Data Management Standard

Revision Notes:	Last Updated: 51/2016	Status: APPROVED
Version 1.0 - 11/2015 *Approved by ISAC,* *Reviewed By Cabinet* *Ratified* Version 1.01 - 5/2016 *Added Enforcement, Exemptions, and Advisement Section for alignment with other approved standards.* *Revision*		

Table of Contents

1. Objective:
The objective of this standard is to clearly define the roles, responsibilities, and specific requirements needed to provide secure and optimal management of data to support the University mission.

This standard addresses the objectives outlined in sections 4.4.3.1 and 4.4.3.2 of the University Information Security Policy.

2. Scope:
The standard applies to all Appalachian State University employees, students, and affiliates and all institutional data (see section 4.4), whether verbal, printed, or electronic, and whether individually controlled, shared, stand alone, or networked.

3. Requirements

3.1 Data Governance Groups

3.1.1 Data Stewards Council
The Data Stewards Council is comprised of all University Data Stewards (see 3.2.2). The Council is responsible for overseeing the development and maintenance of standards needed to ensure

consistent treatment of institutional data (see 4.4) as well as periodically reviewing and reporting on the effectiveness of University data management practices.

3.1.2 Data Management Group

The data management group is responsible for establishing operational practices and initiatives related to data quality, data security, privacy, and compliance. Standing membership of this committee will include but is not limited to the University Data Custodians, Director of Information Analytics, Director of Enterprise Applications, Chief Information Security Officer, University Archivist, and General Counsel.

3.2 Data Management Structure

Roles and responsibilities related to management of institutional data are defined at all levels of the University. The following data management roles are recognized and approved:

3.2.1 Data Trustees - The data trustees are senior institutional officers (e.g., Vice Chancellors, Vice Provosts, Deans, etc.) who have both oversight and policy-level responsibility for defined institutional data sets. Data Trustees work with the Chief Information Officer (CIO) to ensure that the appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire university.

Responsibilities include:

- Establishment of university-wide data management policies and standards
- Oversight of data management related to university functions for their units
- Promoting appropriate data use, data quality and management procedures
- Assigning Data Stewards for specific institutional data sets

3.2.2 Data Stewards - Data stewards are University employees with planning and management responsibility for defined institutional data sets (e.g. student data, finance data, personnel data, research data, and alumni data). Data stewards are responsible for ensuring that the management of individual data sets conforms with relevant University policies and standards.

Responsibilities include:

- Establishing procedures to ensure that data elements within institutional data sets are defined, described, and assigned an appropriate Data Classification level (see 3.3)
- Ensuring that data quality and data definition standards are developed and implemented
- Coordinating and resolving stewardship issues and data definitions of data elements that cross multiple functional units
- Regularly coordinating with Chief Information Security Officer, Data Management Group, and General Counsel on management and security of data
- Assigning Data Custodians for their respective areas

3.2.3 Data Custodians / Security Officers

A data custodian is a University employee who has been assigned operational responsibilities for maintaining technical solutions and/or enforcing access procedures related to Institutional Data (including data maintenance roles). Data custodians often work in teams to document, implement, and monitor operational standards and procedures.

Responsibilities include:

- Maintaining technical solutions and executing procedures in compliance with relevant University policies, standards, and data steward requirements
- Managing Data User access and modification requests as authorized by appropriate Data Stewards
- Providing and updating procedures in conjunction with Data Stewards and Data Management Group

3.2.4 Data Users - Data Users are University units or individual University members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the University. This access is granted solely for the conduct of university business.

Responsibilities include:

- Using institutional data only as required for the conduct of university business within the scope of employment, affiliation with the University, or enrollment as a student
- Following the policies and procedures established to store data under secure conditions
- Complying with federal and state laws and regulations as well as university policies, procedures, and standards associated with data privacy
- Implementing safeguards prescribed for Confidential, Sensitive, and Internal Data
- Ensuring the appropriateness, accuracy, and timeliness of institutional data used for the conduct of university business
- Reporting any unauthorized access, data misuse, or data quality issues to the appropriate data steward for remediation
- Accepting and completing the University Confidentiality Statement if work duties require access to Confidential Data
- Completing any training required for access to a specific data set, such as FERPA or HIPAA training

3.3 Data Classifications

All data elements shall be classified in one of four data classification levels. All institutional records will be classified based on the data element(s) that have the most restrictive classification.

The following data classifications have been defined:

Data Classification Level	Description	Defined By
Confidential Data Examples: • Social Security Numbers • Credit Card Numbers • Bank Routing Numbers • Protected Health Info. Example Compliance Areas: NC Identity Theft Protection Act (GS 75-65) GLBA (CFI)	Data whose unauthorized disclosure and/or loss of control would reasonably result in significant financial losses, unacceptable risks, or impairment to the efficient conduct of the University mission. Confidential Data **often** have these attributes: • Protection of this data is prescribed within legal and/or contractual requirements. • Not considered a public record subject to disclosure (G.S. 132).	Office of General Counsel ITS Office of Information Security

HIPAA (PHI) PCI-DSS (CHD)	• Handling of this data addressed by detailed data security requirements.	
Sensitive Data Examples: • Employee Performance • Student Socioeconomic Indicators	Data that is considered private and must be protected, but has lesser degree of impact associated with unauthorized disclosure and/or loss of control versus Confidential Data. Sensitive Data **often** have these attributes: • Protection measures not prescribed by legal or contractual requirements. • Access rights established around identified processes and needs. • Handling of this data requires elevated data security requirements.	Data Stewards in consultation with Office of General Counsel and ITS Office of Information Security.
Internal Data Examples: • FERPA Academic Records • Non-Confidential Personnel Records • Budget and Salary Information	Data that is proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data. Internal Data **often** have these attributes: • Access established for fulfillment of daily business requirements • Handling of this data requires general security requirements.	Data Stewards
Public Data Examples: • Public Web Pages • Press Releases	Institutional information that has few restrictions or is intended for public use.	Data Stewards

3.5 Data Access Controls

Access to institutional data shall be driven by the application of a role based access control model. The two following role types will be applied when evaluating and implementing access requirements.

3.5.1 Data Maintenance Roles: The access for data maintenance in administrative systems will be determined based on the employee position and location, and will be governed by the business requirements as determined by the Data Custodians.

3.5.2 Data Inquiry Roles: The access for data inquiry will be determined by the required data set and associated data classification level, and will be governed by the Data Steward assigned the requested data set.

4.0 Enforcement, Exemptions, and Advisement

4.1 Authority and Enforceability - This standard is established under the authority of the Chief Information Security Officer (Information Security Policy 4.3.3). In the event of violation of this standard, the Chief Information Security Officer may require that non-compliant University practices be discontinued or temporarily suspended until the objectives of this standard (see section 3.0) are established and/or verified.

4.2 Exemptions - Exemptions to this standard must be undergo a formal risk evaluation and receive signed approval by the Data Trustees.

4.3 Review and Advisement - Collaborative advisement concerning these standards are provided by the Data Trustees, Chief Information Officer, Office of General Counsel, Data Stewards Council, Data Management Group, and Information Security Advisory Group.

5. Definitions

5.1 "Data" - Data refers to information created, gathered and consumed for reference or analysis.

5.2 "Data Element" - A data element is an atomic unit of data that has precise meaning or precise semantics.

5.3 "Administrative System" - A system at the University that contains institutional data, and is used for operation of business.

5.4 "Institutional Data" - Institutional data refers to one or more data elements that meets one or more of the following criteria:

- Any Data that originates in an academic or administrative system.
- Any Data contained within the University data warehouse.

5.5 "Data Classification" - A data classification is a common category of data elements that specifies their availability, access requirements, and requisite protection levels.

5.6 "Data Quality" is a perception or an assessment of data's fitness to serve its purpose in a given context.

5.7 "Data Set" - A data set is a discrete collection of data that is managed by an authorized University unit or individual.

5.8 "Data Maintenance" - The action of managing or editing the data inside an administrative system for the purpose of doing business at the University.

5.9 "Data Inquiry" - The action of querying data from an environment designed for that purpose with the intent of informing and influencing decision making.

6. REFERENCES

6.1 University Information Security Policy (Key Control Requirements 4.4.3.1, 4.4.3.2)

6.2 University Statement of Confidentiality

6.3 University Identity Theft Prevention Plan

6.4 University Payment Card Services Policy