MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy/Procedure (OP)
OP 44.10: Information Technology (IT) Operations

Approval Authority:	University President
Policy Type:	University Operating Policy and Procedure
Policy Owner:	Vice President for Administration and Finance
Responsible Office:	Department of Information Technology
Next Scheduled Review:	05/01/2024

I. Policy Statement

Midwestern State University ("MSU" or "University"), a component institution of the Texas Tech University System ("System" or "TTUS"), recognizes that Information Technology (IT) is critical for the University and must be managed in compliance with state and federal laws and regulations.

II. Reason for Policy

The purpose of this Operating Policy/Procedure (OP) is to establish policies regarding information technology operations and resources at MSU.

III. Application of Policy

This policy applies to all faculty, staff, students and others authorized users of MSU electronic and information resources.

IV. Definitions

For purposes of this OP:

Chief Information Officer (CIO) – The individual responsible for management of the University's information resources. The CIO serves as the Information Resource Manager (IRM) for MSU, as referenced in the *Texas Administrative Code*. The CIO has final authority on all MSU IT-related issues, including exceptions to existing IT policies.

Chief Information Security Officer (CISO) – The individual responsible for the University's information and data security.

Electronic and Information Resources (EIR) - Electronic and information resources (EIR), as defined *Texas Administrative Code* §213.1(9), includes information technology and any equipment or interconnected system or subsystem of equipment used to create,

convert, duplicate, store, or deliver data or information. MSU's EIR Accessibility Coordinator provides leadership and guidance, ensures compliance, and promotes EIR accessibility for the University. The specific job duty of the University's EIR Accessibility Coordinator is to ensure that MSU is in compliance for electronic delivery of content. The contact information for the MSU EIR Accessibility Coordinator is located in Section VI's related resources.

Information Resources – Defined by *Texas Administrative Code* §211.1(3) as the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors. MSU's CIO serves as the University's Information Resource Manager (IRM), defined by *Texas Administrative Code* §211.1(4) as a senior official within the organization who oversees the acquisition and use of information technology within a state agency or institution of higher education, and ensures that all information resources are acquired appropriately, implemented effectively, and in compliance with relevant regulations and policies.

V. Procedures and Responsibilities

A. All faculty, staff, students, and other authorized users of MSU IT resources are responsible for complying with this OP on information technology operations and all other applicable operating policies regarding the use of MSU IT resources, including the Acceptable Use Policy.

B. All MSU information technology infrastructures are managed by the MSU Office of the Chief Information Officer (CIO). No other areas, departments, or individuals may duplicate, modify, build, add, or attach to the IT infrastructure without explicit approval from the MSU CIO. (Examples of IT infrastructure include, but are not limited to, the following: logical and physical data and video networks over wired and wireless connections, video conferencing, email, security, network-based virtualization services, enterprise systems, authentication, and data center operations.)

C. Per Texas statutes, MSU information resources[1] are strategic assets of the state of Texas that must be managed as valuable state resources.[2]

1. Use of functional mailboxes is required when provisioning services such as subscriptions, departmental social media accounts, etc. to ensure the strategic management and continuation of the service for the University in the event of personnel changes.

2. Use of MSU information resources is subject to University OPs and other applicable laws. Unauthorized use is prohibited, usage may be subject to security testing and monitoring, misuse is subject to criminal prosecution, and

[1] As defined by *Texas Government Code* §2054.003(7).
[2] Mandated by *Texas Government Code* §2054.001(a)(1).

users have no expectation of privacy except as otherwise provided by applicable privacy laws.[3]

D. In accordance with *Texas Administrative Code* §202 and *Texas Administrative Code* §2054

1. All MSU employees must complete cybersecurity online training annually.

2. All designated area and department IT staff must complete the online cybersecurity training for IT professionals annually.

3. Any service provider with access to a state computer system or database must complete an annual cybersecurity training program provided by MSU. For the purposes of this section:

   a. the term "service provider" has the same meaning as "contractor" and includes subcontractors, officers, or employees of the service provider;

   b. the term "access" is defined as "any person who has been given an account to access any State (or local) information system."

E. All procurement of information resources, including, but not limited to, equipment, hardware, software, and professional services is subject to review and approval by the CIO. All IT assets are inventoried by the IT Department. Additional review may be conducted, as needed. To expedite evaluation and the procurement process, departments should contact the MSU Office of the CIO early in the decision-making process, prior to submitting procurement documents.

F. Any procurement of information resources requiring system integration with institutional enterprise information systems must be reviewed and approved by the MSU CIO prior to implementation.

G. All procurement of information resources, including, but not limited to, Internet/cloud computing services, telecommunications equipment/services and networking equipment/supplies, regardless of cost, are subject to review and approval by the MSU CIO. To expedite evaluation and the procurement process, departments should contact the MSU Office of the CIO early in the decision-making process, prior to submitting procurement documents.

H. Any contract involving data sharing/transfer of MSU data must be reviewed and approved by the MSU Office of the CIO prior to implementation.

I. All electronic and information resources (EIR) must comply with the accessibility requirements outlined in OP 44.02: Electronic and Information Resources Accessibility. (Electronic and information resources include information technology

[3] Mandated by Security Controls Standards Catalog AC-8.

and any equipment or interconnected systems or subsystem of equipment that is used in the creation, conversion, duplication, or delivery of data or information.[4])

J. MSU departments, employees, and contractors must take reasonable and necessary steps to ensure privacy of student education records, personally identifiable information (PII), protected health information (PHI), and other confidential or sensitive information at MSU. For information regarding information privacy and confidentiality, see OP 44.11: Information Resources Use and Security Policy.

1. All institutional data that is classified as Confidential, Sensitive, Regulated, Mission-Critical, or is otherwise subject to restricted access requirements, must be stored or processed only on information resources located in the University Data Center.

2. All PHI data used for authorized MSU research projects or in the course of patient treatment on campus must be stored in our HIPAA-compliant data center, or at other HIPAA-compliant locations approved by the MSU CIO. Contact the MSU Office of the CIO for more information.

K. All use of information resources is subject to MSU IT security policies, as referenced in OP 44.11: Information Resources Use and Security Policy.

L. Use of social media for University business is subject to all applicable MSU IT OPs and policies, including the Acceptable Use policy.

M. Any faculty, staff, or student conduct on personal social media that violates local, state, or federal law or University policy may result in disciplinary action. Human Resources will assist the relevant administrators with addressing issues involving employees. Student Affairs will review and address issues involving students.

N. The MSU CIO serves as the Information Resource Manager (IRM) for Midwestern State University, as referenced in the *Texas Administrative Code*.

O. The MSU Chief Information Security Officer (CISO) is the Information Security Officer for Midwestern State University, as referenced in the *Texas Administrative Code*.

P. The MSU CIO serves as the University EIR accessibility coordinator, as referenced in *Texas Administrative Codes* 206 and 213, to ensure that Midwestern State University is in compliance for electronic delivery of content.

Q. The MSU CIO has final authority on all MSU IT-related issues, including exceptions to existing IT policies.

VI. Related Statutes, Policies and Procedures, and Resources

Related Policies

[4] Defined by *Texas Administrative Code* §213.1(9).

OP 44.02: Electronic and Information Resources Accessibility

Related Resources:
MSU EIR Accessibility Coordinator
(940) 397-4278
eircoordinator@msutexas.edu

VII. Responsible Office

Chief Information Officer
Phone: (940) 397-4278
E-mail: cio@msutexas.edu

VIII. History

6 Aug. 1999:	In an effort to have one comprehensive policy and procedure statement for information systems, the MSU Board of Regents adopted and approved a new policy/procedure - Policy/Procedure 4.181 – Information Systems Policies and Procedures – to replace the existing Policies 4.181 (Computer Security and Privacy), 4.182 (Copyright and Computer Software Policy), and 3.338 (Personnel Computer and Software Policy.
5 Nov. 2010:	Revised because the reauthorization of the Higher Education Act includes disclosures requirements regarding policies and procedures for copyrighted material.
5 Aug. 2011:	Section C (Guidelines) added per a financial audit recommendation.
5 Aug. 2021:	MSU Board of Regents renumbered former MSU Policy/Procedure 4.181 – Information Technology Policies and Procedures to Operational Policy/Procedure (OP) 44.10: Information Technology Policy and Procedures.
20 May 2022:	OP 44.10 completely revised and renamed Information Technology (IT) Operations to provide emphasis on the purpose and intent of Information Technology and to align with the Texas Tech University System. Adopted and approved by MSU Interim President James Johnston.