Subject: Corporate Policy for the Ethical Use of Artificial Intelligence	
Identification: Version 2.0	**Use:** Public
Responsible: Gustavo Henrique, AI Governance Specialist	**Issued:** january 2026

1. Nature and Conditions of Use (Template)

This document is an original template created by Gustavo Henrique to guide the development of a ***Corporate Policy for the Ethical Use of Artificial Intelligence***. This document does not, by itself, constitute an active policy of any organization unless it is formally adopted, adapted, and approved by the interested organization.

When institutionalizing this model, the adopting organization must: (I) identify the internal owner of the document; (II) define the applicable governance structure, such as an AI Committee or equivalent body; and (III) publish the official version in its normative repository.

2. Purpose

This document establishes fundamental guidelines, responsibilities, and controls to ensure the responsible use of Artificial Intelligence (AI) systems in the corporate environment, with a focus on ensuring:

2.1. Ethical, responsible, and transparent adoption of AI;
2.2. Compliance with legal and regulatory standards;
2.3. Protection of personal data and sensitive information;
2.4. Minimization of operational, reputational, and regulatory risks;
2.5. Human oversight in automated decision-making.

3. Scope of Application

This policy applies to all employees, managers, interns, service providers, partners, and third parties who:

3.1. Use AI systems on behalf of the adopting organization;
3.2. Develop, implement, or acquire AI solutions;
3.3. Make decisions based on AI within the corporate context.

Included in the scope of AI implementation projects:

3.4. Generative AI systems;
3.5. Decision automation tools;
3.6. Corporate platforms integrated with AI;
3.7. Machine learning models, computer vision, and Natural Language Processing (NLP).

4. Legal and Normative References

This policy template was developed with reference to the following relevant standards and legislation. The adopting organization must assess and ensure applicable compliance:

4.1. Law No. 13,709/2018: General Personal Data Protection Law (LGPD – Brazil);
4.2. Bill No. 2,338/2023: Artificial Intelligence Legal Framework in Brazil, currently under legislative review.
4.3. ISO/IEC 42001:2023: Artificial Intelligence Management System;
4.4. ISO/IEC 27001: Information Security Management;
4.5. OECD Recommendations on Trustworthy Artificial Intelligence (2019).

The adoption of the ISO standards mentioned in this document refers to conceptual and structural alignment with international best practices and does not necessarily imply formal certification, unless explicitly stated by the organization.

Disclaimer**:** The legal terms and titles translated in this document are intended for informational purposes only and do not constitute official translations. For legal accuracy, consult the original versions in Portuguese or the official legal sources.

5. Definitions

For the purposes of this policy, the following definitions apply:

5.1. AI System: A technical system that uses computational algorithms to generate inferences, predictions, or make automated decisions;
5.2. Generative AI: Technology that creates content based on prompts or instructions provided by humans;
5.3. Shadow AI: The use of AI systems without proper institutional authorization or oversight;
5.4. Sensitive Data: Personal data considered sensitive under applicable legislation;
5.5. Algorithmic Bias: Systematic distortions in the outputs generated by AI systems;
5.6. Explainability: The ability to understand and interpret the decisions and outputs generated by

AI systems.

5.7. Adopting Organization (or "Organization"): The entity that adopts and approves this policy, thereby making it an official corporate document.

6. AI Usage Principles

The use of AI within the adopting organization must strictly adhere to the following principles:

6.1. Transparency and explainability;
6.2. Fairness and non-discrimination;
6.3. Security, robustness, and resilience;
6.4. Privacy and data protection;
6.5. Human responsibility;
6.6. Continuous human oversight.

7. Acceptable Use Guidelines (In addition to the ethical principles of this policy)

7.1. Authorization and Control:

- All AI tools or systems must receive prior approval from the governance body designated by the adopting organization (e.g., IT Governance, AI Committee, Information Security, Privacy, or equivalent), in accordance with the internal responsibility matrix;
- The use of unregistered AI solutions is strictly prohibited.

7.2. Data Use:

- The input of personal, sensitive, or confidential data into unauthorized systems is prohibited;
- Data processing must comply with the principles of the LGPD (Brazilian General Data Protection Law).

7.3. Automated Decisions:

- Decisions with significant impact must be reviewed by responsible professionals;
- Affected parties must be informed whenever AI influences decision-making;
- For the purposes of this policy, a distinction is made between fully automated decisions, with no human intervention, and AI-assisted decisions, where the technology supports human judgment;
- Fully automated decisions that affect the interests of data subjects must strictly observe

the rights established under data protection legislation.

7.4. Improper Use:

- It is prohibited to use AI for illegal, discriminatory, deceptive, or manipulative purposes;
- Usage must comply with relevant contracts, licenses, and terms of service.

8. AI Governance Structure

The adopting organization must establish a governance structure for AI, which may be implemented through an AI Governance Committee or an equivalent formally designated body.

Once established, the governance body (AI Governance Committee or equivalent) must be composed, at a minimum, of representatives from Information Technology, Legal, Privacy, and Information Security (or equivalent areas), in accordance with the applicable organizational structure.

8.1. Responsibilities of the AI Governance Body (Committee or Equivalent):

- Assess and classify risks associated with AI systems;
- Approve tools and applications;
- Conduct algorithmic impact assessments for AI systems classified as high risk, especially when involving sensitive personal data, critical decisions, or significant impacts on individuals or the organization;
- Monitor compliance, bias, and incidents;
- Update policies and controls as necessary.

The AI governance body (Committee or equivalent) must meet periodically, maintaining formal records of deliberations, assigning responsibilities, and setting deadlines for implementing decisions. High-risk cases or significant disagreements must be escalated to senior management.

9. Information Security and Privacy

9.1. Data used in AI systems must be anonymized or processed under a valid legal basis;
9.2. Systems must ensure the ability to delete or correct data;
9.3. International data transfers require legal justification;
9.4. Maintaining usage logs for audit purposes is mandatory.

10. Prevention and Mitigation of Shadow AI

10.1. All AI solutions must be listed in the official inventory of the adopting organization;
10.2. Unauthorized use will be monitored and investigated;
10.3. Violations may result in disciplinary measures, in accordance with the internal policies of the adopting organization, and, when applicable, notification to the competent authorities.

11. Responsibilities

11.1. User Responsibilities:

- Use AI in an ethical, legal, and transparent manner;
- Log usage and human interventions;
- Report deviations or incidents.

11.2. IT and Governance Responsibilities:

- Maintain an up-to-date inventory of AI tools;
- Monitor risks and compliance;
- Restrict unauthorized access.

12. Monitoring, Audit, and Control

12.1. Periodic audits must assess risks, bias, and security;
12.2. Evidence must be stored in accordance with the internal policies of the adopting organization;
12.3. Non-compliances must result in corrective action plans.

13. Sanctions and Disciplinary Measures

The following measures are indicative and must be aligned with the code of conduct, disciplinary framework, and internal policies of the adopting organization, subject to formal approval. Non-compliance with this policy may result in:

- Formal warnings;
- Suspension of access;
- Disciplinary actions, including termination of employment;
- Notification to the National Data Protection Authority (ANPD), when the incident involves personal data and meets the legal criteria for mandatory reporting.

14. Final Provisions

This policy was developed by Gustavo Henrique as an original template and may be adopted by other organizations, in whole or in part, provided it is adapted to the internal context, validated by the relevant departments, and formally approved by the responsible governing bodies.

Once institutionalized, the adopting organization must identify: (I) the internal owner of the document; (II) the applicable AI governance structure; and (III) the periodic review cycle, in order to incorporate regulatory, technological, and organizational changes.

Annex I – Compliance Verification Record

This checklist must be completed by the person responsible for the AI solution and validated by the governance body defined by the adopting organization (e.g., IT Governance, AI Committee, or equivalent), and retained as evidence for internal and external audits.

(   ) Tool approved by the designated governance body (e.g., AI Committee or equivalent);
(   ) Included in the adopting organization's corporate inventory;
(   ) Documented risk assessment;
(   ) Human review conducted;
(   ) Communication to affected parties;
(   ) Audit record maintained.

Responsible for the AI Solution
Name:
Position:
Department:
Date:

AI Governance Body / AI Committee
Representative’s Name:
Position:
Date: