

Dynamic Group

Responsible Artificial Intelligence Policy

Approved by the Board of Directors on October 14, 2026

1. Purpose and Scope

Dynamic Group establishes this Policy to promote the responsible use of artificial intelligence (AI), incorporating individual rights, information security, fairness and environmental sustainability into the development and use of AI.

This Policy applies to AI systems, models and tools developed internally, commissioned, purchased or used by business units across the Group, including AI services provided by third parties. Related matters shall be handled under the Company's existing allocation of responsibilities and management requirements.

2. Policy Principles

1. Respecting data privacy in the use and/or development of AI

The development and use of AI shall respect data privacy. Data shall be processed in accordance with applicable requirements and legitimate purposes, limited to what is necessary, and handled in a manner that protects the rights of data subjects. Personal data shall not be provided to unauthorized AI systems or services.

2. Protecting the cybersecurity of systems in the use and/or development of AI

The development and use of AI shall comply with the Company's existing information security requirements. Relevant systems, data and models shall be protected against unauthorized access, use, disclosure or alteration to maintain the security of systems and information.

3. Avoiding potential bias in the use and/or development of AI

The development and use of AI shall consider potential bias arising from data, models and application practices to avoid discrimination or unjustified differential treatment. Inappropriate outcomes shall be corrected, or the manner of use adjusted, as appropriate to the circumstances.

4. Keeping humans “in the loop” for critical decisions and allowing human intervention

Decisions involving individual rights, operational safety or other critical matters shall retain meaningful human participation and judgment and shall not be left entirely to autonomous AI decision-making. Relevant personnel shall be able to intervene in, correct or stop AI operations and the use of their outcomes when necessary.

5. Ensuring transparency of AI systems and explainability of AI generated results/decisions

Users shall be informed of the purposes, operation and limitations of AI systems. The principal basis for AI generated results/decisions shall be explained in an understandable manner, enabling relevant personnel to recognize AI involvement and appropriately assess its outcomes.

6. Establishing clear accountability for outcomes produced by AI models/tools

Accountability for outcomes produced by AI models/tools shall be clearly assigned to responsible units or personnel according to the application's purpose and the Company's existing allocation of responsibilities. The use of AI shall not relieve relevant personnel of responsibility for assessing, adopting and subsequently handling its outcomes. Responsibility shall not be avoided on the grounds that an outcome was produced by AI.

7. Defining clear boundaries for what the AI can and cannot do

Each AI application shall clearly define its permitted tasks, scope of use and prohibited activities and shall operate within those boundaries. AI shall not be used for unauthorized purposes or beyond its capabilities and limitations of use.

8. Requiring (own/third-party) AI data centers/models to have a low ecological footprint

The Company shall require its own AI data centers/models and those of third parties it uses to have a low ecological footprint. Energy use, water use, greenhouse gas emissions and related resource consumption shall be considered in their development, selection and use to reduce the environmental burden of AI.

9. Not using/deploying AI systems that engage in manipulative behavior, exploitation of vulnerabilities, social scoring or unauthorized biometric surveillance (i.e. prohibited systems as per EU AI Act)

The Company shall not use or deploy AI systems that engage in manipulative behavior, exploit the vulnerabilities of individuals or groups, conduct social scoring or perform unauthorized biometric surveillance. This prohibition shall be incorporated into the selection and use of AI to prevent infringements of individual autonomy, dignity and fundamental rights.

3. Effective Date

This Policy shall take effect upon approval by resolution of the Board of Directors.