Technology Resources Acceptable Use Policy
TEC 2.0

Office of Information Technology

Policy Type: Administrative
Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

POLICY DATES

Issued: 6/01/1995
Revised by: Tina Stuchell
Edited: 2/22/2024
Reviewed: 2/22/2024

It is the policy of the Office of Information Technology of the University of Mount Union that the technological resources are intended to be used primarily for educational purposes, communications and to carry out the legitimate business of the University. Appropriate use of the resources includes instruction, independent study and research, and the official work of the offices and recognized student organizations. The privilege of using computer and network resources extended by the University to specific individuals and organizations is not transferable.

Table of Contents

Definitions

Term	Definition
Technology Resources	May be defined to include university owned software applications, file and print services, wireless access, network resources, internet, email, library resources, ID Card system, multi media resources, desktops, laptops, tablets, printers, desktop applications and computer resources, etc.
Network	University network comprised of switches, routers, wiring, internet, and wireless

Policy Details

Mount Union makes available technological resources that may be used by University students, faculty and staff. These resources may include administrative software applications, file and print services, VPN, wireless access, network resources, email, library resources, ID card system, multi-media resources, desktop applications and computer resources.

These resources are intended to be used primarily for educational purposes, communications, and to carry out the legitimate business of the University. Appropriate use of the resources includes instruction, independent study and research, and the official work of the offices and recognized student organizations. The privilege of using computer and network resources extended by the University to specific individuals and organizations is not transferable.

The responsible, considerate and ethical behavior expected by Mount Union in all aspects of the community extends to cover the use of campus computer and network resources and the use of networks throughout the world to which Mount Union provides computer access. The University's guidelines for appropriate use are not meant to be an exhaustive list of what may or may not be done with the University's computer or network resources.

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

Those who make use of the network and computing resources must conform at all times to the policies contained herein, as well as the regulations and guidelines of the University as specified in the Student Handbook and the various employee handbooks. These policies exist to safeguard the security and functionality of the campus network and all components therein

The Technology Resource Acceptable Use Policy is comprised of several components described below including unacceptable use, Technology User Code of Conduct, Network Use, Email Use, Hardware & Software Support, Data Security, and Microsoft OneDrive for Business Use. Additional polices that should be reviewed by faculty, staff and students include the Information Security Policy, Environmental Print Policy, Information Security, Mobile Device, Portable Equipment Usage and Liability, Unified Communications Policy, Loaner Equipment Policy as these additional polices may pertain to them.

Unacceptable use of the University's computer and network resources are described below:

I. Misuse of Service
   a. Any action that renders facilities unusable to those who rely on them or that interferes with another's use of facilities constitutes misuse. Examples are failure to respect the priorities posted at a public machine, overuse of resources, damage to software or hardware, sending repeated unwanted electronic mail, neglect or damage of software or hardware, and failure to report known problems.

II. Breach of Security
   a. Any attempt to circumvent the protection that Mount Union has in place to prevent unauthorized access or any action that reduces the security of the University's computer and network resources is unacceptable use. Examples are attempts to misappropriate passwords, attempts to gain unauthorized access or sharing your password with others and violating federal, state and local laws related to privacy.

III. Illegal Use
   a. Any use of computer or network resources in the commission of an illegal act is unacceptable. Examples are violation of licensing agreements, attempting to break into a computer or sending harassing or threatening electronic mail. There are federal, state and local laws that govern certain aspects of computer and telecommunications use. All laws pertaining to tangible documents or instruments apply equally to electronic files. This includes student records. Members of the University community are expected to respect these laws. Any use, even if not specifically prohibited, which falls within these broad categories should be considered inappropriate. If you are unsure of the propriety of an action, contact the Office of Information Technology (IT) for clarification.
   b. Much like laws that govern print and recorded media, U.S. Copyright law protects copyright owners from unauthorized reproduction, adaptation or distribution of digital media. While users in educational settings enjoy limited permission to use copyrighted works under the "fair use" provisions of the copyright law, students and faculty who are engaged in developing web pages and other electronic media are advised to read further what the law allows under these circumstances. A very useful text Commonsense Copyright: A guide for Educators and Librarians by R. S. Talab is available in our Library
   c. Some points include:
      i. Excerpts must be brief and confined to a campus network
      ii. Faculty may keep copies of student work for a maximum of two years as examples of exemplary work.
      iii. Students may show multimedia projects developed in University classes for interview and potential employment as long as they have followed fair uses practices.

IV. Peer-to-Peer File Sharing
   a. Peer-to-peer file sharing is prohibited. The Office of Information Technology monitors traffic patterns in order to guarantee acceptable network performance for all users. If IT becomes aware of policy violations or illegal activities in the course of investigating network congestion or problem determination, IT will further investigate by inspecting content stored or shared on its network.
   b. A minimum response to violators of copyright laws, as well as those impeding network performances, will be a warning to cease and desist. In certain circumstances, including those

involving repeat offenders, violators will have their access blocked and be turned over to the University judicial process. If contacted by the RIAA (The Recording Industry Association of America), DMCA (Digital Millennium Copyright Act) or by the courts and asked to identify those who are sharing or downloading based on IP addresses, Mount Union will comply with the law.

c. Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject a student, faculty or staff member to civil and criminal liabilities. Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act 9Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work Infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. Willful copyright Infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information visit the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq

V. Systematic Monitoring and Access and Disclosure without Consent

a. Mount Union is not obligated to monitor the content of email or file space. The Office of Information Technology, however, maintains the rights to monitor, trace, intercept, or block any network traffic for security or management purposes. Mount Union will, as a courtesy, normally try to inform users prior to any inspection, monitoring or disclosure of email or electronic files, except when such notification would be detrimental to an investigation of possible violation of law or University policy. Users are required to comply with University requests for access to and copies of email records and electronic files when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to disciplinary or legal action pursuant to applicable law or policy, including, but not limited to, appropriate University personnel policies or Codes of conduct.

b. In summary, Mount Union shall only permit the individual monitoring, inspection or disclosure of electronic mail, electronic files or network traffic:

   i. When prior consent has been obtained in writing from the employee and/or student. Consent is given when an individual signs her/his contract or registration. Any employee or student who refuses consent may be denied access to the Internet and electronic mail.
   ii. When required by and consistent with law.
   iii. When there is probable cause or substantiated reason to believe that violations of law or of Mount Union or state policies have taken place.
   iv. When it is for a valid business purpose and there are compelling circumstances; and/or
   v. Under time-dependent, critical operational circumstances.

VI. Remedial Action and Sanctions for Violations of Technology Policies

a. Final technical authority for the Mount Union computer network rests with the Office of Information Technology, who may issue training notices, alerts, or warnings for any minor or inadvertent misuse of service or breach of security. Any illegal activity will be reported immediately to the appropriate University official. Final disciplinary authority for misconduct or misuse by members of the Mount Union community rests with the appropriate authorities outlined in the Student Handbook and the various employee handbooks.

b. Access to Mount Union’s email, network and Internet services are a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the user. This may occur when there is probable cause or a substantiated reason to believe that violations of policy or law have taken place or in exceptional cases when required to meet time-dependent, critical operational needs. Any employee or student who abuses the privilege of University facilitated access to the Internet and email may be subject to disciplinary action up to and including termination or expulsion. If necessary, the University also reserves the right to advise appropriate legal officials of any violations and institute legal proceedings against violators of this

policy. Any policy violations should be reported to Helpdesk@mountunion.edu. Acts of retaliation for reporting instances of misuse are prohibited, both by the University and under state and federal law. Reports of misuse cannot be made anonymously, due to the ability of the system to track the originator of any electronic communications.

VII. Automatic voice and video services devices

a. Automatic voice and video services devices such as Amazon Alexa, Amazon, Echo, Apple Homepod, Google Home, Portal from Facebook, etc. are not permitted to be used on campus within faculty, staff offices, conference spaces, etc. where conversations can be in violation of FERPA and inadvertently recorded on those devices.

Technology User Code of Conduct

I. The following Code of Conduct is intended to instruct technology users in acceptable behavior regarding their use of Mount Union technological resources. This document is not intended to be exhaustive if all possible behaviors that may be deemed inappropriate. Users are expected to adhere to all policies set forth by the University regarding the use of technology resources. Failure to follow the expectations set forth in this Code of Conduct or any other policy of the University regarding use of technology may result in sanctions against the user, including, but not limited to, loss of access to technology resources and/or disciplinary action.

a. Users are responsible for how their accounts are used; therefore, every effort must be made to protect against unauthorized access to accounts. Users must have a password which will protect their accounts from unauthorized use, and which will not be guessed easily (be complex) or be dictionary words. If a user discovers that someone has made unauthorized use of her/his account, she/he should change the password immediately and report the intrusion to the Office of Information Technology. Users are required to change their password every 90 days. Users should not use the same password for multiple systems.

b. Users may not intentionally seek information about, browse or obtain copies of or modify files or passwords belonging to other people, whether at Mount Union or elsewhere, unless specifically authorized to do so by those individuals. Also, users may not attempt to intercept, capture, alter or interfere in any way with information on campus or global network paths.

c. Users must not attempt to decrypt or translate encrypted material or obtain system privileges to which they are not entitled. Attempts to do any of the above will be considered serious violations.

d. If users encounter or observe a gap in system or network security, they must report the gap to the Office of Information Technology. Users must refrain from exploiting any such gaps in security.

e. Users must refrain from any action that interferes with the supervisory or accounting functions of the system or that is likely to have such effects.

f. Users must be sensitive to the public nature of shared facilities and take care not to display sounds or messages that could create an atmosphere of discomfort or harassment for others.

g. Users must avoid tying up computing resources for game playing or other trivial applications, sending frivolous or excessive mail or messages locally or over an affiliated network or printing excessive copies of documents, files, images, or data.

h. Users may not prevent others from using shared resources by running unattended processes or placing signs on devices to “reserve” them without authorization.

i. Users may not copy, cross-assemble or reverse-compile any software or data that the University has obtained under a contract or license that prohibits such actions. If it is unclear if it is permissible to take such actions, users should assume that they may not do so.

j. Software may not be copied or used illegally. Website materials must be cited appropriately, and permission obtained for the publishing, performing or distribution of copyrighted material.

k. Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings must meet the same standards for distribution or display as if they were tangible documents or instruments. Users are free to publish their opinions, but they must be clearly and accurately identified as coming from the particular user or, if a user is acting as the authorized agent of a group recognized by the University, as coming from the group she/he is authorized to represent. Attempts to alter the “From” line or other attribution of origin in electronic mail, messages or postings will be considered violations of university policies.

l. Users may not take any action that damages Mount Union technology resources in any way, including technology found in classrooms, public computing labs, departmental labs, residence halls and University houses, or any other campus location.
m. Users may not establish any computer to function as a server without the knowledge and approval of the Office of Information Technology.
n. Users are required to utilize anti-virus software on their computers. Anti-virus software must be updated regularly.
o. Users may not deploy any network electronic equipment or install wireless access points without express permission from the Office of Information Technology.
p. Users who utilize the Mount Union email system are required to comply with state and federal law, University policies, and normal standards of professional and personal courtesy and conduct.
q. Employees should never store Mount Union data on unsanctioned storage devices, including cloud storage site (i.e. Dropbox), thumb drives and home computers.

Network Use

The Mount Union network is provided for the academic use of students and faculty of the University, as well as to the University administration for conducting official University business. Academic use is determined to be any legitimate use of the network for the purpose of assisting in the conduct of the University's academic mission. The official conduct of University business is limited to efforts on behalf of the management and administration of the University. The network provides access to the Internet from all offices, residence hall rooms and computer labs, in addition to public access stations in the library. Students living in on campus housing are accorded the privilege of using the network for personal use, as long as such use is in keeping with all applicable policies of the University and state and federal laws and is not excessive (resulting in diminished service to fellow students).

User access to the network is governed by the acceptable use policy of the University, as well as by the following.

Servers

All servers operating on campus must do so with the knowledge and consent of the Office of Information Technology. A server is defined as any computer providing services of any type to other computers on the network or on external networks. Such services could include DNS, DHCP, SNMP, email and application, file and/or printer sharing. In order to request the deployment of a server on the network, written petition must be made, stating:

- The legitimate academic use of the server.
- Intended server operating system.
- All intended server functions and applications, including protocols and services; and
- The identity and function of target subordinate computers/users.

Any computer acting as a server without prior authorization as stated above will be removed from the network. All licensing, operation and support of the hardware and software utilized will be the responsibility of the petitioner, if such petition is granted.

Accounts

All authorized users will be provided an account by which to access the necessary network resources of Mount Union. The information regarding this account, including the account name and password, is privileged, and must not be disseminated to anyone other than the account owner for any purpose. Account holders should protect their passwords and keep them confidential. Passwords should be changed frequently.

Any problem resulting from irresponsible use of a password (e.g., a password that can be easily guessed or oral or written dissemination of a password, as well as passwords that are stored in scripts or saved on an individual machine) may be treated as grounds for action against the account holder. Any attempt to determine the passwords of other users is strictly prohibited.

The following are categories of authorized users:

- Full-time staff of the University
- Current faculty members
- Current students

The following categories of users may be authorized to utilize the University network based on the legitimate need for access

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

to such resources:

- Part-time staff of the University
- Volunteer staff of the University
- Student employees
- Current students on transfer
- Retired members of the faculty and staff
- Guests & approved third-party vendors

Other categories of users may be granted special permission to obtain access to the system at the discretion of the University. Student employees who need to access administrative software and resources due to their employment must be given approval for this access by an office administrator.

Special Access

From time to time, circumstances dictate the provision of short-term, special access to university systems. Such access must be in accordance with the strictest adherence to the user policies stated above and may only be granted by the Office of Information Technology after review of a written petition. The petition must state the purpose of the access, the source username, and the department. Such access will typically be provided only for a limited time and will be allowed only from designated computers. All such petitions that are approved will be maintained on file in the Office of Information Technology. All connections made through such petitions will be monitored.

Network Electronic Equipment

Network electronic equipment, including switches, hubs wireless access points, and routers, may only be installed on campus with the knowledge and consent of the Office of Information Technology. In order to request the deployment of this equipment on the network, written petition must be made stating:

- The legitimate academic use of the equipment.
- The type of equipment wishing to be deployed and for what purpose.
- All intended functions, including protocols and services; and
- The identity and function of target subordinate computers/users.

Any network electronic equipment deployed without prior authorization as stated above will be removed from the network. If a petition is granted, all licensing, operation and support of the hardware and software utilized will be the responsibility of the petitioner.

VPN (Virtual Private Network)

VPN is a resource made available to faculty, staff, and non-residential Mount Union students. VPN will allow a user to connect to the campus network from an off-campus ISP (Internet Service Provider) and make it appear to the user that they were physically connected to the Mount Union network. VPN will allow users to gain access to specific tools that are not cloud based. If misuse of this resource occurs or if the user does not comply with the VPN Policy of Mount Union, the Office of Information Technology reserves the right to terminate any VPN connection without notice. Any party found to have violated the VPN rules may be subject to disciplinary action, including termination of VPN access.

Wireless

Wireless technology is available within most indoor areas of Mount Union and some specific outdoor areas (Academic Mall, Stadium). Use of the wireless network implies consent to abide by all University policies pertaining to the use of computer resources at Mount Union. Users may not install wireless access points. Any unauthorized wireless access points deployed will be removed from the network and users may face disciplinary actions.

Campus ID Card System

The Campus ID Card System is a network resource and as such is protected by the rules of this policy. Any party found to violate this policy or damage devices specific to this system, such as door card, vending machine, or cash register, may be subject to disciplinary action.

Web Pages

The Mount Union website (including Raider Experience, Athletics site, alumni site, etc.) are network resources and as such are protected by the rules of this policy. Any party found to violate this policy may be subject to disciplinary action. Any Mount Union entity may request an organizational or office/department web page. By using the site, you automatically agree to this policy. To request an organizational, departmental or office web page please contact the Information Technology Helpdesk or Office of Marketing. Every Mount Union entity must provide a contact person, who is willing to respond to comments or questions concerning the information the home page and on related documents provided by the

entity. The name and email address of the contact person must appear at the bottom of the home page along with the date of the last update of the page and/or related documents. In the case of copyrighted material, the representative is responsible for obtaining the necessary permission for posting such material. All material must be suitable for viewing and/or reading by individuals of all ages and conform to copyright laws. These are not limitations of free speech but represent the policies of this Institution.

Social Media

Social media is defined by Mount Union as public forms of communication that are used via the Internet. This form of communication combines integrated technology, social interaction, and the construction of words and/or pictures. Such sites are as follows but not limited to: LinkedIn, Facebook, X (formerly Twitter), MySpace, YouTube, Shutterfly, Flickr, Plurk, Blogs, Wiki, Digg, etc. or any social site that can be created by a person and utilized as marketing the institution in any manner. Personal sites are permitted and are not held to the approved identity standards of Mount Union, however, any reference to the institution must adhere to the values of the institution. Please reference the Identity Standards to ensure the proper usage of Mount Union policies for written or video communication. Anyone choosing to create a social media site representing an office, department, organization and/or any site that would be connected to the brand of Mount Union must contact the Office of Marketing. Additional policies pertaining to social media include Social Media Policy and Student Social Media Policy, please review these policies for additional information.

Campus Telephony (VOIP)/Unified Communications Services

The campus Unified Communications Services includes voice/telephony, instant messaging (IM), presence, etc. (Tools available in MS Teams). These services including voice-messaging, Voice messaging is an electronic voice messaging system that gives users a convenient and dependable way to communicate with people. Voice messaging answers calls when the user is on or away from her/his phone. Users of MS Teams should be aware of Mount Union's Unified Communication policy. Users of these services agree to abide by this policy. This policy can be found under University Polices on the main web site.

Email

Mount Union email is intended to serve the communication needs of the University community. Access to the email system is a privilege. Any email addresses or accounts assigned by the University to individuals, sub-units or functions of the University are the property of the University. The Mount Union network is not intended for private correspondence, as such, all communications on the University's computer systems, whether personal or business related, are the property of Mount Union. Email users are required to comply with state and federal law, University policies and normal standards of professional and personal courtesy and conduct. Unacceptable uses of email and Internet access include, but are not limited to, the following:

- Use for any purposes that violate a federal, state, or local law.
- Use for any commercial activities, including commercial advertising unless specific to the charter, mission or duties of Mount Union.
- Use to publish post, distribute, disseminate, or link to any:
- Inappropriate, profane, defamatory, infringing, obscene, indecent, harassing, or unlawful topic, name, material, or information
    - Software or other material protected by intellectual property laws, rights of privacy or publicity or other proprietary rights, unless the individual owns/ controls such rights or has received all necessary consents for the use of such software and other materials
    - Software or other material that contains viruses, corrupted fi les or that may or are intended to damage the operation of another's computer
- Use to gather or otherwise collect information about others for commercial or private use, including email addresses, without the express consent of the individuals.
- Use for fund raising, political campaign activities or public relations activities not specifically related to Mount Union activities.
- Use to conduct or forward illegal contests, phishing attempts, pyramid schemes, chain letters or to spam.
- Use to sell access to the Internet.
- Use to conduct any activity that adversely affects the availability, confidentiality, or integrity of Mount Union's technology.

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

- Use to benefit personal or financial interests of any employee or student.
- Use for mass email purposes. UMUToday should be used to get an announcement out to a broader audience.

Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion or endorsement by University of Mount Union."

Restriction of Email Privileges in Response to Resource Limitations, Administrative Procedures, or Policy Violations

The Office of Information Technology of Mount Union sets the amount of disk space available for mailboxes and file space in conjunction with licensing agreements. On occasion it may become necessary for IT to impose additional limitations on the use of email due to technical necessities or to require purges of information stored on the University servers to preserve the integrity of the system. Users are advised to implement a data recovery plan, for example storing files on a backup hard drive or making paper copies, as well as regularly archiving their email messages.

Security

Email, as a public record, is subject to the Freedom of Information Act and to subpoena by a court of law. Users should be aware that any information submitted via email is not confidential and could be observed by a third party while it is in transit. Encryption encourages the false belief that privacy can be guaranteed. Users should never put anything in an email message that must be kept confidential. Email users should assume that anyone could accidentally or intentionally view the content of their message. Email security is a joint responsibility of Mount Union Office of Information Technology and email users. The University will provide the security offered by the currently used software, as well as a "firewall" to prevent unauthorized access to the mail server. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of the account by unauthorized individuals. Users may not divulge passwords for Mount Union accounts to any other person or allow other persons use of their Mount Union account for any reasons.

Archiving and Retention

The Office of Information Technology does not archive documents. Mount Union institutional records, such as transcripts, invoices, etc. are kept in accordance with the universities retention policy. Email and file space are not archived by the institution. Employees are required to follow the university's retention policy as it relates to institutional data. Offices of the institution may use the institutional approved documents retention software, etrieve by Softdocs, for data retention purposes.

Eligibility for Email Privileges

Students are eligible for email privileges if the student is officially registered at Mount Union. Student's Faculty and staff email privileges start on the date employment begins and ends at the close of the business day of the date of employment termination. The Mount Union Office of Information Technology may, under its sole discretion, attempt to redirect email for a reasonable period of time as determined by the University for purposes consistent with this policy and the University's mission. The University may elect to terminate the individual's email account or continue the account, subject to approval by appropriate University supervisory and systems operational authority. Employees are not permitted to forward Mount Union Email to any other email service providers. The Office of Human Resources at Mount Union is responsible for notifying the Office of Information Technology of the date of employment termination for faculty and staff. Retires and those students who are graduates after 2014 are eligible to keep their Mount Union email active. Mount Union Retirees are permitted to retain their Mount Union email only as long as they annually complete the data security training. Failure to complete the training results in email account being disabled. For more information related to email accounts see the Office of Information Technology Customer Service Policy and Account Creation Policy.

Hardware and Software Support

University-Owned Desktop Computers

The following outlines support levels provided by the Office of Information Technology for system and application software on university-owned desktops and laptops used by faculty, staff and administrators at the University.

Hardware

All University-owned desktop computers are covered under a warranty period, which varies depending on vendor and model. If a service problem is determined to be hardware-related, support will be obtained for that unit in accordance with the terms of the warranty.

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

Support Levels for System and Application Software Used on Mount Union Owned equipment

Level I

Level I software products represent a core set of office automation applications that the University has deemed necessary for fulfillment of position requirements and for which it offers support to faculty, staff and administrators using the applications. These products receive the highest level of user and technical support from the Office of Information Technology. Upgrade and maintenance efforts toward these products supersede efforts on all other administrative products and represent the core set of products initially installed on user desktops. Recommendations for additions and deletions to the core set of applications will be considered and approved by the appropriate governance structure of the University and provided in writing to the Office of Information Technology. Upgrades and fixes to these products will automatically take place and be coordinated by the Office of Information Technology. Examples include Microsoft O365, MS Teams.

Administrative Systems Software

Mount Union utilizes several specialized applications for administrative purposes. All of these applications must be used in the context of all federal guidelines including the Family Educational Right to Privacy Act

(www.ed.gov/policy/gen/guid/fpco/ferpa/index. html). Examples of administrative software include, but are not limited to, the following: Slate, Colleague, Self-Service, Raiser's Edge, CSGold ID Card system, Adirondack Housing & Code of Conduct, D2L Brightspace, Ellucian Experience, EMS, etc.

Level II

Level II products represent unique products that are required by a limited number of individual users for administrative tasks specific to their positions. Products at this level will may be installed locally or on servers, with the user's data files stored on network servers or MS OneDrive for backup and recovery purposes. Generally, users of these products will consist of less than a dozen users per product. The Office of Information Technology will make the final determination concerning whether these products will be installed on the network or local drives based on the product's function and application requirements. These products receive a limited level of user and technical support from information technology due to their limited deployment and specialized focus. Users of these products should plan on becoming familiar with these products to a greater degree than products supported at Level I since limited expertise will be developed in the Office of Information Technology to support the product. Upgrades to these products will need to be coordinated and requested by users of the product. Automatic upgrades of the product will not normally be done by the Office of Information Technology. All copies of the product will be maintained at the same version and release level throughout the University. Recommendations with supporting rationale for additions and deletions to this set of applications will be coordinated and recommended by the individual department in conjunction with the Office of Information Technology.

Level III

Level III products represent unique products that are not included in the Level I or II categories above. The user will install products at this level on the user's local disk drive with consent and assistance from the Office of Information Technology. These products will not typically be installed on servers, although application files may be stored on network servers or MS OneDrive for security purposes. These products receive the lowest level of user and technical support from the Office of Information Technology due to their limited deployment, unique focus and individual user preferences. Users of these products should plan on becoming completely familiar with these products and should have expectations of supporting the product themselves. The Office of Information Technology assistance will be available only as time permits after Level I and Level II support needs are met. Upgrades to these products will be at the user's discretion, but the University's management reserves the right to remove any illegally obtained or installed software from any University owned computer, or to remove any software that is adversely affecting the operation of any networks to which the computer is connected. The Office of Information Technology will also conduct software audits periodically to ensure that the University is in compliance with state and federal laws concerning software use. The user should ensure that all copyright and license requirements are documented and on file for any software installed on her/his computer.

****** Additional software should not be purchased without the knowledge and consent of the Office of Information Technology. ALL UNIVERSITY TECHNOLOGY PURCHASES MUST GO THROUGH THE OFFICE OF INFORMATION TECHNOLOGY.******

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

Personally Owned Computers on Campus

Hardware

No hardware support is available for non-University owned equipment for faculty & staff members. There are several local companies that provide warranty and out-of-warranty repair service on personal computers. You can contact the Helpdesk for recommended vendors.

Other

Personally owned computers belonging to faculty or staff members in use on campus will be supported for network connectivity only, and then only if they meet the minimum system requirements found in the current user packet or information technology website. Such support will be limited to establishing network connectivity and assistance with logging in to the appropriate domain. Personally owned computers belonging to the students will be supported by the helpdesk in a limited manor. Students can find out additional information on this service by visiting the Helpdesk or the IT web site. Additional computer services offered to students can be found on the Office of Information Technology web site.

Not Supported

Any computers not specified above, as well as those computers in use by faculty and staff that are not located on campus, will not be supported unless the computer is University-owned and is being used in the course of administrative or academic business.

Data Security

Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today's environment because data is a valuable asset. Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize the University's ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate business contracts and customer privacy; or reduce credibility and reputation with its students, faculty, staff, friends, and alumni. The main objective is to ensure that data is protected in all of its forms, on all media. This applies to all University data. Storage on any locations not sanctioned by the University is prohibited. This includes locations such as home computers, thumb drives, non-institutional supported cloud storage locations (i.e. Dropbox, personal cloud storage, etc.).

A breach could have severe consequences to Mount Union. The goals are to educate users about their obligation for protection of all data assets, to ensure the security and integrity of all University data. It is the responsible of the individual to keep Mount Union data secure on any device, including but not limited to desktops, laptops, portable hard drives, mobile devices such as cell phones, etc. Individuals are prohibited from downloading, storing, or recording of data that include any information which if lost or stolen could be used for identity theft purposes. Faculty and Staff are required to participate in data security training on an annual basis during compliancy days. Additional Information on data security can be found in the Office of Information Technology's Data Security Policy, Mobile Device Policy, etc.

Cell Phones

Any faculty, staff or student who carries a cell phone that access Mount Union email or applications whereby they are accessing Mount Union data must comply with the Office of Information Technology policies. Users are expected to secure their device by using passwords, changing them regularly, always lock the device when not in use, encrypting data and securing their device to prevent theft. Any Mount Union data that is stored on a mobile device is the responsibility of the owner. If Mount Union data is stored on a mobile device and the device is lost it must be reported to the Office of Information Technology immediately.

Users are expected to adhere to all policies set forth by the University regarding the use of technology resources. Failure to follow the expectations set forth in this section or any other policy of the University regarding use of technology may result in sanctions against the user, including, but not limited to, loss of access to technology resources and/or disciplinary action. Additional information can be found in the Office of Information Technology's mobile device policy.

Microsoft OneDrive for Business

Microsoft OneDrive for Business is a cloud-based storage system for work/educational related files. MS OneDrive for Business is the endorsed cloud file sharing solution for the campus. There are security practices that must be followed to ensure the service is being used properly. The guidelines listed below should be followed at all times when making use of MS OneDrive for Business.

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

Data Classification

Confidential Data

- Confidential Data includes data which, if accessed by unauthorized entities could cause personal or institutional financial loss or constitute a violation of statute, act or law. Examples of confidential data include but are not limited to:
    - Social Security Numbers
    - Bank account or credit card numbers
    - Data covered by the Federal Educational Rights and Privacy Act (FERPA)
    - Data covered by the Health Insurance Portability and Accountability Act (HIPAA)
    - Trade secrets or information that may be purchased for the creation of a patent.
    - Login/password credentials.

Confidential data should not be stored on this service.

Sensitive Data

- Sensitive data is information generally used internally at the university or with its authorized partners. If released to unauthorized individuals, this data would not result in any financial loss or legal compliance issues but would negatively impact the privacy of the individuals named or the integrity or reputation of the university. This includes but is not limited to the following:
    - Employees who have chosen to suppress their directory information.
    - Identities of donors or other third-party partner information maintained by the University not specifically designated for public release.
    - Proprietary financial, budgetary or personnel information not explicitly approved by authorized parties for public release.
    - Emails and other communications regarding internal matters which have not been specifically approved for public release.

Sensitive data may be stored and shared in OneDrive but must be stored and shared in a secure manner.

Public Data

- Data is 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, and 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.

Public data may be stored and shared in OneDrive but must be stored and shared in a secure manner.

Unclassified Data

- Data that does not meet the criteria as confidential, sensitive, or private as defined above shall be considered non-classified data. Please note that this classification does not imply that the data does not need to be properly managed. Such data may be subject to open records requests.

Unclassified data may be stored and shared in OneDrive but must be stored and shared in a secure manner.

How to Use OneDrive Securely.

- Ensure virus/malware detection software is installed with the latest definitions.
- Do not use a public machine to access MS OneDrive (i.e. hotel lobby computer).
- Do not use public Wi-Fi to access MS OneDrive. Use a secure network.
- Keep your operating system and software up to date.
- Password protect your workstation or device and use idle-time screen saver passwords where possible.
- Do not sync files to a machine or device that is not issued and secured by the university.
- Do not store personal files in OneDrive for Business.

Applies to: Faculty, Staff, Student Employees, Students, and Volunteers

Best Practices for sharing files.

- Use folders to share groups of files with others online.
- Use institutional tools such as MS Teams.
- Share files with specific individuals, never with “everyone” or the “public.”
- Be careful sending links to shared folders because they can often be forwarded to others who you did not provide access to.
- Remember that once a file is shared with someone and they download it to their device, they can share it with others.
- Remove individuals when they no longer require access to files or folders.
- Sharing the contents of the stored files on MS OneDrive with foreign nationals could result in violation of US Export control regulations. You are responsible for knowing who you are sharing files with.
- Personal cloud storage locations should not be used to store Mount Union data.

For additional information or questions on these guidelines please contact the Office of Information Technology.

International Travel

If you are planning to travel internationally, you must notify certain offices. Please review the Information Security Policy before traveling.

Policy Updates and Reviews

This policy will be reviewed on a regular basis. Updates may be made without notification. It is the user’s responsibility to review applicable policies on a regular basis.

Indemnification of Mount Union

Users agree by virtue of access to the University’s computing and email systems, to indemnify, defend and hold harmless the University for any suits, claims, losses, expenses or damages including, but not limited to, litigation costs and attorney’s fees arising from or related to the user’s access to or use of university email and computing systems, services and facilities.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology	Provides and maintains the campus's information technology resources.

Contacts

Position	Office	Telephone	Email/URL
Executive Director of IT & CIO or Director of IT for Security	Office of Information Technology	330-823-2854	IT@mountunion.edu

History

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.
Issued: 6/01/1995
Revised by: Tina Stuchell
Edited: 2/22/2024
Reviewed: 2/22/2024