Information Security Policy
TEC 4.0
Office of Information Technology

Policy type: Administrative
Applies to: Faculty, staff, student employees, students, and volunteers

POLICY DATES

Issued: 2/8/2011
Revised Last: 12/3/2024
Edited by: Tina Stuchell
Reviewed: 12/3/2024

University of Mount Union expects all institutional information stewards who have access to and responsibilities for institutional information to manage it according to the rules regarding storage, disclosure, access, classification of information as set forth in this policy.

The Purpose of this policy is to maintain and protect the university informational assets and comply with applicable federal and state legislations. These guidelines are to define baseline security controls for protecting institutional data. Security breaches are more commonplace than ever, and universities continue to be popular targets for attacks. Critical university resources, such as research, business transactions, and student and employee personal data must be protected from intrusion and inappropriate use or disclosure. Devices must be set up and routinely maintained and updated so that they prevent intrusion and other malicious activities.

This policy is reviewed and updated on an annual basis by the CIO & Director of IT for Security. This is an administrative type of policy which all major changes to this policy must be approved by President Council and Policy Review Council.

Definitions

Term	Definition
Artificial Intelligence	Artificial intelligence (AI) is a field of science concerned with building computers and machines that can reason, learn and act in such a way that would normally require human intelligence. AI is the ability of machines, especially computer systems, to exhibit intelligence. AI technologies allow computers to perform a variety of advanced functions.
Electronic Storage Media	Is defined as any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP Disks, Magnetic tapes, SD Cards, etc.
Information System	Is generally defined as any electronic system that stores, processes or transmits information. For the purpose of this policy, it is any electronic system that stores, processes or transmits institutional data.
Institutional Data	Is defined as any data that is owned or licensed by the University.
Least Privilege	Is information security principle whereby a user or service is provisioned the minimum amount of access necessary to perform a defined set of tasks.
Multi-factor Authentication	The process by which more than one factor of authentication is used to verify the identity of a user requesting access to resources. There are three common factors of authentication: something you know (e.g., Password, pin, etc.), something you have (e.ge. smart card, digital certificate, etc.) and something you are (e.g., fingerprint, retinal pattern, etc.). Use of username and password combination is considered single factor authentication, even if multiple passwords are required. Username and password used in conjunction with a smartcard is two-factor authentication. Multi-factor authentication represents the use of two or three factors.
Privileged Access	Is defined as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the local administrators, domain administrators and enterprise administrator's groups would all be considered to have privileged access. In a traditional

Applies to: Faculty, staff, student employees, students, and volunteers

Term	Definition
	UNIX or Linux environment, users with root level access would be considered to have privileged access. In an application environment, users with "super-user" or system administrator roles and responsibilities would be considered to have privileged access.
Confidential Data	Institutional data that is not to be released under any circumstance is to be protected. It can include but is not limited to PII data, credit card data, social security numbers, grades, bank account numbers, or any other information that is likely to raise public interest.
Controlled Classified Information (CUI)	A category of unclassified information within the U.S. Federal government.
Bank Account Numbers	Any routing or identification numbers that can be used to determine banking information including both institutionally owned and University agent owned account information.
Private Identifiable Information (PII)	Any information that could be used in the process of identity theft.
Directory Data	Defined per The Family Educational Rights and Privacy Act (FERPA) as information such as a student's name, address, telephone number, date and place of birth, honors and awards, dates of attendance.
NIST Special Publication 800-171	NIST Is a Federal standard that standardizes security controls applied to CUI and systems and processes involved with this data within federally funded environments.
Environment	Environment is defined as the systems upon which CUI resides and the physical infrastructure that houses systems. Examples might be a student records system residing on servers in a datacenter. The room(s) or area(s) housing the computer systems along with the computer systems themselves define the environments to which this policy applies.
NIST 800-171 Framework	The NIST 800-171 framework consists of 110 elements covering administrative, technical, and operational security controls designed to focus on protecting the confidentiality of unclassified-but controlled information. Those controls are: Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection
Compensating Control	A compensating control is a mechanism that is put in place to satisfy the requirement for security measure that is deemed too difficult or impractical to implement at the present time. Compensating controls requirement need to mitigate the underlying risk that the requirement is designed to address. The Office of Information Technology will assist responsible parties regarding compensating controls
PII	Personal Identifiable Information (PII) is any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (including address).
GLBA	Gramm-Leach-Bliley-Act – requires financial institutions, companies that offer consumers financial products or services to explain their information sharing practices to their customers and to safeguard sensitive data.
Local Administrative Privileges	Local Administrative Privileges means the granting of "administrator" or equivalent rights on a particular University device, such as a University issued laptop or desktop unit.

Applies to: Faculty, staff, student employees, students, and volunteers

Term	Definition

Policy Details

Privacy practices and security standards serve to preserve and protect institutional information. This policy incorporates a set of requirements for protecting the University's institutional information. The purpose of this policy is to ensure that all individuals within its scope understand their responsibility in reducing the risk of compromise and take appropriate security measures to protect university resources. Access to university resources is a privilege, not a right, and implies user responsibilities. Such access is subject to university policies, standards, guidelines and procedures, and federal and state laws.

This policy is reviewed on an annual basis by the CIO and Director of IT for Security. Major changes for this policy are approved through President Council.

Data Classifications and Handling

To safeguard the university's institutional information, the following practices for electronic transmission and storage of confidential information. All institutional data must be protected in a reasonable and appropriate manner based on the level of sensitivity, value and/or criticality that the data has to the University. This requirement acknowledges that different types of data require different sets of security controls. The University has defined three classifications of data for this purpose: Confidential, Restricted and Public.

This policy establishes three institutional information security classifications:

1. Confidential (Level 1) Data
2. Restricted (Level 2) Data
3. Public (Level 3) Data

Unless otherwise classified, all information used in the conduct of university business is restricted (Level 2). Institutional information that has been explicitly made available to the public, with no authentication required is public (Level 3).

Highly Confidential (Level 1) Data

Highly Confidential Data: Data should be classified this way when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. The highest level of security controls should be applied to highly confidential data. Examples of highly confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements.

- Social Security Number
- Credit Card Number
- Driver's License Number
- Bank Account Number
- Protected Health Information, as defined by the Health Insurance Portability and Accountability Act (HIPPA)

Confidential (Level 2) Data

Confidential Data: Data should be classified this way when unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as confidential or public data should be treated as restricted data. A reasonable level or security controls should be applied to restricted data.

Applies to: Faculty, staff, student employees, students, and volunteers

Public (Level 3) Data
Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of public data include:

- Press Releases
- University Catalog Information
- Research publications

While little or no controls are required to protect the confidentiality of public data some level of controls is required to prevent unauthorized modification or destruction of public data.

Data Storage:
Institutional data storage can be separated by the type of data on approved institutional file/storage spaces. For example:

- Credit Card Data may not be stored anytime, in any format written or electronic, under any circumstance by any application or user on Mount Union Campus. Credit Card Processing can only be completed by authorized merchants as defined by the VP of Business Affairs and the Controller. Those accepting credit card information must follow guidelines established by the Business Office and comply with Credit Card Security Policy.
- Social Security Numbers and grades when required to be stored can only be stored on encrypted server drives. It is not to be stored on USB drives, or other mobile media, including mobile devices such as laptops or tablets. Under no circumstances should Social Security Numbers be included in reports and distributed to others.
- Bank Account Numbers must only be stored by agents who require that information and when needed should only be stored encrypted when in digital formats or should be locked and have physical access limited in non-electronic media formats.
- Confidential Data should never be stored on non-university owned systems including personal laptops, desktops, tablets, or phones regardless of security settings. Confidential information may only be stored when required for business use and then must be stored in secured formats or locations.
- PII when stored must be encrypted if in electronic format. If stored in non-electronic media, it must be physically secured with limited physical access.
- Effective April 4, 2022, faculty and staff are not permitted to write to usb thumb/storage drives.

Any other institutional data must always be stored in encrypted format.

Data Collection:
The collection of the *social security number* by any agent of the university and its use as an identifier must be avoided, except as required by law.

The collection of *credit card* data must be avoided except where required for transaction purposes and where agents of the institution have been authorized to do so, and only in locations as specified by the Credit Card Security (PCI) Policy. Credit Card data is **NOT TO BE** collected by any departments or divisions not explicitly defined in the credit card security policy and approved by the controller of the university.

The collection of *bank account numbers* must be avoided when possible. When necessary, it must only be collected by the Office of Business Affairs.

Data Release:
Confidential Data including PII data should never be released, email, social media, fax, etc.

Directory Data may be released publicly without consent, given the university has told the relevant parties about the data and providing them with a reasonable amount of time to inform the University to not disclose such information. Per FERPA this must be completed once a year.

The need-to-know email lists are used to notify offices of data that must be modified in systems across the institution. The data that is passed, such as address changes, title changes, student withdrawals, employees leaving the institution, etc. should be only used in order to perform one's job and should not be shared with others.

Applies to: Faculty, staff, student employees, students, and volunteers

Data Moving:
To limit the impact of improper or accidental moving of data various procedures have been put in place including limiting access and permissions only as required, implementation of shadow volume copy and other backup procedures. Mount Union data stored on USB drives must be stored/transported using encrypted thumb drives. Data should only be moved by those authorized for such purposes. Examples include:

- Backup purposes
- Validation/testing of data for support purposes.

Data Deletion:
When disposing of any confidential data in paper form, all data must be shredded in a crosscut manner. The university currently has several Shred-It boxes located around campus that must be used for this purpose, if additional locations are needed it is the responsibility of the department to obtain this service through the Business Office and any associated costs.

Confidential electronic data to be destroyed should be destroyed in a manner that completely removes the data from the physical media it is located on. If unsure how to accomplish this obtain assistance through the Office of Information Technology.

Physical media that once had the potential to contain confidential data should be completely destroyed. Various methods might include but are not limited to include degaussing. The Office of Information Technology had a degaussing machine.

To limit the impact of improper or accidental deletion of data various procedures have been put in place including limiting access and permissions only as required, implementation of shadow volume copy, and other backup procedures.

Controlled Unclassified Information

Controlled Unclassified Information is any information in any form that law, regulation, or governmental policy requires having safeguarding or disseminating controls. The University of Mount Union may receive data shared by the federal government or may create data or information as part of sponsored projects or to conduct federal business. This data, information and related documents may be classified as Controlled Unclassified Information (CUI). The University is obligated to ensure that all systems and processes involved with CUI are compliant with National Institutes of Standards and Technology (NIST) standard found in NIST Special Publication 800-171. This policy provides requirements and guidance so individuals in receipt or development of CUI can conduct research or other business in compliance with CUI regulation. Non-compliance may result in fines or the inability to continue receiving Federal funds associated with the use of this data whether directly received from the government or indirectly through associated covered contracts and contractors.

This policy applies to all data that is classified as CUI as well as technology, system, service, network, department, or personnel that transmit, process, or store CUI. It covers transmission of data and information that is transmitted in any manner, including electronic and paper. This policy applies whether the network connections are remote (cloud) or campus based.

Any person, department or college who handles CUI on behalf of the University must abide by this policy. This policy provides requirements and guidance for all use of CUI for the University. These are the minimum requirements for securing CUI. All environments involved with CUI must comply fully with the NIST 800-171 standards and this policy either directly or through compensating controls.

Individual users and departments must take actions to protect CUI from unauthorized disclosure and follow the requirements as specified in NIST 800-171. Periodic risk assessment to organizational operations, assets, and individuals, resulting from the operation of information systems and the associated processing, storage or transmission of CUI will be conducted. All environments that are involved with CUI must also operate in a manner that allows incident reporting within 72 hours of cyber incidents involving CUI.

Applies to: Faculty, staff, student employees, students, and volunteers

Additional Resource: NIST 800171
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (nist.gov)

Protecting Personal Identifiable Information (PII)

Limit collection of PII

- Only collect what is needed for specific business purposes
- Limit the number of copies of reports, and files containing PII
- Every time you create: a form, application, survey, run a query, run a report, or generate a file, consider if all PII included is truly necessary
- Remember the less you collect the less you need to protect

Limit Use of PII

- Always remember federal and state law limit the sharing of PII data
- Remember federal law, FERPA, requires written consent to disclose PII from education records unless an exception applies
- FERPA school official exception: PII may be disclosed without consent to other school officials only where there is a legitimate educational interest
- PII data can only be shared with third parties acting as school officials
- Remember to think before sharing data internally, and to consider if there is a legitimate educational interest and need for sharing such data..
- Use fictional personal data for training and presentations
- Remember University policy requires that the sharing of data with external partners, vendors and servicers must be strictly controlled.
- Data required to be shared in the support of research, accreditors or third-party surveys, even when aggregate data is requested, must be reviewed and discussed with the Office of Institutional Research.
- Always think twice before sharing PII.

Safeguard PII

- Safeguard PII data in all formats (this includes electronic and paper formats)
- PII must be protected at rest and in transit
- Data should be protected from loss or unauthorized access
    - Remember sharing of passwords is prohibited
    - Maintain strong passwords
    - Secure all paper containing PII including keep a clean desk and file documents containing PII in locked cabinets
    - Lock your computer screen when not in use
- Always email PII securely
- Always pick up print outs containing PII immediately
- Printers and copiers should be in an access-controlled environment
- PII should never be stored on unsecure/public computers, or portable devices (flash drives, phones).
- Shred paper containing PII in Shred Bins located throughout campus
- Delete/dispose of PII securely at the end of retention period

Governance of PII and its use is administered by the University's Office of Information Technology with assistance from University Compliance Committee, Risk and Safety Committee and Audit Committee of the Board of Trustees. It is important that we remain vigilant about protecting the University's information and compliancy.

If there is a business need that requires PII information to be used outside of the University enterprise systems, or if you have concerns about the protection or use of PII, contact the Office of Information Technology.

Applies to: Faculty, staff, student employees, students, and volunteers

Local Hard Drive Encryption
Effective April 2022 all university faculty and staff laptops and desktops hard drives will be encrypted in order to safeguard data provide the device is lost or stolen.

GLBA Compliancy

The Gramm-Leach-Bliley Act (GLBA) addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply with the Act. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical.

GLBA Compliance covers the entirety of the activities and practices of the following offices and individuals:

- Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records, or student records.
- Academic and administrative offices that transmit confidential information to off-site locations as part of a periodic review or submission requirement.
- Centers and Institutes that provides services and acquire personal or financial information from participants or constituents.
- Faculty serving as directors, coordinators, or program directors for programs collecting protected data.
- Faculty, staff and administrators with contracts to use, access, or provide protected data to or receive from a non-campus entity.

GLBA Compliance covers the following types of data:

- Personal Identifiable Information (PII) – also known as protected data, as defined herein. PII includes first and last name, social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender and ethnicity.
- Financial Information – Information that the University has obtained from faculty, staff, students, alumni, auxiliary agencies, and patrons in the process of offering financial aid or conducting business. Examples include bank and credit and account numbers and income and credit histories.
- Student Financial Information – Information that the University has obtained from a student in the process of offering a financial aid award, services or such information provided to the University by another's.

To continue to protect private information and data and to comply with the provisions of the Federal Trade Commission's safeguard rules implementing applicable provisions of the GLBA, the University expects individuals to comply with this policy. This policy forms part of the overall strategic information security program and includes information that the University receives during its course of business, information as required by GLBA, and any other confidential financial information the University has chosen to include within scope.

All University employees that interact with PII data during their daily activities are required to comply with GLBA regulations and take training course while handling the personally identifiable information (PII).

Director of IT for Security oversees the institution information security program along with support of the CIO and SVP.

Annual Internal Risk Assessment
An annual internal risk assessment is conducted each year. This assessment identifies internal and external risks related to customer information, employee information and network security. This assessment looks at the controls and possibilities of risks. The information from this assessment is shared with President Council and Audit & Risk Committee of the BOT on an annual basis.

Safeguards Regarding Customer Data

Applies to: Faculty, staff, student employees, students, and volunteers

- Access to customer data is only given to new employees when approval is granted by supervisor and "owner/steward" of specific customer data. An IT form must be completed and then must be signed of on by supervisor and owner of the data. Below is a chart indicating owner/steward of the data, by position.

Area of Data	○ Owner
Financial	Controller
HR	Director of HR
Payroll	Controller
Student	Registrar
Financial Aid	Director of Financial Aid
Admissions	Director of Admissions
Alumni/Advancement	Director of Alumni

- Accounts who access customer/administrative data are reviewed on an annual basis and is included in annual GLBA audit.
- Customer data for all administrative areas are held in systems that are cloud/SaaS based and is encrypted by vendor in database and in transit.
- Multifactor authentication – Multifactor authentication is turned on for all systems accessing customer information where available.
- All upgrades to administrative systems are conducted by vendor and kept current.
- No software applications storing customer data are built by the institution only vendor provided applications are in use.
- Printed data is securely disposed of through shred-it bins, located in specific locations/offices on campus.
- System logs are managed by the vendor. IT is working with vendors to review user activity on a regular basis.

Security Training for Faculty and Staff

All University faculty, staff and retirees who still retain a Mount Union email address are required to take security training on an annual basis. The university strives for 100% completion annually.

GLBA requires companies that offer consumers financial products to safeguard financial and sensitive data. The Office of Information Technology (IT) also conducts phishing tests to faculty and staff on a quarterly basis as a requirement of GLBA and in an effort to increase user awareness on data and cyber security. IT uses Knowbe4 for conducting of annual training and phishing tests. Individuals who have repeat failures are subject to the following repercussions.

Failed once:

- Individuals are notified immediately by system and lets them know that they got caught.
- Are automatically enrolled into phishing remediation training. User will be given two weeks to take this training. If training is not completed Supervisor and area Vice President will be notified.

Failed consecutively twice:

- Same as above (failure once) plus
- Director of IT for security will contact user directly for additional discussion and training.

Failed consecutively three times

- Same as above (failed consecutively twice) plus
- Notification to HR for submission into personnel file
- Meeting required with Director of IT for Security, Supervisor and VP.

Failed consecutively four times

- All of the above and recommendation of suspension or dismissal for individuals with access to sensitive and/or financial data.

Failed consecutively five or more times

- All of the above and regardless of the position recommendation of suspension or dismissal.

Example:

Applies to: Faculty, staff, student employees, students, and volunteers

Employee A fails once – is automatically notified and takes remediation training. Employee A fails consecutive tests (back-to-back testing are failed) the above steps are taken depending on the number of repeat failures. Employee A fails on or consecutive tests, then passes test – Once employee passes a test, their count restarts over.

Incident Response Team
An incident response team is in place that consists of representatives from the following offices:

- Business Affairs
- HR
- Marketing
- Student Affairs
- Alumni/Advancement
- IT
- Academic Affairs/Registrar
- Enrollment Services/Admissions

This team meets quarterly and annually to conduct a tabletop exercise.

Additional information can be found in the Information Security Plan in the Office of Information Technology

Network Security

Network attacks launched from the Internet or from the University's network can cause significant damage and harm to information resources including the unauthorized disclosure of confidential information. To provide defensive measures against attacks, firewall and network filtering technology is used in a structured and consistent manner.

The University maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network mediated threats. Firewalls and IDS systems are deployed at the campus border and IPS systems are deployed on core services to augment normal system security measures to prevent denial of service attacks, malicious code, or other traffic that threatens systems within the network or that violates university information security.

Firewalls and IDS/IPS systems are maintained on a regular basis. Rules on these systems are reviewed monthly. The responsibility to maintain, monitor and update firewalls and IDS/IPS systems is the responsibility of the Director of IT for Security. When events occur, it is the responsibility of the Director of IT for Security to notify the CIO with required notification and response expectations as soon as possible after an event. Logging of these regular reviews are required.

Log Management
The creation and retention of system audit logs to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is an important element of network security. Reviewing and management of system logs is an important of system and network security. The University partners with Bitlyft to assist with log management. Monitoring organizational critical systems, including inbound and outbound communications traffic, to detect attacks.

Maintaining visibility, remediation and indication of any potential attacks is completed by Bitlyft, a key security partner of the University, monitoring critical systems including Firewalls, Office 365, Microsoft Exchange, and Active Directory. Review of Bitlyft findings is conducted on a weekly basis by the Director of IT for security. In addition, monthly review meetings are conducted with Bitlyft and critical findings and alerts in the event of an audit log process failure are reported on an immediate basis. Director of IT for Security is responsible for the oversight of log management.

Vendor Management
Prior to selection as a potential supplier for goods and services to Mount Union, potential vendors are required to be considered as holding a "qualified" status with the University. This may be accomplished in a variety of ways such as

checking references, site visits, or trade publications. The financial stability of public entities may be investigated with publications or services such as Dun & Bradstreet. For privately held companies, audited financial statements, bank or trade references may be requested.

To comply with Federal regulations set forth in the Gramm-Leach-Bliley Act (GLBA), all vendors for IT purchases relating to computer software and systems, cloud software, and data back-up will be asked to provide SOC2 reports and a copy of their most recent audited financial statements. The Director of Information Technology for Security and the Purchasing Office will review these documents to determine vendor eligibility. Vendors that do not provide satisfactory copies of these documents may not be approved for use. SOC2 and financial health for key vendors will be reviewed on an annual basis by the Purchasing Office and Director of IT for Security. The list of key vendors will be kept within the Purchasing Office. For more information see the University's Purchasing Policies and Procedures document.

Network Scans

Independent network testing is completed on an annual basis. This is a requirement of the Office of Information Technology. These tests consist of both internal and external penetration tests and external PCI scans. These tests are overseen by the Director of IT for Security and results are shared with CIO, President Council Members and the Board of Trustees. The results of these scans are audited and reviewed on a regular basis and any necessary steps are taken as a result of these tests to improve network security. These tests include general IT controls, penetration testing, and others that may be completed to meet compliancy requirements.

Local Administrative Privileges

This section defines the rules regarding the granting and use of local administrative privileges. Local administrative privileges mean the granting of administrator or equivalent rights on a particular University device, such as a University owned laptop or desktop device. The majority of the campus community use general user-level accounts. The need for local administrative privileges is seen as an exception.

Routinely, users are assigned a user-level account for their Mount Union work that provides access to common services and applications, such as web browsers, email, MS Office software, file storage and shared printer access. Users with user-level accounts **CAN NOT** generally install new applications nor upgrade software components. Some users, by the nature of their work, require additional software that is not included in the standard software suite available on managed devices. In most cases, technical support staff available within the Office of Information Technology can install additional licensed software on behalf of the user upon request. In other cases, local administrative privileges may be required to support a user's needs. This should be on rare occasions.

An important security practice in this regard is the principle of least privileges. The principle advocates that user should use an account that is granted only the minimum access permissions necessary to complete a task and nothing more for a limited time.

The issuance of the policy applies to the University owned devices. Use of local administrative privileges is limited to the following circumstances:

- The approval is granted for a limited time. Limited time is defined as time needed to accomplish needed task. (Usually max of 1 day/24 hours). With the *make me admin* tool, Local admin privileges is only granted for 10 minutes at a time.
- Local Admin Privileges would only be granted for faculty and staff only.
- The nature of the user's work requires the *frequent* ability to install or upgrade nonstandard software on the device. *Frequent* is defined as anticipated to average more than once per month. Typically, such users are software developers, system administrators but can include others utilizing specialized software.
- When required software will not operate without local administrative privileges.
- When local administrative privileges are the only mode available within a device (i.e., mobile devices such as iOS and Android based smartphones and tablets). (No approval required).
- When required by IT technical support in the normal course of system administration (No approval required).

Users granted local administrative privileges must comply with the following:

- User is responsible on an ongoing basis to keep abreast of any security updates relevant to additional installed software as released by its publisher(s) and perform timely installation of such updates.

Applies to: Faculty, staff, student employees, students, and volunteers

- Software that captures, displays, or manipulates network traffic in a "promiscuous" or other mode may not be installed unless such is required in the normal course of assigned work responsibilities.
- Software that interferes, inhibits, disables, or bypasses installed anti-malware, antivirus software may not be used. Anti-malware software may be temporarily disabled, when necessary, to prevent issues during software installation only.
- Third-party software may not be installed or used to enable remote desktop access to a University device. Where available, approved remote desktop access service can be requested through the IT Helpdesk and approved by the Director of IT for Security.
- Additional local accounts (with or without administrative privileges) may not be created unless they are documented by the vendor as a requirement of software to be installed.
- Automatic updates may not be disabled (where it may be configured for the operating system and other standard applications).
- Existing local accounts and services may not be disabled.
- The Office of Information Technology's ability to support the University owned system may not be impeded.
- Only software in compliance with its copyright and licensing may be installed.
- Only software applications and tools required for a user's work in support of the University can be installed.

The assumption of local administrative privileges on a University device carries certain inherent responsibilities and increased risks. These include the potential loss of data, compliance with copyright laws and increased threat of compromise.

- Data Security: Local administrative privileges increase susceptibility to spyware, malware and potentially damaging security breaches due to the elevated level of rights and permissions associated with administrative privileges.
- Data Loss: Safeguards intended to prevent inadvertent, irreversible actions can be inhibited by local administrative privileges. Users are solely responsible for any data that is stored locally and as such must exercise due diligence in providing a backup mechanism to ensure against the potential loss of any important data. Failure to implement a backup mechanism can result in permanent loss of such data.
- Software Licensing & Copyright Laws: Adherence to copyrights and licensing agreements is mandatory for all installed software. Users do not have the authorization to agree to software terms and conditions (end User License Agreements) on behalf of the University. Contact the Purchasing office for more information.

Requesting Local Administrative Privileges:
By default, users are granted user access level on their devices. Local administrator access is granted on an as-request/needed basis for a particular device based on a justification of need for a limited amount of time.

To request local administrative privileges for new software installation:

1. User must comply with University policies.
2. Fill out the form titled Local Administrative Privilege Request Form, print out and sign the form, have it signed by supervisor. This form to be used for ONLY NEW software installation.
3. Email the form to itsecurity@mountunion.edu AND helpdesk@mountunion.edu.
4. The submission will be reviewed by Director of IT for Security and CIO, and, if approved, signed copy will be sent back to you by return email.
5. Once approval is granted a one-time access will be given to you to allow you the capability to install the necessary needed application/software.

For updates to existing software:

1. User must comply with university policies.
2. Use the *make me admin* tool to request and get granted local admin privileges for 10 minutes.

Applies to: Faculty, staff, student employees, students, and volunteers

International Travel

University faculty, staff, and students who travel internationally with laptops, phones, and other mobile devices, are subject to many risks namely that of loss, theft, or seizure of devices, data, and login credentials. Additional threats include device infiltration or malware compromising sensitive information.

When you leave the United States, you need to know your responsibilities under export control regulations. In particular if you are traveling with your laptop or any other electronic devices these items along with the underlying technology, any data on your device, proprietary information, confidential records and encryption software are all subject to export control regulations. Some foreign governments have regulations that permit the seizure of travelers' computers and the review of their contents.

Depending on where you plan to travel abroad, electronic communication devices, may be subject to involuntary official governmental review and possible duplication of the hard drive's contents. The University requires the use of encryption on all University-owned devices. Use of encryption to protect information may be forbidden in some countries, you should check before you travel abroad to ensure compliance with foreign countries' laws. And, if your encryption product allows you to "hide" information, those "hidden" areas can be detected, and you could be subject to criminal charges by the country's government. Because it is difficult to monitor encrypted traffic, use of secure ("https") websites and/or use of virtual private networks (VPNs) may be blocked by some countries.

Some countries may censor certain content or sites. Attempts to circumvent national censorship of websites, such as some mainstream western social media sites, is discouraged by the University. You should only use VPN to access necessary files and sites to conduct business or studies. If you are found to be using a product to circumvent the blocking of censored websites, you may be warned, have your electronic devices confiscated, or you may become subject to criminal charges.

Personal privacy may not be respected. Even private spaces such as hotel rooms, rental cars, and taxis may be subject to video, audio or other monitoring. This type of surveillance may be able to track your whereabouts, what you may be doing, what's on your electronic device, and what you may be entering into it. Conversations either in person or on a phone may be monitored. Local colleagues may be required to report any conversations held with foreigners.

The following are rules that must be followed when traveling abroad for Mount Union business or academic purposes:

- Notify your Supervisor, Dept. Chair, Dean, Information Technology and Human Resources that you are traveling out of the country including the following information. **The Office of Information Technology needs to be notified 14 days prior to travel.**
    - Dates of travel
    - Exact location of travel
    - Which devices you are traveling with
    - Any additional staff, faculty, or students that you are traveling with
    - Indicate who your emergency contact is while traveling abroad
- DO NOT TAKE Mount Union laptop, tablet, phone, etc. if traveling to a country that is a level 2 or higher indicated by the state department.
- Follow best practices while traveling internationally, including do not use free internet or unsecure networks.
- Be sure that any device with an operating system and software is fully patched and up to date with all institutional recommended security software before departing.
- Research your destination on the State Department website (https://travel.state.gov/content/passports/en/alertswarnings.html)
- Enroll in STEP which provides alerts. https://travel.state.gov/content/travel.html
- When your devices are not in use, turn off or lock the devices.
- DO NOT store high-risk or moderate-risk data (e.ge., social security numbers, ID numbers, protected health information, credit card numbers, bank account numbers, class lists, student, or employee information, or PII data on any devices you are taking with you.
- Do NOT travel with any Mount Union data that is not necessary.

Applies to: Faculty, staff, student employees, students, and volunteers

- DO NOT copy high-risk or moderate-risk data to memory sticks or other easily lost media.
- Upon your return, immediately change your network/email password and the passwords of any accounts used while abroad.
- Upon your return, immediately visit the IT Helpdesk to have your device scanned to ensure no malware is on it.
- For some countries: DO NOT travel with encrypted devices unless you have advance approval from those countries. China, for example, severely restricts the import of unapproved encryption. If you attempt to cross the border with an encrypted device, you may be asked for the decryption key or your device may be confiscated.
- The U.S. Government prohibits traveling with encrypted devices to countries that are considered to support terrorism, namely Cuba, Iran, North Korea, Sudan and Syria. Do NOT bring encrypted devices to these countries.
- Use caution when connecting a USB device to an unknown computer or charger as it may become infected with malware.
- Set Wi-Fi to "do not automatically connect to Wi-Fi on all devices capable of wireless connections.
- DO NOT update your computer while connected to a public or hotel wireless network.
- Disable Bluetooth on your laptop, mobile phone, or other devices.
- Backup your device before traveling in case your device is wiped.
- Tape over any integrated laptop cameras or disable them to prevent a hacker from viewing you while you use your laptop.
- Be aware that Mount Union firewalls block contents coming from many countries. So, there is a chance that you may not be able to reach Mount Union resources from outside the U.S.
- You are responsible for the safety of Mount Union owned devices and Mount Union data. So, in the event this device or data is lost, stolen, or compromised you will be held accountable.
- Be aware that you may need to purchase international calling plans ahead of your travel.
- Leave unneeded car keys, house keys, smart cards, credit cards, swipe cards, or fobs you would use to access your workplace or other areas, and any other access control devices you may have at home.
- Clean out your purse or wallet of any financial information such as bank account numbers, logins and passwords, any FRID cards should be carried inside an RF-shielded cover.

Artificial Intelligence (AI) Security

Artificial Intelligence is the science of making machines that can simulate human intelligence.

Guiding Principles: The Institution has developed guiding principles around the use of AI. The purpose of these guiding principles, as an institution of learning, is to outline our commitment to responsible, ethical, beneficial AI development and deployment, ensuring that an AI systems align with UMU's mission and values and contribute positively to society.

We strive to:

1. **Make ethical choices**. We will ensure integrity is the highest priority. We will address bias, fairness, privacy, transparency, and accountability in all AI-related decisions.
2. **Leverage AI to Empower Institutional Success**. We will embrace AI's potential to enhance our capabilities, stimulate innovation, and drive operational efficiency.
3. **Keep "Humans in the Loop."** We will maintain the perspective that AI cannot substitute for human judgment. Human judgment should never be replaced by AI.
4. **Respond to Continuous Change.** We will balance careful consideration, agility, and urgency to respond to continuous change.
5. **Safeguard Confidential Information**. We will protect confidential information through security measures. We will follow data privacy regulations and strive to protect UMU faculty, staff and student data.

AI Security Guidelines:
It is essential to recognize the potential benefits and challenges presented by the use of AI systems to perform professional tasks. As the use of generative AI tools continues to grow, it is important to understand how to use these tools safely and appropriately. Generative AI can create new content (text, images, video, etc..) based on user input, but with any technology, it has its limitations. It is essential to understand that generative AI is not infallible and can

sometimes generate incorrect information. It is also important to consider the ethical and privacy implications of using these tools, and to use them in a manner that is respectful and compliant with university policies.

- Not all AI systems offer the same level of data privacy and protection. If there is any doubt, Do NOT use any nonpublic data with an AI system. This is especially important for any personally identifiable information (PII).
- It is important to acknowledge the use of AI generated content or analysis.
- AI systems are known to demonstrate biases, and these can vary from system to system based on the training sets. It is important to monitor the output of AI System.
- University policies governing workplace behavior continue to apply when a university employee uses AI in their university work. The employee and student generating output from AI is responsible for the appropriate us of that output.
- If you are using AI tools that are not under a university contract or agreement, you should ONLY be using data that is classified as PUBLIC (low sensitivity).
- Faculty, staff and students should be aware of OpenAI Usage Policies disallow the use of its products for other specific activities. Usage policies | OpenAI
- AI tools can generate incomplete, incorrect, or biased responses, so any output should be closely reviewed and verified by a human.
- The National Institute of Standards and Technology (NIST) has published a draft AI Risk Management Framework AI Risk Management Framework | NIST to help organizations use a formal approach to managing AI risks. The Framework lists the following attributes of trustworthy AI:
    - Valid and Reliable. Trustworthy AI produces accurate results within expected timeframes.
    - Safe. Trustworthy AI produces results that conform to safety expectations for the environment in which the AI is used (e.ge., Healthcare, transportation, etc.)
    - Fair/Bias is Managed. Bias can manifest in many ways; standards and expectations for bias minimization should be defined prior to using AI.
    - Secure and Resilient. Security is judged according to the standard triad of confidentiality, integrity and availability. Resilience is the degree to which the AI can withstand and recover from attack.
    - Transparent and Accountable. Transparency refers to the ability to understand information about the AI system itself, as well as understanding when one is working with AI generated (rather than human-generated) information. Accountability is the shared responsibility of the creators/vendors of the AI as well as those who have chosen to implement AI for a particular purpose.
    - Explainable and Interpretable. These terms relate to the ability to explain how an output was generated, and how to understand the meaning of the output.
    - Privacy-enhanced. This refers to privacy from both a legal and ethical standpoint.

  Appendix B of the framework includes a discussion of risks that are unique to AI. It is recommended to review these risks to understand how AI risk differs from more familiar technology risks.
- Any implementation of artificial intelligence is subject to applicable university policies and standards, including a security review process. If you have questions, please contact ITSecurity@mountunion.edu.
- If you have questions about using Artificial Intelligence tools in your teaching, including syllabus language, developing assessments, etc., please contact the Center for Faculty Development or Digital Learning.
- You should be aware of Data classification and handling guidelines. Please see the section titled Data Classification and Handling Guidelines prior in this policy. To help you determine the classification of particular data, please answer the following questions:
    - Is the confidentiality of the data important?
        - YES – Is the information so sensitive, that disclosure would have a definite and significant impact on the university?
            - YES – Information is HIGHLY CONFIDENTIAL (Level 1)
            - NO – Information is CONFIDENTIAL (Level 2)
        - NO – Is the Information intended for the public?
            - YES – information is PUBLIC (Level 3)
            - NO – Information is CONFIDENTIAL (Level 2)

Applies to: Faculty, staff, student employees, students, and volunteers

Responsibilities

Position or Office	Responsibilities
Office of Information Technology (CIO and Director of IT For Security)	Update of Policy & Protection of Data
Users of Data	Protecting institutional data
VPs, Deans, Directors, Department Heads, Supervisors	Implementation of this policy within their respective units.
VP Business Affairs & CIO, Director of IT for Security	Oversight of information security

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330.823.2854	IT@mountunion.edu

History

This policy was established in 2000, last modified in 2011 part of the PCI compliancy efforts and was placed into the new format in 2016.

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.

Issued: 2/8/2011
Revised Last: 12/3/2024
Edited by: Tina Stuchell
Reviewed: 12/3/2024