OUR INFORMATION SECURITY POLICY

This Information Security Policy has been established by the management of ARY Holding for implementation at ARY Holding and its affiliated entities. By implementing this policy, ARY Holding's management undertakes to provide the necessary resources and procedures to ensure the confidentiality, integrity and availability of services within the scope of the Information Security Management System (ISMS) and to meet the following fundamental principles.

The information security policy is the responsibility of not only the IT department but also all employees working within ARY Holding and its affiliated companies. Each employee is obliged to protect the organisation's information assets by applying the procedures established within the scope of the Information Security Management System (ISMS).

a) The unauthorized use, alteration, disclosure or damage of all information assets within the scope will be prevented, whether deliberate or accidental.
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 for customers' business purposes will be used only for those purposes and will not be disclosed to third parties.
d) Necessary resources will be provided to meet the business requirements of its customers with infrastructure, processes and personnel in accordance with the requirements of legal regulations.
e) The confidentiality of corporate and personal information or information produced and/or used by ARY Holding and its affiliated institutions, regardless of whether it belongs to third parties, will be guaranteed in all cases. In this context, no compromise can be made on the processing and storage of personal data and confidentiality classified data by taking the necessary technical and administrative measures in accordance with the laws and regulations of the countries to which they operate.
f) Access control will be provided in accordance with the "need to know" principle and information will be protected from unauthorized access.
g) Risks will be reduced to acceptable levels through the design, implementation and maintenance of the ISMS.
h) Knowledge; It will be protected in all cases, regardless of the forms of use such as electronic communication of information, sharing with third parties, use for research purposes, storage in physical or electronic media.
i) Information assets will be defined with their confidentiality degrees and their confidentiality and integrity will be ensured by the application of the employees.
j) ARY Holding and its affiliated companies will comply with the requirements established by the laws, regulations, circulars and contracts of the country.
k) Business continuity management will be implemented to protect services provided to customers from the effects of major disasters and operational failures. A business continuity plan will be established, maintained and tested.
l) Training to raise information security awareness and to encourage staff contribution to the system will be provided regularly to all employees and newly hired personnel. Training is mandatory.

m) All actual or suspected information security violations will be reported, and measures will be taken to prevent recurrence.
n) In employees' work areas, in accordance with 'Clean Screen / Clean Desk' principles, measures will be taken to prevent anyone from seeing information other than 'Unclassified' material.
o) ARY Holding aims to be adapted to ISO 27001:2022 as the overarching ISMS standard and applies ISO 27002:2022 (ISMS) as technical guidance for implementation. In addition, ARY Holding implements ISO 27701:2025 (PIMS) for personal data protection.
p) ARY Holding's current strategic business plan and risk management framework serve to identify, define, evaluate and control the risks relevant to establishing and maintaining the ISMS.
q) The risk assessment, applicability statement, and risk response plan describe how information-related risks are controlled. The Information Security Manager and Information Systems Manager are responsible for the management and maintenance of the risk response plan. Additional risk assessments may be conducted, if necessary, to determine appropriate controls for specific risks.
r) Specifically, business continuity and emergency response plans, data backup procedures, protection against malware and cyber attacks, access control systems, and information security incident reporting are fundamental to this policy.

All employees of ARY Holding and its affiliated entities, as well as certain external parties defined in the ISMS, are required to comply with this policy and the ISMS that implements it. All staff and specified external parties will receive appropriate training.

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

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

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

APPROVERS

Author	Controller	Approver	Approver
Sefa SAKARYA	Bahadır KARA	Bülent GÜNEY	Ercüment TÜRKER
IT Governance Senior Specialist	IT Governance Manager	CIO	COO