FPO V
FUTURE POINT OF VIEW

AI Ethics Policy

Guiding the Organization on How to Build
Ethical Artificial Intelligence Tools

The following document is provided solely as a guide. It is only intended as an outline to assist in establishing your own policies and processes. It is expected that you would adapt this document and the contents herein to align with your unique business objectives, requirements, and needs. It does not intend to purport that this is the only way to implement the given topic security measures. Many sources may have been used in developing this content under Fair Use Rights as provided by U.S. Copyright Act Sections 107 and 108 and other applicable intellectual property law.

Your access to and use of this document and its content are at your own risk. By using this document, you understand and agree that the document and its content are provided to you on an "AS IS" basis. Future Point of View does not guarantee or warrant that the document or its content shall cover all possible issues/risks/methods/considerations – and instead, hereby specifically disclaims that the document is all-encompassing.

If you are new to the topic or to generative AI in general, please reach out to the FPOV team so we can help guide you as you embark on your journey of using generative artificial intelligence tools in a responsible manner.

1. Purpose

Artificial Intelligence (AI) is an emerging field that holds immense potential to shape the future. However, the development of AI tools must be done with caution and ethical considerations in mind. The purpose of this policy is to provide guidelines for creating ethical AI tools that are designed to benefit our constituency and society.

The purpose of this policy is to establish guidelines for the creation of responsible and ethical artificial intelligence tools that will be used by [Company Name] in an external and internal fashion and could inadvertently cause harm to people inside or outside COMPANY whether that be users of an AI system or individuals who are being impacted by the artificial intelligence decision-making in some form or fashion.

The policy aims to promote awareness of the potential risks associated with AI-generated content and to ensure that employees use these tools in a manner that aligns with the company's values, legal obligations, and industry best practices.

2. Scope

This policy applies to all [COMPANY NAME] employees involved in the development of AI tools, including but not limited to researchers, engineers, designers, and developers.

3. Definitions

Artificial Intelligence Tools: Software applications or platforms that leverage artificial intelligence to create, modify, or generate content, including but not limited to text, images, videos, and audio.

4. General Guidelines

In the development and implementation of artificial intelligence tools, COMPANY team members will strive for the following ideals:

4.1. *Respect for Human Rights:* AI tools should be designed to respect and protect human rights, including but not limited to privacy, security, and freedom of expression. Developers must prioritize user safety and ensure that AI tools do not cause harm to individuals or communities.

FPO
FUTURE POINT OF VIEW

4.2. *Fairness and Equity:* AI tools must be designed to promote fairness and equity, regardless of a person's race, ethnicity, gender, religion, sexual orientation, or socio-economic status. Developers must take steps to eliminate bias and discrimination from the data used to train AI models and ensure that AI tools do not perpetuate or amplify existing inequalities.

4.3. *Transparency:* AI tools must be transparent, and users must be informed of how they work and what data they use. Developers must provide clear explanations of the reasoning behind AI tool decisions and enable users to access, correct, and delete their data.

4.4. *Accountability:* Developers must be accountable for the impact of AI tools they create. This includes taking responsibility for any unintended consequences of AI tools and addressing any negative impacts they may have on society.

4.5. *Continuous Learning and Improvement:* Developers must engage in continuous learning and improvement to ensure that AI tools are up to date with current ethical and technical standards. This includes ongoing research and development, testing, and evaluation of AI tools.

5. Development of Co-Working AI Tools

All platforms COMPANY develops for use in co-working, whether that be software, robots, or applications, shall have the following safeguards in place:

5.1. Ambient sensor technologies and situational awareness, where applicable.

5.2. Monitoring in place to protect the safety of human team members in both highly controlled and uncontrolled/unmanaged environments.

5.3. Safeguards in place that allow for an emergency shutdown of the system or robot.

6. Human Agency and Oversight

All platforms COMPANY develops that are used to assess the quality of a person, whether it be their potential employment or promotion, quality of work, or in any way impacts a human's livelihood, life, or safety, requires close human inspection and periodic audits to ensure the system is not unfairly harming or disadvantaging an individual.

Oversight must include the aim of increasing the accuracy of AI systems and the assurance that they uphold human values in automated decision-making and work to build trust in the technology.

AI systems are required to meet all necessary regulatory standards and should be regularly audited by a third party for risk and bias.

Human intervention should be present at every stage of the AI development lifecycle. This includes the design cycle of the system as well as monitoring of the system's operation. There must be human command oversight involving the overall activity of the AI system and the ability to decide when and how to use the system in any particular situation. Human discretion must be established before and during the use of the system and a human must have the ability to override a decision made by the system.

Developers and users of an AI system must be trained and retrained on how an AI system works and its limitations, how to anticipate when a system may misleading or wrong and why. Users should have a healthy level of skepticism in the system's output and offered a sense of how often the system could go wrong. They should understand that their expertise is meant to complement the system and be provided with a list of factors to consider when using and monitoring a system.

In the development of all AI systems, the following should be considered:
- A consideration of the appropriate level of human control for the system based on its use case
- A description of the level of human control or involvement
- A system owner who understands the appropriate time to intervene with the system
- A description of the detection and response mechanisms that have been established to assess whether something could go wrong
- A "stop button" or procedure to safely abort an operation when needed that has been documented

7. Technical Robustness and Safety

AI systems must be developed with a preventative approach to risk and harm. This includes a resilience to attacks and an emphasis on security. Developers should effort to ensure a system is resilient to attack vectors such as data poisoning or the corruption of a model or its hardware or software. Because insufficient security process can result in erroneous decisions or physical harm, a security first mindset must be present in the development of any AI system as well as its implementation.

AI systems must have safeguards in place to ensure that the system is doing what it is intended to do without harming humans. Minimization standards should be present for unintended consequences and errors based on the magnitude of the risk posed by the system. Safety measures should be developed and tested proactively.

A well-formed development and evaluation process should be in place to support, mitigate, and correct unintended risks from inaccurate predictions. This is especially necessary in the case when an AI system directly impacts human lives or well-being.

8. Privacy and Data Protection

AI systems must ensure privacy and data protection. This includes information provided by a user and the information gained by the system during user interaction. Because interactions can help to infer important insights into a user's preferences, extra precautions must be in place to help ensure that this information is not made public, nor is it used to unfairly discriminate a user based on their choices.

9. Data Integrity

Because of the danger of bias or inaccuracy, ensuring the quality of the data sets being used by an AI system is essential. Therefore, data sets must be tested and documented throughout the development of the system as well as during its deployment and use. This must also apply to AI systems in use by the COMPANY but developed by a third party.

10. Transparency

Data sets and processes used in any AI system being deployed by the COMPANY should be documented to the fullest extent possible. This includes data gathering, data labeling, and the algorithms being used.

The decisions being made by the system should be able to be understood and traced by human beings. When a system has a significant impact on individuals, its decision-making process should be understood by a human operator.

When a user is interacting with an AI system, it should be disclosed in a manner that is reasonable for a user to understand this fact.

11. Implementation

To ensure compliance with this policy, the following steps must be taken:

11.1. All individuals and organizations involved in the development of AI tools must undergo training on the ethical principles outlined in this policy.

11.2. Ethical considerations must be integrated into the design and development of AI tools from the outset.

11.3. All AI tools must undergo a thorough ethical review before release.

11.4. Regular evaluations must be conducted to ensure that AI tools continue to comply with ethical standards and identify areas for improvement.

11.5. This policy must be regularly reviewed and updated to reflect changes in ethical and technical standards.

12. Disclosure

12.1. Employees must clearly disclose the use of AI tools when the tool is being used externally by non-employees to help support a COMPANY function, unless explicitly exempted by management for specific cases.

12.2. Employees must be transparent about the limitations and potential biases of AI, especially when presenting it to stakeholders or using it for decision-making purposes.

13. Training and Education

13.1. [Company Name] is committed to providing employees with the necessary resources and training to develop AI tools effectively and responsibly. Employees are encouraged to participate in relevant training programs and to stay informed about industry best practices.

14. Compliance and Enforcement

14.1. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment. Employees are encouraged to report any suspected violations of this policy to their supervisor, department head, or the designated compliance officer.

14.2. [Company Name] reserves the right to amend or update this policy as needed to reflect changes in technology, legislation, or industry best

practices. Employees will be notified of any significant changes to the policy and are expected to adhere to the updated guidelines.

15. Conclusion

The development of ethical AI tools is essential for ensuring that AI benefits society while minimizing any potential harm. This policy outlines the necessary steps that developers must take to create AI tools that promote human rights, fairness, transparency, accountability, and continuous learning and improvement. By following these guidelines, we can create AI tools that are beneficial to society while minimizing any negative impacts.

12. Revision History

Date of Change	Responsible	Summary of Change
MM-DD-YYYY		Initial Release

FPOV
FUTURE POINT OF VIEW