

INFORMATION SECURITY POLICY

1. PURPOSE

For Aydem Renewable Energy Inc. ("AYEAŞ"), information systems and the corporate data processed within these systems are critical to the continuity of daily operations and core services. This Policy aims to ensure, protect, maintain, and manage the confidentiality, integrity, and availability of AYEAS's information systems and information assets. Within the scope of Information Security Management, AYEAS also aims to ensure compliance with all applicable national, sectoral, and legal regulations, as well as relevant legislation, standards, and regulatory requirements, and to implement these requirements through a systematic approach.

2. SCOPE

This Policy applies to all AYEAS employees, third parties accessing corporate data, all information systems in which information is processed, and all related physical environments.

3. RESPONSIBILITIES

This Policy, which defines AYEAS's information security strategy and roadmap, has been prepared by Senior Management and approved by the Board of Directors.

The Board of Directors oversees the establishment and maintenance of an effective Information Security Governance Framework throughout the organization. The Board is committed to providing the resources necessary for the implementation and continuous improvement of the Information Security Management System (ISMS).

To ensure compliance with applicable laws and regulations, the Board of Directors has appointed an Information Systems Security Officer with sufficient technical expertise and experience, who operates independently from operational information technology activities. The Information Systems Security Officer reports directly to the Board of Directors and performs oversight and coordination duties within the scope of information security governance.

Information security activities are planned and implemented in alignment with the Company's strategic objectives, risk management approach, and applicable regulatory requirements.

3.1. EMPLOYEES

Regardless of their position or role, all AYEAS employees are responsible for complying with information security policies, procedures, and instructions within the business processes under their responsibility.

AYEAS respects the privacy of its employees; however, it reserves the right to monitor activities conducted on its information systems when necessary.

3.2. THIRD PARTIES

Information Security requirements applicable to third parties providing goods and services to AYEAS, as well as their personnel, are defined through contractual agreements.

Accordingly, suppliers are expected to comply with AYEAS Policies and Procedures governing third-party relationships, including but not limited to information security requirements.

4. GENERAL PRINCIPLES

AYEAŞ regards Information Security as one of the fundamental pillars of corporate sustainability and adopts the following principles:

- Compliance with Legal and Regulatory Requirements
- Continuous Improvement of Information Security Systems
- Asset Management and Risk Assessment Processes
- Data Protection and Backup Management
- Physical and Environmental Security
- Information Systems Business Continuity
- Operations and Change Management
- Access Control
- Definition of Information Security Requirements for Outsourced Information System Services
- Monitoring and Responding to Information Security Threats
- Information Security Incident and Incident Reporting Process
- Information Security Awareness Program
- Acceptable Use
- Clean Desk and Clear Screen Policy

This Policy shall be reviewed at least once annually and updated whenever necessary. The current version of the Policy shall be communicated to employees and published on the Company's corporate website.

Approved by the Board of Directors Resolution No. 2026/18 dated 3 April 2026.