Policy for Protecting University Information in Digital Form

No. 7105

Policy Effective Date:
7/1/2008

Last Revision Date:
1/29/2018

Policy Owner:
Scott Midkiff

Policy Author:
(Contact Person)
Brenda van Gelder

Affected Parties:
Faculty
Staff

1.0 Purpose

Virginia Tech is committed to ensuring the proper handling of the information that it collects and uses to carry out its missions. The purpose of this policy is to safeguard university information from unauthorized disclosure and inappropriate use when used in digital form.

2.0 Policy

All university information must be handled with an appropriate level of security when used in conjunction with electronic information systems to protect against unauthorized access, alteration, or disclosure. Such security is required to minimize the potential for physical, financial, or reputational harm to the university or to one or more of its faculty members, staff members, students, alumni, friends, or business partners.

The focus of this policy is on university information that exists in a digital format, whether stored in a database, used in an application, or used in a report. All appropriate measures must be taken to hold university information securely through its creation, storage, transmission, use, and deletion.

2.1 Scope

This policy applies to all university information in, or derived from, digital form. University information includes information collected by or used by university personnel in the conduct of their university responsibilities, whether the information resides in university-owned digital systems or elsewhere. It includes information collected and used for learning, discovery, engagement, support, and administration. University information in digital form may exist in a variety of formats, ranging from highly structured elements in a database to unstructured, narrative information. Further, university information may be gathered or used at the direction of the university but reside in applications hosted by vendors or other third parties, on university premises or off premises.

3.0 Procedures

Standards and guidelines, as well as specific considerations and tools, are available on the website of the Vice President for Information Technology (http://www.it.vt.edu/resources/policies/index.html). Additional guidance is provided at the Sensitive Information Security website (www.security.vt.edu/sensitiveinfo.html).

3.1 Verification

Once a year, each university employee who has electronic or physical access to university sensitive information must affirm that they take appropriate security measures in accordance with policy, standards, and procedures. (See www.security.vt.edu/sensitiveinfo.html). This is accomplished by checking a box that automatically appears on the online form during the account creation and annual password change processes.

4.0 Definitions

Digital form refers to the technology of computers and data communications, and includes products of those systems, including printed reports.

Sensitive information includes all university information that could cause physical, financial, or reputational harm to the university or to members of the university community if released inappropriately. Under Virginia Tech's Risk Classification Standard (https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf), data classified as high risk would be considered sensitive information.

5.0 References

University Policy 7010, Policy for Securing Technology Resources and Services
http://www.policies.vt.edu/7010.pdf

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

University Policy 7200, University Information Technology Security Program
http://www.policies.vt.edu/7200.pdf

University Policy 1060, Policy on Social Security Numbers
http://www.policies.vt.edu/1060.pdf

University Policy 7025, Safeguarding Nonpublic Customer Information
http://www.policies.vt.edu/7025.pdf

Standard for Administrative Data Management
http://it.vt.edu/content/dam/it_vt_edu/policies/AdministrativeDataManagementStandard.pdf

Virginia Tech Risk Classifications
http://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf

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

Family Educational Rights and Privacy Act of 1974
https://registrar.vt.edu/contact/FERPA.html

Gramm-Leach-Bliley Act
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

Health Insurance Portability and Accountability Act
http://aspe.hhs.gov/admnsimp/pl104191.htm

Virginia Tech student privacy/FERPA
https://registrar.vt.edu/contact/FERPA.html

6.0 Approval and Revisions

Approved July 1, 2008 by the Vice President for Information Technology, Earving L. Blythe. June 16,

2009: Technical corrections to hyperlinks.

- Revision 1
  Updated verbiage, references, and hyperlinks.
  Approved January 29, 2018 by Vice President for Information Technology and Chief Information Officer, Scott F. Midkiff.