
Subject: University Information Technology Security Program

1. Purpose 1
2. Policy 1
3. Procedures..... 1
4. References.....2
5. Approval and Revisions.....2

1. Purpose

Virginia Tech 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. Virginia Tech’s Management Agreement 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. 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), 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 EDUCAUSE association, the Center for Internet Security, the National Institute of Standards and Technology and the Virginia Alliance for Secure Computing and Networking, will serve as resources for additional effective security practices.

3. Procedures

The ISO/IEC 27002 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 university policies, including those pertaining to information technology, can be found at the Virginia Tech Policies website <http://www.policies.vt.edu/index.php>. In addition, all policies and standards governing information technology security can be found at the Virginia Tech Information Technology website <http://www.it.vt.edu/administration/policies/>.

4. References

“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.

<http://www.iso27001security.com/html/27002.html>

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.

<http://www.educause.edu>

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.

<http://www.iso.org/iso/home.html>

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.

<http://www.iec.ch/>

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 Virginia Tech.

<http://vascan.org/>

Center for Internet Security (CIS). The Center for Internet Security (CIS) is an organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls.

<https://www.cisecurity.org/>

National Institute of Science and Technology (NIST). NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security

<https://www.nist.gov/>

Virginia Tech Policy 7010, Policy for Securing Technology Resources and Services

<http://www.policies.vt.edu/7010.pdf>

5. Approval and Revisions

Approved April 28, 2006 by Earving L. Blythe, Vice President for Information Technology.

Approved June 12, 2006 by the Virginia Tech Board of Visitors.

September 7, 2006: Technical revision – reference to former Policy 2016 updated to reference current Policy 7010: Policy for Securing Technology Resources and Services.

- Revision 1

ISO references updated from ISO 17799 to ISO 27002. Section 3 technical revision and corrected reference to IT policy and standards website.

Approved January 29, 2018 by Vice President for Information Technology and Chief Information Officer, Scott F. Midkiff.