Artificial Intelligence (AI) Policy

The purpose of this policy is to establish Artificial Intelligence (AI) best practices. AI tools must be used to ensure management is aware of the use of AI, AI is used legally, and exit strategies from AI tools are understood. The use of AI is not discouraged so long as AI is used within the parameters set forth in this Policy.

Policy Owner: Executive Council

Scope and Definitions

This policy governs the use of third-party or publicly available AI applications and tools.

> **Artificial Intelligence (AI)**. Applications that simulate human intelligence to generate responses, work products, or perform tasks.
>
> **Generative Tools**. In the context of AI, generative tools use machine language learning to create text, images, audio, and video, based on a user's prompt.
>
> **Third-Party**. In the context of this policy, means unrelated entities or persons who provide AI applications and tools.
>
> **Use Case**. Also called a "Business Case," where the intended benefit of the system is evaluated against other factors such as risk and cost.

Exclusions

AI as part of search engines or other website tools are excluded. However, use of these tools is still governed by other policies such as Cybersecurity and Acceptable Use.

Prohibitions

AI applications and tools must be authorized by executive management. Unauthorized AI tools are strictly prohibited. AI Tools that violate legal regulations, including but not limited to privacy regulations, or otherwise violate ethical standards including but not limited to discriminatory practices or unauthorized data collection, are also not permitted. Employees may not use AI applications or tools, even if approved, if such use would constitute a violation of other policies, including but not limited to Cybersecurity and Acceptable Use.

For example, employees are strictly prohibited from sending information to a third-party AI website in violation of privacy laws, exactly as employees are generally prohibited from sending any sensitive information to an authorized third-party. In such an event, the employee would follow our current Security Incident notification process.

Authorization: Use Cases

Employees wishing to utilize AI will need to obtain approval from executive management and establish a Use Case for the AI. Employees will be required to present the following information:

- Name of the AI application or tool

- Purpose or intended benefit of the AI
- Whether the AI function is bundled with a current approved application or tool
- The cost of the AI solution
- Whether or not the cost has been budgeted
- Whether the tool will be used or included as a product, application, or service sold to clients
- Whether sensitive information (including but not limited to personally identifiable information of individuals [employees or members], trade secrets, and confidential information of third parties) will be provided to the AI and what security controls the AI has for this information
- Whether the AI tool can generate contents that could potentially violate Intellectual Property rights, and the controls to prevent IP misuse
- As appropriate, whether quality assurance and testing is part of the process for using the AI application or tool
- Exit strategies if the tool violates Acceptable Use or is otherwise no longer viable

Certain AI tools may require additional due diligence, such as the AI vendor being a critical vendor and part of the organization's Vendor Management Program.

Acceptable Use of AI

To use AI tools responsibly in the workplace, employees are required to review output for quality, and under certain circumstances test to ensure the AI tool is functioning as designed. Employees should focus on AI tools that provide the following measurable benefits:

- Automation of repetitive tasks
- Streamlining and/or centralizing processes or functions
- Development of procedures, standards, and documentation
- Analysis of large datasets, including trend analysis

This is not an exclusive list of permissible uses of AI in the workplace. Staff should stop using AI tools immediately if review or testing of AI tools have any of the following characteristics:

- Promotion of illegal discrimination or other illegal acts
- Failure to ensure security of sensitive data or compliance with privacy rights
- Failure to reliably operate in accordance with the AI's Use Case

Any employee using AI in violation of its approved Use Case (for example, sending sensitive information to an AI not authorized to process this information) is subject to discipline up to and including termination. Certain unauthorized uses of AI could also be violation of federal and state laws, subjecting the employee to criminal prosecution.

Disclosure of AI Use

Employees are required to disclose the use of AI whenever AI is used to assist the development of products or services. Any such use must be disclosed on the company website. If an AI tool is used to assist with the development of documentation or work product, in addition to reviewing the

output, employees are required to prominently display that an AI tool was used. Employees must also state a person reviewed the output before the documentation or work product is published.

Termination of the Use of AI

CU*Answers reserves the right to terminate the use of AI at any time, including but not limited to the risk that AI use may conflict with state AI laws.