Policy 1207
Appropriate Use of Information Technology Resources

Date of Current Revision: December 2020
Responsible Office: Assistant Vice President for Information Technology and CIO

1. PURPOSE

The purpose of this policy is to provide direction to members of the university community regarding safe and responsible use of university technology resources and to outline the obligations they have as a whole and individually to abide by established standards of acceptable use.

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia § 23.1-1600; § 23.1-1301. The Board has delegated the authority to manage the university to the president.

STATE OR FEDERAL STATUTE AND/OR REGULATION

Consistent with the University's Memorandum of Understanding granting Level III delegation from the Commonwealth under the Virginia Restructured Higher Education Financial and Administrative Operations Act of 2005 and in keeping with the other university technology policies, JMU exercises independent authority for issuing policy and establishing requirements related to technology management for the institution.

3. DEFINITIONS

Harassment:
A form of discrimination consisting of unwelcome or offensive physical, verbal or written conduct that shows aversion or hostility toward a person on the basis of age, color, disability, gender identity, genetic information, national origin, parental status, political affiliation, race, religion, sex, sexual orientation, or veteran status in the following situations:

1. When submitting to or rejecting the conduct is made the basis for an evaluation, personnel action, or recommendation for a personnel action affecting an employee, or an evaluation, action or recommendation for an action affecting a student; or

2. When the conduct has the purpose or effect of unreasonably interfering with the performance of an employee or a student, and the conduct creates a hostile, intimidating, or offensive learning or working environment.

Harassment specifically includes instances of sexual violence of any type perpetrated against a member of the university community.

System Security Mechanism:
A procedure, program, or device used with a computer to implement or enforce access controls, auditing, authentication, confidentiality, authorization, policy settings, or other security measures.

University (JMU) Information Technology Resources:
These include, but are not limited to, equipment, software, systems, networks, data, and communication devices (stationary and mobile) owned, leased, or otherwise provided by JMU.

4. APPLICABILITY

This policy applies to all members of the university community who use the university's information technology (IT) resources. This includes, but is not limited to, students (applicants, current and graduates), faculty, staff, guests, and external individuals or organizations. The policy applies regardless of the methods of access, whether initiated from on or off campus and whether using university-owned, privately-owned, or third-party systems or networks.

5. POLICY

JMU provides a variety of public and non-public information technology resources to provide services, encourage free exchange of ideas and support information sharing. Access to these resources is a privilege governed by certain regulations and restrictions. These include university policies, procedures, and standards, as well as applicable local, state, and federal laws/regulations.

Authorized users are offered the most reliable and reasonably broad access to information technology resources possible. In return for these access privileges, the user agrees to behave ethically, appropriately, and responsibly in their use of the resources. This means that each person who accesses or uses university information technology resources accepts the responsibilities outlined here and in other university policies and standards. In addition, users will adhere to applicable local, state, and federal laws/regulations.

Under some circumstances, actions must be taken to preserve the security, integrity and/or availability of university information technology resources or to respond to legal inquiries. Therefore, at the discretion of university senior management, files, data, or communications may be reviewed as necessary with cause, and individuals are not entitled to any expectation of privacy. The university also reserves the right to suspend or discontinue access to university information technology resources as necessary.

6. PROCEDURES

Due to the openness of JMU's network, virtually all systems are connected internally and to external resources as well. Improper operation of such systems can result in compromise or operational disruption of the JMU network and related services and data. Thus, there are special requirements related specifically to network-connected devices. These requirements apply to all devices connected to or accessing the JMU network.

Though specific requirements/operating practices may vary somewhat with specific aspects of the environment, users are expected to follow best practices for effective and secure operations. For example, it is expected that available protections such as security configuration settings, anti-virus software, software/service updates, and account/account-level access controls are used whenever one is accessing JMU information technology resources.

More specific requirements for the use of JMU information technology resources are communicated through university information technology policies and standards and those otherwise related. Users are responsible to ask questions and assure their own understanding of these requirements

7. RESPONSIBILITIES

7.1 User Responsibilities:

As a user of JMU information technology resources, each user shall:

- use only those information technology resources for which they have authorization
- use information technology resources and data only for their intended purposes
- refuse to provide or share access to university information technology resources with those who are not authorized
- abide by applicable laws/regulations and university policies, including, but not limited to, those related to copyright and intellectual property
- respect the security (confidentiality, integrity, and availability) of information technology resources
- respect the privacy and personal rights of others including, but not limited to, the right to be free from intimidation or harassment
- use and operate information technology resources in a manner that respects established controls and minimizes the risk of adverse effects or unavailability to others
- accept responsibility for behavior, for any use of user credentials, and for the operation of any device(s) they own, use, or are assigned
- upon notification, comply with requests to discontinue activity or behavior that violates this or other applicable policies or regulations
- not use university information technology resources for personal/financial gain, political activities, or fraudulent, harassing, or illegal activities
- report any violation of security or appropriate use to abuse@jmu.edu or to the university's information security officer
- report suspected possible fraudulent transactions involving university information technology resources to Audit and Management Services (see Policy 1603 - Fraud, Waste and Abuse Reporting)

7.2 University employees:

Further, in using university information technology resources, employees shall:

- refrain from operating computer games using university information technology resources, other than for academic instruction

- comply with any statute or regulation applicable to university employees including, but not limited to, Commonwealth of Virginia DHRM Policy 1.75 (Use of Electronic Communication and Social Media) and Code of Virginia sections prohibiting employees from accessing sexually-explicit materials
- adhere to university policies and standards for procurement/development of technology systems/services and their operation, maintenance or modification

7.3 Other Responsibilities:

The university's assistant vice president (AVP) for information technology and CIO, information security officer, and other IT staff have responsibilities assigned by the university as part of their job responsibilities.

Because of their leadership positions and control over resources, AVPs, deans, and other academic/administrative unit heads, along with principal investigators (PIs) can play a critical role in the use and protection of JMU information resources. They are expected to influence appropriate use outcomes by:

- ensuring that security is given appropriate consideration, along with functionality, performance, ease-of-use, cost, and availability, in the planning and implementation of new projects and services
- making computer security a staffing, funding, and training priority. Additionally, PIs can specify the cost associated with security as a direct cost in grant proposals
- encouraging responsible attitudes and behaviors within the units they lead by communicating the importance of addressing security issues and by requiring all staff members to be accountable for the security of their network-connected devices
- acknowledging that administration of information technology resources takes specialized skills and helping ensure that qualified people and necessary resources are available; and enabling quick and effective response to violations of appropriate use or when a security breach occurs

7.4 All departments, offices and employees that generate, receive or maintain public records under the terms of this policy are also responsible for compliance with Policy 1109 - Records Management.

8. SANCTIONS

8.1 Regarding employees, sanctions will be commensurate with the severity and/or frequency of the offense, and may include termination of employment.

8.2 Regarding students, sanctions will be commensurate with the severity and/or frequency of the offense, and may include suspension or expulsion.

8.3 In addition, 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
- Finally, the violator may be subject to criminal or civil penalties as they apply

8.4 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. In the case an investigation is begun related to policy and/or legal violations, the university's officials reserve the right to access, examine, intercept, monitor, and copy the files, network transmissions, and/or on-line sessions of any user. The university may choose to suspend a user's access to its resources in connection with investigation of (but not limited to) any of the following:

- violations or suspected violations of security and/or policies
- activities which may be contributing to poor computer performance
- computer malfunctions

8.5 In connection with such investigations, users whose files, network transmissions, or computer sessions are affected are deemed to have acknowledged that they are not entitled to any expectation of privacy with regard to their files, data or communications, which may be shared with appropriate investigating officials. In general, the university will exercise discretion as far as is appropriate given the case.

8.6 The university's Office of Audit and Management Services (as well as appropriate JMU or external law enforcement agencies) may be notified of the violation and provided with information and materials relating to the investigation and/or violation.

9. EXCLUSIONS

None.

10. INTERPRETATION

Authority to interpret this policy rests with the president, and is generally delegated to the assistant vice president for information technology and CIO.

Previous Version: April 2016
Approved by the president: April 2002.