

INFORMATION SYSTEMS AND SECURITY POLICY

Publication Date 11.11.2021 | Revision Date 25.07.2025 R3

The Information, Information Systems, and Security Policy, an annex to the Integrated Management System Policy, demonstrates Ateş Wind Power's corporate commitment to protecting, securing, and effectively managing information assets. This policy provides guidance for establishing a secure, transparent, and controllable information management system based on the principles of confidentiality, integrity, and availability. Compliance with all relevant legislation and international standards, particularly the Capital Markets Board's Communiqué on Information Systems Management, forms the foundation.

The Information, Information Systems, and Security Policy applies to all employees, managers, subcontractors, suppliers, business partners, and representatives of Ateş Wind Power. It covers all factories within Ateş Wind Power.

Within the scope of this policy, Ateş Wind Power accepts, undertakes, and declares the following principles:

- Store information in electronic and/or printed formats according to appropriate classification; share it only with authorized personnel based on the nature of the information and back it up using suitable methods; avoid unnecessary replication.
- Ensure that all employees and other stakeholders commit contractually to maintaining information confidentiality in line with their legal position; preserve the provisions of relevant legislation; provide necessary training and/or guidance regarding information and information systems.
- Do not provide external stakeholders with direct access to information; instead, allow them to use information systems directly or provide necessary information, while retaining obligations under applicable legislation.
- Establish physical and electronic infrastructure for collecting, processing, and securing information, taking into account the company's requirements and capabilities.
- Operate electronic systems in an integrated manner to ensure data security and integrity; monitor system updates and apply them in a timely manner; renew systems and hardware in line with technological developments and company needs.
- Provide employees and other stakeholders with necessary systems and hardware to access required information; implement authorization and security measures within this scope.
- Always consider the confidentiality, integrity, and availability of information and information systems; address information breaches promptly; establish measures and systems as required by legislation; regularly monitor relevant regulations.
- Use up-to-date systems, applications, and equipment to ensure information security; implement preventive, corrective, and protective controls against cybersecurity threats.
- Conduct regular information security and confidentiality training to ensure that all employees and stakeholders are aware of their responsibilities regarding information security.
- Systematically assess information security risks and manage them through appropriate control mechanisms.
- Ensure the continuity of information systems and implement business continuity and disaster recovery plans to address potential system interruptions.

Our Information, Information Systems, and Security Policy is integrated into all company processes. At every stage, from daily operations to strategic decisions, information security principles are considered. Necessary technical, financial, and human resources are provided; relevant legislation, international standards, and technological developments are regularly monitored, and expert support is obtained when necessary.

The Finance Director holds primary responsibility for the effective implementation of the Information, Information Systems, and Security Policy, ensuring its application and reporting results to the Board of Directors. Additionally, all employees and business partners are responsible for fulfilling their obligations regarding information security. Top Management regularly monitors and evaluates the practices carried out under the Information, Information Systems, and Security Policy.

This policy is reviewed by Top Management at least once a year and updated according to legislative changes, audit results, and information security needs.