Subject: Acceptable Use and Administration of Computer and Communication Systems

1. 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 user of these systems and services is expected to know and follow this policy.

2. Policy

This policy applies to any individual using or administering Virginia Tech computer and/or communication networks, systems, and/or data using any device. Such individuals must comply with 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 (http://it.vt.edu/resources/policies/index.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 capabilities and facilities 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 handbooks, 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;
- 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. Violators of this policy are subject to university disciplinary action as prescribed in the undergraduate and graduate honor codes, and the student and faculty handbooks, and university policies. 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, and the Virginia Computer Crimes Act. It should be understood that 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. Procedures

3.1 Reporting Suspected Security Breaches

In the case of potential cybersecurity incidents or data exposure, there are specific steps that must be implemented in working with university officials to determine a course of action to ensure compliance with university policies and federal and state regulations.

The Information Technology Security Office (ITSO) manages and coordinates detection, identification, containment, eradication, and recovery efforts of reported cyber security incidents with Virginia Tech departments' IT and other personnel. Any suspected breach should be immediately reported to the appropriate Dean, Director, or Department Head and to the ITSO. For more information on dealing with data exposure issues, see Dealing with Data Exposures (https://security.vt.edu/incident/dealing_with_data_exposure.html).

4. Definitions

5. 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

6. 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.