Policy 1214
University Information Technology Security Program

Date of Current Revision: July 2021
Responsible Officer: Assistant Vice President for Information Technology and CIO

1. PURPOSE

James Madison University has a highly complex and resource rich information technology environment upon which there is increasing reliance to provide mission-critical academic, instructional, and administrative functions. Safeguarding the institution's computing assets in the face of growing security threats is a significant challenge requiring a strong, persistent, and coordinated program that leverages widely accepted, effective security practices appropriate for the higher education environment. This policy states the codes of practice with which the university aligns its information technology security program.

The Commonwealth of Virginia Restructured Higher Education Financial and Administrative Operations Act of 2005 grants institutions additional authority over financial and administrative operations, on condition that certain commitments to the Commonwealth are met. Chapters 824 and 829 of the 2008 Virginia Acts of the Assembly and JMU's Memorandum of Understanding with the Commonwealth provides full-delegated responsibility for management of the institution's information technology security activities. This delegation includes the authority to conduct these activities in accordance with industry best practices appropriately tailored for the specific circumstances of the university, in lieu of following Commonwealth-determined specifications. This policy documents the industry best practices with which the university will align its security activities.

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

None.

4. APPLICABILITY

This policy applies to the management of all university computing assets.

5. POLICY

The university's information technology security program will be based upon best practices recommended in the “Code of Practice for Information Security Management” published by the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 27002:2013), appropriately tailored to the specific circumstances of the

university. The program will also incorporate security requirements of applicable regulations, such as the Family Educational Rights and Privacy Act, Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. Professional organizations, such as the national EDUCAUSE association and the Virginia Alliance for Secure Computing and Networking, will serve as resources for additional effective security practices.

6. PROCEDURES

6.1 The ISO/IEC 27002:2013 Code of Practice and other sources noted in the policy statement will be used to guide development and ongoing enhancement of additional information technology security policies as needed. All policies governing information technology security can be found at the web site https://www.jmu.edu/computing/policies-and-standards.shtml

6.2 For more information related to this policy, refer to the following:

"Code of Practice for Information Security Management" (ISO/IEC 27002:2013). This international standard defines guidelines and general principles for the effective management of information security within an organization. It is a risk-based framework widely used to guide establishment of security standards and management practices.

EDUCAUSE is a nonprofit association dedicated to the advancement of higher education through the effective use of information technology. Members include representatives from institutions of higher education, higher education technology companies, and other related organizations.

International Organization for Standards (ISO). The world's largest developer of standards, the organization is made up of representatives from governmental and private sector standard bodies, e.g., the American National Standards Institute.

International Electrotechnical Commission (IEC). The IEC is a global organization that develops and publishes standards addressing electrical, electronic, and related technologies. Membership comes from government, the private sector, consumer groups, professional associations, and others.

Virginia Alliance for Secure Computing and Networking (VA SCAN). VA SCAN was formed to help strengthen information technology security programs within Virginia. The alliance was organized and is operated by security practitioners and researchers from several Virginia higher education institutions, including JMU.

7. RESPONSIBILITIES

Information Technology is responsible for the security of computing assets.

8. SANCTIONS

None.

9. EXCLUSIONS

None.

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: December 2020
Approved by the president: September 2008