MIDWESTERN STATE UNIVERSITY

Information Security Handbook

Department of Information Technology
Midwestern State University
Revised: May 2018

FOREWORD

The information age has changed our lives in ways that we can all feel: how we communicate, how we work, how we research, how we navigate our world, using extremely powerful information retrieval devices that in many cases fit right in the palms of our hands.

No longer is data processed or housed only on large central machines with access only by directly wired specialized systems. Access to information today is worldwide and instantaneous. Along with this new level of access and mobility come new challenges for organizations such as Midwestern State University. Never before has there been a time when our organizational data has been so available and at the same time so vulnerable to loss or public exposure. The threats facing our University today are many and their scope is breathtaking.

This handbook is written to help guide your understanding of organizational requirements for securing information in your individual areas and to serve as a ready reference for day-to-day operation of Midwestern State University information resources.

Each one of us acts as a human firewall. Our defenses against outside and inside threats to information privacy and our operating environment are only as good as our individual best efforts.

The artist and poet, Khalil Gibran, wrote:

> *"If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees."*

Never have Mr. Gibran's sentiments been more apropos than in today's information security environment.

Jim Hall
Chief Information Security Officer
Department of Information Technology
Midwestern State University

Table of Contents

I. Introduction and Overview of the Midwestern State University Information Security Handbook

The Midwestern State University (MSU) Information Security Handbook is written under the authority granted to the Chief Information Security Officer by MSU policy ***4.197*** and contains computing guidelines for University faculty, staff, students, campus guests, and vendors. The primary designee of the University for all Information Technology (IT) security related issues is the Chief Information Security Officer (CISO). Departments that work with faculty, staff, and student information whether financial, medical, academic, or any other sensitive information must read this handbook to become familiar with the guidelines listed within. This handbook also addresses Texas and federal laws such as Texas Administrative Code (TAC), Federal Education Rights and Privacy Act (FERPA), Health Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Digital Millennium Copyright Act (DMCA), and copyright law infringement.

II. Addressing Security Within the University Community

MSU supports the responsible use of its information resources. The information contained in this handbook is aligned with the requirements outlined in the Texas Administrative Code Title 1, Part 10, Chapter 202 , Subchapter C, entitled '***Security Standards for Institutions of Higher Education***' and MSU's "***4.197 - Information Resources Use and Security Policy***."

Information resources include, but are not limited to:

- Computers
- Servers
- Wired and wireless networks
- Computer-attached devices
- Network-attached devices
- Voice systems
- Cable systems
- Computer applications
- Digital signage

General User Access

This section defines the security standards and responsibilities of all Users of Information Resources at the University. All individuals using MSU information resources are prohibited from using a computer account for which they are not authorized, or obtaining a password for a computer account not assigned to them. It is the responsibility of all individuals (faculty, staff, students, and vendors) using MSU's information resources to protect the privacy of their account(s).

Password Guidelines

Users are responsible for the security of their passwords. Personal account information should not be released to friends, relatives, roommates, etc. Faculty and staff may visit or call the IT help desk to request that a password be reset. After the initial password is reset by IT personnel, faculty, staff, and students are immediately required to change the password after the first time it is used to ensure password confidentiality. All verification of personal information needed to complete a password reset is carried out according to applicable state and federal laws.

New or changed passwords must meet the following standards**:**

- Passwords should not be given by e-mail. A password given by phone will require the caller to provide information proving their identity.

- The network authentication system login requires complex passwords which must contain a character from at least three (3) out of the following four (4) character sets:
    - Capital letter (A-Z)
    - Lowercase letter (a-z)
    - Digit (0-9)
    - Special characters (such as !, $, #, %)
- Passwords must include a minimum of six (6) characters; longer is better.
- Passwords must not include any part of the username for which it allows access.
- All Users are required to change their network passwords at least once every 90 days, and password histories are automatically kept to ensure the passwords are not reused immediately. After a password is changed by an account holder, it cannot be changed again for 30 days.
- If any misuse of MSU's information resources is found, it is to be reported immediately to the appropriate management personnel. Any employee found to have violated this procedure may be subject to suspension of their MSU network and system access and/or disciplinary actions.

One of the most common security problems that Users encounter is unauthorized use of their computer accounts generally caused by sharing account credentials with others (i.e. other MSU employees, family, friends, and sometimes phishers). Account and password sharing is prohibited in all circumstances unless a documented shared account must be used to complete a task. A user must never log in as anyone other than himself or herself, and should not allow anyone to log in with his or her network account. Passwords should never be shared, written down, or disclosed to anyone - not even supervisors.

Authentication of Users

In order to use the University's computing environment, Users receive a unique network account that allows them to authenticate. Wherever possible campus systems should utilize IT managed authentication services to provide access in order to allow for proper access logging.

If a system cannot allow for the use of IT managed authentication services, an exception must be granted by the offices of the Chief Information Security Officer and the Chief Information Officer. The exception request must include plans for monitoring security logs for system access, patching, maintenance procedures, and revision frequency.

User Access to University Resources

A network account is provisioned for all MSU Users and is the account used to gain access to University resources (desktop, e-mail, internet, etc.) All Users are given specific e-mail quotas. Users will receive access to User and departmental file shares upon request. Contractors are given access on a case-by-case basis and at the request of the hiring department and will not receive an MSU e-mail address.

Users must never give their network account login information to anyone and should never ask another User to share his or her login information with them.

A User's access to University resources will be terminated upon appropriate notification and documentation.

Network Access

This section defines the responsibilities of all Users at the University with regard to network access. The owner or designated assignee of a computer that is attached to the MSU network is responsible for both the security of that computer system and for any intentional or unintentional activities from or to the network connections. Owners or designated assignees are responsible for all network activity originating from their equipment, regardless of who generates it. Any network-intensive application or defective computer that causes network overload shall be reviewed, and if necessary, steps shall be taken to protect other Users and the overall MSU network. This includes contacting the offending party (if applicable) and disconnecting the defective computer system from the network until the problem is resolved. If the condition is an imminent hazard to the MSU network or disrupts the activities of others, the defective computer system or the subnet to which it is attached will be disabled without notice. The operator of the defective computer system will not be allowed to re-connect to the network until they follow explicit instructions from IT or IT help desk staff for securing the machine.

Non MSU-owned hardware must never be connected to the MSU wired network.

It is the responsibility of every person using MSU's information resources to refrain from engaging in any act that may seriously compromise, damage, or disrupt the MSU network. This includes, but is not limited to, tampering with components of a local area network (LAN) or the backbone, blocking communication lines, interfering with the operational readiness of a computer, creating/operating unsanctioned servers or personal Web servers or File Transfer Protocol (FTP) sites, or accessing/delivering unsanctioned streaming audio, video, or high bandwidth content such as gaming, music sharing, or non-University sanctioned video conferencing.

The content of any files or services made available to others over the network is the sole responsibility of the User with ownership of and/or administrative authority over the computer providing the service. It is this User's responsibility to be aware of all applicable federal (FERPA, HIPAA, GLBA, DMCA) and state laws, as well as MSU policies. The User shall be liable for any violations of these laws and policies.

Network/internet connections used to share copyrighted materials (files, programs, songs, videos/movies, etc.) without permission of the copyright owner(s) violate the Digital Millennium Copyright Act (DMCA). When informed by the copyright holder of a potential copyright violation, the University is required by federal law to remove the copyrighted materials from the system in question. If MSU is unable to remove these materials for any reason, network access for the system in question will be terminated until the removal of the infringed materials is verified.

Users should refrain from using an Internet Protocol (IP) address not automatically assigned to them and should not attempt to create unauthorized network connections or unauthorized extensions, or re-transmission of any computer or network services.

If any misuse of MSU's network resources is found, it is to be reported immediately to the appropriate management personnel and may be subject to criminal prosecution.

Handling of Sensitive/Confidential Information

MSU personnel who deal with sensitive and/or confidential information concerning students and employees must be cognizant of their responsibilities concerning that information and exercise due caution when dealing with confidential or sensitive information. Measures should be taken against

disclosing information to unauthorized employees, contractors, vendors, parents, etc.

Sensitive/confidential information typically falls under the provisions of laws and regulations that impose security requirements designed to prevent unauthorized access to those records. Examples of such laws are the Health Information Portability and Accountability Act (HIPAA), which regulates access to Protected Health Information, and the Gramm-Leach-Bliley Act (GLBA), which regulates access to non-public financial information about a University customer or employee, and Family Educational Rights and Privacy Act (FERPA), a law that protects the privacy of student education records.

In order to properly secure information:

- Privacy screens are recommended for any computer that displays sensitive or confidential information and is used in public areas
- Workstations must be locked when left unattended for any length of time
- Workstations should be required to have a password to regain access when the workstation goes into sleep mode
- Confidential or sensitive printed information should not be left in plain view, should be secured when not in use (locked file cabinet, desk), and locked away after business hours
- Disposal of electronic as well as paper records is subject to the retention requirements set up by the State of Texas and the MSU records retention officer
- Should paper records need to be destroyed, the information should be shredded before discarding
- Disposal of MSU electronic media must be completed per the ***Media Sanitization and Disposal*** section of this handbook.

Example of confidential/sensitive information includes but is not limited to:

- Passwords
- Social Security Numbers
- Performance reviews
- Most student information including schedules, grades, and student payroll information
- Confidential memos
- Medical information
- Credit card numbers
- Employee payroll information
- Budgetary/financial information

Any abuse or disclosure of confidential or sensitive information whether accidental or deliberate, must be reported immediately to the appropriate management personnel.

III. Acceptable Use of University Information Resources

The purpose of this section is to outline guidance, rules, and acceptable practices for the use of information resources at MSU. All Users of the University's computing environment are also responsible for adherence to any State or Federal regulations regarding computer use at the University. This applies to all Users of the MSU wired network, wireless network, web services, e-mail, and computing resources, including any and all technical systems and services provided or owned by the University. Access to computing resources at the University is a privilege, not a right, and is granted with restrictions, responsibilities, and proper documentation for use.

MSU reserves the right to limit, restrict, or extend privileges and access to its resources.

Security Awareness Training

Understanding the importance of information security and individual responsibilities and accountability pertaining to information security are paramount to achieving organizational security goals. This can be accomplished with a combination of general information security awareness training and targeted function-specific training. All MSU personnel who use information resources are required to participate in annual security awareness training.

New employees are required to complete security awareness training prior to, or at least within 30 days of employment. No access to systems containing confidential information will be granted until training has been completed.

Annual security awareness training for all employees will be made available on August 1st of each year and must be completed by April 30th of the following year. Accounts for Users not completing the security awareness training program will be disabled.

MSU makes this training available on the web and it can be accessed by the Security Awareness Training link provided here.

All Users must acknowledge they have read, understand, and will comply with University requirements regarding computer security policies and procedures as part of the annual Security Awareness Training program.

Network Access Accounts

All new employees at MSU are given specific information on getting and protecting their User accounts either during or prior to new employee orientation. In addition, they are required to sign the ***"Information Resources Use and Security Policy Agreement"***, which outlines their duties and responsibilities with all University information. Users are responsible for all activity performed with their MSU network access account.

All accounts may be disabled, revoked, or deleted if account privileges are no longer commensurate with an individual's function at the University or their need-to-know due to changes in their status.

All accounts may be disabled, revoked, or deleted if it is determined the account has been compromised or misused.

Disabled, revoked, or deleted accounts may be reinstated at the direction of the Chief Information Officer or Chief Information Security Officer.

Under normal circumstances, accounts will persist under the following schedule:

- ***Student Accounts*** – 13 months after the student is no longer associated with MSU
- ***Employee (Faculty/Staff) Accounts*** – account will be disabled based on the separation date listed in the terminating EPAF in Banner or upon dismissal
- ***Consultant/Support Accounts*** - Until the account is no longer needed
- ***Emeritus Retiree Accounts*** - Until the account is no longer needed; Banner INB access will be disabled on the separation date listed in the terminating EPAF in Banner.

If a User has problems with a network account, he or she can contact the MSU help desk by calling (940) 397-4278.

Banner INB Access Accounts

All employees requiring access to business functions and data hosted in the Banner system are granted Internet Native Banner (INB) access based on approval of the data owner of the system for which access has been requested. Banner systems and the appropriate data owners are listed below:

System	Data Owner
Banner Student	Registrar (msuregistrar@mwsu.edu) Director of Admissions (msudirectorofadmissions@mwsu.edu)
Banner Financial Aid	Director of Financial Aid (msudirectoroffinancialaid@mwsu.edu)
Banner Human Resources	Director of Human Resources (msudirectorofhumanresources@mwsu.edu) Director of Payroll (msudirectorofpayroll@mwsu.edu)
Banner Finance	Controller (msucontroller@mwsu.edu)

Requests for INB access are to be made directly to the data owner. Once the data owner has determined what access should be granted for a specific new User, he or she will send an e-mail to helpdesk@mwsu.edu with the requested account creations and/or permission changes. The Help Desk Analyst will then:

- verify the identity and employment information for the User being given access,
- complete the requested account creations and/or permission changes,
- notify the User of any User name and/or password changes, and
- notify the data owner that the request has been completed

INB access will not be granted until a User has completed security awareness training.

Departmentally Managed Accounts

For access to sensitive information managed by a department, account management should comply with the standards outlined above. In addition, naming conventions must not cause contention with centrally managed e-mail addresses or usernames. Should the potential for contention arise, the applicable system(s) should not be connected to the campus network until a mutually satisfactory arrangement is reached.

Vendor Accounts

Employees of independent contractors and vendors needing accounts for access to MSU information resources are required as well to sign the "***Information Resources Use and Security Policy Agreement***" before they are given access to any University information resources.

Vendor accounts are monitored by IT and are granted least-privilege access to resources with a documented requirement. All requests for vendor access must include an end date.

Guest Accounts

Official guests of the University can request an account for use at the University but are under the same restrictions as those on a Vendor account (e.g., must sign agreement, limited secure access, expiration dates, etc.) and are required to have a University sponsor to gain access to the MSU

network.

Assignment/Use of University Equipment
All MSU information resources equipment is tagged for inventory purposes and assigned either to an individual or department by Information Technology in coordination with the owning department.

All personnel requiring the use of individual workstations or assigned laptops are considered the custodians of that equipment and as such are expected to follow University guidelines concerning the securing of that equipment and University data on the equipment.

Equipment taken off campus (e.g., desktops, laptops, printers) require the custodian of that equipment to sign a yearly Request to Remove Tracked Property From Campus Form stating where the equipment is to be housed.

Personal information including iTunes music files, movies, photos, etc. shall not be placed on any University network shared resource and is subject to removal without notice.

- 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 except in accordance with MSU Faculty Intellectual Property Rights Policies 3.139 and 3.140. Users may not promote any commercial activity using University information resources. Examples include attempting to sell football/basketball tickets or used textbooks 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.

Any abuse or theft of University equipment whether accidental or deliberate, should be reported immediately to appropriate management personnel.

Midwestern State University E-mail
This section defines the responsibilities of all Users at the University with regard to e-mail.

E-mail accounts are only created after proper documentation has been supplied to the University. Any person using e-mail should not send excessive e-mail, attachments, or messages locally or over the network. As a general guideline when sending out an e-mail to a large audience, the e-mail messages should be of sufficient general value that it would justify being sent as a memorandum if e-mail were not available. Campus-wide e-mail discussions should use a Listserv (automated mail subscription

service) when possible. The IT department can make these available on request for faculty and staff with proper authorization from supervisors of that department.

Electronic mailboxes are not deemed to be private and are subject to review by management personnel after appropriate management approval is first obtained. All inbound and outbound e-mails are archived centrally in line with the e-discovery guidelines in the Federal Rules of Civil Procedure.

No User of MSU e-mail may take any of the following actions:

- Send 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
- Send or forward an e-mail through a MSU system or network for any purpose if such e-mail transmission violates laws, regulations or University policies and procedures
- Use any e-mail system other than an approved MSU e-mail system to conduct University business or to represent oneself or one's business on behalf of the University. Examples of e-mail systems that are not approved include a personal e-mail (i.e. username@gmail.com) account or a personal MSU alumni account (i.e. username@alumni.mwsu.edu)
- Send nuisance e-mail or other online messages such as chain letters
- Send obscene or harassing messages
- Send unsolicited e-mail messages to a large number of Users unless explicitly approved by the appropriate University authority
- Impersonate any other person or group by modifying e-mail header information to deceive recipients

Any misuse of University e-mail whether accidental or deliberate, should be reported immediately to appropriate management personnel. The University reserves its right to limit capacity on individual e-mail accounts for archival storage and other University purposes.

Each User shall ensure that sensitive or confidential data is transmitted by e-mail only if the following conditions are met:

- All e-mail communications of confidential data are encrypted before being transmitted
- No sensitive data will be transmitted in the "Subject" line of an e-mail
- Before transmitting an e-mail that contains sensitive data, the User double-checks the message and any attachment to verify that no unintended information is included and that the proper document is attached
- Before transmitting an e-mail that contains sensitive data, the User double-checks the identity of the recipient

Authorized Software

The University has standard software applications that are applied to all University owned workstations at time of installation. Designated software licensed by the University for home use may be installed on personally owned and/or home computers.

All software purchased or installed must be licensed to and owned by the university. IT maintains a library of centrally-licensed software, licenses, and software documentation. Departmentally purchased software shall be installed in consultation with MSU IT.

Software purchased or installed by an individual, using personal funds, will be licensed to and owned by the individual and is not to be installed on MSU systems.

University departments are responsible for assuring that all software used and purchased by their department is fully licensed. The primary User of each computer is responsible to keep records of licenses for each item of software purchased or installed by the individual.

No person shall make or distribute by any means, copies of software without first possessing a lawful copy, and then only in compliance with the applicable software license. All copies must carry a complete copy of the applicable software license documentation. Copies made under license purchased by the university remain the property of the university.

License keys, installation codes, and other installation credentials shall be obtained only from legitimate sources, and shall not be shared except only by authorized individuals acting within the scope of their employment. Unauthorized possession and/or distribution of installation credentials is a violation of the ***Information Resources Use and Security Policy Agreement***.

Software versions rendered obsolete by virtue of upgrade may not be used after the upgrade has been performed, except only as may be permitted under the applicable software license.

Software found to be obtained and/or used contrary to the policies of the University, will be removed from any computer on which it is found. User-installed software will be removed if the software is detrimental to the University network environment.

Software that should never be installed on MSU systems:

- Peer to peer file sharing software
- Freeware/shareware *NOT* specifically checked by MSU IT
- Licensed software *NOT* owned by MSU
- Security products not standardized for use on MSU systems by MSU IT
- Internet access anonymization software

Authorized Computer Lab Software

Faculty may request certain software be applied to a computing lab if required for teaching classes. If a User needs software installed in the academic computing labs, electronic classrooms, or presentation classrooms for the purposes of teaching MSU accredited courses, he or she may make the request through the MSU help desk at extension 4278 or helpdesk@mwsu.edu.

Software installation in campus computer lab facilities must be completed per the requirements below:

- All software will be tested in advance by a qualified member of IT staff
- Installations will be done on a master image workstation from which all computers in the labs are loaded
- All requests for new software in the computer labs must be submitted to IT for testing no later than 30 days before the start of classes for the semester in which the software is to be used
- Lab software installations will be done from MSU purchased/licensed software or from IT approved and tested open source or freeware
- No personally owned software will be installed in MSU computer labs

- Software to be installed must be installed on all computers in a lab facility. If a proper number of licenses is not to be purchased to allow the software to run concurrently on all systems, the software must be network licensed
- Software to be installed in MSU computer labs will support the currently installed and tested operating system in use
- Software requested for installation in MSU computer labs must be suitable for intended academic class work
- All software is subject to administrative review by IT management. Software packages deemed inappropriate for use in computer labs may be refused. Examples of such software would be anything that compromises the basic configuration of the workstation or network security
- Security or hacking tools that could be used to compromise the network or any other software that would act contrary to the ***"Information Resources Use and Security Policy Agreement"*** will also not be allowed

Some software packages may be intended only for use as a demonstration. These packages may be installed on the instructor workstation only with the approval of IT. These demonstration packages may not be subject to all the guidelines and requirements listed above. If a User has a software package to use in the computer lab, it is recommended he or she contact IT well in advance of any aforementioned deadlines to discuss whether the software is best suited as a demonstration or for general computer lab installation.

If the software is for demonstration only, it will likely be less expensive possibly or even free to use the single copy on the instructor workstation, rather than purchasing licensing for the entire computer lab.

Virus scanning software is already present in computer labs and is maintained by IT.

Physical Access

Access to all University data center facilities is under the strict control of the Chief Information Officer and is limited to IT personnel. In cases where vendors may need access to the data center, they will be accompanied by IT personnel who will ensure the access is logged with valid entry and exit times.

Public access computer labs are monitored by IT. Any problems with lab equipment can be reported to the MSU help desk by calling (940) 397-4680. Access to the electronic classrooms and departmental labs is strictly regulated by the classes taught in those labs.

Public access computer labs are available to students during regularly scheduled times which are published on the MSU website-lab schedule.

Remote Access (VPN)

Remote access is limited to faculty and staff Users. Students currently are not allowed remote access into MSU with any remote desktop software. The University only allows remote access to protected resources with the use of MSU IT approved security protocols.

To obtain remote access, faculty and staff members must complete the VPN Access Request form completely and return to MSU IT before any VPN remote access will be granted.

Third parties requiring remote access will only be granted access after a management level

sponsoring employee requests the access for the 3rd party and a 3rd Party VPN Access Request form has been completed and filed with MSU IT.

If remote access is necessary, the following restrictions apply:

- Remote access sessions must be encrypted using SSH, VPN, or similar technologies
- Remote access is provisioned to the fewest number of IP addresses possible (preferably only one)
- Proper VPN access request forms have been completed and filed with MSU IT

Wireless Computing

The primary goal of all wireless designs shall be ubiquitous service to the broad university community. Private interests are secondary design criteria. Wireless networks shall be independent of local wired networks except in case of wireless networks that by design provide access to MSU owned wireless devices that must connect to resources in classroom networks to properly function or aid in instruction.

Faculty and staff must use appropriate technology when accessing confidential employee or student data over wireless connections. The MSU wireless network provides two public Service Set Identifiers (SSID) campus-wide.

- ***MSUWirelessNetwork***: This SSID provides an ***unecrypted*** wireless connection for 75 days or if registered as a guest will provide connection for 7 days. Guest Users will have access to the Internet and the University web site only. No transmission of confidential information by wireless connectivity may be done using this SSID. Instructions for connecting to this network are available on the MSU Information Technology website.

- ***MSUSecureWireless***: This SSID provides an ***encrypted*** wireless connection using network access account credentials for faculty, staff, and students. All transmission of confidential information by wireless connectivity must be done using this SSID. Instructions for connecting to this network are available on the MSU Information Technology website.

All wireless access to University networks is to be designed, installed, and operated by MSU IT. Individual departments are prohibited from extending University networks by any means. All wireless access to University networks is to be authenticated by MSU IT managed systems.

Wireless services should be considered “best effort” and not suited for activities requiring highly reliable service levels.

Media Sanitization and Disposal

While the primary purpose of this section is to protect non-public MSU data, it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge all University data from the media before reuse or disposal rather than try to selectively sanitize the data.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the University, all University data must be purged from the media before giving it to the third party. Media containing

MSU data in equipment that will be reused outside the United States must comply with export laws and regulations. MSU departments responsible for electronic protected health information covered by HIPAA must also have media sanitization and disposal policies and procedures in accordance with HIPAA Security Final Rules, Section 164.310, Physical Safeguards, part (d), (1) & (2).

Electronic Storage Media

- If purging is done by overwriting the data, the entire media/device must be overwritten with a minimum of three passes.
- Equipment that can store University data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the University should have all data storage devices removed before disposition. If the equipment leaving University control must retain the data storage devices, all University data must be properly purged.
- National Institute of Standards and Technology (NIST) compliant degaussing is the preferred method of purging data from magnetic media. Be aware that this renders the media unusable.

Paper-Based Media

- Any paper-based or other hard copy media containing confidential University data must be shredded before disposal or transferred to an authorized third party contracted by the University for secure disposition of documents
- Incineration by methods compliant with all relevant health, safety, and environmental laws and regulations is an acceptable method for disposal of paper-based media

Optical Media (e.g. CDs, DVDs, Blu-Ray)

Optical media containing confidential or sensitive University data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

Smartphones/Handheld Devices

Mobile devices like smartphones (e.g. Android, iPhone), MP3 players, and even cell phones, store information and often contain personal or other sensitive information. Any University data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.

Other Media Types

For other media and additional guidelines, refer to NIST Special Publication 800-88, Revision1: Guidelines for Media Sanitization, Appendix A, Minimum Sanitization Recommendations.

IT can facilitate the proper disposal of magnetic media such as hard drives, optical media, etc. To request assistance with proper disposal of such media please contact the IT help desk at extension 4278 or helpdesk@mwsu.edu.

Malicious Code Protection

Users should not willfully introduce virus-infected media or other foreign materials into any University systems. Standardized IT-managed anti-virus software is required on all University devices and on all devices connected to the network, including off-campus computers.

IT will monitor network activity and take appropriate action to control infection. Any server or client known to be an infecting agent will be disconnected. Infected systems will not be re-connected to the MSU network until certified to be safe by IT staff.

Users will not intentionally develop or experiment with malicious programs and are prohibited from knowingly propagating malicious programs including opening attachments from unknown sources.

Standardized MSU anti-virus solutions will provide malicious program detection, protection, eradication, logging, and reporting capabilities for IT systems and Users. Malicious program protection should eliminate or quarantine malicious programs detected; provide an alert notification; automatically and periodically runs scans on memory and storage devices; automatically scans all files retrieved through a network connection or from an input storage device; allow only authorized personnel to modify program settings; and maintain a log of protection activities.

Systems and Services Acquisition

When acquiring new Information Resources and Services the following procedures must be followed:

- During project inception/planning, well ahead of purchase, the CISO shall be involved to perform an information security review, document and address security requirements, weigh cost against operational requirements, and provide risk analysis. As the project moves forward both Information Technology and the CISO should review all potential contracts to make certain that risk is properly evaluated and recommend changes to contract language if needed. All contracts for Information Resources must specify security requirements and Midwestern State University will vary security strength requirements based on system risk posture.

- Midwestern State University data owners must obtain, protect and make available to authorized personnel adequate documentation to secure university information systems.

- Midwestern State University CISO will require vendors to secure university information, systems, and information under their control to the level required by assessed risk posture.

- Midwestern State University Data Custodians must monitor cloud services and report security discrepancies to vendors for correction.

- Midwestern State University information owners must approve security-related information system changes through a formal change management process prior to implementation. Using a formal change management process, Midwestern State University must correct security flaws in information systems as soon as practical considering risk posture.

- Discrete line item budget information must be provided for all systems with regard to information security and sufficient resources must be allocated to support information security requirements throughout the lifecycle of the system.

- Information security requirements, security testing and audit controls across the development and/or acquisition must be maintained for the lifecycle of university information systems. Roles and responsibilities for managing information security requirements must be maintained across the lifecycle of university information systems.

- Newly acquired systems must separate production and test environments and their associated data except in cases where the risk to production information is low and data owners and custodians involved in testing are authorized access to the data. All acquisitions must be subject to continuing information security review and approval as part of the change management process throughout the lifecycle of the system.

IV. Other Issues

Malicious Code and E-mail

All Users must refrain from downloading e-mail from people they don't know or opening attachments that look suspicious as they can bring malicious code such as viruses, Trojans, etc. into the University's environment.

An e-mail may look legitimate but usually has red flags that help identify it as suspicious. Words may be misspelled, floating the cursor over the hyperlink may indicate that the URL behind the link is not what is expected, the e-mail asks for information that is not common (example: your password) or may indicate a User must do something to verify User information. Always contact the sender if there is any question with regard to the veracity or provenance of an e-mail.

If any e-mail looks suspicious, the purported sender should be contacted to verify the veracity of the communication.

V. Security Within the University's Computing Environment

All enterprise-wide servers that deliver services across the University network are either under the management of or audited by IT. Any department or person that wishes to connect a server to the infrastructure of the University's network environment must notify the IT Department for guidance and approval.

Requirements for Midwestern State University Servers

No server may be connected to the MSU network unless and until it complies with the following minimum technical and security standards:

- All servers that deliver services across the University network must be part of the University's network
- The server must run an approved and appropriately licensed server operating system supported by IT
- The server must employ intrusion protection measures appropriate to its operating system, such as virus protection software, an independent intrusion protection appliance, and/or a host based firewall
- Applications that require e-mail services (e.g., SMTP) must be configured to direct all outbound e-mail through a designated, IT administered, e-mail gateway. Outbound e-mail not configured in this manner will be blocked
- Vulnerability patches and updates must be applied regularly, typically within 72 hours of becoming available and vendor certified. If compliance with this standard will conflict with operation or support of any application(s) hosted on the server, the server administrator must contact IT to identify alternative protective measures

Any departments that plan to buy new servers that will be used to house confidential information of any type must request project approval and guidance from the Chief Information Officer.

Prior to the sale or transfer of any hardware, IT requires that:

- Notification to the department is made so that inventory records can be updated as to the status of the hardware
- An assessment is made by the data owners to remove data from any associated storage device and how that data will be removed (i.e. transferred to another location or destroyed)
- Confidential or sensitive information on that equipment be destroyed or relocated to type of secured media approved by IT
- Computer systems that are brought back in from the field as part of the faculty and staff desktop computing or computer lab refresh programs or from other deployments are inventoried and inspected. The returned hardware is to be re-imaged with a current IT-built system image appropriate for the hardware. Once this process is completed successfully, the systems are moved to a secured storage area and are ready for re-assignment

The following services are prohibited outside of the centrally administered services provided by IT and must be disabled whenever the server is connected to the University network unless previously approved by IT:

- Anonymous File Transfer Protocol (TFTP)
- Domain Name Service (DNS). This service is allowed only on the University's centrally administered DNS servers
- Dynamic Host Configuration Protocol (DHCP). This service is allowed only on the University's centrally administered DHCP servers

System administrators must subscribe to notification and/or automated update services appropriate to the server hardware and software for which they are responsible.

The server must authenticate all Users other than local administrators, using the University's centrally administered login service and identity management credentials (i.e., Network Id and password) if the operating system or application permits. All communication of authentication credentials between the authenticating client and server must be encrypted. Authentication credentials must always be encrypted while in transit from a client or when at rest on the server. The server must enforce MSU's password standards.

The server must capture and archive critical User, network, system, and security event logs to enable review of system data for forensic and recovery purposes. The system administrator must review these logs for signs of malicious activity on a regular basis. Such logs should be retained for a period sufficient to address business requirements, document changes to access permissions, and provide an adequate history of transactions to satisfy audit requirements. Maintaining external copies of these logs is also recommended. Based upon risk assessment, server logs should:

- Provide the means for authorized personnel to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or result in the release of confidential information;
- Maintain audit trails to establish accountability for updates to mission critical information, hardware and software, and automated security or access rules; and
- Maintain a sufficiently complete history of transactions to permit an audit of the server by logging and tracing the activities of individuals through the system

- To the extent possible, the system administrator must configure the server operating system and/or resident applications to display a log-on banner to anyone requesting a connection to the server or application

The server must not be administered remotely unless the remote access methodology has been specifically approved by the Chief Information Security Officer. At a minimum, information transmitted during remote administration sessions must be encrypted. The server should accept remote administration commands from the fewest number of predefined hosts. Vendor accounts used for this purpose must be inactive at all times except when the vendor is actively engaged in providing support services.

Backup and Recovery

Backups are completed according to a risk assessment of the data and services provided. Restoration of software and data from backups should be tested on a regular basis to assure viability in the event of a service disruption. If backup media contains sensitive or confidential data, the data on the backup media or the media itself must be encrypted. Depending on the level of risk, IT may designate specific backup procedures.

Server Hardening

Server hardening consists of creating a baseline for the security on servers at MSU. In general:

- The server must not be used for multiple purposes that would put its security or performance at risk
- Physical access to any server and backup media must be restricted to persons with a legitimate need for such access
- University servers should never be connected to any other network outside the University's without prior authorization from the appropriate personnel in IT
- System and application logging should be enhanced
- Requirements to achieve compliance with externally imposed standards must be identified and addressed before access to servers is given
- University policy shall apply to all information and accounts on externally constrained servers

Incident Management

Any individual who knows or suspects that an information security incident has occurred must notify IT immediately at 940-397-4278 or securityincidents@mwsu.edu.

Any attempt to interfere with, prevent, obstruct, retaliate for or dissuade the reporting of an information security incident, critical security concern, policy violation, or information resource vulnerability is strictly prohibited and should be reported to the Chief Information Security Officer.

The Chief Information Security Officer will aggregate information security incident data and share it on a regular basis with MSU's Compliance Committee, CIO, and Data Owners and Custodians. If criminal activity is suspected, the CISO will notify the MSU Police Department. These data may include number and type(s) of security incidents and other information.

In some cases, action will be necessary to limit the magnitude and scope of the information security incident. Should any action be necessary which has a likelihood of having a substantial impact on business processes, the unit or department head or Data Owner, CIO, and Data Custodians will be notified in advance. Reasonable efforts will be made by IT to minimize the impact. In rare cases it may be necessary to take action without receiving input from individuals who manage the affected information resources. In those cases, authorization from the President will be sought before action is taken.

If a security incident is confirmed by the Chief Information Security Officer, the following individuals shall be notified: Chief Information Officer, unit or department head, and dean (if in an academic area). If investigation of a potential information security incident will take more than the estimated timeframe for incident assessment, the Chief Information Security Officer shall report the potential information security incident to the CIO, unit or department head, dean (if in an academic area), and vice president or associate vice president (if administrative area).

IT will work in concert with Data Owners to take action to identify and either eliminate or mitigate the vulnerabilities resulting in the security incident.

The Chief Information Security Officer will provide recommendations to the affected department and coordinate any remaining efforts needed to eliminate or mitigate the vulnerabilities.

If a decision has been made to notify individuals affected by the Information Security Incident, the Chief Information Security Officer will work with the Chief Information Officer, Director of Public Information and Marketing, and General Counsel to develop and implement an incident specific data breach notification process. Individuals will be notified as expediently as possible without unreasonable delay. Any media inquiries regarding the information security incident are to be directed to the Director of Public Information and Marketing.

Network Configuration

Prior to connecting any server to the university network, the system administrator will:

- Disable all default accounts except those required to provide necessary services
- Change the default passwords for all enabled accounts, consistent with university password standards
- Terminate or disable all unnecessary User and support accounts
- Establish a minimal number of User accounts with administration privileges
- Apportion User accounts and/or groups to achieve proper separation of duties and to avoid the granting of excess privileges to any individual User or group
- Use the local administrator account only to perform server management functions
- Register the server with IT for security and for server protection by the University's network edge protection mechanisms (e.g., perimeter firewall, etc.)

VI. Laws and Resources Concerning Security – University, State, and Federal

- Midwestern State University Information Security Office
- Texas Administrative Code Title 1, Part 10, Chapter 202, Subchapter C (Information Security Standards for Higher Education)
- Texas Penal Code, Chapter 33 (Computer Crimes)
- Texas Penal Code, Chapter 33(a) (Telecommunications Crimes)
- Texas Penal Code, Title 8 Chapter 37 sec. 37.10 (Tampering with a Governmental Record)
- U.S. Penal Code, Title 18, Section 1030 (Fraud and related activity in connection with computers)
- U. S. Penal Code, Title 18, Chapter 47 Section 1030 (Fraud and related activity in connection with computers)
- U.S. Penal Code, Title 18, Chapter 47 (Fraud and False Statements)
- Copyright Law of the United States
- Digital Millennium Copyright Act
- Computer Software Rental Amendments Act of 1990
- Texas Open Records Act
- FERPA (Family Educational Rights and Privacy Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- GLBA (Gramm-Leach-Bliley Act)

Appendix A

Definitions

The following words and terms, when used in this handbook, shall have the following meanings, unless the context clearly indicates otherwise.

Access – The physical or logical capability to interact with, or otherwise make use of information resources.

Business Continuity Planning (BCP) – The process of identifying mission critical data systems, critical personnel, and business functions, analyzing the risks and probabilities of service disruptions and developing procedures to restore those systems and functions.

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.

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.

Confidential Information – 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).

Control – A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Community – The group of people at the University that includes but is not limited to, all information resources management personnel, owners, system administrators, and Users (faculty, staff and students) of the University's information resources.

Custodian of an Information Resource – A person responsible for implementing the information owner-defined controls and access to an information resource. Custodians may include state employees, vendors, and any third party acting as an agent of, or otherwise on behalf of the state entity.

Digital Millennium Copyright Act (DMCA) – The DMCA seeks to update the U.S. copyright law for the digital age in preparation for the ratification of the World Intellectual Property Organization (WIPO) treaties.

Electronic Communication – A process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (e-mail), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

Encryption (encrypt, encipher, or encode) – The conversion of plaintext information into a code or cipher text using a variable, called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Family Education Rights and Privacy Act (FERPA) – A federal law protecting the privacy of student education records.

Firewall – A software or hardware device or system that filters communications between networks that have different security domains based on a defined set of rules. A firewall may be configured to deny, permit, encrypt, decrypt, or serve as an intermediary (proxy) for network traffic.

Gramm-Leach Bliley Act (GLBA) – Includes provisions to protect consumers' personal financial information.

Health Insurance Portability and Accountability Act of 1996 (HIPPA) – Protects the privacy of individually identifiable health information held by covered entities and the individual's rights with respect to that information.

Incident – An incident is the act of violating an explicit or implied security policy according to NIST Special Publication 800-61. This definition relies on the existence of a security policy that, while generally understood, varies among organizations.

Information Owner – A person with statutory or operational authority for specified information (e.g., supporting a specific business function) and responsibility for establishing the controls for its generation, collection, processing, access, dissemination, and disposal. The Information Owner may also be responsible for other information resources including personnel, equipment, and information technology that support the Information Owner's business function.

Information Resources – Is defined in §2054.003(7), Government Code and/or other applicable state or federal legislation.

Information Security Program – The elements, structure, objectives, and resources that establish an information resources security function within an institution of higher education, or state agency.

Information Technology (IT) – The entity at Midwestern State University that is responsible for the enforcement of the security policies at the University.

Intrusion Detection System (IDS) – Hardware or a software application that can be installed on network devices or host operating systems to monitor network traffic and host log entries for signs of known and likely methods of intruder activity and attacks. Suspicious activities trigger administrator alarms and other configurable responses.

Intrusion Prevention System (IPS) – Hardware or a software application that can be installed on a network or host operating system to monitor network and/or system activities for malicious or unwanted behavior and can automatically block or prevent those activities. (Firewalls, routers, IDS devices, and anti-virus gateways all may have IPS capabilities). IPS can make access control decisions based on application content.

Mission Critical Information – Information that is defined by the institution of higher education, or

state agency to be essential to the institution of higher education, or state agency function(s).

Platform – The foundation technology of a computer system. The hardware and systems software that together provide support for an application program. (Ref: Practices for Protecting Information Resources Assets.)

Risk Assessment – The process of identifying, evaluating, and documenting the level of impact that may result from the operation of an information system on an organization's mission, functions, image, reputation, assets, or individuals. Risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Risk Management – Decisions to accept risk exposures or to reduce vulnerabilities and to align information resources risk exposure with the organization's risk tolerance.

Router – A device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any intersection where one network meets another.

Sanitize – A Process to remove information from media such that data recovery is not possible: includes removing all confidential labels, markings, and activity logs.

Security Incident – An event which results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources.

Sensitive Personal Information – A category of personal identity information as defined by §521.002(a)(2), Business and Commerce Code

Software - Defined by 48 CFR 2.101 means (i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and (ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

Storage Device – Any fixed or removable device, which contains data and maintains the data after power is removed from the device such as a DVD/CD-ROM, external or internal hard drive, Universal Serial Bus (USB) flash drive, memory card, or media player.

Test – A simulated or, otherwise documented event for which results and records are kept.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

University – Refer specifically to Midwestern State University, an institution of higher education as defined by the Texas Education Code- Section §61.003.

User of an Information Resource – An individual or automated application authorized to access an information resource in accordance with the information owner-defined controls and access rules.

Vulnerability Assessment – A documented evaluation containing information which includes the susceptibility of a particular system to a specific attack.

Wireless Access (WA) – Using one or more of the following technologies to access the information resources systems of a state agency or institution of higher education:

Wireless Local Area Networks (WLAN) – Based on the IEEE 802.11 family of standards.

Wireless Personal Area Networks (WPAN) – Based on the Bluetooth and/or Infrared (IR) technologies.

Appendix B

Information Technology/Information Security Contacts

- Vice President for Administration and Finance (vpaf@mwsu.edu)
    - Chief Information Security Officer (ciso@mwsu.edu)
    - Chief Information Officer (cio@mwsu.edu)
        - Administrative Systems Manager (administrativesystems@mwsu.edu)
        - PC/Networking Services Manager (networkmanager@mwsu.edu)
        - Classroom Technology (classroomtechnology@mwsu.edu)
        - Help Desk (helpdesk@mwsu.edu)

Appendix C

Creating Strong Passwords

- Keep passwords private – never share a password with anyone else
- Do not write down your passwords
- Use passwords of at least six (6) characters or more (longer is better)
- Use a combination of upper case letters, lower case letters, numbers, and special characters (for example: !, @, &, %, +) in all passwords
- Avoid using people's or pet's names, or words found in the dictionary; it's also best to avoid using key dates (birthdays, anniversaries, etc.)
- Substituting look-alike characters for letters or numbers is no longer sufficient (for example, Password" and "P@ssw0rd")
- A strong password should look like a series of random characters
- On the web, if you think your password may have been compromised, change it at once and then check your website accounts for misuse. If you think your MSU network credential may have been compromised, change the password at once and then call the help desk at 4278 on campus or (940) 397-4278 off campus

Password Managers

There are many good password manager software products on the market today. Some are free; none are very expensive. Using one of these products, you can create truly random, very long, and unique passwords for each site, and because the software will remember them for you, you never have to worry about what your password is. Your password manager will store and encrypt the passwords for you, and log you in automatically. You will have vastly improved security, with only one master password to remember.

A good product for this type of use is the free KeePass product (use version 1.x as the 2.x version is not free.)

Example

The example shown below shows a simple process for creation of a password that is very hard to crack.

	Possible steps to follow	Example
1	Think of a phrase or sentence with at least eight words. It should be something easy for you to remember but hard for someone who knows you to guess. It could be a line from a favorite poem, story, a line from a movie or book, a song lyric, or a quotation you like.	It was the best of times, it was the worst of times.
2	Remove all but the first letter of each word in your phrase. Remove spaces and punctuation.	iwtbotiwtwot
3	Replace several of the lowercase letters with uppercase ones, at random.	iwtBotiWtwoT

	Possible steps to follow	Example
4	Now substitute a number for at least one of the letters. (1 or i and 0 for o, etc.)	iwtBot1Wtw0T
5	Finally, use special characters ($, &, +, !, @) to replace a letter or two -- preferably a letter that is repeated in the phrase. You can also add an extra character to the mix. (! For I and @ for o, etc.)	**!wtB@t1Wtw0T**

There are many methods that could be used to derive a strong password. The guidance provided here is a simple and effective option.

Appendix D

Forms

1. VPN Access Request Form
2. 3rd Party VPN Access Request Form
3. Information Resources Use and Security Policy Agreement
4. Request To Remove Tracked Property From Campus
5. YouTube Channel Request Form

Appendix E

Personally Identifiable Information (PII)
Any instance of an individual's first name (or first initial) plus the last name and any one or more of the following:

- Social Security number
- Driver license or state-issued ID number
- Military ID number
- Passport number
- Credit card (or debit card) number, CVV2, and expiration date
- Financial account numbers (with or without access codes or passwords)
- Customer account numbers
- Unlisted telephone numbers
- Date or place of birth
- Mother's maiden name
- PINs or passwords
- Password challenge question responses
- Account balances or histories
- Wage & salary information
- Tax filing status
- Biometric data that can be used to identify an individual, including finger or voice prints
- Digital or physical copies of handwritten signature
- E-mail addresses
- Medical record numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Medical histories
- National or ethnic origin
- Religious affiliation(s)
- Physical characteristics (height, weight, hair color, eye color, etc.)
- Insurance policy numbers
- Credit or payment history data
- Full face photographic images and any comparable images
- Certificate/license numbers
- Internet Protocol (IP) address numbers

In general, personally identifiable information does not include information that is lawfully obtained from publicly available records, or from federal, state or local government records lawfully made available to the general public.

Modification Log

Date	Modified By	Description of Modification
6-1-2017	Jim Hall	Initial document creation.
7-20-2017	Jim Hall	Addition of foreword.
8-2-2017	Jim Hall	Addition of Banner INB access account information.
10-25-2017	Jim Hall	Clarifications of language and addition of definition for “software” and “security incident.”
10-30-2017	Jim Hall	Added YouTube channel request form to forms section.
12-11-2017	Jim Hall	Added faculty intellectual property policies 3.139 and 3.140 to the Assignment/Use of University Equipment section.
1-16-2018	Jim Hall	Multiple formatting and spacing changes. Addition of CIO and CISO to definitions.
5-25-2018	Jim Hall	Added “Systems and Services Acquisition” section.