



# Artificial Intelligence Governance Policy

TABLE OF CONTENTS

1. OVERVIEW .....3

2. OBJECTIVE .....3

3. SCOPE .....3

4. DEFINITION OF TERMS .....4

5. ROLES AND RESPONSIBILITIES.....4

6. ETHICAL PRINCIPLES .....5

7. SECURITY AND PRIVACY .....5

8. DOCUMENTATION AND COMPLIANCE .....6

9. POLICY REVIEW .....6

10. EFFECTIVITY .....6



## 1. OVERVIEW

- 1.1. The Artificial Intelligence (AI) Governance Policy sets rules and standards for the use of AI technologies within EMAPTA. This policy aims to guide employees involved in AI-related activities to ensure that AI is used responsibly, aligning with ethical, legal, security, and privacy principles. By providing a structured approach, EMAPTA aims to leverage AI technologies to enhance business processes while safeguarding data and maintaining trust with clients and employees.

## 2. OBJECTIVE

- 2.1. The objective of this policy is to:
  - 2.1.1. Ensure responsible development, deployment, and use of AI technologies within EMAPTA.
  - 2.1.2. Guide employees in the ethical, legal, and secure use of AI tools.
  - 2.1.3. Protect confidential and sensitive data from misuse or unauthorized access.
  - 2.1.4. Ensure AI technologies are used to support business objectives without compromising security, privacy, and compliance standards.

## 3. SCOPE

- 3.1. This policy applies to all EMAPTA employees using AI technologies to accomplish work tasks and projects. AI Technologies covered by this policy include, but are not limited to:
  - 3.1.1. Intelligent Chatbots (e.g., ChatGPT)
  - 3.1.2. Video Generators
  - 3.1.3. Image Generators
  - 3.1.4. Writing Assistants
  - 3.1.5. Note Takers
  - 3.1.6. Text-to-Speech or Speech-to-Text Tools
  - 3.1.7. Auto-Content Creation Tools
  - 3.1.8. Email Management Tools with AI-generated responses
  - 3.1.9. AI Calendar Tools
- 3.2. The scope encompasses ethical principles, data privacy and security, human oversight, and training related to the use of AI technologies.

#### 4. DEFINITION OF TERMS

- 4.1. **AI:** Artificial Intelligence, the simulation of human intelligence processes by machines, especially computer systems.
- 4.2. **Chatbot:** An AI program designed to simulate conversation with human users.
- 4.3. **Video Generator:** AI tools that create video content from text or other inputs.
- 4.4. **Image Generator:** AI tools that create images based on text descriptions or other inputs.
- 4.5. **Writing Assistant:** AI tools that assist in generating written content.
- 4.6. **EMAPTA-Owned Information:** Data and information owned by EMAPTA.
- 4.7. **Employee Personal Information and Sensitive PII:** Personal Identifiable Information (PII) of employees that is sensitive in nature.
- 4.8. **Client-Owned Information:** Data and information owned by EMAPTA's clients.

#### 5. ROLES AND RESPONSIBILITIES

- 5.1. Chief Information Officer (CIO) and Chief Technology Officer (CTO):
  - 5.1.1. Ensure the effective adoption of AI technologies aligns with business objectives and complies with EMAPTA's security, privacy, and business policies.
- 5.2. Information Security Department:
  - 5.2.1. Enforce security standards for technology usage, including AI technologies.
  - 5.2.2. Perform security assessments of AI systems and third-party vendors/tools.
- 5.3. IT Infrastructure Department:
  - 5.3.1. Ensure the availability of infrastructure supporting AI technologies and its compatibility with existing technologies within Emapta.
- 5.4. All Employees:
  - 5.4.1. Comply with Information Security Policies and refrain from using unvetted AI technologies for processing confidential information.
  - 5.4.2. Follow the rules and limitations under this policy when utilizing AI technologies.

5.4.3. Undergo training provided by EMAPTA for AI adoption.

## 6. ETHICAL PRINCIPLES

- 6.1. The use of AI technologies must comply with EMAPTA's Code of Conduct, Code of Ethics, and Employee Handbook. Additionally, the use of AI should adhere to these ethical principles:
- 6.1.1. AI technology should be used as guiding tools, with human decisions always being the final decision in situations where AI decisions may affect safety, privacy, security, and business continuity.
  - 6.1.2. AI technology should not harm the well-being of employees or clients.
  - 6.1.3. AI technology should act in the best interests of the company, clients, and employees, resulting in a net positive impact.
  - 6.1.4. AI technology should be developed and deployed fairly and justly, without discrimination or bias.
  - 6.1.5. AI technology should always be subject to human oversight and overseen by individuals with the necessary expertise.
  - 6.1.6. AI technology usage must comply with all applicable laws, regulations, and industry standards.

## 7. SECURITY AND PRIVACY

- 7.1. Protecting sensitive data is crucial to maintaining trust and complying with legal regulations. Key security and privacy rules for AI technologies include:
- 7.1.1. AI technologies must be assessed by EMAPTA's Information Security Department and Data Protection Officer before official use.
  - 7.1.2. Employees must not enter confidential information into AI technologies without authorization.
  - 7.1.3. Employees should redact confidential, proprietary, and personally identifiable information before using AI tools.
  - 7.1.4. Confidential information should not be stored on third-party platforms indefinitely and must be deleted after obtaining the AI output.
  - 7.1.5. Access to AI tools must be restricted to authorized personnel, following IAM Standards.

7.1.6. Only vetted AI tools with proper security and privacy controls should be used.

7.1.7. Regular auditing of AI technologies will be conducted by the InfoSec Department.

## 8. DOCUMENTATION AND COMPLIANCE

8.1. Employees must maintain proper documentation of AI tool usage, including user manuals, technical specifications, and testing results. This documentation must be reviewed and approved by the Global Technology Department. An inventory of all vetted AI technologies must be maintained by the Information Security Department.

## 9. POLICY REVIEW

9.1. The AI Governance Policy shall be reviewed annually to ensure its relevance and effectiveness. The review process will include input from key stakeholders to assess alignment with emerging technologies, regulatory changes, and organizational objectives. Updates and revisions to the policy will be proposed as needed to maintain its efficacy and support the secure use of AI technologies within EMAPTA.

## 10. EFFECTIVITY

10.1. This policy is effective immediately upon approval and will remain in effect until modified or rescinded by the company.



**POLICY/PROCESS OWNER:** Information Security Manager

**DOCUMENT CONTROL NO.:** EVSI.ITD.00.0000

**EFFECTIVITY DATE:** August 2024

	NAME / DESIGNATION	DATE
<b>AUTHOR</b>	Jappy Damaso – Information Security Manager	July 2024
<b>REVIEWED</b>	Pasindu Withanage – Vice President of Product management	August 2024
	Luis Sicat III – Chief Information Security Officer (CISO)	August 2024
<b>APPROVED</b>	Henry Vassall Jones – Chief Information Officer (CIO)	August 2024

REVIEW AND REVISION HISTORY			
DATE:	ACTION	Control No. (for Revision)	DESCRIPTION / COMMENT
May 2023	Created	1.0	First release of the Policy -Justin Arrojado-
August 2024	Reviewed and updated Template updated	1.1	Modified "5.3.1. Ensure the availability of infrastructure supporting AI technologies and its compatibility with existing technologies within Emapta." -Shihani Punchihewage-