

---

## ARTIFICIAL INTELLIGENCE (AI) POLICY

### 1. OBJECTIVES

1.1 This Policy establishes concepts, principles, scope, 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, enhancement of operational efficiency, expansion of competitive capacity, and improvement of service quality. The adoption of AI aims to ensure positive and sustainable impacts for the Company and society, in line with ethical and governance principles.

### 2. DEFINITIONS

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

2.2 **Artificial Intelligence (AI):** a set of technologies that enable the creation of computer 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 the 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 department 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 structures, or embedded assumptions in training, 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-raising and training:** to continuously promote awareness-raising 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 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, whenever possible and applicable, to maximize 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 auditability:** 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. SCOPE 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 jointly commit to implementing and monitoring this Policy, ensuring 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 may 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 such solutions according to their criticality and organizational objectives. Any AI application 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 on those with continuous access to corporate data.

4.5 Governed AI solutions must undergo periodic testing and reviews to ensure compliance with the principles established in this Policy.

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

- a. **Governed AI solutions management:** VTI 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. **Governed AI risk management:** AI risk management will be conducted based on the corporate risk map of the compliance department, enabling the identification and mitigation of vulnerabilities.
- c. **Management of governed AI solutions results:** responsibility for monitoring the results of governed AI solutions lies with the department to which the solution is linked, ensuring its efficiency and strategic alignment. If adjustments or corrections are required, VTI must be formally engaged for evaluation and necessary actions.
- d. **Awareness-raising and training:** the people management department, together with the IT and innovation departments, is responsible for implementing awareness-raising and training programs to promote a culture of development and responsible and ethical use of AI within the Company.

## INFORMATION TECHNOLOGY VICE PRESIDENCY – VPI

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