Acceptable Use Policies for Information Technology at the University of Mary

Purpose

This policy governs the use of information technology systems and electronic resources at the University of Mary (UMary).

The Acceptable Use Policies for Information Technology at the University of Mary promotes the efficient, secure, ethical, and lawful use of the university's information technology resources. The university's computing systems, networks, and associated facilities are intended to support its mission and to enhance the educational environment. Any use of these resources deemed inconsistent with the mission and purpose of the university will be considered a violation of this policy.

Policy Statement

This policy shall be applicable to all students, staff, faculty and contractors/vendors (defined hereafter as 'users') who have access to or who are responsible for any university system account at any university facility. This policy also applies to anyone who has access to the university network, who stores electronically any non-public information elsewhere, or who use a university-owned desktop, laptop or tablet computer. By using the university's information technology resources, all users agree to the rules, regulations, and guidelines contained in this Acceptable Use Policy.

Information technology systems and electronic resources are managed by the Office of Information Technology (OIT), and are provided to the members of the university community with the understanding that they will use them with mutual respect, cooperation and collaboration, and in compliance with all applicable policies, laws and regulations.

Information technology resources are finite, but their usage is growing and expanding; the resources must be shared generally and as with any interconnection of electronic resources, one individual can have a dramatic effect on others within the network. Therefore, the use of the network and electronic resources is a revocable privilege.

All constituents will benefit if all users of the electronic systems avoid any activities that cause problems for other users. The university reserves the rights to monitor, limit, and restrict electronic messages, network/systems traffic, and the public or private information stored on computers owned, maintained, or managed by the university. For security purposes, the university reserves the right to update the operating systems and any software installed on university-owned computes and IT systems with or without notice. Anyone who uses computers not owned, maintained, or managed by the university that abuse campus services may be denied access to campus resources. Email/voice mail, web pages, and digital content are subject to archiving, monitoring, or review, and/or disclosure by those other than the intended recipient.

Technology Systems and Electronic Resources

The university requires access to its information technology systems and electronic resources (hereinafter "Systems") to be authorized and pre-approved, and that users understand that laws currently exist that prohibit the following:

1. Electronic libeling or defamation
2. Sending/posting/broadcasting messages that incite hate or violence
3. Transmitting repeated unwanted personal advances
4. Falsifying information or impersonation
5. Unauthorized use of, providing, or copying of protected intellectual or copyrighted property

University Network

The university network is a private network separate and distinct from the public internet. Therefore, access to and use of this network must comply with all university policies, rules and regulations, and with all local, state, and federal laws. Examples of prohibited activities outside of prescribed course or business-related activities include but are not limited to:

1. Posting or transmission of confidential information
2. Use of offensive or discriminatory language
3. Transmission or display of graphic images, sounds or text that is sexual or offensive in nature
4. Unauthorized use of other users' passwords or accounts
5. Use of the Systems for personal profit or gain
6. Use of the Systems to harass, threaten, or otherwise invade the privacy of others
7. The installation or use of any servers, routers, switches, or wireless access points on the network not expressly approved by the Office of Information Technology
8. Deliberate attempts to cause breaches of the network, servers, telecommunications systems or security or to examine network traffic
9. Initiation of activities which unduly consume computing or network resources
10. Use of applications, for example P2P, to receive and/or distribute copyrighted materials, such as movies, music, and video
11. Tampering with computer files, software, or knowingly introducing a virus or malicious code to the university systems
12. Unauthorized changes to university web pages
13. Playing games in computer labs for entertainment
14. Excessive use of network bandwidth, storage, and any computer resources for purposes unrelated to University activities

Virtual Private Network (VPN)

The university's remote access Virtual Private Network (VPN) service allows university computers to connect to the University of Mary data network from off-campus, thereby granting those computers the same access, rights, and privileges as computers attached to the campus network directly. Users and machines connected to the VPN must have a valid business need to connect to the VPN, and abide by all information technology policies of the university. It is the responsibility of supervisors and department heads to determine under what circumstances it is appropriate for an employee to use the VPN to conduct university business.

1. Only VPN clients provided by OIT may be used to connect to the VPN.
2. It is the responsibility of all VPN users to keep secure all files, keys, and passwords required to connect to the VPN.

3. It is the responsibility of users with VPN privileges to ensure that unauthorized users are not allowed access to UMary's internal networks.
4. Personally-owned computers will not be allowed access to the VPN.

Provisions for Private Computers Connected to the University Network

The following applies to anyone connecting a private computer to the University network via the university housing network (ResNet), a wireless LAN connection, a regular network connection in an office, or any other network connection. The owner of the computer is responsible for the behavior of all users on the computer, and all network traffic to and from the computer, whether or not the owner is aware of the traffic generated. A private computer connected to the network may not be used to provide network access for anyone who is not authorized to use the university systems. The private computer may not be used as a router or bridge between the University network and external networks, such as those of an Internet Service Provider (ISP). Should OIT staff have any reason to believe that a private computer connected to the university network is using the resources inappropriately, network traffic to and from that computer will be monitored. If justified, the system will be disconnected from the network, and action will be taken with the appropriate authorities.

Any residential student with an authorized network account may use the in-room ResNet connection for scholarly purposes, for official university business, and for personal use, so long as the usage (1) does not violate any law or regulation; (2) does not involve extraordinarily high utilization of university resources or substantially interfere with the performance of the University network; (3) does not result in commercial gain or profit; and (4) is not in violation of any part of this policy.

Users are responsible for the security and integrity of their systems. In cases where a computer is compromised, the user shall either shut down the system or remove it from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading. If users suspect electronic intrusion or hacking of a personal computer system and would like assistance, contact OIT immediately.

Personal servers and network equipment will never be connected to the University network without prior authorization from OIT.

Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts and system integrity. A poorly chosen password can result in the compromise of the university's entire network.

A password authenticates the holder as an authorized user of the university's computer system that uses the institution's Active Directory for authentication, authorization and auditing, and must be protected from disclosure to others. Each user is responsible for the security of their password(s). It must not be shared with others and may only be used by the person for whom the password was created. Therefore, a password may not be posted in a place accessible by others and must not be inserted into email messages or other forms of electronic communication.

User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user. Generic, or shared

usernames/passwords are not authorized.

UMary employees shall not use any University of Mary Active Directory username and password as a means to access IT systems or online services not owned and/or managed by the University of Mary. Any exceptions to this rule must be approved by the requesting employee's respective Vice President or designee.

All UMary employees and students will register in the self-service password reset portal located at https://access.umary.edu.

Active Directory Password Construction

Users must select passwords that contain at least eight (8) alphanumeric characters and characters from three of the following four categories:

1. English uppercase characters (A through Z)
2. English lowercase characters (a through z)
3. Base 10 digits (0 through 9)
4. Non-alphanumeric characters (for example, !, $, #, %)

Active Directory Password Changes

All users who are staff/faculty or vendors/contractors and have user-level passwords (e.g., network, domain, email, desktop computer, etc.) must change their passwords every 60 days.

All users who are students and have user-level passwords (e.g., network, domain, email, desktop computer, etc.) must change their passwords every 180 days.

User-level passwords must be unique for 24 consecutive password changes, i.e., a password cannot be reused for 24 password changes.

All users will receive an automated pop-up notification, when logging in to a university computer, notifying them their password will expire in 14 days and, if necessary, that their password will expire in 1 day. If the current password is not changed before it expires, a password change will be prompted upon the user's first log in attempt after the expiration date and the user will not be able to log in to the university network until the password is changed.

Email

Users must understand that email is not absolutely private and should practice caution in sending messages that a user would not want everyone to see. OIT does not make a practice of monitoring email and other files; however, when there is a reasonable suspicion of wrongdoing or computer misconduct, the university reserves the right to examine material stored on or transmitted through its Systems.

Employees and students will not use their UMary email accounts to subscribe to unofficial online services, e.g., Netflix, Ancestry.com, MyFitnessPal, etc. Any unofficial online subscriptions that use a UMary email account must be approved by the respective Vice President.

Equipment Usage

While computer equipment and access to the Systems is provided for work and education purposes, incidental personal use is permitted as long as it is not inconsistent with this Policy and it doesn't interfere with employment and education responsibilities.

Eating and drinking is not permitted in the immediate area of any computer in open labs and classrooms.

Basic IT Systems Access Requirements

The University of Mary's basic IT systems access requirements include, but are not limited to:

1. Identify system users, processes acting on behalf of authorized users, and devices.
2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
3. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
4. Limit system access to the types of transactions and functions that authorized users are permitted to execute.
5. Employ the principle of least privilege, including for specific security functions and privileged accounts.
6. Use non-privileged accounts or roles when accessing non-security functions.
7. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
8. Protect and monitor the physical facility and support infrastructure for organizational systems.

Security Training (Employees)

Employees will complete annual Cyber Security Training including, at a minimum, the following courses:

1. Password Security
2. Email and Messaging Safety
3. Browser Security Basics
4. Cybersecurity
5. Protection Against Malware

Employee training will be completed by October 31st. New hires will complete training within one month of hire. Employees who do not complete training will have access to all IT systems disabled until completion.

Security Training (Students)

Students will complete annual Cyber Security Training including, at a minimum, the following courses:

1. Password Security Basics for Students

2. Email and Messaging Safety for Students
3. Cybersecurity Overview for Students

Student training will be completed by October 31st. Students who do not complete training will be placed on hold (preventing registration) until completion, and communications to be sent to advisors by the Registrar.

Violation, Remediation, and Intervention

Any suspicion of a password being compromised, on a system that uses the school's Active Directory for authentication, authorization, and auditing, must be promptly reported to OIT. Active Directory accounts suspected of being compromised or misused will be disabled by OIT. OIT will disable Active Directory accounts promptly at notice of termination by the human resources department or the employee's department supervisor. The university may also impose restrictions pertaining to computer use, including a loss of computing privileges on a temporary or permanent basis, a decrease of disk quota, and the removal of files in the System's temporary or scratch area.

In addition to liability and penalties that may be imposed under federal, state, or local laws, users of the Systems who fail to fulfill their responsibilities and engage in prohibited conduct may be subject to disciplinary action. The university may restrict or suspend user privileges while the alleged violation(s) are being investigated and disciplinary action pursued. Disciplinary action shall be taken by the appropriate officer relative to student, faculty, staff, and/or affiliate violations. A violation may also result in a referral to law enforcement authorities.

In accordance with the university's policies and state and federal laws, OIT may monitor the university network for activity that violates this Acceptable Use Policy.

Disclaimers

The president of the university has the discretion to suspend or rescind all or any part of this policy or related procedure(s). The president shall notify appropriate personnel of the suspension or rescission.

The university makes no warranties of any kind, either express or implied, for the Internet services it provides. The university will not be responsible for any damages suffered by users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

The university is not responsible for the accuracy or quality of information obtained through its internet services, including e-mail. Users assume responsibility for any damages suffered as a result of information obtained through these sources.

The user agrees to indemnify and hold harmless the university, the board of trustees, and university employees and contractors from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the University's hardware, software, and network facilities. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.

Approved

December 2019 by the President of the University of Mary