THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: GP-004.02 - Acceptable Use of Generative AI	
Version 1	Effective Date: 10/26/2023

No./Title: GP-004.02-Acceptable Use of Generative AI	**Resp. Office:** Office of CyberSecurity	**Effective Date:** 10/26/2023
Category: General Security Provisions	**Last Review:** 10/26/2023	**Next Review:** 10/26/2025
Contact: Chris Madeksho	(901) 448-1579	mmadeksh@uthsc.edu

Purpose

To give guidance as a foundation for leveraging generative artificial intelligence (AI) responsibly and ethically across all UTHSC environments.

Scope

This standard applies to members of the UTHSC community who have a need to access UTHSC IT Resources.

Definitions

Data Security Levels – a ranking of 1-3 that is determined based on classification and impact questions for the data's confidentiality, integrity, and availability. These rankings are explained in GP-002-Data & System Classification.

Generative Artificial Intelligence (AI) – a branch of artificial intelligence that enables machines to create original content.

Intellectual Property - proprietary or confidential information into generative AI, including unpublished research findings, internal university data or documents, or any information protected by intellectual property rights without express written consent from all stakeholders.

Research Data – any information that has been collected, observed, generated, or created to validate original research findings. Researchers must consider the nature and sensitivity of scholarly data before using generative AI to support research.

UTHSC IT Resource - Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems), and information.

Responsibilities

Data Owners are ultimately responsible for the data and information being collected and maintained by their department or division, usually a member of senior management. The data owner addresses the following:

- **Review and categorization** – Review and categorize data and information collected by their area of responsibility.
- **Assignment of data classification labels** – Assign data classification based on the data's potential impact level.

The **Chief Information Security Officer (CISO)** is responsible for providing strategy and direction for assessment, planning, and implementation of all security standards, and practices, and ensuring compliance to same.

Researchers cannot put data that are confidential, contain sensitive information, or are subject to specific legal or ethical requirements (e.g., human subjects' data) into any generative AI without proper anonymization and evaluation of potential risks, as well as express written consent from any other necessary parties.

Users of UTHSC IT Resources are responsible for complying with this Standard.

Practice

1. UTHSC Community members must adhere to the University of Tennessee System Administration (UTSA) acceptable use policy and UTHSC acceptable use standard.
2. Users should assume that all consumer generative AI products make data publicly available unless otherwise indicated per explicit official agreement with the University of Tennessee.
3. All UTHSC data need to be classified and an impact level determined based on GP-002-Data & System Classification. Per the classification standard, all data that has not been explicitly classified is considered Level 3 or high-risk data by default.
4. Specific data levels should be handled in different ways when using generative AI products.
    a. Level 1 confidentially-ranked data – Generative AI can safely process publicly available information, general academic concepts, and non-sensitive data. The use of Level 1 data must still comply with UTHSC standards and be considered relative to its ethical and reputational implications.

   b. Level 2 or Level 3 confidentially-ranked data – Do not enter private or confidential data, including but not limited to, personally identifiable information (PII) such as social security numbers, contact details, name/image/likeness, or any information covered by FERPA, HIPAA, or other regulations, into any generative AI product. This would also include research data and intellectual property that is classified as Level 2 or 3 data.

5. Thoroughly anticipate the impact of using generative AI **before** entering information into a tool. It is important to remember that once data is entered, neither the individual who entered it nor the institution can directly remove it. Furthermore, be cautious of claims by product providers. There is no consistent definition of or criteria around vendor statements of using "AI" in a product. These "AI"-enhanced products may not offer superior performance to other non-AI products, nor perform equally well, in that they may not have the same standards for output.
6. Think critically. Evaluate and corroborate information obtained from generative AI tools by consulting additional sources or seeking expert advice
7. Understand expectations. When using generative AI for writing support, review the requirements of the publisher/reviewer/recipient of the finished product regarding disclosure requirements. Some journals, offices, publishers, or educators may require that generative AI be cited in work, potentially in different ways.
8. Stay informed**.** Follow conversations around AI technology and further updates and guidance from the university to incorporate the latest improvements and address any emerging risks as generative AI continues to develop.

Additional Risks and Limitations of Generative AI

1. **Misinformation and inaccuracies:** Generative AI may generate responses that are not always accurate or up to date. Users should independently verify the information provided by generative AI, especially when it comes to specific facts or rapidly evolving subjects.
2. **Bias and unintentional harm:** Generative AI can inadvertently reflect biases present in the training data. It is crucial to critically evaluate and contextualize the responses generated by generative AI to ensure fair and unbiased information dissemination.

3. **Inappropriate content:** Although generative AI providers may have made efforts to filter out inappropriate content, generative AI may produce or respond to content that is offensive, inappropriate, or violates ethical standards.
4. **Algorithmic implications:** AI can deduce and infer algorithmic criteria other than original intent. This situation can lead to or exacerbate potential bias through the inclusion or reweighting of unintentional variables. For example, if certain populations are underrepresented in the data used to train AI algorithms, results may be skewed.

References

1. IT-0110-Acceptable Use of Information Technology Resources
2. GP-002-Data & System Classification

GP-004-Acceptable Use of IT Resources