Policy for Securing Technology Resources and Services

No. 7010

Policy Effective Date:
3/22/2006

Last Revision Date:
11/27/2023

Policy Owner:
Amy Sebring

Policy Author: *(Contact Person)*
Brenda van Gelder

Affected Parties:
Undergraduate
Graduate
Faculty
Staff
Other

1.0 Purpose

Information technology resources and services are essential to the mission and business of the university. Every facet of the enterprise is affected by the resources attached to the network. Outages of the network or information services will adversely affect the daily operations and functions of the university. Therefore, the university engages in information technology security practices including but not limited to routine automated monitoring and maintenance of network traffic and endpoints connected to university systems. This policy ensures that all technology resources and services are as stable, secure, and trustworthy as possible.

2.0 Policy

Information technology resources and services must be securely maintained in compliance with the regulations, policies and standards contained herein and on the Division of Information Technology website (it.vt.edu) and must be associated with an individual who is responsible for ensuring their continued security.

By using technology resources on the university-owned network and infrastructure, departments and individual users consent to university practices required for securing university systems. University-owned technology resources will undergo automated routine monitoring of that resource for security purposes. The university may access or disclose electronic information for legitimate business purposes and will be limited to the minimum degree to accomplish the specified purposes, as described in Policy 7035, "Privacy Policy for Employees' Electronic Communications."

2.1 Scope

This policy applies to any technology resource or service that:

- Is owned or managed by the university;
- Is connected to the university network;
- Connects to another university technology resource or service; or
- Stores university data or information.

This policy applies whether the network connections are remote or campus-based.

The owner of a technology resource may use it at his or her discretion; however, once it is connected to the university network, or other technology resource or service that is used to store university data, it is subject to applicable laws and regulations and to university policies and standards.

2.2 Responsibilities

The Vice President for Information Technology and Chief Information Officer (VPIT & CIO) is responsible for creating and maintaining information technology (IT) related

security policies and standards across the university and is assigned the authority for ensuring compliance with those standards. IT-related policies and standards are posted on the Division of IT website.

The IT Security Office (ITSO) will ensure that security training and tools are available and that security standards are published and updated. In collaboration with approved vendors and other units as appropriate, ITSO is responsible for deploying and maintaining automated tools and processes that ensure university IT resources are operating properly from a security standpoint, to ensure compliance, and to protect against security threats to the university and individual users of IT resources. Such threats pose risks to sensitive data about individuals as well as potential disruption of university operations services which could impact all users, possibly for long periods of time.

University departments must regularly analyze risks for their technology assets using the Virginia Tech IT Risk Assessment process.

University departments and organizations are responsible for assigning each technology resource to an accountable individual who is responsible for ensuring the continued security of that resource as required by Division of IT policies and standards. Every technology resource user is responsible for security and acceptable use of the material he or she chooses to access, store, print, send, display or share with others.

Departments and individual users must take actions to minimize security vulnerabilities that may exist on departmental and individual technology resources that they attach to a university network. They must adhere to the Minimum Security Standards and other standards as published on the Division of IT website (it.vt.edu) standards and policies section.

Individuals – including individual students – using personal technology resources are responsible for complying with the university's Minimum Security Standards.

Training and consultation is available by contacting the IT Security Office at itso-g@vt.edu.

3.0 Enforcement

Every technology resource user is subject to applicable laws and regulations and to university policies. Sanctions for violations may be determined by these laws and regulations in addition to and independent of any actions taken by the university. Violators are subject to disciplinary action as prescribed in the Honor Codes, the Student Code of Conduct, and Human Resources policies and procedures. Violations of this policy are considered serious and consequences for a specific violation may include the following:

- Any technology resource that is determined by the university to not meet the security standards may be refused connection to the university network.
- University network traffic to and from any technology resource or service regardless of ownership is subject to routine automated monitoring. If such methods identify possible inappropriate use of the network or violation of the Acceptable Use Policy (Policy 7000), appropriate responsive action will be taken. The university reserves the right to disconnect any resource from the network until suspected security incidents or Acceptable Use violations can be resolved.
- In cases where university network resources and privileges are threatened by improperly maintained resources (university owned or privately owned), the IT Security Office will offer mitigation strategies and, when necessary, act to eliminate the threat.

For clarification or assistance with this policy, contact the IT Security Office or visit their website (security.vt.edu).

4.0 Definitions

Technology resource – any item such as a computer, tablet, smartphone, server or similar device and associated peripherals owned by Virginia Tech or used to store university data, including those in cloud services and for research contracts or private activities associated with the university, and privately-owned technology devices that are connected to the Virginia Tech network or used to store university data.

Service – a set of computer and network applications that perform work, often operating on data using standard protocols.

Department – the fundamental organizational unit of the university for the purpose of management.

5.0 References

Policy 7000, Acceptable Use and Administration of Computer and Communication Systems
https://policies.vt.edu/7000.pdf

Acceptable Use Standard
http://www.vt.edu/acceptable-use.html

Continuity of Operations plan
https://emergency.vt.edu/plans/COOPs.html

Information Technology Risk Assessment Assistance
https://security.vt.edu/policies-and-compliance/it_risk_assessments/

Information Technology Security Office Website
http://www.security.vt.edu/

Information Technology Security policies and standards
https://it.vt.edu/resources/policies.html#SecurityData

Minimum Security Standards
https://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf

Policy 7100, Administrative Data Management and Access Policy
http://www.policies.vt.edu/7100.pdf

Frequently Asked Questions (FAQ About IT Security Monitoring
https://evpcoo.vt.edu/Initiatives/ittransformation/projects/cybersecurity/improved-endpoint-protection.html

Board of Visitors Resolution Approved March 20, 2023
https://bov.vt.edu/assets/Minutes-March%2019-20,%202023-30.pdf

6.0 Approval and Revisions

Approved March 22, 2006 by the Vice President for Information Technology, Earving L. Blythe.

September 7, 2006: Technical revision – policy renumbered to Information Technology Policy 7010 from former General University Policy 2016.

- Revision 1
  Section 2.2: responsibilities updated and clarified.

  Approved January 22, 2007 by the university President, Charles W. Steger.

- Revision 2
  Wording clarified and webpage referral links repaired.

  Approved March 14, 2016 by the Vice President for Information Technology and Chief Information Officer, Dr. Scott F. Midkiff.

- Revision 3
  Simplified the Procedures section in accordance with security standards, updated references and added website information.

  Approved October 29, 2020 by the Vice President for Information Technology and Chief Information Officer, Dr. Scott F. Midkiff.

- Revision 4
  - Sections 2.0, 3.0 and 3.1 were modified to include roles and responsibilities related to routine automated monitoring of university-owned technology resources and network traffic.
  - It also affirms consent of those who use the university network and/or university-owned technology resources that are subject to such IT security practices.

  Approved November 27, 2023 by Executive Vice President and Chief Operating Officer, Amy Sebring.