Acceptable Use of AI Tools at Our Organization

Executive Summary

Our Organization is committed to maintaining a safe and secure environment for all employees and organizations we partner with through the responsible use of Artificial Intelligence (AI) technology.

To achieve this, we have implemented an Acceptable Use of AI Tools Policy outlining the principles and guidelines that Our Organization staff must adhere to when using AI capabilities. The policy aims to ensure that all Our Organization employees use AI systems that align with the organization's values, policies, and standards. It applies to everyone at Our Organization who uses AI systems to perform their work.

The policy provides clear guidelines for the appropriate use of AI tools in the workplace, particularly when handling the organization's and its clients' and partners' sensitive and confidential information. It outlines the dos and don'ts of using AI tools, given their increasing prevalence in day-to-day work.

The policy aims to ensure that all Our Organization employees use AI tools safely and securely. The policy requires employees to follow security best practices, such as evaluating security risks and safeguarding confidential data when using AI tools.

This policy brief and purpose, scope, definitions, and security best practices are detailed below:

Policy Purpose

Our Acceptable Use of AI Tools policy outlines best practices for *securely* using AI tools in the workplace, especially with sensitive data and proprietary organization information.

As equity, bias, and trust issues arise with AI tools we use, we also will rely on this policy to guide our use of *appropriate* AI in our workplace.

Scope

The use of AI tools has revolutionized the way we work. These tools have the potential to automate tasks, improve decision-making, and provide valuable insights into our operations. However, their use also poses new information security and data

protection challenges. To mitigate these risks, this policy guides employees on using AI tools safely and securely, especially when sharing potentially sensitive organization information.

Definitions

Generative AI is AI that can learn from and mimic large amounts of data to create new content based on inputs or prompts, such as text, images, music, audio, and videos. Generative AI is powered by foundation models (large AI models) that can multi-task and perform out-of-the-box tasks, such as summarization, Q&A, classification, and more.

Large Language Model (LLM) is a type of language model notable for its ability to achieve general-purpose language understanding and generation. LLMs acquire these abilities by using massive amounts of data to learn billions of parameters during training and consuming large computational resources during their training and operation. LLMs are artificial neural networks pre-trained using self-supervised and semi-supervised learning.

Machine Learning is a branch of artificial intelligence that enables computers to learn from data and perform tasks normally requiring human intelligence. Machine learning algorithms use statistical methods to find patterns in data and make predictions or decisions based on inputs or prompts. Machine learning primarily focuses on making decisions based on historical inputs instead of generating new responses.

Security Best Practices

All employees must follow these security best practices when using AI tools:

- Use of reputable AI tools: Employees should use only Our Organization's reputable, approved AI tools. AI tools used by employees must meet our security and data protection standards.
- Evaluation of AI tools: The evaluation of new AI tools is the responsibility of the _____ department/title holder. This includes reviewing the tool's security features, terms of service, and privacy policy.
- Protection of confidential data: Employees must not upload or share any personal, proprietary, or protected data without prior approval from the appropriate department. This includes data related to employees, clients, or partners.
- Access control: Employees must not give access to AI tools outside the organization without prior approval from the appropriate department or manager and subsequent processes as required to meet security compliance requirements. This includes sharing login credentials or other sensitive information with third parties.

- Review Output: Employees must review output for accuracy and relevance before using the results of generative AI. That includes generated natural language and code.
- Evaluate equity, bias, and trust concerns: As equity, bias, and trust issues arise with AI tools, it is the responsibility of staff to bring these issues to their supervisor. Further, it is the responsibility of the _____ department/title holder to evaluate and make recommendations to the organization on using or refusing to use the AI tool, as appropriate with the policies of our organization regarding bias, equity, and inclusion.

Acceptable Use of AI Technology

- The generative AI tool use should be limited to business-related purposes and aligned with our organization's standards.
- All assets created using generative AI systems must be professional and respectful. Employees should avoid using offensive or abusive language and engaging in any behavior that could be considered discriminatory, harassing, or biased when applying generative techniques.
- Staff should not share any confidential or sensitive information with AI technology, including but not limited to passwords, certificates, personally identifiable information (PII), secrets, and tokens.
- Multi-factor authentication should be in place across all third-party tools and technologies used for generative AI services.
- Generative AI systems must comply with all applicable laws and regulations, including data protection and privacy laws.
- Our Organization reserves the right to review and monitor all communications shared with generative AI systems, including but not limited to messages, prompts, attachments, and files.

Risk-Based Classification

We acknowledge that not all use cases need to be held to the same standard for the use of AI tools. This basic classification can be used to provide additional context as to which tool may be the most appropriate for the task and if additional approval or discussion needs to occur before a tool can move from evaluation into use.

• Low risk uses: drafting email responses, summarization of meetings or documents, ideation and exploration
• Moderate risk uses: internal analysis of metrics, initial code generation
• High risk uses: decisions affecting people, constituents, finances or security, automating approval or incorporated into workflow

Staff Responsibility When Using AI Technology

- Employees are responsible for ensuring they use AI technology in compliance with this Acceptable Usage Policy and any other relevant organization policies or procedures.
- All employees must be aware of their responsibilities for protecting confidential and sensitive information and take all necessary steps to safeguard the privacy and security of this information when using generative AI technology.
- Managers and supervisors are responsible for ensuring their teams know and comply with this policy. They must also report policy violations to Our Organization's _____ department/title holder.
- Our Organization's _____ department/title holder is responsible for agreeing on and documenting an approved list of AI systems to ensure that only authorized applications of these technology capabilities are applied by the organization.

In using AI technology,

- Always obtain explicit consent before using AI tools to create content that involves another person.
- Create content that is appropriate and respectful towards all employees and clients.
- Keep confidential information confidential by not sharing it with unauthorized individuals, including external parties that provide generative AI services.
- Use generative AI systems responsibly that do not compromise our organization's or its data's security or integrity.
- When using generative AI, comply with all applicable laws and regulations, including data protection and privacy laws.

Approved AI technology

Currently, over 300 AI tools generate content, art, and video, so maintaining a comprehensive list is impractical. When considering using a generative AI tool, please review its policies to ensure the AI systems are safe, secure, and trustworthy. For more information on acceptable review, contact Our Organization's _____ department/title holder

In general, our policy is to use AI Tools within the framework of an organization account which restricts the data shared publicly.

- Microsoft AI-capable applications and features available under the Our Organization's Microsoft 365 tenant (CoPilot)

- Google Gemini applications and features available under the Our Organization's Google account.
- Third party tools where Our Organization has a contract or license agreement protecting our data from being used in the LLM of the vendor. Other legal protections such as copyright protection should also be found in the terms and conditions of the third party vendor.

- …other internal or public tools as appropriate and evaluated. Our evaluation process is _____.

Training and Education

Our Organization provides a collaborative learning environment. We encourage our staff to keep updated with the ongoing AI use and adoption changes. Staff should check with their supervisors for available training resources.

Updates and Review

This Acceptable Use of AI Tools Policy will be updated periodically to reflect the dynamic and changing nature of the use of AI tools in our sector. Changes to this policy will be informed by the potential risks and biases that these tools can interject into our work and by changing cybersecurity recommendations.