

The background of the page is a photograph of a modern building with a curved glass facade, reflecting the sky and surrounding environment. The image is overlaid with a dark blue geometric shape in the top left corner and a red diagonal line running from the top left towards the center. The text 'RESPONSIBLE ARTIFICIAL INTELLIGENCE POLICY' is written in large, white, sans-serif capital letters across the middle of the image.

RESPONSIBLE ARTIFICIAL INTELLIGENCE POLICY

DCS

Responsible Artificial Intelligence Policy

1 Purpose

This Responsible Artificial Intelligence Policy ("Policy") sets out the fundamental principles and corporate governance approach governing the safe, ethical, responsible and legally compliant development, use and management of artificial intelligence ("AI") and, in particular, generative artificial intelligence ("GenAI") technologies within the Company.

The primary purpose of the Policy is to leverage the speed and efficiency offered by artificial intelligence technologies while ensuring the protection of Company data, trade secrets, personal data, intellectual property rights and corporate reputation; and to establish a corporate AI governance framework based on human oversight, accountability, transparency, security and a risk-based approach throughout the AI lifecycle.

Within this framework, the aim is to apply the technical, legal, ethical and organisational governance principles concerning artificial intelligence technologies throughout their lifecycle through a holistic approach.

The development, use and management of AI technologies shall be based on respect for human rights, ethical principles, information security, protection of personal data and compliance with applicable legislation. In this regard, European Union regulations, principle decisions and guidelines issued by the Personal Data Protection Board, and relevant national and international legislation, standards and good practices shall be taken into account.

Taking into account the approach set out by the Personal Data Protection Board, DCS considers that completely prohibiting the use of artificial intelligence technologies is not a realistic method and may encourage uncontrolled use ("Shadow AI").

Accordingly, rather than adopting a prohibitive approach, DCS adopts a Responsible Artificial Intelligence approach based on the principles of guidance, balance, awareness, human oversight and accountability.

2 Scope

This Policy is binding on all employees, managers, interns, consultants, external contractors, suppliers and other third parties acting on behalf of the Company, including members of the Board of Directors, who access the Company's information systems or process Company data.

This Policy covers all artificial intelligence systems, AI-enabled applications and related processes developed, procured, used or managed for business purposes, irrespective of whether such artificial intelligence systems or AI-enabled applications have been developed within the Company, procured from third parties or made available as a publicly accessible service.

The processes, control mechanisms, operational rules and implementation principles concerning the application of the principles and governance requirements set out in this Policy are regulated under the **Artificial Intelligence Use Procedure**.

3 Definitions

Artificial Intelligence (AI): Machine-based systems capable of operating with varying levels of autonomy and generating outputs such as predictions, content, recommendations or decisions based on the inputs they receive.

Generative Artificial Intelligence (GenAI): Artificial intelligence systems trained on large-scale datasets that can generate new content such as text, images, audio, video or software code in response to a user-provided prompt.

Artificial Intelligence Lifecycle: All processes including the planning, development, procurement, testing, use, monitoring, updating and decommissioning of artificial intelligence systems.

Responsible Artificial Intelligence: The development, use and management of artificial intelligence technologies throughout their lifecycle in accordance with ethical principles, human rights, information security, personal data protection, transparency, accountability and applicable legislation.

Artificial Intelligence Governance: The corporate governance approach that establishes the roles, responsibilities, processes, control mechanisms and decision-making structures relating to the development, use and management of artificial intelligence systems.

Personal Data / Special Categories of Personal Data: Any information relating to an identified or identifiable natural person, and special categories of personal data, as defined under Law No. 6698 on the Protection of Personal Data.

Artificial Intelligence Committee (AIC): The corporate committee established within the Company to carry out decision-making, assessment and coordination activities relating to responsible artificial intelligence governance.

AI Officer / Contact Person: The person or persons appointed to coordinate the implementation of responsible artificial intelligence governance within the Company.

4 Policy Statements

DCS regards artificial intelligence technologies not merely as technologies that deliver operational efficiency, but as a strategic capability that strengthens its corporate expertise, builds trust with its customers, supports ethical values, accelerates sustainable digital transformation and creates long-term sustainable value.

DCS considers Responsible Artificial Intelligence governance an integral part of its corporate governance approach, ethical culture and sustainable digital transformation approach.

Senior Management leads responsible artificial intelligence governance and supports the effective implementation of this Policy in line with the Company's corporate values, Business Ethics Principles and Code of Conduct, and other relevant policies and regulations.

The following fundamental principles shall apply to the development, use and management of artificial intelligence technologies within the Company.

4.1 Human Oversight Principle

Artificial intelligence (AI) is not an autonomous decision-maker that replaces human judgement and responsibility for decision-making; it is a tool that supports decision-making processes. Therefore, outputs generated by AI should not be used on their own for the purpose of making decisions.

In particular, AI outputs that may have a significant legal, financial or operational impact, or a significant impact on individuals, should be critically reviewed, verified and, where necessary, approved by a competent and responsible person before use. The level of review and verification should be proportionate to the risk associated with the decision.

DCS adopts a human-centred approach under which artificial intelligence technologies are developed, used and managed in a manner that supports human expertise and judgement and is based on effective human oversight. Human oversight shall be determined in accordance with the intended purpose, risk level and impact on the relevant process and, where necessary, supported by a Human-in-the-Loop approach.

4.2 Accountability Principle

Ultimate responsibility for any decision or action based on AI output rests with the employee using the AI, not with the AI system. Artificial intelligence systems do not eliminate or transfer human responsibility.

Artificial intelligence outputs should not be used, without the necessary verification, as the sole basis for a decision or action; decisions must be capable of being justified, traceable and accountable.

4.3 Transparency Principle

DCS adopts transparency as a fundamental principle in the development, use and management of artificial intelligence technologies. In artificial intelligence systems that interact directly with natural persons, it shall be clearly, understandably and appropriately stated that the relevant persons are communicating with an artificial intelligence system.

For content generated or materially altered by artificial intelligence that may create the impression that it is authentic, it shall be appropriately disclosed that the content has been generated or altered by artificial intelligence where required by applicable legislation or where deemed necessary due to the nature of the content.

4.4 Fairness and Non-Discrimination Principle

DCS is committed to the development, use and management of artificial intelligence technologies in a fair, impartial manner that respects human rights. Care shall be taken to ensure that artificial intelligence systems do not result in unfair discrimination based on age, sex, language, religion, belief, ethnic origin, disability status or similar characteristics.

Risks of bias and discrimination that may arise from the use of artificial intelligence systems shall be taken into account; human oversight, output verification and risk-based control mechanisms shall be applied in order to mitigate such risks.

4.5 Security and Privacy Principle

Data protection and information security are fundamental elements that shall be observed throughout the entire lifecycle of artificial intelligence technologies, including their development, selection, use, management and decommissioning.

DCS applies the principles of "Privacy by Design" and "Privacy by Default".

4.6 Data Minimisation and Risk-Based Approach Principle

DCS applies the principles of necessity, proportionality, data minimisation and a risk-based approach when transferring data to artificial intelligence systems. As a rule, personal data, trade secrets and other sensitive information that are not necessary for the business purpose shall not be shared with artificial intelligence systems.

Risks shall be assessed by taking into account the nature, sensitivity and intended use of the data to be transferred to artificial intelligence systems; care shall be taken to ensure the implementation of appropriate technical, administrative and organisational measures.

4.7 Reliability and Accuracy Principle

DCS adopts as a principle the assessment of the accuracy, reliability, consistency and fitness for the intended purpose of outputs obtained from artificial intelligence systems. Artificial intelligence outputs shall not be used, without the necessary verification, as the sole basis for a decision or action.

4.8 Continuous Improvement Principle

DCS regularly reviews and continuously improves its artificial intelligence governance processes, control mechanisms and corporate practices in light of technological developments, changes in legislation, audit results, feedback, good practices and experience gained.

5 | Applicable Legislation and Corporate Documents

DCS bases the development, use and management of artificial intelligence technologies on compliance with applicable national and international legislation, decisions and guidelines of relevant regulatory authorities, international standards, and corporate policies and procedures.

In preparing this Policy, particular consideration has been given to the following regulations, standards and guidelines:

- Law No. 6698 on the Protection of Personal Data, related secondary legislation and decisions of the Personal Data Protection Board;
- The documents "Guideline on Generative Artificial Intelligence and the Protection of Personal Data (in 15 Questions)" and "Use of Generative Artificial Intelligence Tools in Workplaces" published by the Personal Data Protection Authority;
- Customs legislation and regulations concerning foreign trade, trade secrets and professional confidentiality;
- Regulation (EU) 2024/1689 on Artificial Intelligence (EU AI Act) and related regulations;
- The Turkish Commercial Code, intellectual and industrial property legislation and other relevant national regulations;
- The National Artificial Intelligence Strategy and relevant public policies;
- The Artificial Intelligence Use Procedure, Information Security and Data Protection Policy, Personal Data Protection and Processing Policy, Human Rights Policy, Business Ethics Principles and Code of Conduct, Corporate Risk Management Policy, and other relevant policies and procedures.

This Policy shall be implemented together with the corporate policies, procedures and other internal regulations referred to above. In the event of a conflict with other corporate policies or procedures, the provision that provides a higher level of protection for individual rights, information security and the Company's interests shall apply. In cases of doubt, the matter shall be referred to the AI Officer for assessment.

6 | Responsibilities

6.1 Employees

- Act in accordance with this Policy, the Artificial Intelligence Use Procedure, and other relevant Company policies, procedures and internal regulations.
- Use artificial intelligence technologies in an ethical, secure, transparent and responsible manner.
- Do not use outputs obtained from artificial intelligence systems as the sole basis for a decision or action without carrying out the necessary verifications.
- Promptly report identified risks relating to artificial intelligence use, information security incidents, data breaches or uses contrary to this Policy to the AI Officer.
- Comply with the rules on the protection of Company data, personal data and trade secrets.

6.2 Managers

- Support employees in being informed about and complying with this Policy and relevant Company regulations.
- Oversee the use of artificial intelligence within their areas of responsibility to ensure that it is carried out in accordance with this Policy and relevant corporate regulations.
- Support the assessment of identified risks and non-conformities relating to artificial intelligence use and the implementation of necessary corrective actions.
- Encourage employees to use artificial intelligence technologies securely and responsibly.

6.3 AI Officer / Contact Person

- Coordinate the implementation of this Policy and provide guidance to employees.
- Provide support as the first point of contact for questions, opinions and reports relating to artificial intelligence use.
- Support the effective operation of processes relating to artificial intelligence governance.
- Where necessary, submit significant risks, incidents and improvement proposals relating to artificial intelligence use to the AIC.

6.4 Artificial Intelligence Committee (AIC)

- Oversee the Company's responsible artificial intelligence strategy, the implementation of this Policy and the effectiveness of the artificial intelligence governance framework.
- Regularly assess the effectiveness of this Policy and decide on improvements deemed necessary.
- Conduct assessments relating to high-risk artificial intelligence uses and take the necessary decisions.
- Guide strategic decisions and practices relating to artificial intelligence governance.

6.5 Senior Management

- Ensure the establishment and sustainability of the policies, procedures, resources and organisational structure necessary for the effective implementation of responsible artificial intelligence governance.
- Support the implementation of technical, administrative and organisational measures relating to artificial intelligence use.
- Promote training and awareness-raising activities aimed at increasing employee awareness.
- Ensure that processes relating to artificial intelligence use are managed in accordance with applicable legislation and corporate regulations.

7 | Training and Awareness

DCS conducts regular training and awareness activities to support employees in using artificial intelligence technologies in a secure, ethical and responsible manner.

- Participation by all employees in awareness training concerning this Policy, the Artificial Intelligence Use Procedure, data classification, personal data protection, information security and artificial intelligence risks is essential.
- Additional training and information activities shall be carried out in the event of material changes in artificial intelligence technologies, relevant legislation or corporate practices.
- Artificial intelligence awareness training shall be planned by taking into account employees' duties, responsibilities and needs; additional training and awareness activities shall be organised where deemed necessary.

8 | Monitoring and Compliance

DCS monitors and evaluates the implementation of this Policy and compliance with relevant corporate regulations within the framework of applicable legislation, information security, personal data protection and ethical principles, and takes improvement measures where necessary.

Artificial intelligence systems provided by the Company and the related usage records may, within the framework of applicable legislation, be monitored, logged and, where necessary, reviewed for the purposes of ensuring information security, fulfilling legal obligations, and conducting internal control, internal audit, compliance and disciplinary processes.

Monitoring, logging and audit activities shall be carried out with due regard to the protection of personal data, the privacy of private life, the principle of proportionality and the provisions of applicable legislation.

9 | Non-Compliance with the Policy

In the event of conduct contrary to the provisions of this Policy, necessary actions may be taken in accordance with the relevant Company policies and procedures and the Disciplinary Regulation, taking into account the nature, impact and consequences of the breach.

Where acts contrary to legislation are identified, the necessary legal and administrative processes may be initiated against the relevant person or persons under applicable legislation.

10 | Reporting and Protection of Reporting Persons

DCS provides the necessary mechanisms for employees, suppliers and other stakeholders to report concerns relating to breaches of this Policy confidentially and without fear of retaliation. Where employees encounter a practice contrary to this Policy, a non-conformity or a suspicious situation, they are required to report anyone engaging in such conduct, even if that person is their manager or any other superior.

Reports may be submitted to the Ethics and Compliance Function at etik@dcscustoms.com.tr. The AI Officer may also be contacted on matters relating to artificial intelligence use that require technical assessment or guidance.

DCS grants employees the right to submit reports without disclosing their identity and treats anonymous reports with the same seriousness. All reports are assessed confidentially in accordance with the Reporting, Consultation and Non-Retaliation Policy, and measures are taken to protect the reporting person against retaliation.

DCS assesses all reports concerning breaches of this Policy promptly and fairly. Where a breach is identified, appropriate corrective and preventive actions shall be implemented and, where deemed necessary, relevant disciplinary processes shall be initiated.

11 | Review and Revision

From its effective date, this Policy shall be reviewed at least once (1) per year in terms of compliance with local and international legislation and corporate needs.

The review process shall be carried out under the coordination of the AI Officer, with contributions from the Artificial Intelligence Committee (AIC), Information Technologies, Legal Advisers, and the Sustainability and Compliance Directorate.

The Policy shall be updated where necessary in line with technological developments, applicable legislation, international standards, decisions and guidelines of regulatory authorities, and changes occurring in DCS's activities.

Proposals for amendments and revisions to the Policy shall be prepared by the Sustainability and Compliance Directorate following the assessment of the AIC and submitted to the Board of Directors for approval. Amendments and revisions approved by the Board of Directors shall enter into force and be recorded through the document management system.

DCS