Spelman College®
A Choice to Change the World

Policy Number	Policy Title
6003.00	Data Management & Access Policy

Contacts and Dates	
Responsible Office	**Policy Owner**
Spelman Technology Services	VP/CIO

Effective Date	Last Updated	Next Review
07-01-2016	08-01-2018	08-01-2019

Policy Description
Policy

Purpose

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to its access, or failure to maintain data quality or integrity.

The purpose of this policy is to define access, controls and protection of the College's administrative data. Administrative data maintained by the College is a vital information asset that will be available to all employees who have a legitimate need for it, consistent with the College's responsibility to preserve and protect the integrity of the data, and to ensure the privacy of sensitive data.

The College is the owner of all administrative data; individual units or departments have stewardship responsibilities for data domains, or portions of the data.

Designated Spelman College data domains, data trustees, and data stewards are listed in Appendix A – Listing of Spelman College Data Trustees and Data Stewards. Adjustments to Appendix A will be incorporated as additional enterprise data management systems are implemented, or as organizational and staffing changes warrant. Such changes will not be deemed a revision to this policy.

Scope

Administrative data captured and maintained at Spelman College are a valuable College resource. While data may reside in different database management systems or on different machines, this data in aggregate forms one overarching, enterprise administrative database.

This policy applies to all users of Spelman's administrative database environment and departmental file shares or shared drives.

Policy

Access to non-public administrative data is granted by the appropriately designated Spelman College Data Steward.

By authorizing access to designated categories of administrative data, Data Stewards are acknowledging a legitimate user need for information access, as well as appropriate training and understanding on the part of the requesting user to ensure ongoing administrative data integrity, quality, protection, and privacy. In addition to authorizing new administrative data access requests, Data Stewards are responsible for an annual review of user security access to their respective data domains.

By receiving access to designated categories of administrative data, the requesting data user is acknowledging responsibility for adherence to all relevant Spelman policies, procedures, standards and guidelines.

The College has defined three levels of data classification for administrative data:

- Public
- Restricted
- Highly Sensitive (Confidential)

Additional safeguards and protocols exist to further protect both Restricted and Confidential data, as appropriate.

Users are not to store personal information that is not College or business related, such as music, pictures, graphics or documents on departmental file shares or shared drives.

- **Public** - General administrative data that are intentionally made public are classified as Public Data. This includes all general administrative data that are not legally restricted or judged by Data Stewards to be limited access data. Examples of Public Data include the Spelman Master Course Schedule as well as faculty, staff and student directory data. Public Data are often readily available on Spelman's public website.

- **Restricted** - By default, all administrative data not explicitly defined as either highly sensitive or Public are classified as Restricted Data. Examples of Restricted Data include student grades and faculty/staff salaries.

Appropriate safeguards, including data access authorization and approvals by Data Stewards, must exist for all data that the College is obligated to protect, whether by law, contract, or College policy. Secure credentials are required to access restricted College data. Standards or guidelines governing the access, release, distribution and dissemination of restricted data by individuals authorized to access is controlled and administered by the designated Data Stewards.

- **Highly Sensitive (Confidential)** – By definition, highly sensitive (confidential) data is restricted and includes personal information that can lead to identity theft if exposed or disclosed in an unauthorized manner. Specifically, the college defines the following as highly sensitive data:

  The first name or first initial and last name in combination with and linked to any one or more of the following data elements about the individual:

  - Social security number
  - Driver's license number or state identification card number issued in lieu of a driver's license number
  - Passport number
  - Financial/banking account number, credit card number, or debit card number

Electronic Storage of Highly Sensitive Data Procedures - Additional safeguards and protocols must exist to ensure Spelman constituent privacy and to protect highly sensitive data from unauthorized exposure. Like Restricted Data, access to highly sensitive data may only be authorized by Data Stewards. Further, highly sensitive data must not be stored or kept on any non-network storage device or media. Prohibited storage media includes storage on desktop computers, laptop computers, tablets, cell phones, USB drives, thumb drives, memory cards, CDs, DVDs, local external hard drives, other USB devices and personal cloud storage account (i.e. Dropbox, iCloud, Google Drive) or other storage media not owned or approved by the College, unless specifically approved encryption methodologies have been utilized.

Further, highly sensitive data cannot be distributed, including via email or email attachments, unless via approved encryption methodologies.

Exceptions to the procedures for the electronic storage of highly sensitive data must be approved by the appropriate division Vice President in consultation with the Chief Information Officer. Approved exception requests will be documented to ensure the implementation of acceptable data encryption protocols.

RESPONSIBILITIES OF DATA TRUSTEES, DATA STEWARDS AND DATA USERS

Data Trustee: Data Trustees are the senior College officials (typically at the level of Vice President) who have planning and policy level responsibilities for data within their functional areas and management responsibility for defined segments of institutional data, or data domains. 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. Data Trustees typically serve as the executive sponsors of technology projects involving institutional data management.

Data Trustees work with the Chief Information Officer to prioritize data management related projects and to ensure that the appropriate resources are available to support the data needs of the College.

Data Trustee responsibilities include:

- Assigning and overseeing Data Stewards
- Overseeing the establishment of data policies in their areas
- Determining legal and regulatory requirements for data in their areas
- Promoting and ensuring appropriate data use and data quality
- Addressing institutional data issues that potentially a) compromise data integrity, reliability, or privacy, and/or b) limit or reduce institutional effectiveness or efficiency

Data Stewards: Data Stewards are appointed by Data Trustees. Data Stewards have primary responsibility for the accuracy, integrity, privacy, and security of the College data under his/her stewardship. They have overall responsibility for appropriate system use and data maintenance procedures within their areas, including the administration of any additional policies or procedures to govern the use of legally protected, restricted or sensitive College data. Additional responsibilities include:

- Communicating with and educating data users on appropriate use and protection of institutional data
- Developing and documenting procedures for requesting and authorizing access to restricted administrative data.
- Testing, approving, and authorizing the implementation (go-live or production) of new, upgraded, or updated software programs pertaining to administrative data management and the software system (i.e. Ellucian Banner
- Working with Spelman Technology Services (STS) and appropriate records management officials to determine data retention requirements and archiving strategies for storing and preserving historical operational data.

- Working with STS and the Power Users Group to ensure that a common set of data definitions are consistently used and applied to: a) facilitate data driven decision making, b) enhance the ability for automated system interfaces, and c) generally improve the electronic exchange of data across the enterprise.
- Assure data integrity, respond to questions about the accuracy of data, and correct inconsistencies.
- Assure data collection is complete, accurate, valid, timely, and that data are maintained as close as possible to the source or creation point of the data.
- Establish and maintain business rules regarding the manipulation, modification, or reporting of administrative data elements and to create derived elements in support of accurate data integration efforts, automated business process improvement projects, and/or other College planning and assessment efforts.
- Work with STS to monitor and periodically review (at least once annually) individual user security profiles and authorized data access.

Data Users: Data Users are the individuals who access College data (in accordance with authorization by the appropriate Data Steward) in order to perform their assigned duties or to fulfill their role in the College community. Data Users are responsible for the protection of: a) their access and authentication privileges, b) the proper use of the College's administrative data and its confidentiality, and c) privacy of individuals whose records they access. Users will comply with all reasonable protection and control procedures for administrative data to which they have been granted the ability to view, copy, download, create, modify or delete.

Users who violate this policy may be denied access to the College's information technology resources and may be subject to other disciplinary action, both within and outside of the College. Violations will normally be handled through the College's disciplinary procedures applicable to the relevant user. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed by the Office of Student Affairs. However, the College may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the College or other computing resources and/or to protect the College from liability. The College may also refer suspected violations of an applicable law to appropriate law enforcement agencies.

Definitions

To Whom Policy Applies

To whom and/or what the policy applies; lists groups who must know and adhere to the policy

☒ All College (Faculty, Staff, Students, Trustees, Contractors [unless otherwise negotiated])

□ Divisional

□ Unit/Department Specific

External Regulation (if applicable)

N/A

Tags

N/A

Implementation

Procedures

N/A

Monitoring

N/A

Exceptions/Exclusions (If applicable)

N/A

Background and History

Administrator Access (Policy Owner)

Review, Approval, and Change History: Policy is required to be reviewed annually

Date (MM-DD-YYYY)	**Reviewed by Policy Owner**	**Brief Description of Change** (if applicable)	**Change/Update Approved by** (title, not name)
01-01-2018	☒	Changed text due to outdated or inconsistent information	VP/CIO
	□		
	□		
	□		
	□		
	□		
	□		
	□		
	□		
	□		

Appendix A - Data Trustees and Data Stewards

Data Domain	Data Trustee	Data Steward
Undergraduate Admission Data	VP for Enrollment Management	Director of Admission
Traditional Student Academic Data, Course Schedules and Enrollment Data	VP for Enrollment Management	Registrar
Housing Data	VP for Student Affairs	Director of Housing & Residential Learning
Student Affairs / International Students & Community Standards	VP for Student Affairs	Assistant Dean of Students
Health Services Data	VP for Student Affairs	Director of Student Health Services
Counseling Services	VP for Student Affairs	Director of Counseling Services
Finance & Student Accounting Data	CFO/VP for Business and Financial Affairs	Associate VP / Controller
ID Card/Access Data ID Card	CFO/VP for Business and Financial Affairs	Director of Public Safety
Human Resource Data	CFO/VP for Business and Financial Affairs	Director of Human Resources
Payroll Data	CFO/VP for Business and Financial Affairs	Controller
Public Safety Data	VP for Student Development	Director of Public Safety
Student Financial Aid Data	VP for Enrollment Management	Director of Financial Aid
Advancement /Alumni Data	VP for College Relations	Director of Advancement Information Systems
Fund Raising and Donation Data	VP for Institutional Advancement	
Learning Management System Data	CIO/VP Spelman Technology Services	LMS Application Administrator
Parent Data	VP for Advancement	
Comparative Institutional Data	Provost and VP for Academic Affairs	Director, Institutional Research