ARTICLE 1: PURPOSE

1.1. Beta Enerji ve Teknoloji A.Ş. (hereinafter referred to as the "Company") is committed to establishing and improving the mechanisms required to ensure, manage, monitor, review, maintain, and continuously improve information security. In this regard, the Company implements the Corporate Information Security Management System, referring to the ISO/IEC 27001 Information Security Management System standard. The Company is committed to meeting applicable global standards for information security, fully complying with all related regulations and legislation, and continuously improving and developing the Corporate Information Security Management System. The purpose of this policy is to define the scope, principles, performance criteria, and objectives of the Company's information security, and the mechanisms required for the monitoring and continuous improvement of the Corporate Information Security System.

ARTICLE 2: DEFINITIONS

2.1. In this section, specific terms and concepts used in the policy are briefly explained as follows:
Company: Beta Enerji ve Teknoloji A.Ş.
Policy: Information Security Policy
Employee: Refers to the company's managers and employees.

ARTICLE 3: SCOPE

3.1. This policy covers:

a) Members of the Company’s Board of Directors,
b) The Company’s Employees,
c) Suppliers and service providers,
d) Individuals and organizations working on behalf of the Company, including consultants, lawyers, advisors, external auditors, and other parties engaged in commercial relationships with the Company, including customers ("Business Partners").

The implementation of the information security policy is the responsibility of the Company management and all department managers. Each department manager is primarily responsible for taking all necessary measures within their area of responsibility to ensure compliance with corporate information security policies and procedures, and for controlling

business operations. The company management receives support from the IT department in matters such as the implementation of the information security policy, the establishment, and development of the Corporate Information Security System.

ARTICLE 4: PRINCIPLES AND ESSENTIALS

4.1. Commitment to Information Security

4.1.1. The Company places great importance on ensuring the security of products and services provided to customers and stakeholders. It is committed to carrying out all activities in accordance with the information security policy.

4.2. Compliance with Laws and Information Security Standards

4.2.1. The Company and its employees fully comply with all legal regulations and standards related to information security.

4.3. Risk Management and Information Security Measures

4.3.1. The Company adopts a systematic risk management approach and takes the necessary measures to ensure the security, confidentiality, integrity, availability, and continuity of information assets.

4.4. Raising Information Security Awareness

4.4.1. All employees are provided with training to enhance their technical and behavioral competencies, and these trainings are continuously updated in line with changes in regulations and current developments.

4.5. Information Security Policies and Controls

4.5.1. The Company establishes, publishes, and monitors the implementation of sub-procedures and internal control mechanisms in line with information security policies.

4.6. Information Security Objectives and Continuous Improvement

4.6.1. The Company defines information security objectives and regularly measures the compliance with these objectives, evaluating opportunities for continuous improvement.

4.7. Compliance with Legal Regulations and Contracts

4.7.1. The Company and its employees fully comply with legal regulations, company commitments, and contracts in accordance with information security policies and Information Security Management System standards.

4.8. Continuous Improvement of the Information Security System

4.8.1. Necessary mechanisms are established to continuously improve and develop the

Information Security Management System; updates and improvements are made in the system by following innovations and technological developments.

4.9. Compliance with Information Security Policies and Discipline

4.9.1. Violation of information security policies and procedures may result in disciplinary action and may lead to legal sanctions under the relevant legislation.

ARTICLE 5: DUTIES AND RESPONSIBILITIES

5.1. Board of Directors

5.1.1. The Board of Directors is responsible for the oversight of the implementation of the principles and essentials stated in this policy, as well as for determining and operating the notification, investigation, and sanction mechanisms in cases of violations or suspicious situations that are contrary to these principles and essentials. This responsibility is carried out with the Audit Committee, which works under the Board of Directors.

5.2. Directorate of Digital Transformation and Data Analytics

5.2.1. The Directorate of Digital Transformation and Data Analytics, upon identifying violations or suspicious situations contrary to the principles and essentials in the Policy, will make objective assessments regarding situations that may result in Disciplinary Action, in accordance with the relevant legal provisions.

5.2.2 The Directorate of Digital Transformation and Data Analytics has the authority to:

5.2.2.1. Take defense from an employee, initiate an investigation, suspend the employment contract, terminate the employment contract, and exercise rights in accordance with the Labor Law and applicable legislation if the employee does not act in accordance with the Policy.

5.2.2.2. Stop receiving services from consultants, lawyers, and financial experts who do not comply with the Policy and terminate their service contracts.

5.2.2.3. Suspend, halt, or terminate business relationships with business partners who do not comply with the Policy.

5.3. Employees

5.3.1. Employees are responsible for ensuring compliance with the policies set by the General Manager, adhering to internal and external legislation, and reporting to the Directorate of Digital

Transformation and Data Analytics in the event of encountering behaviors, attitudes, actions, decisions, activities, or applications that are contrary to the Policy.

Email: etikhat@betaenerji.com
Address: Hacı Sabancı Organized Industrial Zone, Çanakkale Cd. No:11 / B, Sarıçam ADANA / Turkey

ARTICLE 6: EFFECTIVENESS

6.1. This Policy has come into force with the decision of the Board of Directors dated 04.04.2025. This Policy will remain in effect until a new announcement is made.

ARTICLE 7: REVIEW

7.1. This Policy will be reviewed regularly once a year by the Information Systems Manager, based on checks related to changes in processes or technical infrastructure. The reviewed and updated Policy will be approved by the Board of Directors.

ARTICLE 8: RELATED POLICIES AND PROCEDURES

Information Security Procedure

Reason for Revision :	New Document

Prepared By	Approved By
Management Systems and Sustainability Engineer	General Manager