RESPONSIBLE ARTIFICIAL INTELLIGENCE POLICY

Zorlu Enerji Elektrik Üretim A.Ş. and its Subsidiaries

Version	Effective Date	Review	Endorsed by
1.0	21.08.2026	As required	Board of Directors

1 Purpose

The purpose of this Policy is to define the ethical principles, governance structure, roles and responsibilities, and control mechanisms that apply to the development, procurement, deployment, use and decommissioning of artificial intelligence (AI) technologies across the operations of Zorlu Enerji Elektrik Üretim A.Ş. and the subsidiaries under its control (together, "Zorlu Enerji" or the "Company").

The Company recognizes that AI offers significant opportunities in the optimization of energy generation and distribution processes, generation forecasting, grid balancing, predictive maintenance, energy efficiency, customer experience and corporate support functions. The Company recognizes that these technologies may create new risks in relation to the protection of personal data, information security, cybersecurity, discrimination, human rights, occupational health and safety, and environmental impact. This Policy is intended to capture those opportunities while managing the associated risks in a systematic manner.

2 Scope

This Policy applies to Zorlu Enerji and all subsidiaries under its control, and to their Board members, executives, all employees, interns, subcontractors and consultants, as well as to business partners and suppliers that develop, provide or operate AI systems on behalf of or for the Company.

The Policy covers all AI systems, including:

- models and algorithms developed in-house;
- AI solutions purchased, licensed or consumed as cloud/SaaS services;

- generative AI (GenAI) and large language model (LLM) based applications and the autonomous agents built on them;
- AI components embedded in operational technology (OT), SCADA, IoT and field equipment;
- AI-enabled decision-support tools used in human resources, procurement, finance, legal, customer relations and corporate communications.

3 Definitions

- AI System: a machine-based system that, for explicit or implicit objectives, infers from the inputs it receives how to generate predictions, recommendations, content or decisions that can influence physical or virtual environments, and that operates with varying levels of autonomy.
- Generative AI (GenAI): AI systems capable of producing text, images, audio, code or synthetic data.
- AI System Owner: the manager accountable for the business purpose, appropriateness and Policy compliance of a given AI system.
- High-Risk AI System: an AI system with the potential to materially affect individuals' fundamental rights, health, safety or employment, the operation of critical infrastructure, or the Company's legal obligations.
- Human Oversight: the ability of a competent individual to monitor, validate, override or halt an AI system and its output.
- Model Drift: the degradation of model performance over time as data or operating conditions change.

4 Reference Frameworks

This Policy has been prepared with reference to national legislation, international standards and recognised good-practice frameworks:

- Turkish Personal Data Protection Law No. 6698 (KVKK) and its secondary legislation, and the EU General Data Protection Regulation (GDPR);
- the EU Artificial Intelligence Act (Regulation (EU) 2024/1689);
- the OECD AI Principles and the UNESCO Recommendation on the Ethics of Artificial Intelligence;
- ISO/IEC 42001 AI Management System, ISO/IEC 23894 AI Risk Management and ISO/IEC 27001 Information Security Management System;
- the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0);

- the UN Guiding Principles on Business and Human Rights and the UN Global Compact;
- the Company's Code of Ethics, Information Security Policy, Personal Data Protection and Processing Policy, Human Rights Policy, Environmental Policy and Supplier Code of Conduct.

5 Core Principles

Zorlu Enerji observes the following principles throughout the entire lifecycle of its AI systems.

5.1. Respecting Data Privacy in the Use and Development of AI

The Company treats the protection of personal data as a fundamental obligation in the use and development of AI.

- Personal data processed within AI systems is processed only for lawful, legitimate and explicitly defined purposes, on a valid legal basis under the KVKK and the GDPR.
- Data minimization applies only the minimum data necessary to achieve the purpose is used. Anonymization, pseudonymization and synthetic data methods are preferred wherever feasible.
- Purpose limitation and defined retention periods apply to training datasets containing personal data; at the end of the retention period the data is destroyed by the Technology and Artificial Intelligence General Directorate.
- Confidential information, trade secrets and information containing personal data may not be entered into external generative AI tools that have not been approved by the Company.
- For high-risk AI systems that process personal data, a Data Protection Impact Assessment (DPIA) is carried out by the Technology and Artificial Intelligence General Directorate prior to deployment.
- Channels are maintained through which data subjects may exercise their rights to be informed, to access, rectify and erase their data, and to contest automated decisions.

5.2. Protecting the Cybersecurity of Systems in the Use and Development of AI

AI systems are protected as an integral part of the Company's information security and OT security management systems.

- AI systems are designed on security-by-design and zero-trust principles and are subject to authentication, authorization and role-based access control.
- Controls are implemented against AI-specific threats such as data poisoning, model theft, adversarial inputs, prompt injections, model evasion and output manipulation.
- AI applications capable of affecting critical energy infrastructure undergo security testing and penetration testing before deployment, and segmentation between OT and IT networks is maintained.

- Depending on the risk level and where required, training data, model weights and inference infrastructure are classified as critical information assets and protected through encryption.
- AI-related security incidents are handled, recorded and reported under the Company's Cyber Attack Incident Management Procedure.
- A data security layer is established through data classification and a data loss prevention (DLP) solution.

5.3. Avoiding Potential Bias in the Use and Development of AI

The Company is committed to preventing discriminatory outcomes arising from the use and development of AI.

- Training and validation datasets are assessed for representativeness, data quality and historical bias.
- AI systems affecting individuals are tested before deployment and at regular intervals thereafter as to whether they produce discrimination on grounds including language, race, ethnic origin, gender, age, disability, religion, belief, marital status, sexual orientation and union membership.
- In human resources processes such as recruitment, performance evaluation, promotion and remuneration, AI output may never be determinative on its own; the final decision is always taken within the framework of the applicable authorities and responsibilities of the managers to whom the relevant business unit reports and of the Human Resources Department.
- Corrective action is initiated where bias is identified; where it cannot be remediated, the system concerned is withdrawn from use.
- The participation of teams drawn from different disciplines and profiles in system design and review processes is encouraged.

5.4. Keeping Humans in the Loop for Critical Decisions and Allowing Human Intervention

The Company applies a human-in-the-loop approach to critical decisions.

- No decision affecting individuals' rights, health, safety or employment, the operation of critical infrastructure, environmental outcomes or material financial results may be taken on a fully automated basis.
- A human overseer with the necessary competence and authority is designated for every AI system.
- The overseer has the authority to validate, disregard or override the system's output and to halt the system where necessary; to this end, all critical systems incorporate an emergency stop (kill-switch) mechanism.
- Awareness training is provided to counter automation bias; overseers are under a duty to question system output.

- Human interventions and overrides are logged and kept auditable.

5.5. Ensuring Transparency of AI Systems and Explainability of AI-Generated Results and Decisions

The Company is committed to transparency regarding the operation of its AI systems and the results they produce.

- Stakeholders are clearly informed when they are interacting with an AI system; AI-based conversational and support channels disclose their nature explicitly.
- Content generated by generative AI and shared with external stakeholders is appropriately labelled or marked.
- For decisions affecting individuals, the principal grounds and variables underlying the decision must be explainable in clear language; models whose outputs cannot be explained may not be used for such decisions.
- Model cards, data sources, assumptions, known limitations and performance metrics are documented and kept up to date.
- The Company discloses its AI approach, its AI governance and its material AI applications publicly through its annual report and sustainability report.

5.6. Establishing Clear Accountability for Outcomes Produced by AI Models and Tools

A clear chain of accountability is defined for the outcomes produced by AI models and tools.

- Responsibility for an outcome produced by an AI system rests with the Company and the designated AI System Owner, never with the system itself.
- Ownership, decision authority, oversight responsibility and escalation routes are recorded in the AI Inventory for every AI system.
- Data sources, model versions, material parameter changes, test results and human approvals are logged so as to ensure traceability.
- Remediation, redress and grievance mechanisms are maintained for adverse impacts arising from AI.
- Audit activities relating to AI governance are included within the audit scope where the relevant Senior Management and the Board of Directors consider it necessary, in line with the independent risk assessment and annual audit planning process of the Internal Audit, Control and Risk Management Department.

5.7. Defining Clear Boundaries for What AI Can and Cannot Do

The Company explicitly defines the purposes for which AI may and may not be used.

- Permitted, approval-dependent and prohibited use cases are listed in the Acceptable Use Rules issued under this Policy (Annex 1) and are updated regularly.
- The use of unapproved AI tools with Company data ("shadow AI") is prohibited; new tools are adopted only with the approval of the Technology and Artificial Intelligence General Directorate.
- AI output may not be relied upon as the sole source for legal opinions, financial statements, regulatory compliance assessments, occupational health and safety decisions or statutory reporting; verification is mandatory.
- The systems accessible to autonomous agents, the types of transactions they may execute, and the applicable transaction limits are defined in advance; such agents may not be granted authority to execute financial transactions or to enter into contracts.
- Where these boundaries are exceeded, the Internal Audit, Control and Risk Management General Directorate carries out the necessary investigation in respect of matters involving a breach in accordance with the Zorlu Holding Code of Ethics, submits its findings to the Ethics Committees for decision and follows up on the resulting actions.
- Where the boundaries defined in this Policy and the related procedures are exceeded, an investigation is carried out considering the nature and impact of the incident, whether it was intentional and whether it has recurred. Where the outcome of the investigation so requires, sanctions may be applied under the Company's relevant policies, procedures and ethical principles.

5.8. Requiring Own and Third-Party AI Data Centres and Models to Have a Low Ecological Footprint

As an energy company, Zorlu Enerji regards the management of the environmental footprint of AI as an integral part of its net-zero commitment.

- The Company's own data centers and IT infrastructure, together with third-party data centers and models used on the Company's behalf, are expected to have a low environmental footprint.
- Energy efficiency (PUE), water usage effectiveness (WUE), share of renewable energy use and hardware lifecycle management are applied as assessment criteria in this respect.
- In the selection of cloud and AI service providers, renewable energy use, greenhouse gas reduction targets and emissions transparency form part of the pre-contract assessment criteria, and providers are required to disclose consumption and emissions data.
- The smallest model fit for purpose is preferred; unnecessary training and inference workloads are avoided, and efficiency techniques such as model distillation, quantization and caching are evaluated.

- Energy consumption attributable to AI and the associated greenhouse gas emissions are monitored; a methodology is developed for their inclusion in the Company's Scope 2 and Scope 3 emissions inventory, and they are incorporated into the inventory as that methodology matures.
- The environmental cost of AI and the efficiency gains it delivers are assessed together when evaluating new applications.

5.9. Not Using or Deploying Prohibited AI Systems

Zorlu Enerji does not develop, procure, deploy or use the practices prohibited under the EU Artificial Intelligence Act. Accordingly, the Company:

- does not use AI systems that deploy subliminal, manipulative or deceptive techniques to distort behavior in a manner that may cause harm;
- does not use AI systems that exploit vulnerabilities arising from age, disability, socioeconomic circumstances or other conditions of vulnerability;
- does not use social scoring systems that lead to unjustified or disproportionate treatment based on social behavior or personal characteristics;
- does not engage in unauthorized or unlawful biometric surveillance, real-time remote biometric identification in publicly accessible spaces, or the untargeted scraping of facial images from the internet;
- does not use systems that infer sensitive categories such as race, political opinions, union membership, religion or belief, or sexual life from biometric data;
- does not use emotion recognition systems intended to infer the emotional state of employees in the workplace;
- does not use systems that seek to predict the risk of criminal offending solely based on profiling or personality traits.

6 Roles and Responsibilities for Accountability

This Policy is approved by the Board of Directors of Zorlu Enerji. The Technology and Artificial Intelligence General Directorate is responsible for publishing and updating the Policy and for coordinating its implementation. The relevant business units are responsible for the use of AI tools within their own processes and for verifying the outputs obtained; in decisions taken with AI support, ultimate responsibility rests in all cases with the authorized person taking the decision. The Policy is reviewed where the need arises.

7 Lifecycle Management and Risk Assessment

- As a matter of principle, all Corporate AI systems used within the Company are recorded in a central AI Inventory.
- Each system is classified as critical, high, medium or low risk. The risk level determines the scope of the controls applied.
- An AI Impact Assessment is carried out before the deployment of high-risk systems, addressing fundamental rights, data protection, security, bias and environmental impact together.
- Following deployment, accuracy, model drift, error rates and user feedback are monitored on a regular basis; where defined thresholds are exceeded, use of the system is reviewed and, where necessary, the system is suspended.
- AI-related incidents and near misses are recorded and subjected to root cause analysis, and the lessons learned (the improvement areas or corrective/preventive actions identified as a result of the analysis) are shared.

8 Third-Party and Supplier Management

- Suppliers providing AI products and services are assessed against the principles of this Policy during selection.
- Contracts include provisions on data use and retention, the exclusion of Company data from the training of provider models, security requirements, bias testing, explainability, incident notification, audit rights and environmental performance transparency.
- Suppliers are required to comply with the Company's Supplier Code of Conduct. In the event of non-compliance, the relevant contractual provisions are invoked.
- The use of third-party models does not diminish the Company's own responsibility under this Policy.

9 Training and Awareness

Regular training on responsible AI use, data privacy, security and ethics is provided to all employees. Advanced, role-specific training programmes are delivered to employees who develop, procure or oversee AI systems and to designated human overseers. AI literacy forms part of the Company's competency development programmes.

10 Reporting of Breaches and Sanctions

Any practice believed to be contrary to this Policy may be reported through the Company's Ethics Line and other reporting channels, without giving a name where preferred. Retaliation against those who make a report is strictly prohibited. Breaches of this Policy are assessed under the Company's Code of Ethics and its related policies and procedures; depending on the nature and impact of the breach, appropriate measures and sanctions may be applied.

11 Monitoring, Measurement and Reporting

The Technology and Artificial Intelligence General Directorate monitors performance indicators relating to the implementation of this Policy — including the number of systems recorded in the inventory, the completion rate of impact assessments, training completion rates, the number of reported incidents, and the energy consumption and associated emissions of AI infrastructure — and reports to the Board of Directors at least once a year. The Company discloses developments in its AI governance publicly through its annual report and sustainability report.

REVIEW and ENDORSEMENT

This Policy has been reviewed and endorsed by the Board of Directors of Zorlu Enerji Elektrik Üretim A.Ş.

Reviewed by	Signature
Chief Information Officer — Önder KAPLANCIK **Sector President — Elif YENER**	

Endorsed by	Signature
Deputy Chairman of the Board — Betül Ebru Edin Board of Directors of Zorlu Enerji Elektrik Üretim A.Ş. | Date of Endorsement: [21.08.2026]	

Annex 1 Acceptable Use Rules

- AI is used not to replace human judgement, but to improve decision quality, efficiency and safety.
- Users are responsible for the accuracy and appropriateness of any output they produce with AI support, as if they had produced that output themselves.

1. Acceptable Areas of Use

- Drafting, summarizing, translating and editing documents.
- Software development, code review and testing support.
- Data analysis, predictive maintenance, generation/consumption forecasting and energy market analytics (for decision-support purposes).
- Access to internal knowledge, training and research activities.
- Corporate data is processed only in tools approved by the Company or covered by a corporate license; corporate data may not be entered into tools accessed through personal accounts.

2. Unacceptable Uses

The following practices — particularly those prohibited under the EU Artificial Intelligence Act — may under no circumstances be developed, procured or used within the Company:

- scoring of individuals or groups based on their social behavior or personal characteristics (social scoring);
- steering behavior through subliminal or manipulative techniques or techniques that exploit individuals' vulnerabilities;
- systems intended for emotion recognition in the workplace;
- classification systems intended to infer sensitive personal characteristics from biometric data;
- real-time remote biometric identification in publicly accessible spaces and the creation of databases through the untargeted scraping of facial images;
- prediction of the likelihood of an individual committing a criminal offence through profiling;
- production of content that misleadingly represents real people or organizations (deepfakes and similar);
- basing sustainability, financial or operational disclosures on unverified AI output;
- uses that give rise to discrimination or that infringe copyright or third-party rights.

3. Data Privacy and Protection of Personal Data

- Trade secrets, confidential contractual information, security configurations and similar sensitive information may not be entered into unapproved tools.
- Personal data is processed under Law No. 6698 and the Company's Personal Data Protection Policy; anonymization and the data minimization principle are applied wherever feasible.
- The use of customer, employee or supplier data in model training is subject to the approval of the business unit that owns the data and of the information security function.

4. Human Oversight and Decision Boundaries

- High-impact use refers to uses whose output directly affects the following areas: individuals' rights and employment processes (recruitment, performance, discipline); occupational health and safety; the operational safety of generation facilities or the grid; financial commitments; public disclosures and reporting; and legal obligations.
- In high-impact areas of use, AI is positioned solely as a decision-support tool; the final decision is taken by the authorized person and the rationale for the decision is recorded.
- AI output may not be used on its own as a justification or basis; it is verified by the relevant user before use.
- Systems capable of generating automated actions incorporate a means of intervention allowing the process to be halted or deactivated by a human.

5. Transparency

- Where external stakeholders are interacting with an AI system (chatbot, automated response and similar), this is disclosed to the stakeholder.
- Content used in publicly available material that has been substantially generated by AI is reviewed by a human before publication.
- AI support used in official outputs is recorded so that it can be traced retrospectively where required.

6. Accuracy and Prevention of Bias

- AI models may produce erroneous or fabricated content; figures, references to legislation and source citations may not be used without verification against the primary source.
- Where a discriminatory, biased or culturally inappropriate tendency is identified in an output, the output is not used, and the matter is reported to the relevant unit.

7. Information Security

- Unapproved AI tools, plug-ins or interfaces may not be installed on corporate devices and systems (the "shadow AI" prohibition).

- Credentials, access keys, and network and OT/SCADA configuration information may not be entered into any AI tool.
- Code generated with AI may not be moved into the production environment without passing through the existing secure software development controls.
- Suspicious behavior, data leakage or suspected rule breaches are reported to the information security function.

8. Resource Use

- Users select the most efficient model and tool appropriate to the purpose and avoid unnecessarily repeated large-scale operations.

9. Reporting of Breaches

- Uses contrary to these rules are reported to the user's line manager, to the Technology and Artificial Intelligence General Directorate or through the Company's ethics reporting channels.
- Those who make a report are protected under the Company's relevant policies; breaches are assessed within the framework of the Company's disciplinary processes.