* - indicates a required field.

* **POLICY NAME:**	**Network and Computer Use Policy**
* **POLICY TYPE:**	Presidential Policy - University Administrative Policy
POLICY #:	E.4.4.
***STATUS:**	Active
***CONTACT OFFICE:**	Information Technologies
***OVERSIGHT EXECUTIVE:**	CIO, Chief Information Officer
***APPLIES TO:**	All System Users
***PURPOSE:**	The UMW computer network consists of local and wide-area networks, many shared enterprise and operational systems and services, individual desktop computers, and other computing devices. Various systems administrators work to ensure that privileges on these systems are properly maintained for all University users. Users of UMW systems have certain responsibilities and are subject to certain requirements and limitations. This policy outlines the responsibilities, requirements, limitations of the UMW computer systems and network users and the consequences of non-compliance with this policy.
DEFINITIONS:	APA, Auditor of Public Accounts CIO, Chief Information Officer ISO, Information Security Officer LAN, Local Area Network
***POLICY STATEMENT:**	Users of information technology resources at the University of Mary Washington must use them responsibly and within limitations. Users who fail to meet their responsibilities or who fail to operate within the limitations may have their network privileges suspended or revoked and may be subject to other disciplinary actions. Using University-owned computers, networks, or other information technology resources constitutes acknowledgment that the user understands and commits to compliance with the University's Network and Computer Use Policy and related policies and procedures. **PRIORITIES OF THE NETWORK** The UMW computer network and other information technology resources should be used and will be maintained and administered, in accordance with the following priorities: Highest and Primary: To support the education, research, and administrative purposes of the University of Mary Washington.

Medium and Secondary: To support other uses indirectly related to the University of Mary ' 'Washington's purposes with education or research benefits, including personal communications.

DISCLAIMER

The University of Mary Washington will investigate credible allegations of violations of the rules set forth below and will impose appropriate sanctions. However, the University assumes no responsibility for user conduct. Investigations of violations will follow the IT Security Incident Response Plan.

Users should be aware that there are many services on the Internet that they might find offensive or that involve risks. Users must accept responsibility for their own navigation of the Internet.

PRIVACY

UMW computer networks, systems, and data are owned by the University of Mary Washington, the Commonwealth of Virginia agency.

All users should be aware that ' 'UMW's electronic communications, systems, and files are monitored for anomalous behavior or content to detect possible compromises of systems and data security.

All users should be aware that during the course of the ordinary management of electronic communications, systems, and files, technical staff may inadvertently be exposed to the content of user files.

All users should be aware that electronic communications and files (e.g., email, spreadsheets) may be public records and subject to provisions of ' 'Virginia's Freedom of Information statutes.

In specific circumstances, the targeted examination of electronic communications and files may be conducted by authorized technical staff under the direction of the UMW senior management.

SAFETY

While unwanted or unsolicited contact cannot be controlled on the network, network users who receive threatening communications in violation of this policy or state or federal law should bring them to the attention of the Department of Information Technologies and/or the University Police.

INTELLECTUAL FREEDOM

The network provides an open forum for the expression of ideas, including viewpoints that are strange, unorthodox, and unpopular. Opinions expressed there must be presented in a manner that is free of obscenity (as defined by Code of Virginia, Section 18.2-372), forgery, and other illegal forms of expression, which are not acceptable uses of the ' 'University's network and are in violation of University policy. In addition, expressions of opinion may not be represented as the views of the University of Mary Washington, and individual users are responsible and accountable for any material posted and transmitted on the network in violation of this or other University policies or state or federal law.

USER RESPONSIBILITIES

Current employees (faculty and staff) and students and employees who have retired from the University's service can have computing accounts. In addition, some other parties, such as scholarly partners of faculty and contractors employed at the University, may be granted computing accounts for limited terms with appropriate sponsorship. To enjoy computer use and network access privileges, each user of University information technologies is expected to meet the responsibilities and limitations listed below. If a user is found to have knowingly violated these responsibilities of, their network access may be suspended or terminated. Depending on the seriousness of the violation, the user may also be subject to other University disciplinary actions, and violations of federal or state laws will result in referral to the appropriate legal authorities.

The following list of responsibilities applies to the use of all university-owned computers and the 'University's networks; additional responsibilities may be associated with specific networks, information technology services, and computers at the University.

- User accounts must be configured and used according to the principle of least privilege, meaning users must only access the information and resources that are necessary to perform their job functions.
- User's accounts must be configured and used according to the concept of separation of duties, meaning more than one person is required to complete certain tasks. Requiring more than one individual to complete a task can prevent fraud and error.
- Users must operate within the appropriate federal or state laws and University policies and must not engage in any conduct that presents a risk to the operational integrity of the systems and their accessibility to other users.
- Users must abide by the terms of all software licensing agreements and copyright laws. Users must not make copies of or make available copyrighted material on the network unless permitted by a license.
- Users must not use the University's network resources to gain or attempt to gain unauthorized access to remote computers, networks, or systems.
- Users shall not engage in any activity that alters wired or wireless network connections, access points, topology, or physical wiring of University-owned resources.
- The use of University computer resources and networks is for legitimate academic or administrative purposes.
- Users may not use University-owned computers or networks to access, produce, or distribute pornography in violation of the law.
- Users will not divulge confidential or highly sensitive data to which they have access concerning faculty, staff, or students without explicit authorization.
- Any network traffic exiting the University is subject not only to provisions of this policy but also to the acceptable use policies of

	any network through which or into which it flows.
	• Users should notify the Division of Information Technologies IT Help Desk (654-2255 or it-abuse@umw.edu about violations of computer laws and policies, as well as about potential vulnerabilities in the security of its computer systems and networks.
	• Users are to respect the rights of other users, including their rights outlined in other University policies for students, faculty, and staff; these rights include but are not limited to privacy, freedom from harassment, and freedom of expression.
	• Users may not place on any University-owned computer system any type of information or software that:
	  ○ Infringes upon the rights of another person.
	  ○ Grants, or attempts to obtain, unauthorized access to another computer account or system.
	• Users may not misrepresent themselves or their data on the network.
	• Users are responsible for the use of their accounts. No user may give anyone else access to their account or use a UMW computer account assigned to another user. A user must not attempt to obtain a password for another ' 'user's computer account.
	• Users are responsible for the security of their passwords and for regularly changing passwords according to good practice and the rules of the system in which the password is used. Users are responsible for making sure no one else knows their passwords. A user who suspects someone knows their password should change the password immediately (or contact Division of Information Technologies (654-2255) if they needs assistance in changing the password).
	• Users of personal computers are responsible for protecting their work by making regular backup copies of their work files and storing the copies in a safe location. They should set the frequency of backup based on their ability to recreate information added since the last backup.
	• Users must not attempt to monitor other 'users' data communications, nor read, copy, change or delete other 'users' files or software without permission of the owner(s).
	• Users must not attempt to circumvent data protection schemes and computer and network protections or exploit security loopholes.
	• Users must not deliberately perform acts that are wasteful of computing or network resources or that unfairly monopolize resources to the exclusion of others.
	• Users must not deliberately perform acts that will impair the operation of computing equipment, peripherals, other devices, or networks. This includes, but is not limited to, tampering with components of a LAN or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
	• Users must not run or install on any of the computer systems of the University or give to another user a program that could result in the eventual damage to a file or computer system and/or the

reproduction of itself. This includes, but is not limited to, the classes of programs known as computer malware, viruses, Trojan horses, and worms.
- Users may not use the ' 'University's computer systems or networks for solicitation of funds or for commercial purposes. This includes solicitations for charitable or community organizations.
- Users may not use the ' 'University's networks to distribute chain letters.
- Users must not illegally download or distribute, including via peer-to-peer file sharing, copyrighted material.

This policy and related material supplement the existing policies in the Student Handbooks and the UMW Employee Handbook for Administrative/Professional Faculty, Classified, and Wage Employees. These cover such acts as theft of computer services (including copyrighted computer programs), theft or mutilation of UMW property such as computer equipment, and the unacknowledged or unauthorized appropriation of ' 'another's computer program, or the results of that program, in whole or in part, for a computer-related exercise or assignment. Ultimately, any and all network conduct or misconduct is subject to the same policies that govern conduct in other University venues, and it is regulated and dealt with as described in the handbooks cited above.

VIOLATIONS
Violations or suspected violations of the policies and principles enumerated above should be reported promptly to the Division of Information Technologies at 654-2255 or it-abuse@umw.edu or to the appropriate University department.

SANCTIONS
Responses for violation of this policy may include, but are not necessarily limited to, the following:

- Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
- Loss of computer and/or network privileges: limitation or removal of computer and/or network privileges, either permanently or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repair or replacement of computer-related material, equipment, hardware, software, data, and/or facilities. In addition, such reimbursement shall include, but not necessarily be limited to, the cost of additional time spent by University employees due to the violation.
- Termination of employment
- Violators may be subject to criminal or civil penalties as they apply.

The University considers any violation to be a serious offense in its efforts to

	preserve the privacy, data, and services of individuals and the University. While monitoring or investigating adherence to this policy and/or legal violations, University officials reserve the right to access, examine, intercept, monitor, and copy any user's files, network transmissions, and/or online sessions. The University may choose to suspend a user's access to its resources in connection with an investigation of (but not limited to) any of the following: • Violations or suspected violations of security and/or policies • Activities that may be contributing to poor computer performance • Computer malfunctions. The University's Office of Human Resources (and appropriate UMW or external law enforcement agencies) may be notified of the violation and provided with information and materials relating to the investigation and/or violation. In connection with investigations, files, data, or communications may be shared with the appropriate investigating officials. In general, the University will exercise discretion as far as is appropriate given the case.
PROCEDURES:	
* General Procedures for Implementation:	The Division of Information Technologies, working with the administrators of UMW computer systems and networks, has the responsibility to protect users' rights, enforce policies and procedures consistent with those rights, and publicize those policies and procedures to their users. The department has the authority to control or refuse access to any user who violates these policies or threatens the rights of other users, and department officials will make reasonable efforts to notify users affected by decisions they have made. Questions or concerns regarding the use of the ' 'University's network, its computers, or other information technology facilities or services should be addressed to the Division of Information Technologies, 540-654-2255, or helpdesk@umw.edu.
* Process for Developing, Approving, and Amending Procedures:	As a result of the required annual review, the CIO or designee will make appropriate changes to the policy and present them to the University President for approval. Additional amendments will be handled on a case-by-case basis at the discretion of the CIO.
* Publication and Communication:	The policy is on the UMW website and is covered in required annual security awareness training for all employees. Data Stewards and Data Security Contacts complete additional annual training. The policy is referenced in the Student Handbook.
* Monitoring, Review, and Reporting:	The policy is part of the Information Security Program and is audited annually by the APA. The ISO is responsible for promoting policy awareness and tracking compliance as part of the annual IT Security Awareness training.

*(How will **compliance** be monitored, reviewed and reported?)*	
RELATED INFORMATION:	
Policy Background:	
* Policy Category:	Information Technology
Category Cross Reference:	
Related Policies:	E.4.8. Monitoring of Employee Electronic Communications or Files
HISTORY:	
* Origination Date:	January 1, 2005
* Approved by:	Hall Cheshire, CIO
* Approval Date:	July 27, 2021
* Effective Date:	July 27, 2021
* Review Process: *(How will the effectiveness be reviewed? By whom? How often?)*	The effectiveness of this policy will be reviewed on an annual basis by the CIO or designee.
* Next Scheduled Review:	August 1, 2023

Revision History:	January 10, 2005 - Updated to reflect new policy formats, University name changes, and other reference updates, and inclusion of user requirement for backup of personal computers (originally in another University policy) August 21, 2006 - Updated to reflect the shift of responsibilities from Executive Vice President to Vice President for Strategy and Policy April 16, 2007- Updated to reflect the change in University-wide email processes February 22, 2008- Updated to reflect the change in responsible office for University-wide email communications and change in language about changing passwords June 18, 2010- Updated to remove references to the Vice President for Strategy and Policy and add new language on file sharing January 10, 2012 - Revised to add test on the review process and sanctions July 1, 2013 – Revised to add clarification to the Purpose statement August 26, 2016 – Reviewed, no changes August 28, 2017 – Reviewed by ISO, no changes July 25, 2018 – Revised by CIO, changes to the privacy section July 15, 2019 – Reviewed by CIO, no changes August 5, 2020 – Revised by ISO, minor changes July 27, 2021 – Revised by ISO, minor changes to privacy and user responsibilities June 17, 2022 – Reviewed by ISO, no changes