INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

PO.BT.01-Rev.00-June 15, 2022

1. PURPOSE

This policy defines the information security systems and practices **of Arzum Elektrikli Ev Aletleri Sanayi ve Ticaret A.Ş.** ("Arzum," "the Company"). Arzum is committed to ensuring information security by managing existing and potential risks within the framework of legal requirements and regulations, and to continuously improving, developing, and reviewing these systems.

At Arzum, the management of information systems is addressed as part of corporate governance practices. Arzum ensures that strategies related to information systems are aligned with business objectives in order to maintain stable, competitive, growing, and secure operations. At Arzum, information systems management focuses on the security, performance, efficiency, accuracy, and continuity of information systems; the necessary funding and human resources are allocated to ensure the proper management of these aspects.

2. SCOPE

This policy aims to ensure the confidentiality, availability, and integrity of the information and information resources defined in the "Scope, Limits, Context, and Stakeholders" document in order to protect Arzum's technology, know-how, personal data and special-category personal data processed in its capacity as a data controller or data processor, and thereby safeguard its reputation.

This policy applies to all employees who use Arzum's information and business systems, as well as consultants working on behalf of the company.

3. DEFINITIONS AND ABBREVIATIONS

ISMS: Information Security Management System

ISMS Team: The ISMS team is the organization that represents management, assumes responsibility for the successful maintenance of the ISMS, and ensures its oversight.

ISMS Internal Auditor: A person who is independent of the implementation and operation of the ISMS, possesses the experience, training, and certifications necessary to conduct ISMS audits, and performs the internal audit of the ISMS. The internal auditor may be a company employee or an external party.

KVKK: Law No. 6698 on the Protection of Personal Data

4. RESPONSIBILITIES

Senior Management: Is responsible for ensuring that the Information Security Policy meets the organization's needs, for providing the necessary support and oversight for its implementation, and for reviewing the policy at least once a year or whenever changes to the organization's policy may be required. The ISMS Representative performs this duty on behalf of senior management and obtains approval from the Deputy General Manager.

ISMS Representative: The individual who assumes responsibility to senior management at every stage, from the establishment to the operation and management of the Information Security Management System.

ISMS Team: The ISMS team, appointed by the Company's senior management, is responsible for ensuring that the Information Security Policy meets the Company's needs, for providing the necessary support and oversight for its implementation, and for reviewing the policy at least once a year or whenever changes to the Company's policy may be required.

All Personnel: All personnel are responsible for fulfilling the requirements of the Information Security Policy in accordance with the demands of their respective roles.

5. IMPLEMENTATION

5.1 Management Support

- Senior management actively supports the ISMS through activities carried out under the ISMS team, the appointment of the ISMS Representative and ISMS Internal Auditor, ISMS investment, expense, and training budgets, and management review activities.
- Senior management provides leadership to achieve ISMS objectives by complying with and promoting compliance with ISMS policies and procedures.
- Senior management emphasizes the importance of managing information security risks for the organization's reputation and business continuity through its management activities and corporate policies.
- At least once a year, it assesses risks and reviews the Information Security Policy to ensure the system's continuity and sustainability.

5.2 Information Security Policy

To ensure that all information held by Arzum is evaluated in terms of confidentiality, integrity, and availability, protected from all internal and external threats, and that operations are carried out effectively, accurately, quickly, and securely, the Company has established the ISO 27001 Information Security Management System (ISMS) and has established it as a policy to meet information security requirements by fulfilling its conditions, maintaining its effectiveness, and continuing continuous improvement activities—while taking into account legal requirements, standard requirements, contractual terms and obligations, and customer requirements, as well as considering current and potential risks—and has communicated this policy to relevant parties. In this regard, the company is making progress by continuously reviewing and updating its personnel, systems, information and assets, personal data inventories, and applicable business rules, along with measurable and achievable objectives, and by ensuring business continuity within the scope of these objectives.

Within the scope of our core objectives for Information Security:

- ✓ To protect our company's reliability and reputation,
- ✓ Ensuring that our information security management system is documented, certified, and continuously improved to meet the requirements of the ISO 27001:2013 standard,
- ✓ To increase information security awareness among all our employees,
- ✓ Within the framework of the strategic business plan and risk management, to identify, determine, assess, and control relevant risks to establish and ensure the continuity of the information security management system,
- ✓ To ensure compliance with all applicable laws, regulations, and contracts related to information security,
- ✓ To systematically manage risks related to information assets,
- ✓ To ensure the confidentiality and integrity of all stakeholder information we receive and are obligated to protect as a result of our company, business relationships, or commercial activities,
- ✓ To prevent the unlawful processing of and access to personal data and special-category personal data contained in personal data inventories and processed within the scope of the Company's activities,
- ✓ To ensure the storage of personal data and special category personal data in compliance with the provisions of the Personal Data Protection Law (KVKK),
- ✓ We are committed to working diligently to serve as a model organization in the industry in terms of information security.

5.2.1 Review and Improvement

The Quality Department and the Information Technology Department are responsible for reviewing the suitability, adequacy, and effectiveness of Arzum's information security management system. Specifically, within the scope of information system controls, the Information Technology Department oversees the clear definition of process owners, roles, activities, and responsibilities for each control process; the periodic definition of control processes; the clear definition of the objectives and purposes of each control process; and the measurability of their performance. Under the leadership of the Information Technology Department, independent reviews of all information security systems are conducted as necessary, and the results are reported to management and retained.

5.2.2 Authority and Responsibility

With regard to the establishment, operation, management, and use of information systems—and to ensure the confidentiality, integrity, and, when necessary, availability of information—senior management establishes mechanisms to ensure, at a minimum, the following activities are carried out:

- Annual review of information security policies and all responsibilities, and approval of updates as necessary,
- Implementing risk management that involves identifying potential risks related to information systems and processes, along with their impacts, and defining activities to mitigate such risks,
- Monitoring and annually evaluating incidents related to information security breaches,
- Providing the necessary resources to conduct annual initiatives and training aimed at raising all employees' awareness of information security and the protection of personal data,
- Ensuring that the processes established for the management of risks related to information systems are monitored and tracked so that they function effectively,
- Appointing an information systems security officer who is responsible for ensuring compliance with and monitoring processes and procedures related to information systems security, who reports to senior management on risks related to information systems security and their management, and who possesses sufficient technical knowledge and experience,
- Reviewing the business continuity plan prepared by the Information Technology Department to ensure the continuity of all critical business processes according to risk priorities, and determining the acceptable downtime and maximum acceptable data loss for critical business processes in the plan.

6. SCOPE

This policy applies to all employees using Arzum's information and business systems, as well as consultants working on behalf of the Company and relevant parties.

7. SANCTIONS

Any violation of this document will result in action taken in accordance with **the Disciplinary Regulations**.

8. EFFECTIVE DATE

This Policy was adopted and entered into force by Board of Directors Resolution No. 2022/018 dated June 15, 2022; any amendments to this Policy are subject to the approval of the Board of Directors.