

15.03.08 Artificial Intelligence in Research



Revised: [July 27, 2026](#)

Next Scheduled Review: July 27, 2031

Click to view [Revision History](#).

Regulation Summary

This regulation establishes a broad framework guiding the ethical, responsible, and innovative use of generative and other forms of Artificial Intelligence (AI) across The Texas A&M University System (system) and its members for research-related purposes. The following principles offer practical guidance on the use of AI in research.

Definitions

Click to view [Definitions](#).

Regulation

1. DATA PRIVACY AND SECURITY

- 1.1 AI use and tools must comply with all applicable data privacy and security laws, system policies, regulations and standards, and member rules, procedures, and security controls.
- 1.2 AI tools and platforms that are externally hosted, operated by third parties, or accessible to the general public must not be used to create, analyze, or process research materials that are based on, use, or incorporate non-public internal information. This includes unpublished research, research subject to dissemination controls, classified research, export-controlled research, and research involving controlled unclassified information (CUI), unless the AI platform or tool is covered by a contractual agreement with the system or a member institution, and implements technical and organizational controls that prevent unauthorized access, retention, use, or disclosure of institutional data. Any agreements for AI platforms or tools that will be used to create, analyze, or process data in classified research, export-controlled research, or research involving CUI must be reviewed by the System Research Security Office (RSO).
- 1.3 AI platforms and tools that are hosted, operated, and controlled by a member or its authorized partners, including systems built using open-source or open-weight models, may be used with non-public internal information, excluding classified or CUI materials, provided they comply with applicable technical and organizational data protection requirements, security controls, and research governance obligations.

2. AI USE IN RESEARCH

- 2.1 Researchers must be aware of shortcomings when using AI tools within their research. Examples of these shortcomings include “AI hallucinations,” where incorrect or misleading results are generated by an AI tool due to the lack of sufficient knowledge or information about a subject. Additionally, AI models are susceptible to bias which may influence the information they generate. Researchers should strive to eliminate bias when developing and training AI models and acknowledge the bias of AI models where applicable.
- 2.2 Researchers must carefully select AI tools used for data analysis. Entering data into an AI tool can result in a loss of privacy and confidentiality. Researchers using previously de-identified data sets should consider other methods of ensuring privacy and confidentiality when those data are entered into AI models for analysis.
- 2.3 Researchers should be aware of ethical frameworks for the use of AI tools within their field of study, including guidelines established by professional associations, to help inform their selection of appropriate uses of AI to answer research questions.
- 2.4 Research involving the evaluation of AI tools as part of a research project may be considered human subjects research depending on the nature of the research and collection of personal information. Such research projects should be evaluated by the responsible Institutional Review Board (IRB) for a determination.
 - 2.4.1 Research involving development of AI models as part of software or other digital tools for use in human or animal healthcare may fall under US Food and Drug Administration (US FDA) medical device regulations and requires IRB review.
 - 2.4.2 If an IRB, or other regulatory committee, lacks sufficient information regarding the use of AI under review, the committee should seek expertise through the use of consulting members or other mechanism.
- 2.5 Generative AI may make up (fabricate) information, sources, and/or source data. It may also manipulate (falsify) data to the extent that it does not accurately reflect the original outcome. It may also present information from a source and not provide appropriate acknowledgement or citation of the source (plagiarism). Research personnel should be aware of these shortcomings and are responsible for verifying the information generated to ensure that there is no potential for research misconduct (falsification, fabrication, and plagiarism) through the use of an AI tool.
 - 2.5.1 It is the responsibility of the researcher to verify information, data, and other outputs generated by any AI tool, which includes verifying the accuracy of the information and maintaining the integrity of the data.
 - 2.5.2 If an incident of fabrication, falsification, or plagiarism results from the use of an AI tool, the research personnel involved may be held responsible for resulting research misconduct allegations depending on the nature of the issue, funding agency guidelines, applicable system and member research misconduct guidelines, and other circumstances. The developing nature of sponsor

guidelines regarding the use of AI in research means that researchers must be aware of these changing expectations to ensure that AI is not used in a manner that could be considered research misconduct.

3. DISCLOSURE OF AI USE IN RESEARCH

3.1 Authorship and Citations

3.1.1 Researchers are responsible for being aware of and adhering to journal, conference, funding agency, book publisher, or other relevant guidelines for citing AI tools as authors or tools that solely created or partially contributed to images and figures in the publication or presentation. Authors should not assume that AI tools can be used as co-authors because AI tools cannot take accountability or responsibility for the submitted work.

3.1.1.1 Generally, journals expect that when using AI tools to generate components of a publication or presentation, authors will disclose its use.

3.1.2 Researchers are responsible for following journal, conference, book publisher, or other relevant guidelines for including AI tools as references for quotations, images and figures, and sources of materials and ideas.

3.2 Research Proposals and Peer Review

3.2.1 Researchers must be aware of all relevant guidelines funding agencies may have regarding the use of AI tools in award and contract proposals and submissions, reports, and other associated documentation submitted to agencies.

3.2.2 Funding agencies may restrict or prohibit reviewers from using AI tools to analyze, evaluate, and critique award applications, R&D contract proposals, and other documents.

3.2.3 Researchers are responsible for being aware of and adhering to a funding agency's guidelines regarding the use of AI in peer review.

3.2.4 Individuals serving as peer reviewers for journals, conference abstracts, or other outlets must adhere to the relevant organization's guidelines for use of AI tools in peer review and the maintenance of confidentiality.

3.3 Incidental use of AI

3.3.1 It is widely recognized that disclosing the incidental use of AI, such as suggesting words or phrases, using digital assistants, checking grammar and spelling, finding references, and brainstorming ideas, is unnecessary.

- 3.3.2 Researchers are expected to keep current on general obligations for disclosing the use of AI in research since the guidelines on the incidental use of AI are subject to change.

Related Statutes, Policies, or Requirements

[System Policy 15.02, Export Control Program Management](#)

[System Regulation 29.01.05 Artificial Intelligence](#)

[System Regulation 15.05.01, Classified Information Management](#)

[System Regulation 15.05.02, Controlled Unclassified Information Management](#)

[System Regulation 15.99.03 Research Misconduct](#)

[Committee on Publication Ethics \(COPE\). \(2023, February 13\). *Authorship and AI tools*.](#)

Member Rule Requirements

A rule is not required to supplement this regulation.

Contact Office

Research
(979) 458-5598