Subject: Policy for Securing Technology Resources and Services

1. Purpose

Information technology resources and services play key roles in the life of the Virginia Tech community. 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 future of the university. This policy is intended to ensure that all technology resources and services are as stable, secure and trustworthy as possible to ensure security for individuals, departments, and the university.

2. Policy

Information technology resources and services must be securely maintained 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 that device is connected to the university network or other technology resource or service or 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 (VPIT)/ Chief Information Officer (CIO) is responsible for creating and maintaining IT related security policies and standards across the university and is assigned the authority for ensuring compliance with those standards.

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

Every technology resource user is responsible for the material he or she chooses to access, store, print, send, display or share with others.

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.

Individuals – including individual students – using personal technology resources are responsible for ensuring the continued security of those resources.

Persons who have these responsibilities for ensuring the security of technology resources must ensure that the resources and users of the resources conform to the policies set forth by the university, including the procedures in section 3.0 below.

University departments must regularly analyze risks for their technology assets, and ensure they have an up-to-date and proven recovery plan in place.

3. 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 security standards, including, but not limited to:

- Maintain the operating system and application software with appropriate updates;
- Install antivirus software and ensure virus definitions are updated regularly;
- Install and maintain appropriate access controls;
- Adhere to strong password requirements in selecting a secure password;
- Maintain adequate physical security for critical, confidential/sensitive resources;
- Ensure that a system has adequate backup for an up-to-date recovery;
- Reduce exposure to system compromise by limiting privileges to those needed by individuals and processes in order to perform their functions; and
- Contact an appropriate help desk for assistance in addressing problems with security procedures.

3.1 Enforcement

Offenders are subject to applicable laws and regulations and to university policies. Sanctions 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 University Policies for Student Life, and employee handbooks. Violations of this policy are considered serious and response to a specific violation may include the following:

- The university reserves the right to assess whether technology resources meet the security standards.
- The university reserves the right to refuse connection to the university network to any technology resource that does not meet the security standards.
- Should it be determined any device is using the network inappropriately, network traffic to and from that device 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 service.
- In cases where university network resources and privileges are threatened by improperly maintained devices (university owned or privately owned), the IT Security Office will act to eliminate the threat.

For clarification or assistance with this policy, contact the IT Security Office.

4. Definitions

Technology resource – any entity 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. It is referenced in the university's administrative systems by a 4-digit organizational number.

Access control – mechanisms for ensuring that resources and services are granted to those users who are entitled to them. Examples of access controls include passwords, permissions, personal firewalls, rule sets, biometrics, smart tokens, and two-factor authentication.

5. References

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

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

Security Web Site--templates and documents for security specific systems
http://www.security.vt.edu/

Virginia Tech Computing Resource Site
http://www.computing.vt.edu/

Information Technology Risk Assessment Assistance
http://security.vt.edu/services/risk_assessment/

6. 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.

- Rev. 1

  Section 2.2: responsibilities updated and clarified.

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

- Rev. 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.