



UNIVERSITY OF MARYLAND
EASTERN SHORE

POLICY ON INFORMATION TECHNOLOGY ACCEPTABLE USE AND RESOURCE ACCESS

POLICY No. X-1.1

Authority: University President

Policy Section: Information Technology

Effective Date: October 9, 2023

Applicable Groups: Campus-wide

Responsible Office: Information
Technology

Policy Location:

www.umes.edu/generalcounsel

1. POLICY STATEMENT:

University of Maryland Eastern Shore strives to promote a culture of openness, trust, integrity, and an environment wherein freedom of expression and scholarly inquiry are encouraged and supported. The intention of the Acceptable Use Standards is not to impose restrictions that are contrary to these values, which are the core of our academic and administrative community. Some computing resources dedicated to specific roles, including administrative systems and teaching systems containing information protected under the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and other state, federal, and international law necessarily limit access in order to protect the privacy of UMES students, faculty, and staff.

Effective security is a team effort involving the participation and support of the entire University of Maryland Eastern Shore team, including its students, faculty, and staff. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. PURPOSE OF POLICY:

The standards set forth the responsible use of University of Maryland Eastern Shore information technology resources. Individuals and groups using UMES resources both on and off campus are responsible for complying with the security standards, including securing passwords, identification numbers, and security codes and using them solely for their intended purposes. Individuals are solely responsible for their personal use of IT resources, including computer accounts and other resources under their control. These standards are in place to protect the UMES community

and to ensure the smooth, secure operation of UMES's information technology systems.

3. **SCOPE:**

The standards apply to all information technology resources, including but not limited to computer systems, data and databases, computer labs, smart devices including cell phones and tablets, e-mail boxes, wired and wireless data and voice networks, applications, software, files, and portable media. UMES provides the resources to support the academic, research, administrative, and instructional objectives of the University. The use of these resources is limited to University students, faculty, staff and other authorized users to accomplish tasks appropriate to the status of the individual.

4. **GENERAL STANDARDS FOR ACCEPTABLE AND RESPONSIBLE USE:**

These guidelines set forth standards for responsible and acceptable use of University computing resources. They supplement existing University policies, agreements, and state and federal laws and regulations. Computing resources include host computer systems, University-sponsored computers and workstations, communications networks, access points, software, and files.

Violation of these standards constitutes unacceptable use of computing resources and may violate other University policies and/or state and federal law. Suspected or known violations should be reported to the Information Security Manager immediately. Violations will be processed and adjudicated by the UMES Judicial System (for students), the UMES Grievance Committee (Faculty), The Office of Administrative Affairs (Staff) and/or law enforcement agencies. Violations may result in revocation of computing resource privileges, academic dishonesty, or Honor proceedings, as well as faculty, staff, or student disciplinary action, civil penalties, and/or criminal prosecution. The guidelines are not intended to be comprehensive, but to define and explain the intent of this policy. Situations not specifically covered by this policy will inevitably arise and should be judged and interpreted in the spirit of this policy.

5. **GENERAL PROHIBITED CONDUCT:**

- 5.1 Altering system hardware or software without authorization, including installation of unlicensed or unapproved software or hardware.
- 5.2 Installing, copying, distributing, or using software in violation of: copyright and/or software agreements; applicable state and federal laws or the

principles described in "Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community."

- 5.3. Non-UMES managed network devices (hubs, switches, access points, etc.) are not authorized to connect to the UMES network.
- 5.4. Avoiding or evading security measures, including by using 3rd party virtual private networks, firewalls, browser plugins, host file modifications or other means.
- 5.5. Disrupting or interfering with the delivery or administration of information technology assets, including network communications, e-mail, hardware, or software.
- 5.6. Attempting to access or accessing an account other than the account provided for your use.
- 5.7. Intercepting or reading electronic communications, including e-mail and chat messages not addressed or assigned to you.
- 5.8. Misrepresenting your identity in an e-mail, chat, or university owned social messaging platform.
- 5.9. Installing, copying distributing, or using digital content in violation of copyright and/or software agreements or applicable federal or state law. This includes the use of file sharing software including but not limited to BitTorrent, uTorrent, Sharefile or other services that allow the illegal download or use of copyrighted media.
- 5.10. Interfering with others' use of shared resources, including computers, lab space, or common technology areas.
- 5.11. Encrypting University data without express permission of the IT department.
- 5.12. Using University resources for commercial or profit-making purposes or to represent the positions or interests of groups unaffiliated or unassociated with the UMES community or the normal professional practices of students, faculty, and staff.
- 5.13. Ignoring or evading departmental or lab policies, procedures, and protocols.
- 5.14. Assisting unauthorized users' access to University IT resources.

- 5.15. Exposing sensitive or confidential information or disclosing information that you do not have the authority to disclose.
- 5.16. Using IT resources for illegal activities, including threats, harassment, copyright infringement, defamation, theft, identity theft, and unauthorized access.
- 5.17. Failing to use good judgement with respect to personal use of IT resources. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

6. SECURITY AND PROPRIETARY INFORMATION:

- 6.1 All mobile and computing devices that connect to the network must be capable of minimum 128-bit encryption for network traffic.
- 6.2 System and user level passwords must comply with University standards. Failing to protect passwords or allowing others access to resources using your account or an account you know the password for is prohibited.
- 6.3 All computing devices must be secured with password protected screen savers with an automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.
- 6.4 Users should assume that attachments or unsolicited message may contain or do contain malware and viruses and avoid opening, executing, or downloading such attachments.
- 6.5 Employees posting to forums, social media, Usenet groups, or other communications platforms that use an UMES e-mail address must include a disclaimer stating that their posting does not represent the views of University of Maryland Eastern Shore unless such posting is part of their normal business duties.

7. SYSTEM AND NETWORK ACCESS:

- 7.1 Accessing data, a server, or an account for any purpose other than conducting University of Maryland Eastern Shore business is prohibited.
- 7.2 Exporting software, technical information, encryption information, or information about the capabilities of information systems is prohibited.
- 7.3 Introduction of malicious programs, including viruses, worms, malware, adware, or similar programs is prohibited.
- 7.4. Port scanning, security scanning, and other types of network scanning is prohibited without the written permission of the information technology unit.
- 7.5. Disrupting network communication by using network sniffing, ping flood, packet spoofing, denial of service, forged routing information, e-mail spoofing, or otherwise misrepresenting network traffic is prohibited.
- 7.6. Providing information about, or lists of UMES students, faculty, or staff to outside parties unless it is part of your normal duties is prohibited.

8. E-MAIL AND ELECTRONIC COMMUNICATION:

- 8.1. Use of UMES resources to access and use the internet requires good judgement on the part of the user. Users must realize that they represent the University and must, when stating an affiliation to the University, include verbiage indicating that the opinions expressed are their own and not necessarily those of University of Maryland Eastern Shore.
- 8.2. Sending unsolicited e-mail messages, including "spam" or "junk mail" or other advertising material to individuals who did not request it is prohibited.
- 8.3. The unauthorized use or forging of e-mail headers is prohibited.
- 8.4. Any form of harassment, including via e-mail, voice mail, and chat services whether through language, frequency, or size of messages is prohibited.
- 8.5. Solicitation of e-mail for any e-mail address other than your own is prohibited.

8.6. Forwarding chain letters, Ponzi or Pyramid scheme messages, or messages not related to University business is prohibited.

8.7. Use of UMES e-mail addresses for any purpose other than University business is prohibited.

9. POLICY COMPLIANCE:

The Information Technology department will verify compliance with these standards through various methods, including but not limited to business reports, internal and external audits, audit tools, and security related hardware and software tools.

The Information Technology team routinely monitors inbound, outbound, and internal network traffic for the purposes of compliance and network maintenance. University of Maryland Eastern Shore reserves the right to audit systems and network traffic to ensure compliance with the standards.

10. PRIVACY:

The maintenance, operation, and security of computing resources require responsible University personnel to monitor and access the system. Users shouldn't have an expectation of privacy, though the University will attempt to preserve user privacy and identity to the best of its ability. Nevertheless, that privacy is subject to the Maryland Access to Public Records Act, other applicable state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations. All IT resources are the property of the institution, and as such, the University reserves the right to search and monitor users' accounts and usage of University IT resources, including e-mail and files.

URL and content filtering is in place for staff accounts that includes adult content, gambling, or similar sites. Attempting to avoid or evade these filters is a violation of this policy. Staff members who wish access to adult content, gambling, or similar sites can apply for an exemption by placing a ticket with the helpdesk that indicates the site or sites the user wishes to unblock and the reasoning behind the request. Requests are approved at the appropriate managerial level for the employee's department. The University necessarily prohibits access to certain websites that are known to contain malware or content that may compromise security, but in the spirit of academic freedom it does not otherwise filter content for faculty or adult students.

Users should be aware that the following conditions apply:

- 10.1 Electronic files and e-mail might be preserved as computer files on centrally administered disks or cloud hosted storage. Therefore, it is possible for people other than the user to see the messages.
- 10.2 E-Mails or files sent by one user become the possession of the receiver and can easily be redistributed by recipients. In this sense, the e-mail messages and files are not private, and all data that should not be preserved should be deleted.
- 10.3 University policy also allows system administrators to view any files, including email messages, in the course of troubleshooting system problems.
- 10.4 In the event of a personnel issue or investigation, IT staff may be required to provide access to University Counsel, Title IX Administrator, or other delegated individuals at the request of a cabinet officer.

11. RELATED POLICIES:


USM Policy X-1.00

APPROVED:



Anastasia Rodriguez (Date)
Vice President of Administration and Finance

10/9/2023



Matthew A. Taylor, Esq. (Date)
General Counsel

10/9/23



Dr. Heidi M. Anderson (Date)
President

10-9-2023