Acceptable Use and Administration of Computer and Communication Systems

No. 7000

Policy Effective Date:
5/29/1991

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

This is a statement of policy regarding the use and administration of Virginia Tech computer and communication systems, network, services, and data. It relates to the use of any computing or communications device, regardless of ownership, while connected to the University network, and to the use of any information technology services provided by or through the University. Every individual using these systems and services is expected to know and follow this policy.

2.0 Policy

Individuals using or administering Virginia Tech computer and communication networks, systems, and/or data with any device must comply with all laws, regulations, and University policies and guidelines, including, but not limited to, the following:

- Standard for *Acceptable Use of Information Systems at Virginia Tech* (https://vt.edu/about/acceptable-use.html)

- Applicable policies and standards listed on the Division of Information Technology website (https://it.vt.edu/resources/policies.html)

2.1 General Use

Computing and communications capabilities at Virginia Tech have been developed to support the University's missions and administrative functions. These can be used in similar fashion to postal mail and telephone services, and so are governed by principles of appropriate use for those services.

Activities involving these capabilities must be in accordance with the University Honor Codes, University policies, Faculty Handbook, Student Code of Conduct, and relevant local, state, federal, and international laws and regulations.

For use and administration to be acceptable, individuals must demonstrate respect of:

- the rights of others to privacy;
- intellectual property rights (e.g., as reflected in licenses and copyrights);
- ownership and integrity of data (including research data);
- sensitivity of data through responsible storage and transmission of sensitive data as documented in the Standard for High Risk Digital Data Protection (http://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf);
- system mechanisms designed to limit access; and the rights of others to be free of intimidation, harassment, and unwarranted annoyance.

2.2 Policy Enforcement

The University regards any violation of this policy as a serious offense. Misuse or deliberate abuse of these services or data will result in investigation and enforcement when necessary. Alleged violations will be subject to established university disciplinary policies and procedures applicable to the relevant individual and their affiliation to the University including, but not limited to faculty, staff, student and alumni.

Offenders may be prosecuted under the terms described in laws such as (but not limited to) the Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, the Junk Fax Act, and the Virginia Computer Crimes Act. This policy statement does not preclude prosecution of cases involving criminal misconduct under the laws and regulations of the Town of Blacksburg, the Commonwealth of Virginia and the United States of America.

3.0 Procedures

The following procedures for reporting and enforcement of violations of this policy, acceptable use requirements for University guests, and reporting suspected security breaches apply to all individuals using University computing and communication systems.

3.1 Reporting and Enforcement

Suspected violations of this policy should be reported by sending an email to abuse@vt.edu which automatically generates a ticket and follow up on the report. Alleged violations are then referred to the appropriate University office or law enforcement agency for further investigation.

The University may temporarily deny access to information technology resources during an investigation if it appears necessary to protect the integrity, security, or continued operation of these resources or to protect from liability during the course of the investigation.

Individuals, including University alumni, who use information technology resources in ways that violate a University policy, law(s), regulations, contractual agreement(s), or an individual's rights, are subject to limitation or termination of user privileges/ removal of access to services and appropriate disciplinary action, legal action, or both.

3.2 Acceptable Use Requirements for University Guests

Units that grant guest access to information technology resources must make their guests aware of these acceptable use requirements. The University accepts no responsibility or liability for any personal or unauthorized use of its resources by guests.

3.3 Reporting Suspected Cybersecurity Breaches

Any suspected cybersecurity incident or data exposure must be immediately reported to the appropriate Dean, Director, or Department Head and to the Information Technology Security Office (ITSO). The Information Technology Security Office (ITSO) manages and coordinates detection, identification, containment, eradication, and recovery efforts of reported cybersecurity incidents with Virginia Tech departments' IT and other personnel. There are specific steps that must be followed in working with University officials in response to cybersecurity breaches and the ITSO is the first point of contact for facilitating that process from start to resolution.

4.0 Definitions

Misuse or abuse: uses of University information technology resources or data that violate existing laws or University policies and procedures (including but not limited to University Information Technology Policies and Standards; Student Honor Codes; Student Code of Conduct; University Human Resources Policies; and University Financial Policies), or that otherwise violate generally accepted ethical norms and principles. Misuse or abuse also includes the sharing or transferring of an individual's university accounts, including network ID, password, or other access codes with one or more other persons, thus enabling the person(s)to gain access to University information technology resources.

5.0 References

Standard for Acceptable Use of Information Systems at Virginia Tech
http://www.vt.edu/about/acceptable-use.html

Standard for High Risk Digital Data Protection
http://it.vt.edu/content/dam/it_vt_edu/policies/Standard-for-High-Risk-Digital-Data-Protection.pdf

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)
https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Junk Fax Act of 2005
https://www.congress.gov/bill/109th-congress/senate-bill/714

6.0 Approval and Revisions

Endorsed by the University Communications Resources Committee, May 29, 1991.

- Revision 1
  - Section 2. Deleted reference to Policy 2005, "Guidelines for University Administrative Information Resource Management."
  - Added reference to Acceptable Use Guidelines.

  Approved June 4, 1999, by Associate Vice President for Information Systems, Michael Williams.

- Revision 2
  Policy broadened to cover those who administer university resources as well as those who use them. New Section 3.1 – Reporting Suspected Security Breaches.

  Approved April 15, 2002 by Vice President for Information Technology, Earving L. Blythe.

- Revision 3
  September 9, 2006: Technical revision – policy renumbered to Information Technology Policy 7000 from former General University Policy 2015.

  Approved September 9, 2006 by Vice President for Information Technology, Earving L. Blythe.

- Revision 4
  Updated to include all networked devices regardless of ownership and general updates of terminology and associated policies and standards.

  Approved April 3, 2018 by Vice President for Information Technology and CIO, Scott F. Midkiff.

- Revision 5
  Updated to clarify procedure for reporting and enforcing violations of this policy. Added a procedure for guests. Added definition of misuse and cited additional regulations.

  Approved October 29, 2020 by Vice President for Information Technology and CIO, Scott F. Midkiff.