technological advancements,
- We ensure the continuity of our digital infrastructure to deliver solutions aligned with customer needs and international standards,
- We protect customer data and all types of personal information through confidentiality policies, processes, and advanced technological solutions,
- We fully comply with all applicable data protection regulations, primarily the Turkish Personal Data Protection Law No. 6698 (KVKK),
- When utilizing emerging technologies such as Generative AI (GenAI), we implement restrictive and supervisory measures to safeguard corporate information assets and mitigate data leakage risks,
- We do not share any data without the explicit consent of the data owner or unless legally required.



Moreover, we continuously improve our business continuity and risk management plans by considering the potential impact of climate change and environmental threats on information security. We develop proactive measures to mitigate the effects of environmental risks such as power outages, natural disasters, or infrastructure damages on information security and service continuity.



We are fully committed to ensuring the adoption and maintenance of an information security culture throughout our organization with the active participation of all our employees.

Executive Board Member, Chief Digital Officer
Tayfun Özçay

DAHA İYİ BİR DÜNYA İÇİN
ÇÖZÜM ÜRETİRİZ

 BORUSAN

