Data Governance

Policy 902

1 Introduction

The purpose of this policy is to outline a Data Governance program to preserve and nurture the open, information-sharing requirements of Appalachian State University's ("Appalachian") academic culture, while protecting Appalachian's Institutional Data from unauthorized access or damage and meeting compliance requirements.

2 Scope

This policy applies to all Appalachian faculty, staff, students, vendors and visitors who access Institutional Data. This policy is not meant to address the release of Institutional Data under public records laws or other legal requirements, such as in response to subpoenas or court orders.

3 Definitions

3.1 Institutional Data

All data, regardless of physical form or characteristic, made or received in connection with the transaction of University business that is in the possession or control of the University (same meaning as defined in [Appalachian Policy 901 – IT Governance Policy](#)).

3.2 Data Element

A unit of Institutional Data that has precise meaning or precise semantics.

3.3 Data Governance

A framework of standards, principles, requirements, authorities, roles, and guidance to provide optimal and secure Institutional Data management to support and advance the University mission.

3.4 Data Trustees

Executive officers of the University, designated by the Chancellor, who are responsible for data-related strategic planning and have oversight authority of Institutional Data for all organizational units and employees, under their charge, that manage and receive Institutional Data.

3.5 Data Steward

A University employee who reports to, and is designated by, a Data Trustee and has the responsibility for protecting Institutional Data in accordance with IT Standards and University policies, and consistent with directions provided by a Data Trustee.

3.6 Data Security Officer

A University employee, designated by a Data Steward, who has been assigned operational responsibilities for maintaining technical solutions and enforcing access procedures and IT Standards related to Institutional Data.

3.7 Information Technology (IT) Standards

Same meaning as defined in [Appalachian Policy 901 – IT Governance Policy](#).

3.8 Data Classification

A common category of Data Elements that specifies their availability, access requirements, and requisite protection levels.

3.9 System of Record

Information Technology (IT) that is identified as the authoritative data source by Appalachian for a subset of Institutional Data or a given Data Element.

4 Policy and Procedure Statements

4.1 Data Governance Program

The Chancellor is the Data Custodian of Institutional Data at Appalachian. The Chancellor has delegated authority and oversight for the administration and implementation of Data Governance to the Chief Information Officer. The Chief Information Officer is responsible for developing and overseeing a Data Governance Program (the "Program") that includes:

a. a data management IT Standard that defines Institutional Data Classification levels and processes associated with Data Classifications;
b. a secure data handling IT Standard that defines approved methods for storing and sharing Institutional Data by Data Classification, and
c. a Data Trustees Council and a Data Stewards Council to assist the Chief Information Officer with carrying out its duties of administering the Data Governance Program, as well as recommend and review Data Governance standards as determined by the Chief Information Officer.

4.2 Data Trustees

4.2.1 Data Trustee Oversight

Each Data Trustee has oversight authority and responsibility for the subset of Institutional Data and System of Records that is managed and administered by the organizational units and personnel the Data Trustee oversees. Data Trustees include the following executive officers:

a. Executive Vice Chancellor and Provost
b. Vice Chancellor of Finance and Operations
c. Vice Chancellor of Student Affairs
d. Vice Chancellor of University Advancement
e. Vice Chancellor and Chief of Staff
f. General Counsel
g. Chief Information Officer
h. Director of Human Resources
i. Director of Institutional Research Assessment and Planning

4.2.2 Data Trustees' Responsibilities

Data Trustees are responsible for:

a. providing oversight of compliance with IT Standards for data management in their organizational units;
b. promoting appropriate data use, data quality and management procedures to advance the University's mission; and
c. assigning one or more Data Stewards within a Data Trustees organizational unit.

4.3 Data Stewards

Data Stewards are responsible for the confidentiality, integrity, and availability of Institutional Data assigned to them by their Data Trustee. Responsibilities include:

a. ensuring security and protection measures are implemented in accordance with relevant IT Standards;
b. designating the System of Record and data definitions for critical Data Elements;
c. designating Data Security Officers, as applicable; and
d. reviewing and approving access requests and access levels in accordance with IT Standards, or delegating approval to the designated Data Security Officer.

4.4 Data Governance Groups

Data Groups are responsible for providing recommendations and assisting with Data Governance as identified below. The Data Governance Groups consist of the Data Trustees Council and the Data Stewards Council.

4.4.1 Data Trustees Council

To promote optimal data management and support consistency across the University, Data Trustees meet periodically in the Data Trustees Council to review Data Governance IT Standards, review the effectiveness of the University's data management practices, and resolve any Data Stewardship disputes from the Data Stewards Council. All disputes not resolved at this level will be sent to the Chancellor for a final decision.

4.4.2 Data Stewards Council

Each Data Trustee will appoint one or two Data Stewards to serve on a Data Stewards Council. The Chief Information Officer, or delegate, and General Counsel, or delegate, will serve on the Data Stewards Council to provide consultation and advisement. The Data Stewards Council is responsible for:

a. classifying Institutional Data in accordance with the Data Management IT Standard, and ensuring consistent terms and definitions are used for key Data Elements that are used across organizational units;
b. reviewing Data Governance IT Standards to ensure consistent treatment and optimal use of Institutional Data;
c. identifying the System of Record for a subset of Institutional Data or a given Data Element;
d. reviewing and reporting the effectiveness of Institutional Data management practices to Data Trustees; and
e. coordinating and resolving Data Stewardship issues that cross multiple functional units, and escalate compliance and risk issues to the Data Trustees Council.

5 Additional References

Appalachian Policy 906 - Acceptable Use Policy
Appalachian Policy 901 - Information Technology Governance Policy
Appalachian Policy 903 - Information Security Policy
Appalachian Policy 105.1 - Record Retention Policy
Appalachian Policy 105.3 - Policy Statement on the Family Educational Rights and Privacy Act of 1974, as Amended - Appalachian State University Policy Manual Policy
Appalachian Policy 105.2 - University Archives Policy

6 Authority

Data Management Standard
Secure Data Handling Standard
Information Security Risk Management Standard
IT Policy, Standards and Guidelines Website

7 Contact Information

Office of the Chief Information Officer (828-262-6278)

8 Original Effective Date

December 7, 2020

9 Revision Dates