**Virginia Polytechnic Institute and State University** **No. 7100 Rev.: 6**
***Policy and Procedures*** **Date: October 17, 2017**

**Subject: Administrative Data Management and Access Policy**

# 1. Purpose

This policy establishes uniform data management practices and responsibilities for assuring the integrity of university data. This policy applies to those data that are used in the administration of the university, regardless of whether the data are used or maintained by administrative or academic units or others and regardless of source and where it resides. The use of university data for anything other than approved university business is prohibited by university policy, state, and federal law.

The data management standards that define these responsibilities and roles are:

- Policy 7100 – this document
- Standard for Administrative Data Management
- Standard for High Risk Digital Data Protection
- Virginia Tech Risk Classifications

# 2. Policy

The university is the owner of all administrative data pertaining to its business and function. Individuals designated as Data Trustees authorize access to university data. Individuals may not access, use, or store some kinds of sensitive data without authorization from the appropriate Data Trustee. Individuals who are authorized by a Data Trustee to access, use, or store sensitive information must follow any restrictions imposed by the Data Trustee. This policy and its accompanying standards and guidelines define the roles and responsibilities of these individuals.

## 2.1 Data Management Roles and Responsibilities

**Vice President for Information Technology and Chief Information Officer (VPIT/ CIO) -** The university official responsible for overseeing the management of university information in digital form. In consultation with the President and the Executive Vice President and Provost, the VPIT/ CIO mediates conflicts and discrepancies between the interest of the data trustees, the university vice presidents, and the needs and interests of the university.

**Data Trustees -** Senior university officials (*typically at the level of Vice President, Vice Provost, or Dean*) who have planning and policy-making responsibilities for university data. The Data Trustees, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability. As needed, this group is convened by the VPIT/CIO.

**Data Stewards -** University officials (*typically at the level of Associate Vice President, Associate Vice Provost,* *University Registrar, University Bursar, or Director*) who oversee the capture, maintenance and dissemination of data for a particular operation. Data Stewards are appointed by the respective Data Trustee. Data Steward responsibilities include risk classification of data based on any legal, ethical, or externally imposed constraint; documenting the process for approving and reviewing access; defining controls related to the confidentiality, integrity, and security of the data; and other activities assigned by a Data Trustee.

**Data Managers -** University staff in a functional area with day-to-day responsibilities for the capture, maintenance, and dissemination of data for a particular operation.

**Data Users -** Individuals who access university data in order to perform their assigned duties or to fulfill their role in the university community. Data Users are responsible for protecting their access privileges, for proper use of the university data they access based on the data's risk classification, and for adherence to IT standards.

**University Information Technology Security Officer -** The university official responsible for maintaining a plan for security policies and practices and for keeping abreast of security-related issues internally within the university community and externally throughout the information technology marketplace.

## 2.2 Data Access Philosophy

The value of data as a university resource is increased through its widespread and appropriate use; its value is diminished through misuse, lack of timely upkeep, or unnecessary restrictions to its access. Furthermore, increased data access and use can help to improve data integrity because discrepancies are identified and errors are subsequently corrected.

As a higher educational institution with a mission to disseminate knowledge, and as a public institution accountable to the Commonwealth of Virginia, Virginia Tech values ease of access to information, including administrative data. Permission to view or query data should be granted to all Data Users for all legitimate purposes in accordance with the Virginia Tech Risk Classification Standard. Update access should be restricted as necessary but granted to university employees at the location where data are initially received or originates whenever this is feasible. Information specifically protected by law or regulation must be rigorously protected from inappropriate access as specified by law or regulation (see Policy 7105 Policy for Protecting University Information in Digital Form (http://www.policies.vt.edu/7105.pdf).

# 3. References

Information Technology Security and Authority Resolution
http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.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

## 4. Approval and Revisions

Original Policy 2005: Guidelines for University Administrative Information Resource Management, approved January 5, 1989 by the Administrative Systems Users Group (ASUG).

Approved November 14, 1989 by the Director of the Office of Institutional Research and Planning Analysis James R. Montgomery

Revision 1: Policy rewritten and renamed “Administrative Data Management and Access Policy”. Approved by Senior Vice President and Provost Peggy S. Meszaros and Executive Vice President Minnis E. Ridenour on September 1, 1999. Signed into policy by Vice President for Information Technology, Earving L. Blythe, September 29, 1999

Revision 2: Minor changes for clarification and to reflect organizational reporting structure changes. Approved by Vice President for Information Systems, Earving L. Blythe, April 15, 2002

Revision 3: Minor changes to reflect organizational structure changes. Policy renumbered to Information Technology Policy 7100 from former General University Policy 2005. Approved by Vice President for Information Technology, Earving L. Blythe, July 18. 2006

Revision 4: Technical revision to correct referenced policy numbers September 11, 2006. Technical revision to correct section 3.2.3 statement to reflect reviewing annually instead of periodically. October 23, 2007.

Revision 5: Updates to position titles and/or responsibilities due to university reorganization April 1, 2008. Approved by Vice President for Information Technology, Earving L. Blythe, April 1, 2008.

Revision 6: Major revisions to update the data risk classifications and to remove procedures that are addressed in IT security standards, September 2017.

Approved October 17, 2017 by the Vice President for Information Technology and CIO, Dr. Scott F. Midkiff.