



## Our Information Security Policy

This Information Security Policy has been established by the management of ARY Holding for implementation at Gemlik Gübre Sanayii A.Ş. By implementing this policy, ARY Holding management undertakes and declares that it will provide the necessary resources and procedures required to fulfill the following fundamental principles essential for ensuring the confidentiality, integrity, and availability of services within the scope of the Information Security Management System (ISMS).

The information security policy is not only the responsibility of the IT department but also of all employees working at Gemlik Gübre Sanayii A.Ş. Each employee is responsible for protecting the organization's information assets by implementing the procedures defined within the scope of the ISMS.

- a) Any intentional or unintentional unauthorized use, modification, disclosure, or damage to all information assets within scope will be prevented.
- b) Information obtained from customers in relation to services within the scope of the ISMS will be ensured to be secure, accurate, and complete.
- c) Information collected from customers for business purposes will be used solely for those purposes and will not be shared with third parties under any circumstances.
- d) Necessary resources will be provided to meet customers' business requirements through infrastructure, processes, and personnel in compliance with applicable legal regulations.
- e) At Gemlik Gübre Sanayii A.Ş., the confidentiality of corporate and personal information, as well as information belonging to third parties, whether produced or used, will be ensured under all circumstances. In this context, personal data and classified information will be processed and stored in compliance with the laws and regulations of the countries in which operations are conducted, with the necessary technical and administrative safeguards applied without compromise.
- f) Access control will be provided in accordance with the "need-to-know" principle, and information will be protected against unauthorized access.
- g) Risks will be reduced to acceptable levels through the design, implementation, and maintenance of the ISMS.
- h) Information will be protected in all circumstances, regardless of its form of use, including electronic communication, sharing with third parties, research use, or storage in physical or electronic media.
- i) Information assets will be classified according to their confidentiality levels, and their confidentiality and integrity will be ensured through proper implementation by employees.
- j) Gemlik Gübre Sanayii A.Ş. will act in full compliance with all applicable laws, regulations, directives, and contractual requirements.
- k) To protect service processes from the effects of major disasters and operational failures, business continuity management will be implemented and a business continuity plan will be established. The continuity of the plan will be maintained and regularly tested.
- l) Training to increase personnel awareness of information security and to encourage their contribution to system effectiveness will be provided regularly to all employees and newly hired staff. Training is mandatory.
- m) All actual or suspected information security breaches will be reported, and preventive measures will be taken to avoid recurrence.
- n) In personnel work areas, in accordance with the "Clean Screen / Clean Desk" principles, measures will be taken to prevent information—other than "Unclassified" information—from being viewed by unauthorized persons.



o) In personnel work areas, in accordance with the “Clean Screen / Clean Desk” principles, measures will be taken to prevent information—other than “Unclassified” information—from being viewed by unauthorized persons.

Gemlik Gübre Sanayii A.Ş. aims to comply with ISO/IEC 27001:2022 as the overarching standard for the implementation of the ISMS and with ISO/IEC 27002:2022 as technical guidance for information security controls. In addition, ARY Holding aims to implement ISO/IEC 27701:2025 (PIMS) for personal data protection.

p) The existing strategic business plan and risk management framework of Gemlik Gübre Sanayii A.Ş. provide the function of identifying, defining, evaluating, and controlling risks necessary for establishing and maintaining the ISMS.

q) Risk assessment, the Statement of Applicability, and the risk treatment plan describe how information-related risks are controlled. The Information Security Manager and Information Systems Manager are responsible for managing and maintaining the risk treatment plan. Additional risk assessments may be conducted, when necessary, to determine appropriate controls for specific risks.

r) In particular, business continuity and emergency plans, data backup operational documentation, protection against viruses and cyber attacks, access control systems, and information security incident reporting are essential elements of this policy.

All employees of Gemlik Gübre Sanayii A.Ş. and specified external parties defined within the ISMS are expected to comply with this policy and the ISMS that implements it. All personnel and designated external parties will receive appropriate training.

The ISMS is subject to continuous and systematic evaluation and improvement.

To support the ISMS framework and periodically review this security policy, ARY Holding management has established an Information Security Committee, including the Information Security Manager and other relevant managers.

This policy will be reviewed at least annually in response to changes in the risk assessment or risk treatment plan.

Ercüment TÜRKER  
COO