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 facilities, including those dealing with voice, data, and video. It relates to the use and administration of telecommunications equipment (including computer networks involving the CBX and Internet) as well as mainframe, midrange, minicomputer, workstation, and personal computer systems. Thus, it covers all activities involving computing and communication facilities of Virginia Tech. Every user of these systems 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 facilities. Not covered are activities solely involving personal property. Related university policies and guidelines that must be respected by such individuals include the following:

- *Acceptable Use of Information Systems at Virginia Tech*

2.1 General Use

Data communication facilities at Virginia Tech have been developed to encourage widespread access and distribution of data and information. Computing systems facilitate manipulation and sharing of data and information. Together, these systems and facilities can be used in similar fashion to mail and telephone services, and so are governed by principles of appropriate use for those services.

University communication and computing resources are used to support the educational, research, and public service missions of the institution. Activities involving these resources must be in accord with the university honor codes, Employee Handbook, student handbooks, and relevant local, state, federal, and international laws and regulations.

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

- the rights of others to privacy;
- intellectual property rights (e.g., as reflected in licenses and copyrights);
- ownership of data;
- system mechanisms designed to limit access; and
- individuals' rights 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 employee handbooks. Offenders may be prosecuted under the terms described in such laws (but not limited to) as the Privacy Act of 1974, PL 93-579, the Computer Fraud and Abuse Act of 1986, 18 USC Section 1030, the Computer Virus Eradication Act of 1989, HR 5061, HR 55, (amendments to 18 USC, section 1030), Interstate Transportation of Stolen Property, 18 USC section 2314 and Aiding and Abetting, 18 USC section 2 and Virginia Computer Crimes Act, VA Article 7.1. 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

Anyone who has reason to suspect a deliberate or significant breach of established security policy or procedure should promptly report it to the appropriate Dean, Director, or Department Head, and to the University Security Office. If it is felt the breach is serious and needs immediate attention, the Virginia Tech Police or local law enforcement should be contacted.

The Information Technology Security Office may be involved with suspected breaches and can also be a resource for those involved in any investigation.

4. Definitions

5. References

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.

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