**BTA-BSB-PO-002**
**31-12-2025-00**

# BATISÖKE INFORMATION SECURITY POLICY

## 1. Introduction: Purpose, Scope and Legal Basis of the Policy

### Strategic Context

This Policy sets out the commitment of Batısöke Söke Çimento Sanayii T.A.Ş. (the "Company"), a publicly listed company within Batı Anadolu Group of Companies, to protecting its information assets and its corporate governance approach in this regard. The secure, uninterrupted and legally compliant management of information systems constitutes a fundamental component of our responsibilities towards stakeholders within the framework of capital markets regulations. This Policy provides a strategic framework that supports sustainable success by minimizing the operational, financial and reputational risks to which the Company may be exposed.

### Purpose of the Policy

The primary purpose of this Policy is to ensure the highest level of protection of the confidentiality, integrity and availability of the Company's information assets. In this context, the governance structure and responsibilities relating to information systems are defined, and the principles for managing information security risks are established. The Policy aims to ensure the establishment and continuity of information systems controls, thereby safeguarding the Company's legal compliance and reducing its risks to a minimum.

### Scope

This Policy covers all information systems owned, used or operated by the Company, or obtained through third parties, as well as information technology infrastructures, applications, databases, information stored in electronic environments, and employees using these systems. External service providers and third parties processing information on behalf of the Company are also subject to the provisions of this Policy within the scope of their contractual obligations.

### Legal Basis

This Policy has been prepared based on the Capital Markets Board Communiqué No. VII-128.10 on Principles Regarding Information Systems Management, the Law No. 6698 on the Protection of Personal Data, the Turkish Commercial Code, and other applicable legislation. The provisions of the Policy are implemented in accordance with the risk-based and proportionality principles set forth in the Communique.

## 2. Governance Structure and Responsibilities

### Board of Directors

- Approves the Information Security Policy and oversees its implementation.
- Evaluates the adequacy of information systems controls.

- Takes strategic decisions by considering risks arising from information systems.

**Senior Management**

- Ensures the implementation of the Policy throughout the Company and allocates necessary resources.
- Oversees the management of information systems risks, monitoring of incidents, and provision of annual training to employees.
- Reviews and approves new information systems and critical projects within the framework of risk assessments.
- Appoints an Information Security Officer with at least five years of professional experience.

**Information Security Officer**

- Responsible for establishing, implementing and maintaining the information security management system.
- Monitors processes related to vulnerabilities, patch management and incident management.
- Performs an approval and oversight role in critical matters such as remote access, privileged access and similar issues.
- Performs duties independently while reporting directly to senior management.

**Department Managers and Employees**

- Department managers ensure the protection of information assets within their areas of responsibility.
- Employees use information systems only within the scope of their authorizations and immediately report any security incidents.

## 3. Fundamental Information Security Principles

### Risk Management

Risks related to information systems are analyzed at least once a year and following significant changes; the results are evaluated by Senior Management.

### Information Asset and Access Management

An inventory of information assets is created and assets are classified. Access rights are granted in accordance with the principle of least privilege and are regularly reviewed. Authentication mechanisms are configured in line with risk levels, and multi-factor authentication is applied for critical systems.

### Authentication and Authorization

Authentication mechanisms are structured based on risk levels, and multi-factor authentication is applied for critical systems and privileged accounts.

**Logging and Monitoring**

Critical transactions, accesses and changes on information systems are logged; such records are protected against unauthorized access and used for audit and review purposes when necessary.

**Physical and Environmental Security**

Critical information technology assets are located in secure areas, and access to these areas is controlled.

**Business Continuity and Incident Management**

Information systems continuity plans are prepared and tested regularly. An Incident Response Plan is implemented for information security incidents.

**Outsourcing and Third-Party Management**

Information security and confidentiality obligations are defined in contracts executed with service providers.

**Legal Compliance**

Policies and practices are carried out in compliance with applicable legislation. Data whose retention period has expired is securely and irreversibly deleted or destroyed in accordance with legislation.

**4. Policy Implementation and Effectiveness**

**User Awareness and Training**

Company employees are provided with awareness and information training at least once a year regarding the Information Security Policy, the rules they must comply with, and the procedures to be followed in the event of an information security incident. Trainings are planned in line with employees' roles and responsibilities, with the aim of establishing an information security culture across the Company.

**Extraordinary Expenditures and Approvals**

Within the scope of information security, a general budget framework is established for expenditures to be made in extraordinary circumstances. Where necessary, approval of the Board of Directors is obtained in accordance with the Company's internal authorization and signature principles.

**Review of the Policy**

The Information Security Policy is reviewed at least annually, taking into account changing business needs, technological developments, emerging threats and regulatory changes. Where deemed necessary, the Policy is updated and submitted for approval.

**Approval and Entry into Force**

This Policy enters into force upon approval by the Board of Directors. Any amendments to the Policy are also subject to Board approval. The current version of the Policy is communicated to employees and relevant stakeholders.