Policy 1201
Information Technology Resource Management

Date of Current Revision: March 2022
Responsible Officer: Assistant Vice President for Information Technology and CIO

1. PURPOSE

In conjunction with JMU Policy 1212 - Information Technology Infrastructure, Architecture and Ongoing Operations and Policy 1213 - Information Technology Project Management, and 1214-Information Security Program, this policy establishes general requirements and responsibilities associated with the management and use of computing and telecommunications resources and services at the university.

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.

3. DEFINITIONS

Access Control:
Access control is the ability to allow or deny use of a certain resource by a particular entity. Access control mechanisms are necessary for management of physical and/or digital resources**.**

Information Technology (IT):
Refers to the Office of Information Technology at the university.

Network:
A system of hardware and software that transmit and receive any combination of voice, video and/or data. Included are the network operating system, various client and server machines and software, the physical paths connecting them, and other supporting hardware such as bridges, routers and switches.

Shared System Resources:
Information technology systems managed by IT or elsewhere that house applications shared by university users for a specific purpose. These systems may be enterprise-level (e.g. HRMS, Canvas, email, etc.), systems operated more locally within the university or by third-party providers. In any case, they are to be identified, assessed and approved by IT as part of the university system inventory.

Workstations:
Generally synonymous with personal computers, desktop computers or laptops, but can refer to any kind of small computer such as a Windows PC or Macintosh.

4. APPLICABILITY

This policy applies to all data and information technology resources owned, operated or contracted by the university.

5. POLICY

The university provides a wide range of information technology resources, including: workstations, shared system resources; voice, data and video networks; electronic services; specialized facilities and data repositories. These and other technology-resources (including those made available through third-party providers) are available to enable scholarship, research, service and administrative support functions of the university. They are supplemented by an appropriate mix of consulting, training, maintenance and support services.

Misuse of the university's information technology resources is a serious offense. Misuses include, but are not limited to, improperly using university data, equipment, software or other resources; accessing university computers with stolen or illegitimate user identification; and compromising the security or performance of shared computer or communication systems. Specific requirements related to appropriate use are outlined in Policy 1207 - Appropriate Use of Technology Resources.

6. PROCEDURES

More detailed requirements, instructions and procedures for use of the university's information technology resources are specified in *JMU Computing Standards* established and maintained by IT.

All users of university information technology resources are required to adhere to these standards, as well as other university policies related to information technology.

7. RESPONSIBILITIES

7.1 General Responsibilities

Information Technology

IT has overall responsibility for ensuring that effective information technology resource management takes place within the university. Establishing and implementing plans, policies, and practices that guide, protect and direct the university's information resource investment and ensure the availability, and effective use of these resources by the university community are central to this effort.

To address specific academic needs, IT works cooperatively with the JMU Libraries and others in Academic Affairs. IT also seeks advice through a variety of standing and ad-hoc groups. Committees and advisory groups are convened to address specific issues or needs. Such groups are generally composed of key stakeholders/users of information technology who advise on

matters related to instructional, research and administrative applications of technology. They may also participate in major information technology policy decisions, provide input to long range plans, or make suggestions on service improvement.

Individual Responsibility

Individual vice presidents, deans, associate/assistant vice presidents, academic/administrative unit heads and faculty, staff and students provide input and share responsibility for effective information technology resource management. Their responsibilities include those directed by university policy or procedure and those that generally ensure a secure and effective technology environment for themselves and others.

7.2 Specific Responsibilities

7.2.1 Acquisition:
University departments must contact IT and complete a Technology Procurement Request **prior** to soliciting the acquisition, development or enhancement of technology systems. This requirement is applicable to all shared system resources (including cloud or other third-party applications systems or services and those to be deployed on campus as well). See Policy 1202 - Information Systems Implementation and Project Management.

IT will assist university departments in performing a business impact analysis to examine development or acquisition alternatives, selection and implementation requirements and life cycle planning. Specific considerations such as installation and configuration of hardware, software and services, security practices, telecommunication requirements and operational responsibilities will be discussed. IT will also assist in identifying and evaluating compatibility issues, compliance obligations and requirements for project documentation and implementation. While specific processes depend on the scope and complexity of the project, general requirements for initiation, classification and management of technology projects are outlined in Policy 1202 - Information Systems Implementation and Project Management. In addition, specific procedures are outlined in *JMU Computing Standards*.

Technology Procurement Requests for information technology resources associated with externally funded projects or university-sponsored programs shall be submitted by the appropriate department head, associate/assistant vice president, dean and vice president. IT will review these requests and costs for necessary computer/communication services may be assigned in accordance with university accounting regulations.

7.2.2 Security:
IT is responsible for establishing and maintaining the physical security of the central computing facilities (including shared file servers managed by IT), the university's communications network and data for which IT is the custodian. IT also has responsibility for data stewardship in other areas. These responsibilities are more fully detailed in Policy 1204 - Information Security and Policy 1205 – Data Stewardship.

Vice presidents, associate/assistant vice presidents, deans and academic/administrative unit heads through their staff are responsible for the availability, confidentiality and integrity of data and software stored on individual workstations, servers or shared system resources to the extent they have access and/or operational control. This responsibility includes ensuring backup of key software systems and data on individual workstations, file servers, or other shared system resources for which they share operating responsibility. They may also include system administration, account management and/or data stewardship responsibilities that have been specifically assigned in keeping with Policy 1205 – Data Stewardship.

7.2.3 Access Control:
The university provides access to its non-public computing resources for the exclusive use of students, faculty, staff and certain other constituents for the purposes of advancing educational pursuits and certain administrative support functions.

IT is responsible for instituting and monitoring appropriate access control measures for shared central computer systems, including centrally-managed administrative and academic computers, shared file servers and other systems for which it has system administration responsibilities.

With the written approval of IT and the appropriate associate/assistant vice president, dean, or academic/administrative unit head, access control responsibilities for private file server volumes may be delegated to individual workgroup managers.

Access to central computing systems is granted by the issuance of individual user credentials and usage restrictions as appropriate. In addition to these general access controls, compliance with procedures for granting access to particular software applications or data sets is also required. Data managers are assigned to approve access to certain data domains, databases and/or applications. These data managers are responsible for ensuring that requests for data/system use are in keeping with assigned responsibilities and university data access provisions. IT is responsible for implementing data access controls - as approved by the appropriate data manager(s) in keeping with the university Data Stewardship Policy (1205).

Individual users assume responsibility for the appropriate and ethical use of the systems and data to which they have access. See Policy 1204 - Information Security, Policy 1205 - Data Stewardship, and Policy 1207 - Appropriate Use of Information Technology Resources for more detail.

7.2.4 Systems Development and Maintenance:
IT provides systems analysis and programming services to support the university's administrative and academic purposes. These services include the design, programming, documentation, testing and enhancement of computer systems for a variety of service functions (e.g. financial accounting, student records administration, payroll processing) as requested by university departments. IT and the initiating department will review a cost/benefit analysis of requested enhancements to ensure appropriate utilization of university resources. IT also provides resource planning and implementation consulting for academic and research projects.

7.2.5 Systems Administration and Operations:
IT is responsible for providing environmental control and systems support for central software application systems and computing/communications components to meet the various administrative and academic needs of the university. Specific tasks include capacity and production planning, operational control, security monitoring and system administration for a variety of standard and ad-hoc production environments.

IT is responsible for providing direction to members of the university community regarding safe and responsible use of technology resources and the responsibilities users have for protecting and efficiently using such resources at JMU. The responsibilities are more fully detailed in Policy 1207 - Appropriate Use of Information Technology Resources and Policy 1204 - Information Security.

7.2.6 Telecommunications and Network Access:
Through its Telecommunications Department, IT delivers voice, data and video services by designing, installing and maintaining the campus network infrastructure, including both cabled and wireless components. IT Telecom also works to provide access to information, systems and services at other sites by providing inter-network connectivity, satellite transfer and other forms of voice/data/video access.

7.3 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

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

9. EXCLUSIONS

Exclusions may be approved by the assistant vice president for information technology and CIO to accommodate special needs or circumstances in support of the university's mission and that do not compromise the access or rights of other students, faculty and staff.

10. INTERPRETATION

The 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: November 2016
Approved by the President: April 2002