

ARTIFICIAL INTELLIGENCE POLICY (AI)

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, enhancing operational efficiency, expanding competitive capacity, and improving service quality. The adoption of AI aims to ensure positive and sustainable impacts for the Company and society, in accordance with ethical and governance principles.

2. CONCEPTS

2.1 **Explainability:** the ability of AI solutions to provide clear explanations about their functioning, 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 large-scale data processing.

2.3 **AI Solutions:** tools, licenses, or software that use Artificial Intelligence 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 leading to distorted predictions or decisions, resulting in prejudice and unfair treatment of individuals or groups, and compromising AI fairness.

3. PRINCIPLES

3.1 **Awareness and training:** to continuously promote awareness of 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 in an ethical manner, ensuring 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, where possible and

applicable, the transparency and explainability of AI solutions, enabling 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 data security and protection standards, ensuring confidentiality and respect for privacy.

3.5 **Accountability:** the responsible use of AI Solutions is the duty of every employee, contractor, supplier, consultant, and partner of the Company.

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

3.7 **Operational security and cybersecurity:** AI solutions must be implemented with robust security measures to prevent vulnerabilities and ensure 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, contractors, and partners. Senior management, employees, contractors, and partners are jointly committed to implementing and monitoring 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, and must only be used for authorized purposes and protected against threats.

4.3 Governance of AI solutions is the responsibility of the Information Technology Vice Presidency (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 for evaluation to ensure compliance with this Policy.

4.4 In corporate and operational environments, only governed AI solutions may be used, whether on proprietary servers or those with continuous access to corporate data.

4.5 Governed AI solutions must undergo periodic testing and review to ensure 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 appropriate levels of protection and compliance:

- a. **Management of governed AI solutions:** the IT area is responsible for classifying and managing governed AI solutions, including licenses and software, according to their criticality and alignment with organizational objectives and the principles of this Policy.
- b. **Risk management of governed AI solutions:** AI risk management will be conducted based on the corporate risk map of the Compliance area, enabling the identification and mitigation of vulnerabilities.
- c. **Gestão de resultados das soluções de IA governadas 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 assigned, ensuring its efficiency and strategic alignment. If adjustments or corrections are required, the IT area must be formally engaged for evaluation and the necessary actions.
- 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 development and the responsible and ethical use of AI within the Company.

VICE PRESIDENCY OF INFORMATION TECHNOLOGY - VPI

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