Administrative Council
Midwestern State University
Approval via Electronic Vote

May 20, 2022 **Meeting No. 22-04**

The Administrative Council approved the policies below via email and they were signed by Interim President Johnston on May 20, 2022. Members voting to approve: Ms. Debbie Barrow, Dr. Martin Camacho, Mr. Fred Dietz, Ms. Dawn Fisher, Ms. Julie Gaynor, Dr. Keith Lamb, Mr. Barry Macha, Mr. Matt Park, Dr. Beth Reissenweber, Mr. Austin Strode. Votes not received: Ms. Reagan Foster, Dr. Kristen Garrison, Dr. Karen Moriarty, Mr. Kyle Owen, Mr. Tony Vidmar, Mr. Kyle Williams.

I. MSU OP 14.08 Payment Card Processing

II. MSU OP 34.20 Procurement, Usage, and Disposal of Radioactive Materials, Radiation Producing Devices, and Lasers

III. MSU OP 44.02 Electronic and Information Resources Accessibility

IV. MSU OP 44.10 Information Technology (IT) ~~Policies and Procedures~~ Operations

V. MSU OP 52.41 Work Breaks

James Johnston, Chair

Betsy Tucker
Betsy Tucker, Secretary

MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy/Procedure (OP) OP 14.08: Payment Card Processing

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

I. Policy Statement

Midwestern State University ("MSU" or "University") seeks to protect the interests of the University and its customers by establishing strong internal business controls and standard revenue collection methods throughout the University.

II. Reason for Policy

The purpose of this Operating Policy/Procedure (OP) is to ensure compliance with the Payment Card Industry Data Security Standard and to protect the cardholder information of patrons that utilize a credit card to transact business with MSU.

III. Application of Policy

This policy establishes policy and procedures for acceptance of payment cards by University departments for sales and services.

IV. Definitions

For purposes of this OP:

Payment Card - A payment card supports cashless payment for goods and services. Examples include, but are not limited to, credit cards, debit cards, and charge cards.

Merchant - Each department processing payment card transactions is referred to as a Merchant.

Merchant ID - A Merchant ID is a unique number used to identify the department and card type. The University Business Office will request the required merchant identification number from the payment card processor and provide them to the Merchant.

Payment Card Industry Data Security Standards (PCI DSS) - PCI DSS is a single approach to safeguarding sensitive data for all types of payment cards. The Standards are a result of collaboration between Visa and MasterCard and are designed to create common industry security requirements.

To download the PCI DSS, go to: https://www.pcisecuritystandards.org/

Payment Card Application - Payment Card Applications can be hardware, software, or a combination of hardware and software which aid in the processing of payment cards. Examples include Point of Sale (POS) devices, web applications/forms which collect or process payment cards, or third-party systems which process payment card transactions.

Payment Card Processor - A payment card processor offers merchants online services for accepting payment online including credit card, debit card, direct debit, bank transfer, and real-time bank transfers.

PCI DSS Self-Assessment Questionnaire (SAQ) - The PCI DSS SAQ is a validation tool intended to assist a Merchant and service provider(s) in self-evaluating their compliance with PCI DSS.

To download a PCI DSS SAQ, go to: https://www.pcisecuritystandards.org/

PCI DSS Data Network - A secure firewalled network within MSU's network, developed according to the PCI DSS standard, for the hosting of computers, servers, or storage which process payment card transactions and data.

Service Provider/Vendor – As used in this policy is a 3rd party payment card processor.

V. Procedures and Responsibilities

A. Payment Card Processor

1. Payment Card Processor. All payment card transactions must go through Midwestern State University's (MSU) payment card processor, currently Heartland Payment Systems.

   Any exceptions to the use of this standard processor must be approved by the University Vice President for Administration and Finance, the Controller, the Chief Information Officer, and the Chief Information Security Officer.

   Current Exceptions for 3rd Party Service Provider/Vendors:

Stripe:	Processes payments for Athletics ticketing.
Rydin:	Processes payments for the MSU Police Department ticketing system.

2. Methods of Processing. MSU processes payment cards both physically and online. Merchants that want to begin processing payment cards, ***must*** use one of the following MSU-approved processing methods:

   a. Online

This is done through MSU's online e-commerce solution Touchnet Marketplace. Any exception to this MUST be reviewed and approved by the Business Office.

b. In Person
Payments may be made in person with campus merchants.

3. Acceptable Vendors. If using a third-party software, the software must connect through the University e-commerce solution Touchnet Marketplace. Any exception to this must be reviewed and approved by the Business Office. Only PCI DSS-compliant vendors may be used. All software contracts and purchase orders must include non-disclosure and/or confidentiality statements. Proof of compliance must be:

   a. a written agreement from the service providers acknowledging they are responsible for the security of cardholder data the service providers possess; and

   b. sent to the Business Office.

B. Establishing and Maintaining Payment Card Services

1. Establishing Accounts. Merchant IDs will not be issued until the Merchant meets **all** of the following requirements.

   a. Complete and submit to the Business Office:

      - Policy Certification
      - PCI DSS Awareness online training

2. Maintaining Accounts. Merchant IDs may be revoked if the Merchant does not meet **all** of the following requirements. The Business Office will reach out to all merchants during the Fall of every year to request updates on each of these in order to comply with PCI DSS certification regulations for the University.

   a. Complete the PCI DSS Self-Assessment Questionnaire (SAQ) annually or **upon any change** to the hardware, software, or payment card processing methodology and submit to the Business Office;

   b. Complete the MSU Merchant Application & Update as requested by the Business Office, or **upon any change** to the hardware, software, or payment card processing methodology and submit to the Business Office;

   c. Complete required PCI DSS Awareness online training annually. Training is required for:

      - Any employees who process payment cards or have access to sensitive payment card information received by their department for payment card transactions
      - Supervisors of the above employees

- Departmental Business Managers whose department accepts credit card payments
- Others who oversee payment card operations in a department;

d. Complete Policy Certification annually. Required by the same individuals listed in Section V.B.2.c of this OP; and

e. Continued compliance with this OP, PCI DSS, and MSU IT Security Policies.

C. Authority and Responsibility

1. The Business Office is responsible for:

a. issuing a payment card Merchant ID and for overseeing the policies and procedures on payment processing;

b. negotiating payment card processing and related services on behalf of any MSU department;

c. performing monthly reconciliation on the bank account, to which payment card receipts are credited;

d. determining if the charges have been assessed against the bank account in accordance with the pending procurement document(s) during the account reconciliation process;

e. assisting merchants with resolving discrepancies related to payment card charges with the MSU payment card processor;

f. verifying that all Merchants are in compliance with MSU policies and current PCI DSS financial controls in regards to protecting cardholder data; and

g. the revocation of a Merchant ID that fails to comply with the PCI DSS and/or this OP.

2. The Information Technology Department is responsible for:

a. the operations and maintenance of the MSU data networks, as well as, the establishment of IT security policies and standards in compliance with PCI DSS, federal, state, and local regulations;

b. developing and maintaining an MSU PCI DSS Data Network for the hosting of computers, servers, and online storage engaged in processing or storage of payment card transactions;

c. assisting any Merchant in assessing its payment card processes, applications, and migration to a PCI DSS-compliant solution for the processing of payment cards;

d. verifying that all Merchants are compliant with the current PCI DSS technical requirements; and

e. annual collection of information to monitor service 3rd party service provider/vendor PCI DSS compliance status.

3. The Merchant is responsible for:

a. all requirements outlined above in Section V.B.2 of this OP;

b. developing a system and procedure to monitor and analyze security alerts and information and distribute these alerts to the appropriate personnel;

c. developing and maintaining departmental policy and procedures for physical inspection of payment card equipment, including frequency and methods of inspection and submitting this policy to the Business Office annually or as requested;

d. verifying that their software, hardware, applications, or other devices, products, etc. and associated processes for processing payment cards meets PCI DSS requirements - assistance from the Business Office and the MSU IT Department may be needed;

e. maintaining and safeguarding all payment card processing equipment according to the PCI DSS standard. The equipment must be able to produce receipts (merchant and/or customer) that masks all but the last four digits of the cardholder's card number;

f. contacting the payment card processor regarding defective payment card processing equipment. The Merchant should return the equipment directly to the payment card processor, provided the payment card processor has instructed the Merchant to return the equipment. The Merchant should obtain a comparable replacement directly from the payment card processor;

g. contacting the Business Office to relocate its purchased payment card processing equipment (media) or dispose of the equipment in accordance with the PCI DSS standard and relevant MSU Operating Policies when the Merchant discontinues the acceptance of payment cards. Purchased equipment should be returned to the payment card processor. Before any payment card processing equipment is transferred to another department or returned to the leasing company, verify all payment card data has been securely removed. If the equipment will be disposed of, all payment card data must be securely removed, or the storage device must be destroyed to prevent unauthorized access to the data;

h. maintaining a record retention and disposal policy in accordance with OP 02.34: Records Management Policy, to keep information storage to a minimum, that information will be used for business and regulatory purposes only, and that information will comply with OP 44.11: Information Resources

Use and Security Policy (Contact the University Librarian at the Moffett Library at (940) 397-4173 for records retention guidance); and

i. responding to card brand chargebacks, disputes, sales draft retrieval requests or other requests from the issuing bank or cardholder within the specified time period providing proper documentation, or determining that the chargeback, dispute or other request is legitimate and should stand as is.

VI. Related Statutes, Policies & Procedures and Websites

Payment Card Industry – Data Security Standards Form

VII. Responsible Offices

Questions or comments regarding this Policy should be directed to:

Vice President for Administration & Finance
vpaf@msutexas.edu
Extension 4117

Business Office
bus.office@msutexas.edu
Extension 4101

Chief Information Officer
cio@msutexas.edu
Extension 4647

Chief Information Security Officer
ciso@msutexas.edu
Extension 4680

VIII. History

20 May 2022: OP 14.08: Payment Card Processing is a new policy recommended during an internal audit review by the Texas Tech University System in February 2022 regarding PCI compliance. Adopted and approved by MSU Interim President James Johnston.

Dr. James Johnston, Interim President
Midwestern State University

Date Signed: 5/20/22

MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy/Procedure (OP)
OP 34.20: Procurement, Usage, and Disposal of Radioactive Materials, Radiation Producing Devices, and Lasers

Approval Authority:	President
Policy Type:	University Operating Policy and Procedure
Policy Owner:	Provost and Vice President for Academic Affairs
Responsible Offices:	Dean, McCoy College of Science, Mathematics and Engineering Dean, Robert D. and Carol Gunn College of Health Sciences and Human Services
Next Scheduled Review:	05/06/2026 (every 5 years once approved)

I. Policy Statement

It is the policy of Midwestern State University ("MSU" or "University"), a component institution of Texas Tech University System ("TTUS"), to protect the health and safety of students, staff and faculty while engaged in the educational and research activities of the University. The purpose of this OP is to establish procedures for the purchase, use, and disposal of radioactive materials, radiation producing devices (RPD), and/or lasers.

II. Reason for Policy

The reason for this OP is to ensure compliance with the Texas Administrative Code (Tex. Admin. Code) pertaining to 25 *Tex. Admin. Code* 289 Radiation Control and Chapter 401 Radioactive Materials & Other Sources of Radiation of Title 5, Subtitle D, of the *Texas Health & Safety Code*. The acquisition, use, and disposal of radioactive materials, radiation producing devices and/or lasers must meet the safety requirements for faculty, staff, and students as well as maintain the regulatory conditions mandated by the state so that the University remains compliant.

III. Application of Policy

The rules and procedures contained in this policy shall apply to all MSU facilities in which Radiation Producing Devices (RPD) are used. Failure to comply will result in fines from the state that will eventually lead to the loss of the RPD.

IV. Definitions

Radioactive Materials (RAM)—Means any material (solid, liquid, or gas) that emits radiation spontaneously.

Radiation—One or more of the following:
(A) gamma and x rays; alpha and beta particles and other atomic or nuclear particles or rays;
(B) emission of radiation from any electronic device to such energy density levels as to reasonably cause bodily harm; or
(C) sonic, ultrasonic, or infrasonic waves from any electronic device or resulting from the operation of an electronic circuit in an electronic device in the energy range to reasonably cause detectable bodily harm.

Radiation Safety Committee (RSC)—The committee tasked with oversight of campus radiation safety, to include procurement, use, and disposal of radioactive materials, radiation producing devices, industrial radiation producing devices, and lasers.

Radiation Safety Officer (RSO)—An individual who has a knowledge of and the authority and responsibility to apply appropriate radiation protection rules, standards, and practices, who must be specifically authorized on a radioactive material license, and who is the primary contact with the agency.

Industrial Radiation Safety Officer (IRSO)— An individual who has a knowledge of and the authority and responsibility to apply appropriate radiation protection rules, standards, and practices, who must be specifically authorized on an industrial radioactive material license, and who is the primary contact with the agency.

Radiation Producing Devices (Machines) (RPD)—Means any device capable of producing ionizing radiation except those devices with radioactive material as the only source of radiation.

Industrial Radiation Producing Devices (Machines) (IRPD)—Means any device capable of producing ionizing radiation that include, but are not limited to, portable/handheld fluorescence x-ray (open beam), fluoroscopy hand held intensified, fluoroscopy x-ray, industrial accelerator, spectrography x-ray, flash x-ray, flash x-ray for bomb detection, educational facility (x-ray for non-human or not live animal use), diffraction x-ray, uncertified cabinet x-ray, and minimal threat radiation machines.

Laser—Means a device that stimulates atoms or molecules to emit light at particular wavelengths and amplifies that light, typically producing a very narrow beam of radiation.

V. Procedures and Responsibilities

A. Radiation Safety Committee

1. MSU's Radiation Safety Committee includes the following individuals:

a. RSO for Gunn College of Health Sciences and Human Services
b. RSO for Vinson Health Center
c. IRSO for McCoy College of Science, Mathematics, and Engineering
d. Dean of the Gunn College of Health Sciences and Human Services
e. Dean of the McCoy College of Science, Mathematics, and Engineering
f. Chemical Safety Manager

2. The Radioactive Material License, the x-ray machine Certificate of Registration, and the Laser Registration, which authorizes the use of radioactive materials (RAM) and radiation producing devices at Midwestern State University, require that all such uses be administered by the Radiation/Laser Safety Committee.

    a. Licenses for equipment used in the Gunn College of Health Sciences and Human Services are stored in Centennial Hall Room 432
    b. Licenses for equipment used in the McCoy College of Science, Mathematics, and Engineering are stored in Bolin Science Hall Room 316.
    c. Licenses for equipment used in Vinson Health Center are stored in Redwine Student Wellness Center Room 138.

3. The Radiation Safety Officer (RSO) and Industrial Radiation Safety Officer (IRSO) (and the Laser Safety Officer (LSO) if/when applicable) are appointed by the vice president for academic affairs, after consultation with the appropriate College deans and department chairs, and serve as standing members of the committee with the Risk Management and Safety Manager and the Chemical Safety Manager. Appointments will be made on or before August 1 of each year.

4. The committee is required to meet annually or as situations demand.

B. Radiation (and Laser) Safety Officers

The RSO, IRSO, and LSO are responsible for making on-site inspections, keeping records, assisting users, and maintaining liaison with federal and state officials.

C. Procurement of Radioactive Materials, Radiation Producing Devices, and Lasers

1. All persons wishing to use RAM,RPD, or lasers must obtain authorization from the Radiation Safety Committee.

    a. Radioactive Materials above the Nuclear Regulatory Commission or State of Texas's threshold for regulating radiation sources (10 μCi) are not currently permitted at MSU.
        i. If any legacy RAMs are found on campus, the Chemical Safety Manager will be contacted in order to dispose of them properly.
        ii. Future acquisition of radioactive materials requires an amendment to existing campus licensing and approval by the RSO and/or IRSO of the department and the Radiation Safety Committee.

    b. Radiation-producing devices are currently permitted at MSU.

i. New RPD requires and approval by the RSO and/or IRSO of the department and the Radiation Safety Committee.

ii. New RPD requires an amendment to existing campus licensing and approval by the RSO and/or IRSO of the department and the Radiation Safety Committee.

c. Lasers with hazard classifications of Class IIIB and IV are not permitted at MSU.

i. If any legacy lasers are found on campus, the RSO and/or IRSO will be contacted in order to dispose of them properly.

ii. Future acquisition of lasers requires an amendment to existing campus licensing and approval by the RSO and/or IRSO of the department and the Radiation Safety committee.

iii. Exemptions to this requirement are all general office supplies purchased from office suppliers. A few examples are classroom laser pointers, laser printers, and projector remote controls. The hazard classifications of these exclusions are Class I, II, IIIA.

D. Procurement of Non-Regulated Equipment/Materials

1. All persons receiving any equipment through purchase, loan, or gift must ensure the following:

   a. The equipment does not contain RAM or produce radiation in a quantity or manner that would result in regulation;
   b. The equipment does not produce or contain licensed material that would require labeling in accordance with TAC 289.202(ggg)(3); and
   c. The equipment operates under all current state and federal requirements or is capable of being upgraded to meet these requirements.

   If the equipment does contain RAM or produces radiation in a quantity or manner that would result in regulation, refer to the previous section (C) of this policy.

2. Departments receiving equipment found to be contaminated above acceptable levels are responsible for the cost of decontamination and/or disposal. Decontamination and/or disposal must be approved by and coordinated through the RSO and/or IRSO.

E. Use of Radioactive Materials/Radiation Producing Devices/Lasers

1. To assure the protection of all university personnel and to maintain compliance with the stipulations of the Midwestern State University Radioactive Material License, the Certificate of Registration for Radiation Machines, and the Certificate of Registration for Industrial Radiation Machines, safe and proper procedures must be followed at all times by the sub licensee and those under this supervision.

2. Specific procedures that must be followed are contained in the following sources:
   a. State of Texas Guidelines in Texas Administrative Code Title 25, Part 1, Chapter 289 and in the 25 Texas Administrative Code 289 Radiation Control and Chapter 401 Radioactive Materials & Other Sources of Radiation of Title 5, Subtitle D, of the Texas Health & Safety Code
   b. Nuclear Regulatory Commission guidelines NRC 10 CFR Part 20
   c. Center for Disease Control Radiation in Medicine
   d. City of Wichita Falls Texas Code of Ordinances, Article VII Division 1, Sections 106-566.

3. The RSO and IRSO are authorized to make routine inspections of laboratory areas where RAM, RPD, and/or lasers are used. The RSO and IRSO are authorized by the Radiation Safety Committee to prohibit work in any area in which there is unsafe and/or unauthorized use of RAM, RPD, and/or lasers.

F. Disposal of Radioactive Materials

The disposal of RAM is strictly controlled by state and federal regulations. Specific procedures that must be followed are contained in the following sources:

1. State of Texas Guidelines: *Texas Administrative Code* Title 25, Part 1, Chapter 289 and in the 25 *Texas Administrative Code* 289 Radiation Control and Chapter 401 Radioactive Materials & Other Sources of Radiation of Title 5, Subtitle D, of the Texas Health & Safety Code

2. Nuclear Regulatory Commission guidelines: NRC 10 CFR Part 20

3. Center for Disease Control: Radiation in Medicine

4. City of Wichita Falls Texas Code of Ordinances, Article VII Division 1, Sections 106-566

To assure compliance with these regulations, materials will be disposed of only after consultation with the Chemical Safety Manager.

G. Emergency Action

Approved emergency actions are specified in the Operating and Safety Procedures for MSU Radiologic Sciences and Operating and Safety Procedures for MSU Industrial Radiation Instruments. In case of emergency, the RSO and/or IRSO will be contacted immediately. The sub licensee under the supervision of the RSO and/or IRSO will perform decontamination procedures.

Emergency Contacts:

- Radiation Safety Officer
  Office Phone: (940) 397-4615
- Radiation Safety Officer (Vinson Health Center)
  Office Phone: (940) 397-4231

E-mail: rso@msutexas.edu

- Industrial Radiation Safety Officer
  Office Phone: (940) 397-4596
  E-mail: irso@msutexas.edu
- Chemical Safety Manager
  Office Phone: (940) 397-4596
- Associate Vice President for Facilities Services
  Office Phone: (940) 397-4288
- Texas Radiation Control Program
  (512) 458-7460 (24-hour emergency number)

VI. Related Statutes, Rules, Policies, Forms, and Websites

Related Statutes/Rules:

Texas Administrative Code Title 25, Part 1, Chapter 289

25 *Texas Administrative Code* 289 Radiation Control and Chapter 401 Radioactive Materials & Other Sources of Radiation of Title 5, Subtitle D, of the Texas Health & Safety Code

NRC 10 CFR Part 20

Center for Disease Control and Prevention, Radiation in Medicine

City of Wichita Falls, Texas Code of Ordinances, Article VII Division 1, Sections 106-566.

Related Policies:

MSU Policy OP 34.08 Chemical Safety
MSU Policy OP 56.02 Faculty Research

VII. Responsible Office(s)

Dean, McCoy College of Science, Mathematics and Engineering
Phone: (940) 397-4253
E-mail: margaret.brownmarsden@msutexas.edu

Dean, Gunn College of Health Sciences & Human Services
Phone: (940) 397-4594
E-mail: jeff.killion@msutexas.edu

VIII. History

20 May 2022:	Adopted and approved by MSU Interim President James Johnston as OP 34.20: Procurement, Usage, and Disposal of Radioactive Materials, Radiation Producing Devices, and Lasers.

James Johnston, Interim President
Midwestern State University

Date Signed: 5/20/22

MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy and Procedure (OP)
OP 44.02: Electronic and Information Resources Accessibility

Approval Authority:	President
Policy Type:	University Operating Policy and Procedure
Policy Owner:	Vice President for Administration and Finance
Responsible Office:	Department of Information Technology (IT)
Next Scheduled Review:	11/01/2023

I. Policy Statement

Midwestern State University (MSU), a component institution of the Texas Tech University System ("System" or "TTUS"), recognizes that access to electronic and information resources is critical for the University and must be managed in compliance with state and federal regulations.

II. Reason for Policy

The purpose of this Operating Policy/Procedure (OP) is to establish rules for the procurement, development, maintenance, and use of electronic and information resources that will be accessible to persons with disabilities.

III. Application of Policy

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

IV. Procedures and Responsibilities

A. Electronic and information resources (EIR) includes information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, duplication, or delivery of data or information.[1]

B. All EIR products developed, procured, or changed through a services contract, and all EIR services provided through hosted or managed services contracts shall comply with the provisions of Chapter 206, State Websites, and Chapter 213, Electronic and Information Resources, of the Texas Administrative Code (TAC), as applicable,

[1] Defined by Texas Administrative Code §213.1(6).

unless such requirement imposes a significant difficulty or expense, as determined and exempted by the MSU President.[2]

C. In order for an EIR product or service to be considered accessible, the product must offer an alternate format or method of comparable quality for providing information, including product documentation, to people with disabilities. Additionally, it must work with the assistive technology commonly used to increase, maintain, or improve functional capabilities for individuals with disabilities.

D. Required accessibility compliance is divided into three areas:

1. Electronic and information resources

   a. Software applications and operating systems

   b. Telecommunications products

   c. Video and multimedia products

   d. Self-contained, closed products

   e. Desktop and portable computers

   The specific technical standards for each of thc above category of EIR are documented at https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=213&sch=C&rl=Y.

2. Procurement

   a. Before any purchases of EIR can be approved, vendors, regardless of originating state, must certify that their products comply with the TAC §206, State Websites, and §213, Electronic and Information Resources, as applicable, and provide credible evidence of the vendor's capability or ability to produce accessible EIR products and services for every product under consideration using one of the following methods:

      (1) Voluntary Product Accessibility Template (VPAT) (http://www.itic.org/public-policy/accessibility);

      (2) Electronic document that addresses the same accessibility criteria in substantively the same format as the VPAT; or

      (3) URL to a web page that explains how to request a completed VPAT for any product under contract.

   b. The degree of accessibility of a given product should be determined by the procuring department. The IT Accessibility Coordinator is available to assist departments and areas in making this determination.

   c. Departments shall coordinate purchases of EIR with Procurement Services and the designated IT Accessibility Coordinator to ensure compliance with the Texas Administrative Code and this policy.

[2] Mandated by Texas Administrative Code §213.37.

d. All purchases must follow the established MSU Texas OPs for procurement.

3. Websites

a. Per the TAC §206, State Websites, all university public entry points must be accessible.

(1) Specific MSU Texas website design guidelines are published at https://msutexas.edu/web-guidelines/.

(2) Specific technical standards for the websites (per TAC §206) is documented at https://texreg.sos.state.tx.us/public/readtacSext.ViewTAC?tac_view=5&ti=1&pt=10&ch=206&sch=C&rl=Y.

b. Key public entry points are web pages that an institution of higher education has specifically designed for the public to access official information. The designated Midwestern State University key public entry points is:

The Midwestern State University home page at https://www.msutexas.edu.

E. Under the provisions of the TAC §213, Electronic and Information Resources, an IT Accessibility Coordinator must be appointed for the university; per OP 44.10, Information Technology (IT) Operations, the MSU Texas CIO has designated the Operations Manager for Information Technology as the MSU IT Accessibility Coordinator.

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

V. Responsible Office

Department of Information Technology
Phone: (940) 397-4278
E-mail: cio@msutexas.edu

VI. History

10 May 2013: To ensure the University's websites are accessible to all users and comply with standards of accessibility, Policy/Procedure 4.181 – Web Accessibility adopted and approved by the MSU Board of Regents.

11 May 2018: Revised to ensure that all web applications and web pages of the MSU website meet applicable federal and state law and regulations in order to better serve persons with disabilities.

5 Aug. 2021: Renumbered by MSU Board of Regents, effective 1 September 2021 (when MSU becomes a component institution of TTUS), as MSU Operating Policy/Procedure (OP) OP 44.02: Web Accessibility.

20 May 2022: Former MSU Policy/Procedure 44.02 completely revised and renamed Electronic and Information Resources Accessibility to align with TTUS. Approved by Interim President James Johnston.

James Johnston, Interim President
Midwestern State University

Date Signed: 5/20/22

~~University Operating Policy/Procedure (OP)~~
~~OP 44.02: Web Accessibility~~

~~**Approval Authority:** President~~
~~**Policy Type:** University Operating Policy and Procedure~~
~~**Policy Owner:** Vice President for Student Affairs~~
~~**Responsible Office:** Vice President for Student Affairs~~
~~**Next Scheduled Review:** X~~

~~I. Policy Statement~~

~~The creation and dissemination of knowledge is a defining characteristic of universities and is fundamental to the mission of Midwestern State University (MSU). The use of digital and web-based delivery of information is increasingly central to carrying out our mission. MSU is committed to ensuring equal access to information for all its constituencies. This policy establishes minimum standards for the accessibility of web-based communication and services considered necessary to meet this goal and ensure compliance with applicable state and federal statutes and administrative law.~~

~~II. Reason for Policy~~

~~All web applications and web pages of the MSU website must meet the requirements in Texas Administration Code (TAC) Rule §206.70 – Accessibility – (1 TAC §206.70), which references the standards in Section 508 of the federal Rehabilitation Act of 1973 that require all electronic and information technology be accessible to people with disabilities. The purpose of the policy is to ensure that MSU complies with the standards in TAC in order to better serve persons with disabilities.~~

~~III. Application of Policy~~

~~The MSU Web Accessibility Policy applies to all individuals responsible for designing, developing, and maintaining MSU web pages and web-based communication.~~

~~IV. Definitions~~

~~**Accessible:** A web page that can be used in a variety of ways and does not depend on a single sense or ability.~~

~~**ADA Coordinator:** The ADA Coordinator for the University manages University programs and responsibilities to assure compliance with the American with Disabilities Act (ADA), Sections 503 and 504 of the Rehabilitation Act of 1973, and other federal and state laws and regulations pertaining to persons with disabilities. The ADA Coordinator is responsible for coordinating University policies and procedures relating to persons with disabilities, tracking University progress relating to its policies and procedures as well as state and federal laws and regulations relating to persons with disabilities, and filing all necessary reports. See infra Responsible Office(s), section VII.~~

~~**EIR (electronic and information resources):** Includes information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, duplication, or delivery of data or information.~~

~~**EIR Accessibility Coordinator:** Per Rule §213.41(d) of Title 1, Part 10, Chapter 213, Subchapter C of the Texas Administrative Code, the head of each institution of higher education shall designate an EIR Accessibility Coordinator who shall be organizationally placed to develop, support and maintain its accessibility policy institution wide. The institution's designation must contain the individual's name and other information in the format published by the department. Such coordinator for MSU shall be the Section 508 Coordinator. See infra Responsible Office(s), section VII.~~

~~**Web-based communication:** The sharing of information, words, or ideas over a network of computers known as the internet.~~

~~**Web-page:** The static or dynamic content displayed on the internet that is identified by a unique Uniform Resource Locator (URL).~~

~~**Website:** Several interrelated and cross-linked web resources designed to function as a collective unit.~~

~~V. Procedures and Responsibilities~~

~~1. Each web-based application or web-page of MSU must contain a link for "Web Accessibility Policy," which directs users to this policy.~~

~~2. As required by 1 TAC Rule §206.70(d) for accessibility, "all new or changed web page/site designs must be tested by the institution of higher education using one or more Section 508 compliance tools in conjunction with manual procedures to validate compliance with this chapter."~~

~~3. Web Accessibility Standard~~

~~1. MSU departments use the internet for publishing information, communicating with the public and business partners, and for delivery of~~

~~applications in support of departmental missions. To ensure that department web pages are accessible despite physical, sensory, or environmental or technological barriers and in accordance with state and federal statutes and administrative law, MSU adopts the Web Content Accessibility Guidelines (WCAG) of the World Wide Web Consortium (W3C) as the standard for web accessibility.~~

~~2. Web pages published or hosted for or by MSU must comply with the current Web Content Accessibility Guidelines (WCAG) 2.0 AA.~~

~~See also OP 16.04 (Americans with Disabilities Act Policy), section V.F (Website Accessibility).~~

~~4. Training~~

~~The University's EIR Accessibility Coordinator and the University's compliance and ethics coordinating committee chairman (see MSU Policy 2.26 C.3.b.) will coordinate training programs in consultation with information technology, the webmaster, and distance education to educate MSU faculty and staff about the need for compliance with web accessibility requirements as well as the procedures to follow in adhering to these requirements.~~

~~5. Grievance Procedures~~

~~Employees or students who believe the University has not met its obligations under the ADA should consult with the University's ADA Coordinator, who serves all MSU sites and has overall responsibility for coordinating the efforts of the University to comply with the Americans with Disabilities Act (ADA) and investigating any complaints regarding the same.~~

~~**2. Related Statutes, Rules/Regulations, Policies, Forms, and Websites**~~

~~Related Statutes:~~
~~Texas Government Code Sections 2054.456, 2054.457~~

~~Related Rules:~~
~~Texas Administrative Code Title 1, Part 10, Chapter 206, Subchapter C, Rule §206.70~~
~~Texas Administrative Code Title 1, Part 10, Chapter 213, Subchapter C, Rule §213.30; Rule §213.32(2); Rule §213.41(d)~~

~~Related MSU Policies:~~
~~3.340: Americans with Disabilities Act~~
~~4.189: Disability Grievance Procedures~~

~~Related Forms/Websites:~~
~~MSU has made the following resources available for assistance:~~
~~https://mwsu.edu/Assets/documents/student-life/disability/ACCESSIBLE-ONLINE-COURSES.pdf~~

~~3. Responsible Office(s)~~

~~NOTE: Per Chapter 213.42(d) of the Texas Administrative Code, the head of each institution of higher education shall designate an EIR (electronic and information resources) Accessibility Coordinator who shall be organizationally placed to develop, support and maintain its accessibility policy institution wide. The institution's designation must contain the individual's name and other information in the format published by the department. Such coordinator for MSU shall be the 508 Coordinator.~~

~~Contact:~~
~~Section 508 Coordinator~~
~~Clark Student Center, Room 168~~
~~3410 Taft Boulevard~~
~~Wichita Falls, TX 76308~~
~~Phone:~~
~~(940) 397-4140~~
~~Email:~~
~~disabilityservices@mwsu.edu~~

~~Contact:~~
~~University ADA Coordinator~~
~~Clark Student Center, Room 168~~
~~3410 Taft Boulevard~~
~~Wichita Falls, TX 76308~~
~~Phone:~~
~~(940) 397-4120~~
~~Email:~~
~~disabilityservices@mwsu.edu~~

~~4. History~~

~~05/10/2013: Approved by the Board of Regents.~~
~~05/11/2018: Approved by the Board of Regents.~~

MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy/Procedure (OP)
OP 44.10: Information Technology (IT) ~~Policies and Procedures~~ 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

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

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

security testing and monitoring, misuse is subject to criminal prosecution, and 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

<u>Related Resources</u>:
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.

James Johnston, Interim President
Midwestern State University

Date Signed: 5/20/22

~~**University Operating Policy/Procedure (OP) 44.10: Information Technology Policies and Procedures**~~
~~**Formerly:**~~
~~**4.181 Administration & Institutional Effectiveness**~~
~~**INFORMATION TECHNOLOGY POLICIES AND PROCEDURES**~~
~~**Date Adopted/Most Recent Revision: 08/05/2011**~~

~~**A. General**~~

~~This policy applies to all users of the university's telecommunications, computer and network services. The university provides telephone, computer and network resources for use by students, faculty, staff and other persons affiliated with the university. The use of these resources is governed by this policy. Any violation of this policy or misuse of these resources, whether deliberate or incidental, may result in disciplinary actions according to university policies, as well as possible legal actions. Violations of security protocols in this policy shall be reported to the supervisor, the Chief Information Officer and the appropriate vice president or the provost.~~

~~B.~~ **Definitions**

~~**1. Telecommunications**~~

~~Hardware, software and personnel to provide audio and digital voice communications on and off campus. This includes the installation, maintenance and design of existing and future voice requirements.~~

~~**2. Computer Systems**~~

~~Midrange, server, and personal computer assets that are used for university administration, student development and academic endeavors. Use of these assets is governed by legal statues for copyrighted software, university developed software policy, and software developer licenses.~~

~~**3. Network Services**~~

~~Operations, equipment, maintenance and technical services that are provided to the university for the continued growth and development of the campus-wide communications network. These services include small computer software and hardware maintenance and installation of university-purchased equipment.~~

C. **Guidelines**

~~The university has established the following guidelines governing the proper use and workload management of Information Technology resources and personnel.~~

~~**1. Telecommunications**~~

~~All telephone outages will be reported by the user through the telephone outage reporting system at Ext. 4555. Requests for new installations, system reprogramming and telephone instrument relocations will be submitted using the Information Technology work order system.~~

~~**2. Computer Systems Programming Requests**~~

~~Information Technology service requests will be submitted using the Information Technology work order system. Once submitted, the data custodian for the area must approve the concept and access to specific data elements. Following approval from the data custodian to proceed, Information Technology will determine actual feasibility of the project and/or report. It is the practice of the university to not perform custom programming on purchased applications unless there is no other viable solution.~~

~~**3. Network Services**~~

~~Trouble resolution, technical solutions, network upgrades and network security services will be provided to the university by Information Technology. All services other than trouble reporting must be requested using the Information Technology work order system. This includes requests for technical solutions or network design.~~

~~4.~~ **Trouble Reporting**

~~Small computer software and hardware trouble reporting will be managed through the Information Technology Help Desk at Ext. 4278 or email at helpdesk@mwsu.edu. Users should report detailed information describing the problem. A work order will be assigned and tracked until completion. New installations of small computers will be accomplished according to the delivery schedule provided by the vendor. Any modifications to this schedule will be determined by the Chief Information Officer.~~

5. Technical Solutions

~~Technical solutions will be provided to the university faculty and staff to satisfy approved requirements for information technology equipment and software. These solutions will conform to the university guidelines established for interoperability and uniformity.~~

~~6. Network Upgrades~~

~~Information Technology will be responsible for the network upgrades that are consistent with university policy and technology availability. All upgrades will provide a migratory path for future conversions and implementations.~~

~~7. Laboratory Management~~

~~Information Technology is responsible for providing technical staffing for the general purpose student labs. This includes the following:~~

- ~~a. Provide general purpose software and qualified student employees for general purpose student labs.~~
- ~~b. Provide supplies and printer services as required during normally scheduled lab periods.~~
- ~~c. Provide first-look maintenance on equipment and outage reporting.~~
- ~~d. Maintain lab physical security and cleanliness.~~

~~8. Electronic Network Access~~

~~Users of the university electronic network facilities and services will indemnify and hold harmless the university against any and all actions or claims of infringement of intellectual property rights arising from the use of a network-based service or facility provided by the university. Network access is provided by password control. All passwords are managed and controlled by Information Technology. The following policies are established for network access:~~

~~a. Use of facilities and services in such a way as could be deemed foul, threatening, inappropriate, harassing, or abusive including but not limited to racial and sexual slurs, is prohibited.~~
~~b. All accounts are for the sole use of the student, faculty or staff of the university. Account information will not be released by Information Technology to any other individual.~~
~~c. Network access shall not be used for any non-university related activity. Use of network access should be consistent with the instructional, research, public service and administrative purposes and goals of the university.~~
~~d. A network access account may be requested by a currently enrolled student, employed faculty/staff member or emeriti faculty/administrator.~~
~~e. Student access will be deactivated upon the student's withdrawal from the university or non-enrollment.~~
~~f. Faculty and staff network access accounts will be deactivated upon termination of employment.~~
~~g. Unauthorized access to the network is strictly prohibited and could result in disciplinary action up to and including legal criminal action. Network account information is for the sole use of the original requester.~~
~~h. Electronic mail is subject to search at any time, with or without notice, as the university administration deems necessary. There should be no expectation of privacy.~~
~~i. Use of university electronic mail accounts to send unsolicited commercial mail is prohibited.~~
~~j. To best serve the general campus population and to conserve limited resources, remote access users will be limited to four (4) hours of on-line time per session.~~

~~9. Copyright and Computer Software~~

~~Midwestern State University and its students, faculty, and staff must maintain legal and ethical standards regarding the use of computer software. The unauthorized duplication of computer software, data or computer manuals, unless appropriate written consent is obtained, is grounds for disciplinary action and referral to the appropriate law enforcement or investigative agency.~~

- ~~a. In strict compliance with Public Law 96-517, Section 10(b), which, in amending Section 117 of Title 17 U.S. Code to allow for the making of computer software back-up copies, state in part "it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy of adaptation of that computer program provided:~~

  1. ~~"That such a new copy or adaptation is created as an essential step in utilization of the computer program in conjunction with a machine and that it is used for no other manner, or~~

2. ~~"That such a new copy and adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful."~~

3. ~~Where appropriate written consent (from the holder of such copyright) is obtained.~~

4. ~~Where the software is in the public domain and that can be proven.~~

b. ~~Under PL 101-650, phonograph records, computer programs, tapes, CDs or videos may not be rented, leased or loaned for direct or indirect commercial advantage. However, the nonprofit lease or lending of computer software (bearing the warning notice prescribed by the Register of Copyrights) to this institution's staff, faculty and students for their nonprofit use is exempt from these restrictions.~~

c. ~~Also exempt (from PL 101-650's restrictions) is the lawful transfer of possession of a lawfully made copy of a computer program between nonprofit education institutions and between such institutions and the individual comprising their staff, faculties, and student bodies.~~

d. ~~Illegal copies of software may not be used on this university's computers.~~

e. ~~Determination made under section 2 and 3 above are to be made by Midwestern State University and not the individual. Any indication of a violation of Section 4 will be promptly and thoroughly investigated.~~

f. ~~Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, is prohibited under this policy. This includes illegally downloading and/or sharing music and video files.~~

1. ~~Violations will result in disciplinary proceedings against the student. Sanctions given will be commensurate with the violation, and may include termination of computer privileges.~~

2. ~~Individuals violating this policy may face legal action, which could include fines and/or imprisonment.~~

10. ~~**Training and Education** (TX Admin. Code 202.77)~~

a. ~~The university will provide training during new employee orientation to familiarize employees with the rules of information security. Employees will be required to receive, sign, and agree to comply with the *Data Standards and Responsibility Agreement*. During orientation, employees will receive a copy of this policy, #4.181, and specific training on the importance of ensuring the confidentiality of information. Additionally, they will be informed of the proper computer use, computer account security, document handling, and verbal release of information. Before computer system access is granted, employees will be required to attend job-specific training provided by the relevant academic and administrative areas throughout the university.~~

b. ~~The university shall establish an ongoing information security awareness education program for all users. At least annually, or more often as needed when security issues arise, employees will be informed regarding information security procedures and safeguards.~~

11. ~~**Computer Security and Privacy**~~

~~All faculty and staff employees and students shall be responsible for complying with the Computer Security and Privacy policies. These policies are as follows:~~

~~a. The university president shall appoint an administrator responsible for developing and maintaining university regulations and procedures regarding security and privacy of computer data, software, and hardware.~~

~~b. Any student's or faculty/staff employee's use of university computing facilities is a privilege that shall be revoked for violation of this policy, regardless of the need for computer use in performing assigned duties or class work. Specific causes for revocations are as follows:~~

1. ~~Student, faculty or staff who intentionally gains access to a computer or file that is protected from general access by the public.~~

2. ~~Gaining unauthorized access to privacy protected information that may reside on university computer systems.~~

3. ~~Purposely placing or injecting a virus into the university computer systems or networks.~~

4. ~~Compromising computer network system security by responding to spam, phishing, and other email requests for release of secure computer system user names and passwords.~~

5. ~~Removing university computer assets from campus without prior approval.~~

6. ~~Connecting personally owned computers and software to the university networks without prior approval.~~

7. ~~Public domain (shareware) will not be downloaded from public access bulletin board systems to any user computer connected to the campus network. All software loaded on university computers will first be approved by Information Technology and certified virus free.~~

8. ~~User departments will identify to Information Technology personnel computer workstations used to store confidential or sensitive information or to run critical applications. The users will be responsible for notifying Information Technology for periodic virus scans.~~

9. ~~Users will not install personal computers onto the universityï¿½s network.~~

~~c. Some jobs or activities of the university involve access to resources critical to computer security and privacy. The university may require faculty/staff employees or students involved in these jobs or activities to disclose personal histories, participate in special training, and /or sign special agreements concerning computer use.~~

~~d. All students and faculty/staff employees shall cooperate with official state and federal law enforcement authorities in aiding the investigation and prosecution of any suspected infraction of security and privacy involving either university personnel or university computing facilities.~~

~~12. Computer System Access Control~~

~~The Chief Information Officer will maintain computer system integrity through the effective use of security controls. In an effort to control access to computing resources, the following policy is in effect:~~

~~a. Only employees of the university or approved student workers may be assigned a logon to allow use of computing resources. All passwords will be changed quarterly.~~

~~b. A logon will be assigned by Information Technology after verification by Human Resources of the individualï¿½s current employment with the university.~~

~~c. Each director level supervisor must determine the level of access (input vs. inquiry) for each employee within his or her supervision. A request for access must be approved through the appropriate area data custodian.~~

~~d. Each employee who is granted access to the university computing resources must be assigned a unique logon. Generic logons are not acceptable.~~

~~e. Assigned logon access and passwords must be protected from unauthorized use. Sharing of passwords or logging on in order for someone else to use the systems is a violation of university policy and strictly prohibited. Users may not request access to another personï¿½s password.~~

~~f. Assigned users shall be held responsible for any disruptive, destructive, or illegal activities originating from their assigned access and will be subject to disciplinary actions for misuse up to and including termination of employment and possible criminal prosecution.~~

~~g. No exceptions will be granted to this policy without written approval from the appropriate vice president.~~

~~13. Password Complexity~~

~~a. **Purpose** ï¿½ The purpose of this policy is to safeguard confidential information. Complex passwords will help protect user accounts and the information contained therein from being compromised by others.~~

~~b. **Scope** ï¿½ This policy applies to all users of the universityï¿½s computer and network services.~~

~~c. **Policy**~~

1. ~~All passwords must be at least eight characters in length, with a maximum length of 32 characters.~~
2. ~~Passwords must not have been used in four previous passwords.~~
3. ~~Passwords must contain at least three of the following four items:~~
    - ~~a. at least one upper case letter (A-Z),~~
    - ~~b. at least one lower case letter (a-z),~~
    - ~~c. at least one number (0-9),~~
    - ~~d. at least one special character (!@#$%^&*()<>?).~~

~~d. **Frequency** ï¿½ Passwords must be changed at least one every 90 days, but no more frequently than once every 30 days.~~

~~14. Computer Operations Center~~

~~The Chief Information Officer will maintain control and supervision of the production, scheduling and output of the Computer Operations Center. The following policies for services provided by the operations center are in effect.~~

~~a. The user departments are responsible for scheduling of processing and reports prior to the actual run time. Schedules will be made according to cycles (semester, month, week, etc.). All efforts will be made to conform to the customer requests providing other conflicts for processing do not take priority.~~

~~b. Input data should be checked for validity and accuracy by the submitting departments.~~

~~c. Output reports should first be checked for accuracy by Information Technology personnel and then rechecked by the user department before distribution and/or use. It is the user department's responsibility for accuracy of the reports.~~

~~d. All non-emergency requests for reports must be initiated by contacting Information Technology. This request will provide detailed information on the task as well as a realistic due date.~~

MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

University Operating Policy/Procedure (OP)
OP 52.41: Work Breaks

Approval Authority: President
Policy Type: University Operating Policy and Procedure
Policy Owner: Vice President for Administration and Finance
Responsible Office: Human Resources
Next Scheduled Review: ~~12/01/2022~~ 04/01/2024

I. Policy Statement

Work breaks are a privilege normally available to Midwestern State University employees; however, such breaks are not always legally required nor always a right under federal or state laws, regulations, or statutes.

II. Reason for Policy

The purpose of this Operating Policy/Procedure (OP) is to establish policies regarding break times for University employees.

III. Application of Policy

This policy applies to all University employees.

IV. Definitions (specific to this policy)

Employee: A benefit eligible employee employed to work at least 20 hours per week for a period of at least four and one-half months.

V. Procedures and Responsibilities

A. **Meal Breaks:** An employee may be given a meal break of 30 minutes to 1 hour in length. Meal breaks are not considered work time as long as the employee is completely relieved from duty. An employee is not completely relieved from duty if the employee is required or allowed to perform any duties, whether active or inactive, during a meal break. It is not necessary for the employee to leave the premises if otherwise completely freed from duties during the meal break. Unauthorized extensions of meal breaks may be deducted from the employee's vacation accrual balance or, in the absence of a vacation balance, the employee may be placed on leave without pay for the excess amount of time taken. Unauthorized extensions of meal breaks may be considered the basis for corrective action.

B. **Rest Periods:** Rest periods not to exceed (15) fifteen minutes in duration, may be allowed as near as is practical to the middle of each half of an eight-hour work day, if the work involved can be interrupted. Supervisors will standardize or stagger breaks among employees within the same area or office in order to maintain uninterrupted service. Supervisors may request that an employee not take breaks during heavy or emergency work periods. Rest periods are considered work time and are given at the discretion of the supervisor for which the employee works. Therefore, whether or not rest periods are granted, their frequency, regularity, and scheduling depend on the nature, level, and urgency of the work to be done and are subject to the approval of the employee's supervisor. Rest period time cannot be accumulated to provide for a prolonged time-off period, to cover lost time, to extend a meal break, or other purposes. Rest periods, when allowed, are for the employee's benefit only during a specific one-half day worked.

C. **Break Time for Nursing Mothers:** Employees who are nursing mothers shall be allowed reasonable break time as needed for the purpose of expressing breast milk. An employee shall be eligible for this benefit up to one year after the child's birth. If additional time is needed, a new request should be submitted to the supervisor for consideration. The frequency and duration of breaks for this purpose may vary as determined by the needs of the mother. Scheduling will be arranged on a case-by-case basis to accommodate the needs of the employee and the employing department. ~~Supervisors must provide a private space, other than a restroom, to be used by a nursing mother to express breast milk.~~ In accordance with federal and state law, the University will provide the following accommodations for a nursing mother to express breast milk: a work schedule, including scheduling break and work patterns, to provide time for the expression of milk; an accessible private location other than a restroom; nearby access to a clean, safe water source; and access to hygienic storage. A space temporarily created or converted into a private space for expressing milk is adequate as long as it is free from any intrusion by co-workers and the public. An employee seeking an accommodation under this policy needs to provide reasonable notice to the direct supervisor as early as possible. An employee is required to provide notice when this time is no longer required.

VI. Related Statutes, Rules, Policies, Forms, and Websites

Title 29 USC (United States Code) Section 207 (Maximum Hours)
Title 29 C.F.R. (Code of Federal Regulations) Part 785 (Hours Worked)
Texas Health and Safety Code Chapter 165 (Breastfeeding)
Texas Government Code Chapter 619 (Right to Express Milk in the Workplace)

VII. Responsible Office

Contact:	Human Resources
Phone:	(940) 397-4221
Email:	human.resources@msutexas.edu

VIII. Revision History

10 Nov. 1989: Adopted and approved by the MSU Board of Regents as Policy/Procedure 3.220: Work Break.

05 Nov. 2010: Revised to include a statement regarding break time for nursing mothers required under the Patient Protection and Affordable Care Act, Section 7 of the Fair Labor Standards Act, as amended 23 March 2010. Title changed to Work Breaks.

07 Aug. 2015: Revised to reflect changes in state law enacted by the 84th Texas Legislature concerning employees who are nursing mothers. Policy restriction "of children less than one year of age" deleted.

05 Aug. 2021: Renumbered by the MSU Board of Regents as Operating Policy/Procedure (OP) 52.41: Work Breaks.

20 May 2022: Revised to clarify a meal break and rest periods, and enable designation as a Texas Mother Friendly Worksite (component institutions Texas Tech University and Angelo State University currently have this designation). Adopted and approved by MSU Interim President James Johnston.

James Johnston, Interim President
Midwestern State University

Date Signed: 5/20/22