MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

Policy 4.197: Information Resources Use and Security Policy

Approval Authority:	University President
Policy Type:	University Operating Policy and Procedure
Policy Owner:	Vice President for Administration and Finance
Responsible Office:	Chief Information Security Officer
Next Scheduled Review:	11/01/2022

I. Policy Statement

It is the policy of Midwestern State University ("MSU" or "University") to:

- Protect information resources based on risk against accidental or unauthorized disclosure, modification, or destruction and assure the confidentiality, integrity, and availability of University data;
- Appropriately reduce the collection, use, or disclosure of social security numbers contained in any medium, including paper records;
- Apply appropriate physical and technical safeguards without creating unjustified obstacles to the conduct of the business of the University and the provision of services to its many constituencies; and
- Comply with applicable state and federal laws, rules, and regulations and University policies and procedures governing information resources.

II. Reason for Policy

Texas Government Code §2054.001 provides that information and information resources possessed by agencies of state government are strategic assets belonging to the residents of this state and must be managed as valuable resources, and it is the policy of this state to coordinate and direct the use of information resources technologies by state agencies and to provide the most cost-effective and useful retrieval and exchange of information between such agencies and branches of state government and the residents of this state and their elected representatives. University assets must be available and protected commensurate with their value and must be administered in conformance with federal and state laws, rules, and regulations, and University policies.

MSU Policy 4.197 provides requirements and guidelines to: establish accountability and prudent and acceptable practices regarding the use and safeguarding of the University's information resources; protect the privacy of personally identifiable information contained in the data that constitutes part of its information resources; ensure compliance with applicable University policies and state and federal laws, rules, and regulations regarding the management and security of information resources; and educate individual users with respect to the responsibilities associated with use of the University's information resources.

MSU Policy 4.197 serves as the foundation for the University's information security program, and provides the University's Chief Information Security Officer the authority to develop an MSU Information Security Handbook to implement procedures necessary for a successful information security program in compliance with MSU Policy 4.197 and applicable state and federal laws, rules, and regulations.

III. Application of Policy

This policy applies to:

- All information resources owned, leased, operated, or under the custodial care of the University;
- All information resources owned, leased, operated, or under the custodial care of third-parties operated on behalf of the University; and
- All individuals accessing, using, holding, or managing University information resources on behalf of the University.

To the extent this policy conflicts with MSU Policy 4.181 (Information Technology Policies and Procedures) this policy controls.

IV. Definitions

a. ***Business Continuity Planning*** - the process of identifying mission critical information systems and business functions, analyzing the risks and probabilities of service disruptions and outages, and developing procedures to continue operations during outages and restore those systems and functions.

b. ***Catalog*** – the Texas Department of Information Resources' (DIR) Security Control Standards Catalog.

c. ***Category I Confidential Information*** – confidential information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).

d. ***Category II Sensitive Information*** – sensitive information that could be subject to release under the Texas Public Information Act and should be controlled prior to release.

e. ***Category III Public Information*** – public information available for release as described in the Texas Public Information Act.

f. ***Chief Information Officer (CIO)*** – the person responsible for information resources across the whole of the University and implementing security controls in accordance with the University's information security program; also serves as the information resources manager (IRM) as defined in Chapter 2054, Subchapter D, Texas Government Code.

g. ***Chief Information Security Officer (CISO)*** – the person responsible for the administration and management of the University's information security program and developing the Information Security Handbook in accordance with this policy.

h. ***Data*** – elemental units, regardless of form or media, which are combined to create information used to support University business processes. Data may include but are not limited to: physical media, digital, video, and audio records, photographs, negatives, etc.

i. ***Incident*** - a security event that results in, or has the potential to result in a breach of the confidentiality, integrity, or availability of information or an information resource. Security incidents result from accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or modification of information resources or information.

j. ***Information*** - data as processed, stored, or transmitted by a computer that the University administration is responsible for generating, collecting, processing, accessing, disseminating, or disposing of in support of a business function.

k. ***Information Resources*** - 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.

l. ***Information Resources Custodian (Custodian)*** – an individual, department, or third-party service provider responsible for keeping and protecting information for the information owner.

m. ***Information Resources Manager (IRM)*** – the executive responsible for information resources across the whole of the University as defined in Chapter 2054, Subchapter D, Texas Government Code. This is the Chief Information Officer at MSU.

n. ***Information Resources Owner (Owner)*** – entity or person that can authorize or deny access to certain information resources, and is responsible for its accuracy, integrity, and timeliness. Note: In the context of this policy and associated standards, owner is a role that has security responsibilities assigned to it by TAC §202.72; it does not imply legal ownership of an information resource. All University information resources are legally owned by the University.

o. ***Information Security*** - the protection of information and information resources from threats in order to ensure business continuity, minimize business risks, and maximize the ability of the University administration to meet its goals and objectives. Information Security ensures the confidentiality, integrity and availability of information resources and information.

p. ***Information Security Handbook*** - the University's Information Security Handbook establishes the information security program framework for the University administration in accordance with this policy.

q. ***Information Security Program*** - collection of controls, policies, procedures, and best practices used to ensure the confidentiality, integrity, and availability of University-owned information resources and information.

r. ***Information System*** - is any organized system for the collection, organization, storage and communication of information; normally includes hardware, software, network infrastructure, information, data, applications, communications, and people.

s. ***Least Privilege*** – the security principle that requires application of the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

t. ***Mission Critical*** - a function, service, or asset that is vital to the operation of the University administration which, if made unavailable, would result in considerable harm to the University and its ability to fulfill its responsibilities.

u. ***TAC 202*** - Texas Administrative Code, Title 1, Part 10, Chapter 202 – information security standards that apply to all state institutions of higher education.

v. ***User*** – an individual, automated application, or process that is authorized by the owner to access the resource, in accordance with state and federal law, University policy, and the owner's procedures and rules. The user has the responsibility to (1) use the resource only for the purpose specified by the owner; (2) comply with controls established by the owner; and (3) prevent the unauthorized disclosure of confidential information. A user is any person who has been authorized by the owner of the information to read, enter, or update that information.

V. Procedures and Responsibilities

a. The University administration is required to adopt and implement an information security program, including an Information Security Handbook, to ensure compliance with applicable University policies and state and federal laws, rules, and regulations. The processes, procedures, controls and standards established to meet the requirements of this policy shall incorporate: (1) TAC Title 1, Part 10, Chapter 202; (2) NIST Special Publication 800-53 (Rev. 4): (3) the Texas Security Control Standards Catalog, Version 1.3 (2/26/2016); and (4) other required information protection standards as applicable, including but not limited to the following:

1. Access Controls: Establishing user identity, administering user accounts, establishing and monitoring user access to information resources to ensure confidential information is accessibly only to authorized users as defined in the Catalog, controls # AC-1, AC-2, AC-3, AC-5, AC-7, AC-8, AC-14, AC-17, AC-18, AC-19, AC-20, AC-22.

2. Awareness and Training: Requirements to ensure every information resources user receives adequate and ongoing training on computer security, maintains training records, and monitors the records for compliance as defined in the Catalog, controls # AT-1, AT-2, AT-3, and AT-4.

3. Audit and Accountability: Providing the means for authorized personnel to audit and establish individual accountability; maintain appropriate audit trails for updates to hardware and software; and maintain a sufficiently complete history to permit an audit of information resources system as defined in the Catalog, control # AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-8, AU-9, AU-11, and AU-12.

4. Security Assessment and Authorization: Designating an individual, independent of the information security program, to annually review the information security program for compliance and effectiveness and report their assessment to the president or his/her designee as defined in the Catalog, control # CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, and CA-9.

5. Configuration Management: Establishing a process to control modifications to hardware, software, and firmware with documentation to ensure information resources are protected as defined in the Catalog, controls # CM-1, CM-2, CM-4, CM-6, CM-7, CM-8, CM-10, and CM-11.

6. Contingency Planning: Develop, distribute, review, update, and communicate a contingency plan for the information system, coordinate contingency planning activities, and protect the contingency plan from unauthorized modification as defined in the Catalog, controls # CP-1, CP-2, CP-3, CP-4, CP-6, CP-9, and CP-10.

7. Identification and Authentication: Establish guidelines to verify the user, process or device for granting access to information system resources as defined in the Catalog, controls # IA-1, IA-2, IA-4, IA-5, IA-6, IA-7, and IA-8.

8. Incident Response: Assess the significance of a security incident based on the business impact and the technical effect, report all incidents immediately to supervisors and the CISO, and resolve the incident as required by federal and state rules as defined in the Catalog, controls # IR-1, IR-2, IR-4, IR-5, IR-6, IR-7, and IR-8.

9. Media Protection: Properly dispose of data processing equipment in accordance with Texas Government Code, Section 441.185, including sanitizing or removal of the storage device and keep records documenting all removals as defined in the Catalog, control # MP-1, MP-2, MP-6, and MP-7.

10. Physical and Environmental Protection: Document and manage physical access to mission critical information resource facilities to ensure protection from unlawful or unauthorized access, use, modification or destruction as defined in the Catalog, controls # PE-1, PE-2, PE-3, PE-6, PE-8, PE-12, PE-13, PE-14, PE-15, and PE-16.

11. Planning: Develop and implement a security plan for the information system that provides an overview of the security requirements or the system and describe the security controls in place or planned for meeting those requirements as defined in the Catalog, control # PL-1, PL-2, and PL-4.

12. Program Management: Ensure an information resources security program consistent with state and federal standards and shall designate an information security officer to administer the program as defined in the Catalog, controls # PM-1, PM-2, PM-3, PM-4, PM-5, PM-6, PM-7, and PM-16.

13. Personnel Security: Ensure all authorized users formally acknowledge that they will comply with the security policies and procedures or they will not be granted access to information resources as defined in the Catalog, control # PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, and PS-8.

14. Risk Assessment: Perform and document a risk assessment of information resources based on the inherent risk, and present the assessment to the president or his/her designee for approval as defined in the Catalog, control # RA-1, RA-2, RA-3, and RA-5.

15. System and Service Acquisition: Include security requirements and/or security specifications in acquisition contracts and include information security, security testing, and audit controls in all phases of system development or acquisition as defined in the Catalog, controls # SA-1, SA-2, SA-3, SA-4, SA-5, SA-9, and SA-10.

16. System and Communication Protection: Ensure confidential information transmitted over the internet is encrypted, and confidential information stored in a public location is encrypted as defined in the Catalog, controls # SC-1, SC-5, SC-7, SC-8, SC-12, SC-13, SC-15, SC-20, SC-21, and SC-22.

17. System and Information Integrity: Establish a security strategy to proactively detect and respond to security threats and events as defined in the Catalog, controls # SI-1, SI-2, SI-3, SI-4, SI-5, and SI-12.

As required by TAC, Title 1, Part 10, §202.71, the University's information security program shall be reviewed biennially and revised for suitability, adequacy, and effectiveness as needed. This review shall be performed by an individual independent of the information security program. This individual shall be designated by the President of the University.

b. Information Security Roles

1. The University President shall:

   (a) ensure the University's compliance with this policy and associated standards;

   (b) designate an individual to serve as the University's Information Security Officer (CISO) who shall:

      (1) serve in the capacity as required by TAC, Title 1, Part 10, §202.71 (b) with authority for the entire institution;

      (2) report to the University's Vice President for Administration and Finance (who reports to the President); and

      (3) have a dotted line reporting relationship to the University's Executive Oversight Compliance and Ethics Committee;

   (c) budget sufficient resources to fund ongoing information security remediation, implementation, and compliance activities (e.g., staffing, training, tools, and monitoring activities) that reduce compliance risk to documented acceptable levels;

   (d) approve the University's information security program and ensure compliance with applicable University policies and state and federal laws regarding the management and security of information resources;

   (e) in accordance with TAC, Title 1, Part 10, §202.71, designate an individual independent of the University's information security program to conduct a biennial review of the program for suitability, adequacy, and effectiveness, and ensure such revisions as needed are made; and

   (f) ensure appropriate corrective and disciplinary action is taken in the event of noncompliance.

2. The Information Resources Manager (IRM) shall implement security controls in accordance with the MSU information security program. The IRM is the University's Chief Information Officer (CIO).

3. The Chief Information Security Officer (CISO) is responsible for the administration and management of the University's information security program and developing the Information Security Handbook in accordance with this policy and shall:

(a) work in partnership with the University community to establish effective and secure processes and information systems and to promote information security as a core institutional value;

(b) develop and maintain in accordance with this policy a current and comprehensive institution-wide information security program that is in compliance with applicable University policies and state and federal laws, rules, and regulations regarding the management and security of information resources; and develop and maintain an Information Security Handbook (to be reviewed and updated at least annually and at other times as appropriate) to implement procedures necessary for a successful information security program in accordance with this policy, that includes risk assessment, action plans, training plans (that include educating individual users with respect to the responsibilities associated with use of the University's information resources), monitoring plans, physical security of information resources and a perimeter protection strategy, and specific risk mitigation strategies to be used by owners and custodians of mission critical information resources to manage identified risks, including business continuity and disaster recovery plans;

(c) develop and recommend institutional policies subject to approval by the Board of Regents in accordance with established University policy and procedures to ensure the protection of University information resources, including during the development or purchase of new computer applications or services;

(d) ensure that annual information security risk assessments are performed and documented by owners of mission critical information resources and information resources containing confidential information/data;

(e) approve, document, and justify any exceptions to any security controls, and include such exceptions in the annual report to the University President;

(f) specify and require use of appropriate security software such as anti-Malware, firewall, configuration management, and other security related software on computing devices owned, leased, or under the custody of any department, operating unit, employee, or other individual providing services to the University;

(g) communicate instances of noncompliance to appropriate administrative officers for corrective, restorative, and/or disciplinary action;

(h) investigate and manage security incidents and inform the University President of incidents posing significant risk to individuals, the University, or other organizations, and report a summary of security-related events to the Texas Department of Information Resources on a monthly basis;

(i) provide updates to the University's Executive Oversight Compliance and Ethics Committee; and

(j) ensure all reporting requirements of TAC, Title 1, Part 10, §202.23 and §202.73 are met, including but limited to a report, at least annually, to the

University President with copies to the MSU Chief Information Officer and the University's Executive Oversight Compliance and Ethics Committee on the status and effectiveness of information resources security controls for the whole institution in accordance in with this policy.

4. Functional Roles

   (a) Information owners have operational authority for specific information and are responsible for authorizing the controls for generation, collection, processing, access, dissemination and disposal of that information.

   (b) A custodian is the person responsible for implementing the information owner-defined controls and access to an information resource. Custodians are responsible for the operation of an information resource. Individuals who obtain, access, or use information provided by information owners for the purpose of performing tasks also act as custodians of the information and are responsible for maintaining the security of the information. Custodians may include employees, vendors, and any third party acting as an agent of, or otherwise on behalf of, the University administration.

   (c) A user is an individual, automated application, or process that is authorized by the owner to access the resource, in accordance with state and federal law, University policy, and the owner's controls and access procedures and rules. The user has the responsibility to (1) use the resource only for the purpose specified by the owner; (2) comply with controls established by the owner; and (3) prevent the unauthorized disclosure of confidential information. A user is any person who has been authorized by the owner of the information to read, enter, or update that information.

   (d) Guests, contractors, consultants, and vendors are considered external parties and shall adhere to this policy.

c. Secure Access and Management of Information and Information Resources

   1. All individuals who hold information security roles are responsible for ensuring the confidentiality, integrity, and availability of information and information resources that they access or use.

   2. Access to information and information resources shall be managed and controlled and shall be granted according to the principle of least privilege.

   3. Information owners and custodians must ensure that access to information and information resources shall be granted to a user only after the user has acknowledged that he or she will comply with this policy and shall be removed upon termination of employment, employment status change or termination of a written agreement. All users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University, must formally acknowledge and comply with MSU Policy 4.197 (Information Resources Use and Security Policy) by executing the Information Resources Use and Security Policy Agreement linked hereto and incorporated herein for all purposes. Any deviations from the terms of the agreement must be approved by the University's Office of the General Counsel.

4. All users of information shall receive annual security awareness training that is based on their information security role.

5. In accordance with applicable laws, this policy, and the University's Information Security Handbook, information shall be classified by information owners as category I, II, III. Information owners and custodians shall ensure that management, use, and access to information shall be based on its classification. The University's information/data classification standard consists of three mutually exclusive information/data classifications based on fit within a spectrum indicating the degree to which access to the information/data must be restricted and information/data integrity and availability must be preserved. The three classifications are as follows:

Information/Data Classification

Data Classification and Description	Examples	Comments
Confidential Information / Data Information (or Data) is classified as confidential if it must be protected from unauthorized disclosure or public release based on state or federal law or regulation, and by applicable legal agreement to the extent permitted by law. ***Historically, this type of information/data has been referred to as Category-I Information/Data.***	Patient billing information and protected health information subject to HIPAA or applicable state law. Student education records subject to FERPA. A credit card number associated with an individual's name. A social security number. Medical research information/data that contains protected health information. Certain student loan information subject to the Gramm-Leach-Bliley Act.	Information (Data) cannot simply be declared to be "confidential." This classification is reserved for information that is protected from public release based on state or federal law, or a legally binding order or agreement. Likewise, data cannot be declared to be "confidential" under all circumstances. Context is an essential element. (In relation to the Federal Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, this category equates to HIGH IMPACT for a Confidentiality, Integrity, and Availability breach.)
Sensitive Information / Data The sensitive classification applies to information/data that is not generally created for or made available for public consumption, but may be subject to release to the public through request via the Texas Public Information Act or similar state or federal law. ***Historically, this type of information/data has been referred to as Category-II Information/Data.***	Operational records, operational statistics, employee salaries, budgets, expenditures. Internal communications that do not contain confidential information. Research information/data that has not yet been published, but which does not contain confidential information protected by law or applicable legal agreement.	This classification likely encompasses the greatest volume of information/data within the University. (In terms of FIPS 199, this category equates to MODERATE IMPACT for a Confidentiality, Integrity, and Availability breach.)

Public Information / Data Published Information/Data includes all Data made available to the public through posting to public websites, distribution through Email, Social Media, print publications, or other Media. ***Historically, this type of Information/Data has been referred to as Category-III Information/Data.***	Statistical reports, fast facts, published research, unrestricted directory information, educational content available to the public at no cost.	Information can migrate from one classification to another based on information life-cycle. Unpublished research may fit the criteria of "controlled information" until published upon which it would become published information. (In terms of FIPS 199, this category equates to LOW IMPACT for a Confidentiality, Integrity, and Availability breach.)

6. Information and information resources shall be protected in accordance with the controls required under this policy and the University's Information Security Handbook and shall be implemented to ensure their logical and physical protection during all phases of their lifecycles.

7. Risks to information resources shall be managed in accordance with the requirements of this policy and the University's Information Security Handbook. The expense of security safeguards shall be commensurate with the value of the information and information resources being protected.

   (a) The University's President will commission University-wide security risk assessments of information resources as required in 1 Texas Administrative Code §202.72, as amended.

   (b) The University's President and the Chief Information Security Officer will develop risk management plans to address risks identified in the risk assessments of information resources.

   (c) The University's President or her/his designee is responsible for approving the applicable risk management plan and making risk management decisions based on the risk assessment and either accept exposures or protect the data according to its value/sensitivity.

   (d) If a public information request for the risk management plan or a risk assessment is received, the Office of the General Counsel for the University shall determine whether the requested information is exempt from disclosure under §2054.077(c) of the Texas Government Code.

d. Information Security Incident Management

1. The University's Chief Information Security Officer is responsible for managing security incidents.

2. Security incidents shall be reported to the University's Chief Information Security Officer and investigated promptly. All users shall cooperate during incident investigations and shall maintain the confidentiality of incidents and associated activities during all phases of incident handling.

e. Business Continuity Planning

Business continuity and disaster recovery plans shall be created and maintained for mission critical resources in accordance with the requirements of this policy and the University's Information Security Handbook.

f. Security Exceptions

Exceptions to security controls may be issued by the University's Chief Information Security Officer. Such exceptions shall be documented and justified and included in the annual report to the University President.

g. Sanctions

Penalties for violating this policy and/or the University's Information Security Handbook include, but are not limited to, the following: disciplinary action, access and usage loss, employment termination, criminal prosecution, civil litigation, and fines. Disciplinary actions imposed for violations of this policy may be grieved or appealed by the individual who is disciplined pursuant to existing University policies and procedures.

VI. Related Statutes, Policies & Procedures and Websites

a. Information Resources Use and Security Policy Agreement

b. MSU Information Resources Use and Security Handbook

c. MSU Policy 4.181 - Information Technology Policies and Procedures

d. Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C
§202.70, 202.71; 202.72; 202.73; 202.74; 202.75; 202.76

e. Texas Administrative Code, Title 1, Part 10, Chapter 203, Subchapter C

e. Texas DIR Security Control Standards Catalog V1.3

f. Texas Public Information Act, §552.139

g. National Institute of Standards and Technology Controls (NIST) Special Publication 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations

h. Payment Card Industry Data Security Standards

i. Texas Penal Code Chapter 33 (Computer Crimes), 33A (Telecommunications Crimes)

VII. Responsible Office(s)

Questions or comments regarding this Policy should be directed to:

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

Chief Information Security Officer
ciso@msutexas.edu
Extension 4680

VIII. History

05/11/2017:	Approved by the MSU Board of Regents.
02/11/2021:	Revised to incorporate references to the remaining 85 National Institute of Standards and Technology (NIST) controls required by the Texas Administrative Code (TAC), Title 1, Part 10, Chapter 202 for information security standards that apply to all state institutions of higher education. Additionally, references to specific named individuals on the last page of the policy were removed and replaced with those position titles (i.e., Vice President for Administration and Finance and Chief Information Security Officer) responsible for administering the policy.