Responsible Official: Director of Technology

Responsible Office: Department of Technology Services and Support

Next Review Date: July 2020

Website Address: https://myumo.moc.edu/services/ir/policies/Public%20Policies/TechServiceSupportPolicy.pdf

TECHNOLOGY SERVICE AND SUPPORT POLICY

POLICY STATEMENT

This policy provides notice of University of Mount Olive's expectations and guidelines to all who use information technology resources and services (including but not limited to computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, and any related materials and services).

The University provides the technology resources for the advancement of the University's educational, service, and business objectives. Any access or use of these resources that interferes, interrupts, or conflicts with these purposes is not acceptable and will be considered a violation of the policy.

REASON FOR POLICY/PURPOSE

The University of Mount Olive provides information technology resources to a large and varied group, including faculty, staff, students, and adjunct instructors. All members of the University community are responsible for using these resources in an effective, efficient, and ethical manner that does not interfere with the reasonable use by other community members. Additionally, University of Mount Olive employees who deal with sensitive data are required to exercise due diligence with regard to privacy and security policies and practices. This policy provides the necessary framework to accomplish these goals.

OPERATIONAL DEFINITIONS

Domain: A common network name under which a collection of network devices are organized

Protocol: The syntax, semantics and synchronization of communication between two or more devices on a computer network

Peer-to-Peer (P2P) protocols: Protocols that allow two or more computers to locate and connect to each other and share files using the only internet as the transmission vehicle

TABLE OF CONTENTS

POLICY/PROCEDURES

1. USER RESPONSIBILITIES

The University expects Technology users to access the Internet, e-mail, and all IT systems primarily for the purpose of conducting University or University-related business with limited personal use in those locations and at the times where personal use is authorized. All technology users are expected to abide by and respect University of Mount Olive's Mission and Covenant.

2. USER PRIVACY

University of Mount Olive reserves the right to examine, monitor, or embargo without prior notice, any data processed on or transmitted through its computer network. These actions will be executed only under the auspices of authorized agents of the University when these agents determine that a user might be in violation of policies with respect to academic honesty, employee conduct, the letter or spirit of its Mission and Covenant, FERPA or any state or federal law not otherwise covered in this policy.

3. TECHNOLOGY FACILITY USAGE

Students, Faculty, Staff, and Adjunct Instructors have access to computing facilities at each of the University's locations. Before entering its computing facilities users must discard all food and drinks and silence cell phones. Upon entering its computing facilities, users must not move, attempt to repair or configure any of the computing equipment. Users should report unserviceable equipment to the nearest University of Mount Olive administrator or use the Footprints ticket system to notify system support of the problem.

4. INTERNET

The University expects that users will access the Internet for academic research or to acquire other information that has relevance to University of Mount Olive's Mission and Covenant. Users should be aware that when accessing the Internet using the University's network and equipment, the institution is legally responsible for content downloaded or stored on its computers. Therefore, users cannot access the Internet for any purpose that would reflect negatively on the University or its representatives, or infringe on copyright with respect to the intellectual property of others. This includes using University information technology to engage in peer-to-peer file sharing of any illegally obtained intellectual property (including, but not limited to, audio/video media or
software) using BitTorrent or similar protocols. Pornographic websites, websites that use peer-to-peer protocols to facilitate illegal file sharing, and websites that host similar activities are blocked because such content violates the Mission and Covenant of University of Mount Olive.

4.1. RESIDENTIAL INTERNET ACCESS

The University provides a very robust and secure wired and wireless network for all residents. While the current network configuration will support MOST gaming hardware in MOST configurations, we have intentionally disabled some of features so it cannot support ALL gaming hardware in ALL configurations. Gaming hardware and protocols are designed to run over home networks, and many of the protocols that these platforms use are dangerous on an enterprise level network and, accordingly, have been disabled. The safety and security of the network must take priority over all other uses for the benefit of all users.

4.1.1. Devices that do not have a web browser cannot login to the University of Mount Olive wireless network. To get these devices online, users must register them with the Department of Technology Services and Support. This is done by bringing the device to the department for MAC address whitelisting. The Department of Technology Services and Support is located on the first floor of the Communications Building.

4.1.2. Devices such as gaming consoles, internet ready Blu-Ray players, and other media players are supported by the network, but are not guaranteed to work as if they were on a home network. Likewise, services like xBox Live and collaborative gameplay are not supported and may not work on University of Mount Olive's network.

4.1.3. Any device that requires "ad-hoc" networking, such as wireless printers or wireless cameras, will not work.

4.1.4. Residential routers such as Linksys, Netgear, D-Link, or others are explicitly not allowed on the network.

4.1.5. Wireless routers are not authorized as they can interfere with the University's native network. If rogue wireless access points are detected, the network will triangulate its location, and Technology Services and Support will disable the port to which it is connected.

4.2. SOCIAL NETWORKS

In order to minimize conflicts that arise from time to time between students who would like to browse social media and students who must use a computer resource to accomplish school work, all social websites are blocked from the main campus computer lab and library computers. Social media is enabled in all classrooms and wireless internet connections.

5. COMPUTER SECURITY

5.1. PASSWORDS

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of University of Mount Olive's entire University network. As such, all users of University of Mount Olive technology (including contractors and vendors with access to University of Mount Olive systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

5.2. GENERAL PASSWORD CONSTRUCTION GUIDELINES

Passwords are used for various purposes at University of Mount Olive. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, PowerCAMPUS, voicemail password, and local router logins. Before selecting a password, all users should understand how to recognize both strong passwords and weak passwords.

5.3. WEAK/POOR PASSWORD CHARACTERISTICS

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.

- Computer terms and names, commands, sites, companies, hardware, software (The words "University of Mount Olive", "Raleigh", "Microsoft" or any derivation)
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

5.4. STRONG/GOOD PASSWORD CHARACTERISTICS

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, user name, etc.

5.5. CONSTRUCTING AN UNFORGETTABLE STRONG PASSWORD

Constructing a strong password that is easy to remember is a fairly a simple process if the password is derived from a pass phrase. A pass phrase is a simple sentence that the user can remember. For example, a pass phrase might be: "How do I select a very strong password?"

- Step One: Strip off the first letter of each word in the sentence and capitalize proper nouns. (**hdIsavsp)**
- Step Two: Add one or more special characters (**hdIsavsp?)**
- Step Three: Add a number that you are not likely to forget (**hdIsavsp?1983)**

This strong password can be changed slightly to make it very simple for the user to change fairly often by simply varying the order of the components (placing the number or special character at the beginning or the phrase instead of the end, changing the special character, or changing the special number):

1983hdIsavsP?

1983?hdIsavsp

1983^hdIsavsp

^hdIsavsp1965

Any of the passwords above meet the characteristics of a strong password, yet are very simple for the user to remember because they are all built on a pass phase the user knows. The user only needs to derive the number and the special character he or she selected.

5.6. PASSWORD CHANGE REQUIREMENTS

All users must change their password every ninety, (90), days. A warning will appear on the user's MyUMO portal homepage or when logging into any workstation in the University of Mount Olive network domain 15 days before the password expires. Any user can change his or her password from Self-Service when outside of the University network or from the workstation he or she logs into from inside of the University network

5.7 EXTENDED LEAVE OF ABSENCE

If an employee engages in any form of electronic communication with any third party—email, Self- Service or MyUMO—and this communication is essential to the continued success of University of Mount Olive, Directors and supervisors will observe the following protocol if the employee must take an extended leave of absence:

5.7.1 EMAIL

The supervisor and the employee scheduled for an extended leave of absence will select the most qualified individual to act as a proxy agent. The supervisor will submit a support ticket consisting of the name of the employee going on extended leave, and the proxy. The support ticket will direct Technology Services and Support to set up an exchange rule to copy email from the employee account to the proxy account. In the event that the employee might receive sensitive personal correspondence during his or her leave, the employee will contact the agencies on and off campus to give these agencies a private email address with instructions to send sensitive email to the private account.

5.7.2 SELF-SERVICE:

The supervisor will contact Technology Services and Support and request that the proxy be given the elevated permissions of a department head in PowerCAMPUS. This permissions level will enable the proxy to effectively advise and interact with students using self-service.

5.7.3 MYUMO

The supervisor will contact the Director of Technology Support who will give the proxy the same permissions on all sites normally used by the employee going on leave. This enables the proxy to do any development or testing normally carried out by the employee going on leave.

5.7.4 TECHNOLOGY WORKERS

There are only two circumstances where technology workers are authorized to change the password of an active domain account. Technology workers can reset a password upon request of the owner of the account, or if given explicit instructions to do so by the President, Executive Vice President, Chief Financial Officer, or the Director of Technology. At no other time, nor under any other circumstances, are technology workers authorized to make changes to the password of an active domain account.

6. MISUSE OF TECHNOLOGY

Misuse or abuse of the University information technology systems, computers, networks, programs, and data is forbidden. Violations in the areas listed below will be considered academic misconduct, misdemeanor, or felony as appropriate to the situation and will be dealt with accordingly. All users are required to report immediately actual or suspected technology misuse to professors, supervisors, or members of University of Mount Olive's Technology Service and Support staff.

7. COMMON FORMS OF TECHNOLOGY MISUSE

7.1. PRIVACY VIOLATIONS

Privacy violations include but are not limited to:

- Attempted unauthorized access to computers inside or outside of the University of Mount Olive domain using the University's technology infrastructure
- Attempting to gain unauthorized access to another users account using subterfuge or social engineering techniques

7.2. VANDALISM

Vandalism includes but is not limited to:

- Alteration or attempted alteration of programs, digital data or other files, as well as resource or equipment
- Installation or attempted installation of software or the intentional spreading of viruses, worms, Trojans, etc
- Attempting to gain unauthorized access to another user's account using subterfuge or social engineering techniques
- Damaging or attempting to damage any component of University of Mount Olive technology infrastructure

7.3 SOFTWARE COPYRIGHT / INTELLECTUAL PROPERTY INFRINGEMENTS

Software copyright / intellectual property infringements include but are not limited to:

- Copying, transmitting, or disclosing data, software or documentation without proper authorization
- Receiving copyrighted intellectual property from a third party who is not authorized to distribute the property
- Using your status as a University of Mount Olive faculty, staff, adjunct, or student to purchase software and giving that software to unauthorized third parties

7.4 HARASSMENT / CYBER STALKING

Harassment / Cyber Stalking infringements include but are not limited to:

- Sending abusive or obscene messages to Mount Olive Community members using any technology or sending the same using University of Mount Olive technology to University of Mount Olive community members
- Using multiple online personas to harass, stalk, or otherwise monitor other users from within the University of Mount Olive domain, using any aspect of its technology infrastructure.

7.5 OTHER FORMS OF TECHNOLOGY MISUSE

Other forms of Technology misuse include but are not limited to:

- Intentionally denying or interfering with a University of Mount Olive Technology service
- Using Technology services to impersonate another user
- Sending mass emails from the University to outside sources without proper authorization
- Reading or modifying files without proper authorization
- Sending chain letters using University of Mount Olive technology
- Storing personal pictures, audio, or video on the University's computers. If Technology Services and Support discover these files during audit, they will contact the owner directly and ask him or her to remove the file(s). The Owner will have 24 hours to comply with the request. Technology Services and Support will document the date and time the infraction was discovered, the date and time the employee or student was contacted, and the date and time the employee or student complied with the request to remove these files.
- Disclosing confidential or otherwise privileged University information or data without permission

- Disclosing a password for any service to any user for any reason. End users do not have authority to disclose a domain or service password to any other user for any reason.

8. SANCTIONS FOR TECHNOLOGY MISUSE

Violations of this policy will be treated as academic or employee misconduct, misdemeanor, or felony as appropriate. For non-criminal matters, penalties range from a warning to loss of the User's account to termination of employment or expulsion from the University. University of Mount Olive executive administrators have discretion to modify the sanctions described below depending on the severity of the infraction.

Technology Services and Support will deny access to the campus Wi-Fi to any user identified by third parties for copywriter infringements using P2P technology until the matter can be investigated and adjudicated. For less serious infringements, a warning will be issued after a User's first policy violation, and the User will be asked to sign a copy of this policy statement to document that he/she understands and is willing to comply with these policies. A second violation will result, at a minimum, in the suspension of the User's account for one week. A third violation will result, at a minimum, in the suspension of the User's account for three months. A fourth violation will result in the permanent loss of privileges.

Misdemeanor or felony violation charges will be prosecuted to the fullest extent of the law and may result in the immediate and permanent loss of privileges. Disciplinary proceedings may also be initiated against violators. Violators of federal and state statutes may expect legal sanctions from the appropriate authorities.

A student User has the right to a fair hearing by the Judiciary Committee concerning the policy violation and the disciplinary action recommended. Appeals of disciplinary actions should follow the procedures set forth in the Student Handbook.

9. INFORMATION TECHNOLOGY SOFTWARE AND EQUIPMENT ALLOCATION AND PURCHASE

9.1. ALLOCATIONS AND OWNERSHIP

9.1.1. PRIMARY COMPUTERS:

The University will provide to each employee, upon request, a primary computer capable of running all supported applications, including those for word processing, spreadsheet, database, electronic mail, Internet access and library catalogue access. The exact configuration of primary computers will evolve along with the evolution of technology. Each machine will come bundled with a basic application suite and electronic mail package and Internet browser. Any costs above the cost of the standard package are to be paid for by departmental funds, with approval from the area Vice President and the Director of Technology Support. Maintenance and repairs will be provided at no cost to employees. Replacement will usually occur on a 3-4 year cycle or as the University's budget permits.

9.1.2. INSTRUCTIONAL SUPPORT EQUIPMENT:

The University will endeavor to provide, or assist academic and outreach units in obtaining computers for instructional purposes, courseware development, and laboratory automation, through start-up funds, external grants, and the annual Information Technology equipment request process. Replacement cycles for computers in this category will be determined on a case-by-case basis. Maintenance and repairs will be provided at no cost to departments.

9.1.3. PRIVATELY-OWNED COMPUTERS AND INFORMATION TECHNOLOGY EQUIPMENT:

Employees may purchase computers through University of Mount Olive or may use computers purchased elsewhere. The University will not provide maintenance and repair for privately owned computers. The Director of Technology Support must approve computers purchased outside of University of Mount Olive before being connected to the University-wide network.

9.2. MAINTENANCE AND SUPPORT

The Department of Technology Services and Support provides support for computers that it purchases for UMO use in all labs, classrooms, and offices. Such support includes hardware maintenance, repair, and network services, operating system upgrades, applications software consulting, and documentation. The Department of Technology Services and Support provides help and troubleshooting services for all traditional students irrespective of where the computer was purchased depending on Technology Support workload. The Department of Technology Services and Support does not provide support for privately owned computers for nontraditional students, faculty, staff, or adjuncts.

9.3 REALLOCATION OF EQUIPMENT

All computers and IT equipment considered the property of University of Mount Olive are under the management of the Department of Technology Services and Support. Computers that are allocated to individual employees cannot be redeployed or modified without prior approval from the Director of Technology Support. Computers and other information technology equipment, which were used by departing employees, are reallocated according to the decision made by the divisional head and the Director of Technology Support. This equipment does not necessarily remain in the same department or division.

9.4 NEW / REPLACEMENT COMPUTER REQUESTS

Requests are routed from individual employees in the fall of the current academic year for new or replacement computers to be purchased in the following school year. These requests are organized and routed to the appropriate Vice President with suggested priorities. Requests are evaluated by the area Vice President and the Director of Technology, and approved, denied, or deferred according to justification and funds available.

9.5 PURCHASING NEW TECHNOLOGY

It is the goal of the Department of Technology Services and Support to ensure that it can support all of the technology available to the University community at a reasonable cost. Generally, all purchase requests should be documented in Strategic Planning Online (SPOL) before the upcoming fiscal year so that they may be budgeted, their purchase recorded and tracked in the SPOL software. Requests for unbudgeted assets must pass though the Director of Technology, Executive Vice President, and Chief Financial Officer of University of Mount Olive for approval.

9.6 SOFTWARE INSTALLATION / WORKSTATION CONFIGURATION

All requests for special workstation configuration or software installation must be made to the Director of Technology Support no later than 45 days before the start of a new semester. The Department of Technology Services and Support strongly recommends that these requests be made by the appropriate academic officer before the faculty leave for winter or summer break to give the department ample time make the appropriate adjustments prior the arrival of students.

10. STAFF & FACULTY TRANSITIONS

All email or data not directly related to student learning (i.e. some class content, emails to students, or work completed by students) is the property of the University of Mount Olive. Consequently, when an employee leaves or accepts a new position, the University must ensure that the managers of the former employee, (or senior administrators), have access to this data in a completely open and transparent

fashion to ensure a smooth transition. Barring exceptional circumstances, the following protocol will be used to handle employee transitions:

10.1. STAFF MEMBER TRANSITIONS

The Human Resource director, or designee, will submit a Technology Services and Support ticket as part of initiating out-processing. This will result in immediate suspension of all access rights to Technology Systems at the college (unless a timeframe is specified, such as 30 days). The staff member's Director or Senior Administrator will be expected to retain:

- All electronic documents that need to be retained (either on the department's shared drive, or in the Director's personal drive depending on the necessary level of security). Unless otherwise notified, Technology Services and Support will delete the user's home drive 30 days after the account has been disabled.
- Make a backup of any e-mails that need to be retained (in the form of an Outlook .PST archive) WITHIN THE 30 DAY OUT-PROCESSING WINDOW. The Technology Services and Support department will also set up e-mail forwarding from the old account to the Director's account for a 30-day period if requested.
- Directors or Executive Administrators have discretion to delegate these responsibilities to subordinates if they coordinate this request through HR.

10.2. FACULTY MEMBER TRANSITIONS

The Human Resource director, or designee, will submit a Technology Services and Support ticket as part of initiating out-processing. This will result in immediate suspension of all access rights to IT systems at the college (unless a timeframe is specified, such as 30 days). The staff member's Director or Senior Administrator will be expected to retain:

- All electronic documents that need to be retained (either on the school's shared drive, or in the Director's personal drive depending on the necessary level of security) Unless otherwise notified, Technology Services and Support will delete the user's home drive 30 days after the account has been disabled.
- Make a backup of any e-mails that need to be retained (in the form of an Outlook .PST archive) WITHIN THE 30 DAY OUT-PROCESSING WINDOW. The Technology Services and Support department will also set up e-mail forwarding from the old account to the Director's account for a period of 30 days.
- Directors or Executive Administrators have discretion to delegate these responsibilities to subordinates if they coordinate this request through HR.

In general, phone extensions and direct inward dialing (DID) numbers are tied to organizational positions. When an UMO employee transitions to another position, Technology Services and Support will wait for the transitioning employee to initiate contact via email, phone call, or support ticket to secure a date and time to complete the DID and extension transition. Any special considerations, requests, or transition instructions that fall outside of the basic procedure described above will require the transitioning employee to file a support ticket.

To ensure complete transparency, Technology Services and Support will only process requests related to employee transitions from Human Resources, The President, The Executive Vice President, or The Vice President for Finance and Administration.

11. STUDENT TRANSITIONS

Students who leave the institution, (through graduation or other means), will have 180 days from the last class recorded in the PowerCAMPUS database to forward any email they wish to keep to a personal email account. Student accounts are automatically deleted on the 181st day after the last class recorded in PowerCAMPUS transpires. If password expiration becomes an issue for the former student, the student can contact Technology Services and Support for password reset assistance.

12. WEB PRESENCE

University of Mount Olive has two official web personas: http://www.umo.edu (website) and https://MyUMO.moc.edu (portal). While both websites are maintained by University of Mount Olive, Students, Staff and Faculty will conduct most business through the portal. Portal has very tight integration with the PowerCAMPUS student information database, and targets content based on one's role at University of Mount Olive (i.e. Student, Adjunct, Staff, or Faculty).

13. CLOUD STORAGE

Cloud storage is a framework for storing data in logical pools that are maintained off site across one or more physical host machines by a hosting company. Some well-known examples of cloud storage are Dropbox, OneDrive, Google Drive, and Box. Leveraging cloud storage makes good business sense in some use cases, and in others, it may or may not. For example, The University of Mount Olive encourages students to use cloud-based storage provided by Google because the university subscribes to Google Applications for Higher Education. Consequently, students get 10 gigabytes of storage free and the storage is ubiquitous. Understandably, Faculty and staff might want to leverage this storage flexibility on the business side of our network. Because the nature of cloud storage presents a risk to data on the business side of the network, and because any data stored on cloud servers belongs to the University, the University's System Administrator must have administrative access to any enterprise cloud storage application to ensure it is properly configured. Because the unique properties of cloud storage present data audit and network security challenges, requests for cloud storage will not be granted on a case by case basis, but rather, on a School / Unit level. Therefore, Faculty or Staff members that wish to use cloud storage will need to approach their respective school Dean or Vice President. The school Dean or Vice President can then submit a support ticket so that the Director of Technology and System Administrator can work on deploying and maintaining the solution.

A cloud application is a software application that exists off site, hosted by a third party. Typical examples of cloud applications are Google Apps, Office 365, Slate, and in some cases, Moodle. The University of Mount Olive Technology Services and Support Department endorses the use of cloud services, particularly Google Apps, to which UMO subscribes. Any cloud application that will significantly affect student learning or the execution of employee work tasks must be presented to Department Vice Presidents or School Deans and vetted by the University's Key stakeholders.

14. VPN ACCESS

Virtual Private Network (VPN) technology provides the means for users to access domain computing resources from outside the domain. VPNs also provide an additional attack vector that can be exploited by hijacking an unsecured endpoint. In order to minimize this attack vector, users requesting VPN must meet one or more of the following criteria:

- Be a member of Technology Services and Support
- Be a member of the Executive Council
- Have a mission critical need to access network resources more than 20 hours a week from off campus

Users will request access to the VPN in writing to their area Vice President. That request will be forwarded to Executive Vice President who will approve or deny the request. Finally, the university will provide the user with the necessary computer hardware (i.e. a computer and VPN) to securely connect to the campus network.

CONTACTS

Department of Technology Services and Support

APPROVED BY

Director of Technology

Executive Council

APPENDICES (INCLUDING ANY FORMS/INSTRUCTIONS)

None

HISTORY/REVISION DATES

Original adoption date(s): December 1999

Last Amended date: February 2019; VPN section (14) added

End Date for Policy (if applicable):

RELATED COMPLIANCE STANDARDS/EXTERNAL POLICY DOCUMENTS:

FR 4.8.1

FR 4.8.2