Acceptable Use of AI Policy

Last Updated: **05/03/2025**
Policy Contact: **Mike Minkler**
Manual: **Information Technology**
Company: **CMIT Solutions of Clayton**

1: Compliance and Ethical Use

The use or development of any AI system that contravenes the law, infringes upon human rights, compromises data security, or endangers the well-being of our customers, employees, or stakeholders is prohibited.

2: General Principles for AI Use

We acknowledge that artificial intelligence (AI) technologies offer considerable societal benefits while carrying potential risks such as bias, discrimination, copyright infringement, exploitation, and harm. Our organization is committed to harnessing AI for positive outcomes while safeguarding against negative impacts. The best AI use cases are not intended to replace employees but remove the mundane, repetitive and time-consuming task so the employee can focus on higher level tasks that take more thought and analysis.

3: Authorized Platforms for Generative AI

CMIT Solutions of Clayton uses the Hatz.AI platform to securely access generative AI. This platform offers multiple Large Language Models (LLMs) within CMIT Solutions of Clayton's secure tenant. Sensitive data will not be used to train public AI models, ensuring protection for both our business and our clients. Employees must use the Hatz.AI platform when working with sensitive company or client data to prevent exposure to the internet and public AI models. Additionally, AI tools integrated into our current technology stack, such as Cooper Copilot within Kaseya tools, are also authorized for use.

4: Restrictions on Personal Use of Company Tools

Employees are strictly prohibited from using company-provided tools for personal purposes. These tools, including AI systems and platforms, are intended solely for business-related activities and must be used in accordance with company policies. Personal use of these tools can compromise data security, violate privacy regulations, and lead to unauthorized access to sensitive information. Employees must ensure that all usage of company tools is aligned with their professional responsibilities and the organization's objectives.

5: Transparency and Accountability

CMIT Solutions of Clayton is adamant about AI systems that are transparent, explainable, fair, and accountable. Any AI system utilized will adhere to relevant regulations and standards, including but not limited to HIPAA, GDPR, PCI, and FTC Safeguards.

6: Data Usage

Third party meeting recording systems such as Read AI are prohibited. These systems can be invasive and stealthy and may create significant risk to our organization. Microsoft Teams is our preferred system for recording and transcribing meetings. Recording and transcribing of meetings must be approved in writing by an owner or the Director of Operations.

There may be situations where an employee attends a meeting with external participants (clients, vendors, other CMIT offices) where the meeting is being recorded and/or transcribed. In these situations, the employee should use their best judgement to determine if the topics to be discussed are of a sensitive nature such that the disclosure and sharing of the information could create risk for CMIT Solutions of Clayton. Sensitive topics might include contractual issues, personnel issues, confidential business issues, etc. You should apply a standard of care that asks yourself "If the recording and transcription of this meeting were placed on the public internet, would that be ok?". If the topics are deemed sensitive, the employee should do the following: (1) inform the organizer that your company policy prohibits you from attending meetings that are being recorded without prior management approval and/or (2) ask that the meeting not be recorded or transcribed and/or (3) leave the meeting.

7: Confidentiality and Privacy

Employees are prohibited from feeding confidential or private information into any **unauthorized** AI system. AI systems available for use by the general public such as ChatGPT do not guarantee the privacy data shared with their systems, and as a result the potential for creating data breaches is significant. Data security and privacy remain paramount throughout AI system usage.

8: Regular Monitoring and Auditing

Routine monitoring and auditing of our AI systems will ensure their ethical and effective functioning.

9: AI Limited to Research and Content Development

The use of AI is approved for the purposes of research and content development. When using AI to generate content, the user is responsible for thoroughly reviewing the results for accuracy and compliance with our AI policies. Any mistakes or errors introduced by faulty AI results is solely the responsibility of the user, not the AI tool used to generate the result.