

OUR ARTIFICIAL INTELLIGENCE POLICY

The purpose of this policy is to set out the overarching framework for the approach adopted by ARY Holding and its affiliated organisations to the use of artificial intelligence (AI) tools.

The safe and responsible use of AI is the responsibility not only of the Information Technology department and the teams responsible for the technical management of AI systems, but also of all employees, managers, interns, consultants and relevant third parties within the scope of this policy who work for or with ARY Holding and its affiliated organisations. Each user must comply with this policy and all other relevant corporate policies, procedures, standards and instructions when using AI systems in the course of their duties.

AI systems must be used where there is a business need, using tools approved by the organisation, only to the extent necessary and in accordance with the following core principles.

- a) AI must be used ethically, safely and responsibly, in compliance with applicable legislation and organisational rules.
- b) The use of AI must comply with the Turkish Personal Data Protection Law No. 6698 (KVKK) and international data protection regulations.
- c) The fact that an AI system can be accessed via the internet, a web address, an application, a plug-in or any other technical means does not mean that ARY Holding has approved it for corporate use.
- d) AI systems in use are documented so that their intended purpose, system owner, data sources, tools and infrastructure, risk level, potential impacts, and technical and organisational controls can be assessed and, where necessary, monitored.
- e) ARY Holding defines duties, authorities and responsibilities for AI management. Roles responsible for the use of AI systems, the associated risks and the implementation of relevant controls are identified.
- f) AI must be used only when required for business purposes. Unnecessary queries, repetition, conversations and use outside the intended purpose must be avoided. Users must express their requests clearly to avoid wasting tokens, quotas, licences and computing resources, and incurring unnecessary costs.
- g) ARY Holding establishes appropriate performance indicators and targets to measure the effectiveness of the AI management system and progress towards its objectives.
- h) The use of AI systems that have not been approved for corporate use is prohibited.

- i) Third-party providers of AI services are subject to the organisation's supplier and information security assessment processes.

Where necessary, the following matters are assessed as a minimum:

- Data processing and retention terms;
- Data location;
- Use of customer data for model training;
- Subcontractors;
- Security controls;
- KVKK/GDPR compliance;
- Data deletion capabilities;
- Incident notification obligations;
- Service continuity;
- Intellectual property and licensing terms;
- Management of model and service changes.

- j) ARY Holding identifies and manages the human resources, technical infrastructure, data sources, tools, knowledge and competencies needed to manage AI systems safely and responsibly. Employees who use AI receive awareness training and other training appropriate to their duties and responsibilities.
- k) Confidential information, personal data, special category personal data and sensitive organisational information must not be uploaded to AI systems that have not been explicitly approved by the organisation. When using approved systems, users must comply with information classification, access authorisation, data protection and relevant security rules.
- l) Paid, licensed or corporate AI accounts provided by ARY Holding must be used exclusively for organisational business. These accounts must not be used for personal conversations, private projects, secondary employment or activities outside the organisation.
- m) Paid AI licences are allocated only to users with a business need. Licences that are unused or no longer required for business purposes are withdrawn and, where necessary, reallocated to other users.
- n) No AI-generated output may be accepted as accurate without the necessary checks. AI is a support tool; ultimate responsibility rests with the person using the AI system and the person approving the output. Copyright, licensing requirements and third-party rights must also be considered when using outputs.
- o) AI outputs alone are not accepted as final decisions, particularly in high-impact or critical business processes. Authorised human oversight and, where necessary, final human approval are ensured in recruitment, employee appraisal, pay and bonuses, disciplinary action, dismissal, financial decisions, legal decisions, customer assessments and similar

high-impact processes. Where an AI output is considered inaccurate, misleading or inappropriate, it must not be used and the necessary correction must be made.

- p) Where AI systems may have significant impacts on interested parties, their intended purpose, the role of AI in the process and any necessary information are disclosed to those parties in accordance with legislation, contractual obligations, business requirements and the risk assessment.
- q) The necessary records of usage, operations, errors, security incidents, changes and model/system versions are maintained in line with the intended purpose and risk level of each AI system.
- r) AI systems are managed throughout their life cycle.

Appropriate controls are applied at each stage: Request → Assessment → Risk/Impact Assessment → Approval → Procurement/Development → Testing → Live Use → Monitoring → Change → Decommissioning.

AI systems are reassessed where necessary following significant changes to the model, data, integrations, intended purpose or access.

AI systems whose intended purpose no longer applies are decommissioned in a controlled manner, and the associated data is managed in accordance with the organisation's data retention and disposal rules.

- s) Source code, system configurations, access credentials, technical documents and similar technical information must not be transferred to AI systems in an uncontrolled manner. The organisation's information security and authorisation rules must be followed when using this information.
- t) AI agents, plug-ins and integrations that can access files on a computer, source code, terminals, browsers or corporate systems must not be used without organisational approval. AI systems must not be granted excessive access or permissions to perform operations. They are granted only the minimum permissions necessary to meet the business need.
- u) There must be a genuine business need to use a new AI tool or purchase a paid AI licence. No new AI tool or licence may be brought into use without assessing the need, benefits, costs and security risks.
- v) Any data leak, incorrect data sharing, unauthorised use, security breach or serious error identified during AI use must be reported to the relevant departments without delay.
- w) ARY Holding manages AI use through the necessary technical and administrative controls. It aims to ensure that AI use complies with the ISO/IEC 42001 Artificial Intelligence Management System (AIMS) standard.

- x) The conformity of the Artificial Intelligence Management System with policies, procedures and relevant ISO/IEC 42001 requirements is reviewed at planned intervals through internal audits or independent assessments.
- y) Management reviews the performance, risks, significant incidents, objectives, audit results and improvement needs of the Artificial Intelligence Management System at planned intervals.
- z) Cause analysis, corrective action and, where necessary, preventive or improvement actions are undertaken to address identified nonconformities, incidents and control deficiencies relating to AI use.

All employees of ARY Holding and its affiliated organisations, together with relevant external parties within scope, are expected to comply with this policy. Any failure to comply is assessed in accordance with applicable legislation, employment contracts and ARY Holding's relevant policies and procedures. Depending on the nature of the breach, AI access or licences may be restricted or revoked, a nonconformity record may be raised and the Disciplinary Procedure may be applied.

This policy is reviewed whenever there is a significant change in AI use, risks, legislation, technology or organisational needs, and at least annually in all cases.

APPROVAL AUTHORITIES

Prepared by	Reviewed by	Approved by	Approved by	Approved by	Approved by
Sefa SAKARYA	Tülay BİLGİN	Bahadır KARA	Mete Can TÜRKEN	Bülent GÜNEY	Ercüment TÜRKER
Senior IT Governance Specialist	Corporate Governance & Sustainability Director	IT Governance Manager	Software Development & Business Intelligence Director	CIO	COO