
ARTIFICIAL INTELLIGENCE (AI) POLICY

1. OBJECTIVES

1.1 This Policy defines concepts, principles, application, and guidelines to ensure the safe, transparent, and responsible use of Artificial Intelligence at Cemig.

1.2 Cemig recognizes artificial intelligence (AI) as a strategic technology for innovation, improving operational efficiency, expanding competitive capacity, and increasing the quality of services. The adoption of AI aims to ensure positive and sustainable impacts for the Company and society, following ethical and governance principles.

2. CONCEPTS

2.1 **Explainability:** the ability of AI solutions to provide clear explanations about their operation, decisions, and decision-making processes.

2.2 **Artificial intelligence (AI):** a set of technologies that enable the creation of computational systems capable of performing complex tasks, such as learning, reasoning, pattern recognition, decision-making, and natural language processing. AI encompasses different approaches, including machine learning, artificial neural networks, optimization algorithms, computer vision, and processing of large volumes of data.

2.3 **AI solutions:** tools, licenses, or software that use AI to process data and make decisions autonomously or under supervision.

2.4 **Governed AI solutions:** AI solutions approved and classified by the IT area according to their criticality and organizational objectives.

2.5 **Bias:** a systemic tendency or inclination that may occur in AI models due to data selection, algorithm structure, or assumptions embedded in the training of AI solutions, potentially generating distorted predictions or decisions, resulting in prejudice and unfair treatment of individuals or groups, thereby compromising AI fairness.

3. PRINCIPLES

3.1 **Awareness and training:** to continuously promote awareness on the topic, the Company provides learning opportunities regarding the responsible use of AI solutions.

3.2 **Ethics, fairness, and inclusion:** AI solutions must be developed and applied ethically, ensuring that they are fair, inclusive, and free from discrimination and bias, respecting human rights and promoting diversity.

3.3 **Explainability and transparency:** practices must be adopted to maximize, whenever possible and applicable, the transparency and explainability of AI solutions, allowing users to identify AI-generated content and understand the general criteria used in automated decisions.

3.4 **Privacy and data protection:** the development and use of AI solutions must follow strict security and data protection standards, ensuring confidentiality and respect for privacy.

3.5 **Responsibility:** the responsible use of AI Solutions is the duty of each employee, third party, supplier, consultant, and partner of the Company.

3.6 **Traceability and audit:** activities related to the development and use of AI solutions must be properly documented, allowing audits and the traceability of automated decisions.

3.7 **Operational security and cybersecurity:** AI solutions must be implemented with robust security measures to avoid vulnerabilities and ensure that there is no risk to the Company's operations, preventing cyberattacks and unauthorized access.

3.8 **Sustainability and social impact:** the development and use of AI solutions must consider environmental and social impacts, seeking solutions that reduce resource consumption and promote social well-being.

4. APPLICATION AND GUIDELINES

4.1 This Policy applies to all Company activities involving AI solutions, covering employees, third parties, and partners. Senior management, employees, third parties, and partners jointly commit to the implementation and monitoring of this Policy, ensuring that it is communicated, understood, and followed at all levels of the organization.

4.2 AI solutions must be designed to ensure security, ethics, and compliance, being used only for authorized purposes and protected against threats.

4.3 Governance of AI solutions is the responsibility of the Vice Presidency of Information Technology - VPI, which must classify and manage these solutions according to their criticality and organizational objectives. Any and all AI applications must be submitted to VPI evaluation in order to ensure compliance with this Policy.

4.4 In the corporate and operational environment, only governed AI solutions may be used, both on the Company's own servers and on servers with continuous access to corporate data.

4.5 Governed AI solutions must be submitted to periodic tests and reviews to ensure their compliance with the principles established in this Policy.

4.6 Cemig adopts specific processes to ensure the governance and security of governed AI solutions, ensuring adequate levels of protection and compliance:

- a. **Management of governed AI solutions:** VTI is responsible for classifying and managing governed AI solutions, including licenses and software, according to their criticality and alignment with the organizational objectives and principles of this Policy.
- b. **Risk management of governed AI solutions:** AI risk management shall be conducted based on the corporate risk map of the compliance area, allowing the identification and mitigation of vulnerabilities.
- c. **Management of results of governed AI solutions:** responsibility for monitoring the results of governed AI solutions lies with the area to which the solution is linked, ensuring its efficiency and strategic alignment. If the need for adjustments and corrections is identified, VTI must be formally contacted for evaluation and necessary measures.
- d. **Awareness and training:** the people management area, together with the IT and innovation areas, is responsible for implementing awareness and training programs to promote a culture of responsible and ethical AI development and use within the Company.

VICE PRESIDENCY OF INFORMATION TECHNOLOGY - VPI

*** Policy approved by the Board of Directors on 04/16/2026**