MIDWESTERN STATE UNIVERSITY

Operating Policies & Procedures Manual

Information Resources Use and Security Policy Agreement

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

All individuals granted access to or use of University Information Resources must be aware of and agree to abide by the following:

I. **Definitions**:

- **University**: Midwestern State University (MSU).
- **University Information Resources**: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf.
- **University Data**: All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records.
- **Confidential Data or Confidential Information**: All University Data that is required to be maintained as private or confidential by applicable law (e.g., patient billing information and protected health information subject to HIPAA or applicable state law; student records subject to FERPA; a credit card associated with a person's name; a social security number; certain student loan information subject to the Gramm-Leach-Bliley Act).
- **User**: Any individual granted access to University Information Resources.

II. General

- University Information Resources are provided for the purpose of conducting the business of University. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties to University (Incidental Use) as permitted by this agreement in accordance with MSU OP 44.11 - Information Resources Use and Security Policy.
- Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University have no expectation of privacy regarding any University Data they create, send, receive, or store on University owned computers, servers, or other information resources owned by, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice.

- Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device.
- All Users must comply with applicable provisions of MSU OP 44.11, including the MSU Information Security Handbook, at all times.
- Users shall never use University Information Resources: to deprive access to individuals otherwise entitled to access University Information; to circumvent University computer security measures; or, in any way that is contrary to the University's mission(s) or applicable law.
- Users must not interfere with the activities of others or use a disproportionate share of University Information Resources. Examples of inappropriate use of resources are shown below. These actions frequently result in complaints and subsequent disciplinary action.
  - Sending an unsolicited message(s) to a large number of recipients (known as "spamming the network").
  - Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer (P2P) applications, streaming media at high bit rates, or serving a multi-user game).
  - Deliberately causing any denial of service, including flooding, attacks on ICMP (Internet Control Message Protocol), or the unauthorized automated use of a service intended solely for human interaction.
- Use of University Information Resources to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the User's official duties as an employee of University and is approved in writing by the President or a specific designee. Viewing, accessing, storage, and/or transmission of sexually explicit materials as Incidental Use is prohibited.
- Users should report misuse of University Information Resources or violations of MSU OP 44.11. How an incident is reported depends upon the nature of the incident:
  - If Users believe that their personal safety is threatened, they may call MSU Police, 397-4239.
  - For other incidents, Users should contact Information Security at 397-4680 or ciso@msutexas.edu.
  - For reporting problems with "spam" or unsolicited mail, Users may notify the Internet service provider (ISP) from which the mail was sent.

III. Confidentiality and Security of Data

- Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with University's records retention policy and records management guidelines (MSU OP 2.34 – Records Management Policy).
- Users must not use or disclose Confidential University Data, or data that is otherwise confidential or restricted, without appropriate authorization. Examples of groups that can provide appropriate authorization include, but are not limited to Office of Admissions, Human Resources Department, Office of the General Counsel, Information Security Office, and the University's Public Information Officer.
  - Users must ensure any individual with whom Confidential University Data is shared is authorized to receive the information.
  - Users may not share University Confidential Data with friends or family members.

    - Users may not share University business data that may be classified as Confidential Data, such as the status of negotiations, terms of contracts, and new research or products or relationships under development.
    - Users will comply with the University's agreements to protect vendor information such as software code, proprietary methodologies, and contract pricing.
- If User's office routinely receives requests for University Confidential Data, work with an appropriate group within the University to develop formal processes for documenting, reviewing, and responding to these requests.
- If Users receive a non-routine request for University Confidential Data from a third party outside of the University, check with an appropriate group within the University to make sure the release of the data is permitted.
- Users must report violations of University policies regarding use and/or disclosure of confidential or restricted information to the Information Security Office at 940-397-4680.
- Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on centrally managed services, rather than local hard drives or portable devices.
- Confidential or essential University Data stored on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smart phone, must be encrypted in accordance with the University's and any other applicable requirements.
- All Confidential University Data must be encrypted during transmission over a network.
- Users who store University Data using commercial cloud services must use services provided or sanctioned by the University, rather than personally obtained cloud services.
- Users must not try to circumvent login procedures on any University Information Resource or otherwise attempt to gain access where they are not allowed. Users may not deliberately scan or probe any University Information Resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences.
- All computers connecting to a University's network must run security software prescribed by the Chief Information Security Officer as necessary to properly secure University Information Resources.
- Devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources may be immediately disconnected by the University from a University network without notice.

IV. E-mail

- E-mails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements.
- Users are to use University provided e-mail accounts, rather than personal e-mail accounts, for conducting University business.
- The following e-mail activities are prohibited when using a University provided e-mail account:
    - Sending an e-mail under another individual's name or e-mail address, except when authorized to do so by the owner of the e-mail account for a work-related purpose.
    - Accessing the content of another User's e-mail account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the User's official duties on behalf of University.
    - Sending or forwarding any e-mail that is suspected by the User to contain computer viruses.
    - Any Incidental Use prohibited by MSU OP 44.11.

  - Any use prohibited by applicable University policy.

V. Incidental Use of Information Resources

- Incidental Use of University Information Resources must not interfere with User's performance of official University business, result in direct costs to the University, expose the University to unnecessary risks, or violate applicable laws or other University policy.
- Users must understand that they have no expectation of privacy in any personal information stored by a User on a University Information Resource, including University e-mail accounts.
- A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located.
- Incidental Use to conduct or promote the User's outside employment, including self-employment, is prohibited.
- Users may not be paid, or otherwise profit, from the use of any University-provided information resource or from any output produced using it. Users may not promote any commercial activity using University information resources. Examples include attempting to sell football/basketball tickets or used text books or advertising a "Make Money Fast" scheme via a newsgroup. Such promotions are considered unsolicited commercial spam and may be illegal as well.
- Incidental Use for purposes of political lobbying or campaigning is prohibited.
- Storage of any e-mail messages, voice messages, files, or documents created as Incidental Use by a User must be nominal.

VI. Additional Requirements for Portable and Remote Computing

- All electronic devices including personal computers, smart phones or other devices used to access, create or store University Information Resources, including e-mail, must be password protected in accordance with University requirements, and passwords must be changed whenever there is suspicion that the password has been compromised.
- University Data created or stored on a User's personal computers, smart phones or other devices, or in data bases that are not part of University's Information Resources are subject to public information requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources.
- University issued mobile computing devices must be encrypted.
- Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted.
- University Data created and/or stored on personal computers, other devices and/or non-University databases should be transferred to University Information Resources as soon as feasible.
- Unattended portable computers, smart phones and other computing devices must be physically secured.
- All remote access to networks owned or managed by the University must be accomplished using a remote access method approved by the University, as applicable.

VII. Password Management

- University issued or required passwords, including digital certificate passwords, personal identification numbers (PIN), digital certificates, security tokens (e.g., smart card), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.

- Users must not give others access to University Information Resources unless they are authorized and authenticated for such access. Users may not extend access to University Information Resources to others without permission.
- Each User will be held responsible for all activities conducted using the User's password or other credentials.

VIII. User Acknowledgment

I understand that I have received and read the University's Information Resources Use and Security Policy – MSU OP 44.11. I understand and agree that my use of University Information Resources is conditioned upon my agreement to comply with the policy and that my failure to comply with this policy, including the MSU Information Security Handbook, may result in access and usage loss, disciplinary action up to and including termination of my employment, 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.

Signature: ____ Date ____________________

Print Name: ___________________________________