IRM-011

University Information Security Program

Effective Date Friday, June 9, 2006

Status Final

Last Revised Thursday, May 1, 2025

Policy Type University

Contact Office Vice President and Chief Information Officer (Office of the)

Oversight Executive
Vice President and Chief Information Officer

Applies To Academic Division, the Medical Center, and the College at Wise.

Table of Contents

Policy Statement
Compliance with Policy

Reason for Policy

The University has a highly complex and resource-rich information technology environment upon which mission-critical academic, instructional, and administrative functions rely. Safeguarding the institution's information technology 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 security program.

Definition of Terms

Terms

Description There are no terms that require definition.

Policy Statement

The University's information security program is 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), appropriately tailored to the specific circumstances of the University. The program also incorporates security requirements of applicable regulations, such as the Family Educational Rights and Privacy Act, Gramm-Leach-Bliley Act, and Health Insurance Portability and Accountability Act. Professional organizations, such as the national EDUCAUSE Association, the Center for Internet Security, and the Virginia Alliance for Secure Computing and Networking, serve as resources for additional effective security practices.

The ISO/IEC 27002 Code of Practice and other sources noted above are used to guide development and ongoing enhancement of additional information security policies as needed. All policies governing information security can be found in the University's Policy Directory and at:

- The Academic Division's IT policy website.
- The Medical Center's IT policy website.
- The College at Wise's IT policy website.

Compliance with Policy:
Failure to comply with the requirements of this policy may result in (1) disciplinary action up to and including termination or expulsion in accordance with relevant University policies; and (2) the University taking measures that may impact the school, department, or unit. The University also recognizes that there may be business needs or academic pursuits that require deviation from this policy or the use of different standards. Any deviation from this policy or the use of different standards requires coordination with and approval from the Contact Office to remain compliant with the requirements of this policy.

Direct questions about this policy to the Office of the Vice President & Chief Information Officer.

Related Information

Center for Internet Security taps into the global IT community to help public and private organizations protect themselves against cyber threats. It provides both prescriptive, prioritized, and simplified set of cybersecurity best practices and consensus-developed secure configuration guidelines for hardening various technologies as well as a community of practitioners to offer timely updates and advice.

EDUCAUSE Association – EDUCAUSE is a nonprofit association whose mission is to advance higher education through the use of information technology. We equip our community with the knowledge, resources, and community-building opportunities needed to help shape strategic IT decisions at every level in higher education.

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.

"Code of Practice for Information Security Management" (ISO/IEC 27002) – 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.

Virginia Alliance for Secure Computing and Networking (VASCAN) – VASCAN was formed to help strengthen information security programs within Virginia. The Alliance was organized and is operated by information security practitioners and researchers from many Virginia higher education institutions, including the University of Virginia.

Policy Background

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. The University of Virginia's Management Agreement with the Commonwealth provides full delegated responsibility for management of the institution's information technology security activities.

Major Category Information Resource Management

Next Scheduled Review Monday, May 1, 2028

Revision History
Confirmed 5/1/25; Updated 9/8/21; 1/15/10; 11/4/08.

Approved By Board of Visitors

Approved Date Friday, June 9, 2006