



MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy/Procedure (“OP”)

OP 44.13: Artificial Intelligence

Approval Authority:	President
Policy Type:	University Operating Policy and Procedure
Policy Owner:	MSU Chief Information Officer
Responsible Office:	MSU Chief Information Officer
SACSCOC Standard(s):	10.2 IS 3 (Public Information Governing Board – Focuses on Approval of Policies); 13.6 IS 8 (Federal and State Responsibilities Oversight of External Funds and Regulatory Compliance); 13.8 IS 9 (Healthy, Safe, and Secure Facilities, Technology, and Safety)
Next Scheduled Review:	09/01/2029 – This OP will be reviewed every three years, or as needed, by the MSU Chief Information Officer, MSU Chief Information Security Officer, and Office of General Counsel, with substantive revisions forwarded to the MSU President.

I. Purpose

The purpose of this OP is for Midwestern State University (“MSU” or “University”), a component institution of the Texas Tech University (“TTU”) System, is to implement and comply with [TTU System Regulation 09.04: Artificial Intelligence](#), and establish institutional responsibilities regarding the use of artificial intelligence technologies in facilitating the missions of MSU, including teaching, research, clinical and outreach activities, and administrative operations. This OP provides a set of foundational policies that are common among all component institutions of the TTU System. Based on unique needs and environments, MSU has tailored its institutional policies for its circumstances, consistent with TTU System regulations and applicable state and federal laws.

Artificial Intelligence (“A.I.”) is technology that can sense, comprehend, reason, solve problems, make decisions, and create new information. As such, A.I. tools are subject to Acceptable Use Policies, applicable state and federal laws, including data privacy rules, and institutional regulations and policies. In situations where A.I. tools are used to synthesize data and / or make a Consequential Decision, it is imperative that reasonable bias mitigation measures are in line with applicable policies and legal statutes and regularly reviewed for issues that may cause harm to any entity subject to the Consequential Decision.

II. Definitions

Artificial Intelligence

Common abbreviations, terms, and conditions specific to MSU OP 44.03 and TTU System Regulation 09.04 - Artificial Intelligence:

- A. *Algorithmic Discrimination*** – Means any condition in which an artificial intelligence system, when deployed, creates an unlawful discrimination of a protected classification in violation of the laws of this state or federal law. "Algorithmic discrimination" does not include the offer, license, or use of a high-risk artificial intelligence system by a developer or deployer for the sole purpose of the developer's or deployer's self-testing, for a non-deployed purpose, to identify, mitigate, or prevent discrimination or otherwise ensure compliance with state and federal law.
- B. *Artificial Intelligence System*** – Means Artificial Intelligence System means the use of machine learning and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, speech or natural language processing, and content generation.
- C. *A.I. Practitioner*** - Means an affiliated staff, faculty, researcher, student, contractor, or vendor of MSU/TTU System that is operationally responsible for the business practices and procedures that are using an artificial intelligence system to facilitate administrative business, research, and/or instructional practices on behalf of one or more institutions within MSU/TTU System.
- D. *Consequential Decision*** - Means a decision that has a material legal, financial, or similarly significant effect on the provision, denial, or conditions of a person's access to MSU/a TTU System's service or benefit.
- E. *Generative Artificial Intelligence***- Means artificial intelligence models that can emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.
- F. *High-Risk Artificial Intelligence System*** - Means High-risk Artificial Intelligence System means any artificial intelligence system that is a substantial factor to a consequential decision.

The term does not include:

An Artificial Intelligence System if the Artificial Intelligence System is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not intended to replace or influence a previously completed human assessment without sufficient human review;

The following operational technologies identified as artificial intelligence technologies are excluded from this system regulation, unless the technologies, when deployed, make, or are a substantial factor in making, a consequential decision:

- (1) anti-malware;
- (2) anti-virus;
- (3) calculators;
- (4) cybersecurity;

- (5) databases;
 - (6) data storage;
 - (7) firewall;
 - (8) fraud detection systems;
 - (9) internet domain registration;
 - (10) internet website loading;
 - (11) networking;
 - (12) operational technology;
 - (13) spam- and robocall-filtering;
 - (14) spell-checking;
 - (15) spreadsheets;
 - (16) web caching;
 - (17) web scraping;
 - (18) web hosting or any similar technology; or
 - (19) any technology that solely communicates in natural language for the sole purpose of providing users with information, making referrals or recommendations relating to customer service, and answering questions and is subject to an acceptable use policy that prohibits generating content that is discriminatory or harmful, as long as the system does not violate any provision of an TTU System Regulation, MSU policy, state, or federal law.
- G. *Operational Technology*** - Means hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise.
- H. *Protected Data*** - Means any information that is subject to state or federal legal protections such as FERPA, HIPAA, or personal data as assigned to it by [Section 541.001, of the Texas Business and Commerce Code](#).
- I. *Confidential Data*** - Means Confidential data means any information that has been designated as “Need to Know” by the institution or the terms and conditions of a research grant.
- J. *Substantial Factor*** – Means a factor that is:
- (1) considered when making a consequential decision;
 - (2) likely to alter the outcome of a consequential decision; and
 - (3) weighed more heavily than any other factor contributing to the consequential decision.

III. Policy/Procedure

A. Information Resources Governance for Artificial Intelligence Systems

A.I. Systems are information technologies simulating human intelligence, subject to TTU System and MSU procurement regulations and policies, Acceptable Use Policy, and to all provisions of institutional data privacy and protection standards including, but not limited to, HIPAA, FERPA, and Intellectual Property data protection standards.

1. MSU users must not input confidential or protected data into A.I. systems not approved for use by MSU.
2. In accordance with [TTU System Regulation 09.04.03.b](#), MSU must establish a governance model that reviews and approves A.I. toolsets and use cases for how A.I. technology is leveraged at their respective institutions. Per [Tex. Gov't Code § 2054.703](#), the governance model should follow the governance model as outlined in the [NIST AI Risk Management Framework](#) published by the [NIST Trustworthy and Responsible Artificial Intelligence Resource Center \(AIRC\)](#).
3. As directed by [Texas Administrative Code \(TAC\) 219](#), MSU:
 - a. Has designated its Chief Information Security Officer as an AI Risk Officer having duties identified by [TAC 219.21.a](#); serving as a member of the A.I. governance model;
 - b. Maintains an inventory of all A.I. systems in use, including identification of those classified as high-risk or heightened scrutiny systems as required by [Tex. Gov't Code § 2054.068](#); and
 - c. Ensures that employees who use a computer at least 25 percent of the employee's required duties complete an artificial intelligence training program certified under [Tex. Gov't Code § 2054.5193](#).
4. A.I. Practitioners are responsible for ensuring that the use of a high-risk A.I. system follows applicable federal, state, and local laws; TTU System Regulations; MSU policies and procedures; and per [Tex. Gov't Code § 2054.702](#), the code of ethics published by the Texas Department of Information Resources.
5. A.I. Practitioners are responsible for ensuring that any intended output of data or consequential decision generated by an A.I. system is vetted for providing outputs or decisions that are factually accurate, free from Algorithmic Discrimination, and do not infringe on any legal protection such as a trademark, patent, or any other applicable intellectual property mechanism. A.I. Practitioners must test their models regularly at a frequency determined by MSU's policy for compliance with the standards. In partnership with the A.I. Risk Officer, testing and audit history records must be retained in accordance with MSU's policies or otherwise for a duration defined by laws, regulations, or contractual requirements such as those included in research award documents.

B. Disclosure of Use

In compliance with [Tex. Gov't Code § 2054.707](#), applications leveraging A.I. for consequential decisions must disclose the use of A.I. to potentially impacted users in accordance with appropriate ethical standards.

C. Instructional Use of Artificial Intelligence

MSU respects academic freedom in the classroom. Faculty must indicate to students, through the course syllabus, what the appropriate uses of artificial intelligence systems are within the context of the specific course of instruction.

D. Artificial Intelligence Use in Research

Researchers must ensure that the A.I. systems leveraged in research projects and creative scholarly activities are deployed, disclosed / reported in a manner that complies with applicable TTU System Regulations, MSU policies and procedures; research compliance protocols, management plans, and data use agreements; state and federal laws; and contractual requirements such as those included in research award documents. In the event that an A.I. system is to be developed or hosted using institutionally owned assets including but not limited to network, servers, and personal computing devices (e.g., laptop computers, tablets, etc.); MSU's information technology department and Chief Information Security Officer ("CISO") must review and approve the deployment prior to conducting research activities. The Principal Investigator of the research award is responsible for identifying and addressing any intellectual property concerns that may arise from the usage of the A.I. system to generate research project deliverables and/or artistic creative works are addressed in a contractual manner acceptable to all parties affiliated with the research grant and MSU's policies.

IV. Related Statutes, Rules, Policies, and Resources

Related Statutes/Rules:

[Tex. Gov't Code § 2054.621](#)

[Texas Administrative Code \(TAC\) §219](#)

Related TTU System Regulations:

[TTU System Regulation 09.04: Artificial Intelligence](#)

Related Resources:

[NIST Trustworthy and Responsible Artificial Intelligence Resource Center \(AIRC\)](#)

[NIST AI Risk Management Framework](#)

[NIST AI RMF Playbook](#)

V. Responsible Office

Contact: MSU Chief Information Officer

Phone: (940) 397-4647

E-mail: paul.chappell@msutexas.edu

Contact: MSU Chief Information Security Officer:

Phone: (940) 397-3297

Email: ISO@msutexas.edu

Contact: MSU Web Services

Phone: (940) 397-6645

E-mail: webmaster@msutexas.edu

VI. Revision History

--/--/2026: Adopted and approved as MSU OP 44.03: Artificial Intelligence by MSU President Stacia Haynie.

Stacia Haynie, President
Midwestern State University

Date Signed: _____