



Policy for Securing Technology Resources and Services

No. 7010

Policy Effective Date:
3/22/2006

Last Revision Date:
10/29/2020

Policy Owner:
Scott Midkiff

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

Affected Parties:
Undergraduate
Graduate
Faculty
Staff
Other

- 1.0 Purpose
- 2.0 Policy
- 3.0 Procedures
- 4.0 Definitions
- 5.0 References
- 6.0 Approval and Revisions

1.0 Purpose

Information technology resources and services are critical resources 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. 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.

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 a device is connected to the university network; or other technology resource or service is used to store university data; it is subject to applicable laws and regulations and to university policies.

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 (it.vt.edu)

The IT Security Office will ensure that security training and security tools are available and that security standards are published and updated.

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.



Virginia Polytechnic Institute and State University

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.

Individuals – including individual students – using personal technology resources are responsible for complying with the university's Minimum Security Standards (https://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf).

University departments must regularly analyze risks for their technology assets using the Virginia Tech IT Risk Assessment process (<https://security.vt.edu/policies/itra.html>),

3.0 Procedures

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

3.1 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 independently 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.
- Network traffic to and from any device determined to be using the network inappropriately or in violation of the Acceptable Use Policy (Policy 7000) may be monitored. The university reserves the right to disconnect any resource from the network until suspected security incidents can be resolved. Attempts to notify the responsible person will be made before any such termination of network access.
- In cases where university network resources and privileges are threatened by improperly maintained devices (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, or similar device and associated peripherals owned by Virginia Tech or used to store university data, including those in 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

Acceptable Use Policy

<https://policies.vt.edu/7000.pdf>

Acceptable Use Standard

<http://www.vt.edu/about/acceptable-use.html>

Continuity of Operations plan

<https://emergency.vt.edu/plans/COOPs.html>

Information Technology Risk Assessment Assistance

<https://security.vt.edu/policies/itra.html>

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>

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.