Policy 1204
Information Security

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

1. PURPOSE

This policy assigns responsibility for the security of university data and information systems. Components of security include confidentiality, availability and integrity.

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

Critical data
Data supporting critical functions (i.e., business processes identified by the vice presidents that significantly affect service levels to students, affect public safety, impact the budget, and/or are the result of governmental regulations). This data is so important to the university that its loss or unavailability is unacceptable.

Information Security Program
The set of managerial, operational and technical controls instituted to protect the integrity, availability and, if needed, confidentiality of information and the technology resources used to enter, store, process, and communicate electronic information.

Information Technology Resources
Specific items such as telecommunications devices, computer systems, media, and other equipment, goods, services and personnel related to the collection, storage or transport of electronic information.

Sensitive Data
Non-public data subject to legal requirements (e.g., Federal or State privacy laws) or other privacy or compliance considerations, which define and regulate its responsible use. The university's Policy 1205 - Data Stewardship defines two types of sensitive data: protected and highly confidential.

4. APPLICABILITY

This policy applies to all information collected and/or processed using university information technology resources.

5. POLICY

University data and information technology resources must be recognized as valuable and worthy of protection. Depending on the scope and nature of the information, constraints and special procedures for access and handling may be required.

One of the fundamental requirements and goals of university information processing, whether manual or automated, is to manage the information resource. This goal drives all others as the university works to protect and deny or disseminate access. The individual data elements and their association to the larger process must be protected and managed. Therefore, controls are necessary at the local office, the department or service unit, the network, and throughout the various computer systems and services used to collect, process, store and disseminate university data.

It is the policy of the university to maintain security of its data and information technology resources. The university will take appropriate steps to secure information technology resources and sensitive information through the development of an institution-wide information technology security program. All systems must include security safeguards that reflect the importance and sensitivity of the information processed on the system.

All users of university information technology resources are required to adhere to detailed requirements included in JMU Computing Standards, as well as other university policies related to information technology.

6. PROCEDURES

In keeping with the responsibilities outlined above, departments and offices shall develop, manage and review local operating policies and procedures to create the proper security posture for sensitive or critical data created and stored locally and on centrally managed computer systems. Integrity constraints, procedures that ensure correct processing of correct data, shall be written as local procedure. Such procedures shall be reviewed as required.

7. RESPONSIBILITIES

7.1 Vice presidents, deans, associate/assistant vice presidents and academic/administrative unit heads shall be responsible for identifying critical functions as specified in Policy 1206 – Contingency Management for Technology-based Information Systems. In addition, they and their staffs are responsible for the security, confidentiality, availability, and integrity of data and software stored on individual workstations or local fileservers and on shared system resources (whether provided on campus or through third-party systems or services) to the extent that they have access and/or access control. This responsibility includes ensuring the backup of key software systems and data on workstations and local file servers. It may also include account management and/or data stewardship responsibilities that have been specifically assigned in keeping with Policy 1205 – Data Stewardship.

7.2 Deans, associate/assistant vice presidents and academic/administrative unit heads are further required to designate a system administrator for any shared file server or application system under their control and not administered by IT.

7.3 This policy also places responsibility on deans, associate/assistant vice presidents and academic/administrative unit heads to: 1) require appropriate computer use as specified in Policy 1207 - Appropriate Use of Information Technology Resources, 2) ensure compliance with information technology policies and standards by people and services under their control, and 3) implement and monitor additional procedures as necessary to provide appropriate security of information and technology resources within their area of responsibility.

7.4 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. As part of the university's Information Security Program, IT will maintain JMU Computing Standards for access to shared system resources as specified in Policy 1205 – Data Stewardship, the campus network and fileservers managed by IT.

7.5 As part of the Information Security Program, IT is responsible for monitoring the university's technology environment and addressing potential vulnerabilities. IT is also responsible for information security incident response. Anyone who becomes aware of a potential information security incident should delay investigative action and report the concern immediately to the information security officer, IT information security staff or abuse@jmu.edu.

7.6 Additionally, the president will appoint a university information security officer who shall be responsible for the administration of the university's Information Security Program and providing technical support to university departments and offices in the development of local security procedures. This program shall extend to all information technology resources of the university. Its emphasis will be on a risk-based approach to protect the university's information technology resources, with particular focus on sensitive information and critical data and applications.

7.7 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 offense and may include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

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: July 2019
Approved by the president: April 2002
.