Boss Governance®
a CottGroup® Company

INFORMATION SECURITY AND PERSONAL DATA MANAGEMENT SYSTEM POLICY

(ISO 27001:2022 & ISO 27701:2019)

Boss Yönetişim Hizmetleri A.Ş. adopts as a fundamental principle, in all activities carried out within the scope of Payroll, Human Resources Management and Consultancy, and Payroll and HR Software, the protection of information assets and personal data, the maintenance of the trust of its customers and relevant stakeholders, and the support of business continuity.

Accordingly, our company establishes, implements, maintains, and continuously improves its processes within the scope of the ISO 27001 Information Security Management System (ISMS) and the ISO 27701 Personal Data Management System (PDMS/PIMS).

As Boss Yönetişim Hizmetleri A.Ş.;

- We commit to protecting the **confidentiality, integrity, availability**, and privacy of information assets and personal data.
- We conduct our information security and personal data management practices in compliance with all applicable requirements, including applicable legislation (the Law on the Protection of Personal Data No. 6698 (KVKK) and related regulations), customer requirements, and contractual obligations.
- Within the scope of the ISMS and PIMS, we include all business processes carried out by our company, our employees, customers, suppliers and solution partners, and all relevant parties that may be affected by our business outcomes.
- We record all company assets within the scope of the Asset Inventory, classify them, assign ownership; and manage access to information assets based on authorization principles. We keep the asset inventory up to date in line with changing needs and risks. • We systematically assess information security and personal data risks; determine, implement, and monitor the effectiveness of the necessary controls to reduce risks to acceptable levels.
- In the processing of personal data, we act in accordance with the principles of purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and security. • In order to manage information security incidents and personal data breaches, we operate an incident management process; and, where necessary, carry out notifications to relevant parties and competent authorities in accordance with applicable legislation and contractual obligations.

- We organize training programs to increase our employees’ awareness of information security and the protection of personal data; clearly define roles and responsibilities and ensure the sustainability of competence.
- In our relationships with third parties, we secure information security and personal data protection requirements through contracts, monitor their implementation, and audit them when necessary.
- We monitor, measure, and analyze the performance of the ISMS and PIMS; regularly evaluate them through internal audits and management review activities, and enhance them through a continuous improvement approach.

The senior management of **Boss Yönetişim Hizmetleri A.Ş.** ensures the provision of the necessary resources, the establishment of objectives, the management of risks, and the adoption of this policy by all employees for the effective operation of the ISMS and PIMS. This policy provides a framework for the establishment and review of ISMS and PIMS objectives.

This policy is a controlled document; it is communicated to all employees, its understanding is ensured, and it is kept appropriately accessible to relevant parties.

SELİM TANKUT AKDAĞ

CEO

07.01.2026