Name of Policy: Southern University System Data Governance Policy **Policy Number:** **Issuing Authority:** SUS Office of the President **Initial Effective Date:** On Presidential Approval	**SOUTHERN UNIVERSITY SYSTEM POLICIES AND PROCEDURES**
___X___**New Policy Proposal** _____**Major revision of existing policy**	_____**Minor revision to existing policy** _____**Reaffirmation of exisitng policy**

I. Policy Statement

Institutional data are key information assets maintained to support the Southern University System's (SUS) central missions of teaching, research, and service. This data refers to collections of data elements relevant to the operations, planning, and/or management of any unit or division within the SUS, or data that are reported or used in official administrative reports. Accordingly, all such data must be consistently represented across all systems that use it, process it and report on it. The data must mean the same thing in every application, and have the same coded values throughout the SUS.

Moreover, to support effective and innovative management, institutional data must be accessible, must correctly represent the information intended, and must be easily integrated across all the SUS's information systems. Accordingly, the purpose of data governance is to develop system-wide policies and procedures which ensure institutional data meets the foregoing criteria within and across the SUS's administrative data systems, particularly student, financial and human resource systems.

The policy will further address the data governance structure and particularly includes policies on data access, data usage, and data integrity and integration. It applies to anyone employed by the SUS who creates data, manages it, or relies on it for decision-making and/or planning. However, it does not apply to data acquired or maintained by SUS personnel primarily for purposes of conducting academic research or to intellectual property that is considered to be educational materials.

This policy applies to all individuals and systems that may access institutional data, whether directly or through data conversion applications such as Microsoft Access, SAS and SPSS software programs.

Members of the University, working with or using institutional data in any manner must comply with extant federal, state and local laws; all applicable System and University policies, procedures and standards; and all applicable contracts and licenses. In particular, users of institutional data must be cognizant of and adhere to federal

Family Education Rights and Privacy Act (FERPA) guidelines. All users of institutional data and their supervisors are responsible for complying with the aforementioned laws, policies and guidelines.

And finally, it is imperative to stress that data governance authority rests ultimately with the SUS President and respective campus Chancellors. As such, this policy will define specific roles and responsibilities of University employees and administrative staff that will assist them in fulfilling this responsibility.

II. Policy Goals

The goals of this SUS data governance policy are to:

A. Protect the privacy and security of data and information under the stewardship of the SUS;

B. Support a culture of responsible data use for informed and actionable decision-making;

C. Promote an integrated view of data across organizational boundaries in the SUS;

D. Promote the efficient use of resources to meet the data and information needs of the SUS community; and

E. Increase the SUS's transparency and accountability to external stakeholders and the public by promoting access to relevant and reliable information.

III. Policy Purpose

The objectives of this policy additionally are to:

A. Set forth best practices for effective data management, with ongoing objectives of increasing efficiencies, managing and mitigating information privacy and security risks, and promoting data quality;

B. Establish a set of standardized terms and definitions to promote consistent interpretations and implementations of policies, procedures, and practices related to data management; and

C. Establish clear lines of accountability and decision-making authority through the definition of roles and responsibilities related to data management.

IV. Best Practices

A. Institutional data is the property of the SUS and shall be managed as a key asset. Institutional data will be managed through defined governance guidelines, standards, policies and procedures.

B. Unnecessary duplication of institutional data is discouraged—Data Custodians (defined below) shall be responsible for sharing institutional data out of official Systems of Record (defined below) when reasonable and according to policies and procedures, so as to minimize redundant storage and processing of that data in multiple repositories. Exceptions will be allowed for purposes of business continuity and fail-over.

C. Unnecessary updating of institutional data is discouraged—When the same institutional data elements exist in multiple Systems of Record, the official values must be kept synchronized. When feasible, manual updates of institutional data should be performed in one institutional record and then automatically copied to as few other additional data repositories as possible. This eliminates redundant processing, increases integrity, and provides better auditing capabilities.

D. Quality standards for institutional data shall be defined and monitored—Data quality standards shall be defined, published, communicated, managed, and applied according to the reliability and risk levels established by appropriate Data Stewards (defined below). Examples of data quality standards include: data validation rules, timeliness of updates, defined error rates, integrity monitoring processes, etc.

E. Institutional Metadata shall be recorded, managed, and utilized— Metadata will be used to model, define, and organize data in order to maximize the value of institutional data. Institutional Metadata will be published and communicated clearly and consistently.

F. Necessary maintenance of institutional data shall be defined— Maintenance of institutional data to ensure appropriate backup, retention, destruction, de-identification, etc. will be defined by appropriate Data

Custodians and Information Technology Resource Management (ITRM) personnel and other system operators.

G. Institutional data shall be protected—Institutional data must be safeguarded and protected according to approved security, privacy and compliance guidelines, laws and regulations established by the SUS, the State of Louisiana and the federal government.

H. Institutional data shall be accessible according to defined needs and roles—Institutional data and Institutional Metadata shall be accessible to all in accordance with defined access and use policies and procedures determined by the Data Management Team/Data Integrity Committee (defined below) and Data Custodians. Users requesting access shall be assigned to appropriate roles that have clear documented guidelines in accordance with all SUS, State of Louisiana and federal laws and regulations.

I. Institutional representatives will be held accountable to their roles and responsibilities—Roles and responsibilities for data management will be clearly defined, and individuals assigned to specific roles will be held accountable to performing data management responsibilities, as a part of their regular job responsibilities.

V. Definitions

A. With regard to SUS Data Governance operations, the terms below are defined as follows:

1. ***Census Date*—**the day when official enrollment is taken for each campus in the SUS. It is the 14th day of instruction for each semester.

2. ***Census Data*—**is all campus enrollment data collected on the Census Date and in conformance with required reporting specifications as established by the Louisiana Board of Regents. Data compliance certification is the responsibility of the Chancellor or a senior level designee. Census data represents the official numbers for mandated reports to the federal government, state agencies, accrediting bodies and various national organizations.

3. ***Classification of Instructional Programs (CIP)***—is the national program classification standard used by colleges and universities in collecting, reporting, and interpreting data on educational programs**.** CIP codes provide a program classification scheme by identifying programs that are broadly similar and grouping them together in terms commonly understood in the field of higher education.

4. ***Code(s)—***are used to classify specific data reporting variables as required for annual financial reporting, GRAD Act performance attainment, Act 1465 Strategic Planning compliance, Board of Regents Annual reporting requirements, Integrated Postsecondary Education Data System (IPEDS) and other external reporting requirements critical to institutional funding maintenance, grant acquisition and retention.

5. ***Confidential Data—***means (i) institutional data that could, by itself or in combination with other such data, be used for identity theft or related crimes, (ii) institutional data whose public disclosure is restricted by law, contract, University policy, professional code, or practice within the applicable unit, discipline, or profession, (iii) records of the University's security measures, and (iv) unauthorized disclosure in advance of the time prescribed for its authorized public release, or whose unauthorized disclosure would otherwise adversely affect the University financially.

6. ***Cross-walk—***is a tool designed to aid users in determining how a program code alpha characters are used when compiling reports for Financial Statements, IPEDS, budget and Facilities and Planning.

7. ***Data Custodian—*** is an individual who has been authorized to be in physical or logical possession of data by the Data Owner (defined below). These individuals are further responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems. The data custodian also has responsibility for ITRM systems that create, receive, store, process or transmit institutional data.

8. ***Data Dictionary—***is a reference tool which provides a description of all the institutional data elements and is a database system that functions as a repository which contains comprehensive information about the SUS's institutional data and documentation of SUS information administrative systems.

At a minimum, the following information should be included in the Data Dictionary:

- Element identification. Information is included to identify each element uniquely, with descriptive components.
- Stewardship responsibility. Every data element will have a designated Data Steward listed in the dictionary.
- Security level. Every data element will be assigned a security level which will be used to determine levels of access.
- Data source of record. Each element has only one System of Record. This information identifies the official name for the element, where it is stored, how it is entered, and what valid values exist for it.
- The system name and the element name used in that database will be the primary key to the registry database.
- Allowable values and validation tables.
- Other names used on reports or on screens to identify a particular element.
- Other systems that use this element. This is an opportunity to document processes that use the same element.

9. ***Data Element—*** is a single data item. For example, a person's name is a data element.

10. ***Data Integrity—***refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element.

11. ***Data Management Team/Data Integrity Committee (Team/Committee)—***members will be responsible for providing guidance and recommendations for strategic directions and priorities, creating and maintaining policies and procedures, creating and overseeing special task groups, and assisting with the development of proposals for special data management needs.

Committee members will be appointed by the Chancellor of each respective campus. Chancellor appointments must include a campus Institutional Research staff person as committee chair. Further, this committee will be responsible for communicating, creating awareness, and making data management policies and procedures available to appropriate data management personnel. This entity shall additionally be responsible for maintaining a web site that includes information and links to relevant, policies and procedures, communicating the status of task force projects, and informing all data management personnel of best practices for managing institutional data. And finally, the Team/Committee will be responsible for the coordination of all internal and external data reporting efforts, meeting state and federal reporting compliance requirements, and ensuring that institutional data in the official System(s) of Record meet SUS business policies.

12. ***Data Owner—***the SUS is the owner of all institutional data; individual units or divisions may have stewardship responsibilities for portions of that data.

13. ***Data Stewards—***have charge over institutional data and are responsible for its safekeeping. Each data steward is responsible for operational policies and procedures governing inquiry and download access, dissemination, usage, collection, maintenance, and protection of the data in a designated data area. The data steward is further responsible for the definition and classification of data in that area as well as verifying its authenticity as needed. Documentation characterizing shared institutional data will be maintained and made available for University use. A data steward may also delegate any or all of his/her data administration duties to another University administrator known as a Data Custodian, however, the data steward retains ultimate responsibility.

14. ***Data Warehouse—***A collection of official institutional databases which hold data for transactions systems and other databases, for the purpose of reporting and queries.

15. ***End-User/Data User—***is any individual who, in order to fulfill their job duties and responsibilities, requires access to institutional information and are therefore granted access. Users are responsible for understanding and complying with all applicable University policies, procedures, and standards for dealing with institutional information and its protection.

16. ***Institutional Data*—**are all of the data and records held by the SUS, in any form or medium, for the administration, operation, or governance of the SUS. Governance scope includes all administrative divisions, units, and affiliated campuses.

17. ***Institutional Database*—**is a collection of information that is organized so that it can easily be accessed, managed, and updated. This database is categorized by such mission critical functions as student progression, financial aid, institutional financing and human resources. For functional areas, information is collected, stored and arrayed in accessible formats for institutional decision-making and external reporting requirements.

18. ***Institutional Information*—**is defined as a collection of institutional data which can be contained in any form, including, but not limited to, documents, databases, spreadsheets, e-mails and websites; represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof; communicated in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and recorded upon any form, including, but not limited to, papers, maps, films, prints, discs, drives, memory sticks, and other information systems.

19. ***Institutional Metadata*—**"Institutional Metadata" is data collected, maintained, and used to describe and define the processes around the management of institutional data. Examples of Institutional Metadata include:

    - Definitions regarding the purpose, usage and context of institutional data;
    - Identification of which system is the official System of Record for institutional data;
    - Who is responsible for management of institutional data;
    - How institutional data is transferred, derived, and stored;
    - What security and privacy practices are used to safeguard institutional data; and
    - Risk and compliance classification for institutional data.

20. ***Integrated Post-Secondary Education Data System (IPEDS)***—is a system of interrelated surveys conducted annually, which gathers information from every college, university, and technical and vocational institution in the United States and other jurisdictions

(such as Puerto Rico) that participates in the federal student financial aid programs**.** It further provides basic data needed to describe—and to analyze trends in—postsecondary education in the United States, in terms of the numbers of students enrolled, staff employed, dollars expended, and degrees earned. Congress, federal agencies, state governments, education providers, professional associations, private businesses, media, students and parents, and others rely on IPEDS data for this basic information. IPEDS data are used at the federal and state level for policy analysis and development and at the institutional level for benchmarking and peer analysis.

21. ***Key holder*—**is a person designated by the SUS to have in their possession the necessary User ID and password to gain access to the Integrated Postsecondary Education Data System (IPEDS) data collection system to complete the survey. The key holder is further responsible for entering data and locking it into the site by each survey completion date.

22. Louisiana Board of Regents Annual Reporting Requirements—

Due Date	Item
January 15*	Statewide Student Profile System, prior Fall Semester
January 31	Aid to Independent Application— Fall Semester
January 31	Quarterly Energy Report
February 16	Student Credit Hour Report (for applicable academic year) Cycle 2
March 4—April 15	IPEDS, (for academic year) Spring Collection
March 15	Statewide Student Profile System, Winter Quarter (LA Tech only)
March 31	Endowed Professorships/Endowed Scholarships
April 30	Quarterly Energy Report
May 1	Certified Campus GRAD ACT Reports
May 15	Student Credit hour Report (for applicable academic year) Cycle 3
May 15	Employee Data System, Spring (for applicable academic year) Semester

***NOTE 1: Actual dates listed above may vary from academic year-to-year and may also vary due to previously designated holidays or closures scheduled by Louisiana state government.**

Due Date	Item
May 18	Annual Tuition and Mandatory Fee Survey, FY (for applicable academic year)
June 15	Statewide Student Profile System, Spring Semester
June 15	Aid to Independent Application—Spring Semester
July 1	Statewide Completers System (applicable academic year)
July 31	Quarterly Energy Report
Early September (applicable year)	Capital Outlay Submission
September 2	Operating Budgets Without Prior Year Actuals
September 3	Annual Tuition and Mandatory Fee Survey FY (applicable academic year)
September 3—October 15	IPEDS, (applicable academic year) Fall Collection
September 7	Operational Fee Pursuant to R.S. 17:3351A(5)(d)(v)
September 15	Student Credit Hour Report (applicable academic year) Cycle 1
September 22	Preliminary Enrollment Survey, Fall (applicable year)
October 1	Operating Budgets With Prior Year Actuals**
October 1st or *120 days after Close of Trust Fund Year*	Financial Reports on Endowed Chairs, Professorships and Scholarships
October 10	Financial Aid Data System
October 15	Act 971 Reports
October 15	Operating Budgets—Non-Formula Entities
October 15	LTC Campuses—Facilities Inventory and Space Utilization System
October 31	Independent Auditors Report for Endowed Chairs, Professorships and Scholarships
October 31	Quarterly Energy Report
November 15	Employee Data System, Fall (applicable academic year) Semester
November 15	Facilities Inventory and Space Utilization System
December 3—January 21	IPEDS, (applicable academic year Winter Collection

****NOTE 2: In support of operational plans and quarterly reporting, SUS campuses are required to update ACT Plans every three (3) years.**

23. ***System of Record—*** is an information system that is designed by a Data Steward as holding official values of institutional information. Official values are the data designed as the most accurate representation of the meaning and context of institutional data elements, which are recorded as facts. Official values are not necessarily the originally entered values, and as such, a System of Record may not necessarily be the system where values are originally entered. When questions arise over the meaning or interpretation of data elements or their values, the System of Record is used to resolve discrepancies.

24. ***University—***refers to the Southern University System which includes the following campuses: Southern University and A & M College at Baton Rouge (SUBR); Southern University at New Orleans (SUNO); Southern University at Shreveport, Louisiana (SUSLA); Southern University Law Center (SULC); and the Southern University Agricultural Research and Extension Center (SUAREC).

VI. Data Governance Structure

Data Governance is the practice of making strategic and effective decisions regarding the SUS's information assets. It assumes a philosophy of freedom of access to institutional data by all members of the University coupled with the responsibility to adhere to all policies and all legal constraints that govern that use. In the interest of attaining effective data governance, the SUS applies formal guidelines to manage the University's information assets and assigns staff to implement them.

A. The following roles and responsibilities are defined, for both individuals and groups, for the purpose of establishing clear governance and accountabilities over institutional data. The terms and conditions for appointments and assignments are outlined for each.

1. **SUS President—**The SUS President, as the head of a State of Louisiana educational institution, has ultimate responsibility for the University's security program and the protection of restricted and highly sensitive data and critical system assets. The President has delegated these responsibilities in the following manner:

    a. **Vice President for Academic and Student Affairs—** the Vice President for Academic and Student Affairs is the lead institutional officer responsible for developing and implementing the University's data governance program. Authority and responsibility resides with the Vice President

for Academic and Student Affairs on policy and System-wide issues.

b. **SUS Director of Institutional Research—**as a voting ex-officio member of the Data Management Team/Data Integrity Committee, he/she oversees the office that maintains the System of Record for student-related data and information and is the official reporting entity for student-related data and information for the SUS. This office leads the University's efforts around data quality and works collaboratively with system and campus leadership to improve the consistency and accuracy of operational and policy research data within the University's administrative data systems. The individual updates the Data Management Team/Data Integrity Committee on data quality issues and is responsible for decisions around mediating and correcting inconsistencies in data definitions.

c. **Chancellors, System Vice-Presidents and Directors—** Chancellors, System vice-presidents and directors (collectively referred to as SUS leadership) have authority and responsibility over policies and procedures regarding access and usage of data within their delegation of authority. The Data Management Team/Data Integrity Committee serves in an advisory capacity to SUS leadership on strategic matters and conflict resolution issues.

d. **Vice President for Information Technology Resource Management (ITRM)—**The Vice President for Information Technology Resource Management is responsible for setting and enforcing standards and guidelines for data management technologies and systems related to computing infrastructures, data processing performance, data delivery and integration, data architectures and structures, metadata repositories, and access control mechanisms.

e. **Data Stewards—**Institutional data shall have one or more designated stewards. Data Stewards are typically senior administrators responsible for functional operations such as Finance and Business, Human Resources, Student Services and other activities that involve institutional information processing.

Data Stewards also ensure applicable federal, state and SUS policies, standards, regulations and laws are met with regard to data in their respective areas. They are further responsible for minimizing the use, storage and exposure of sensitive information. And finally, they have responsibility to restrict the use and exposure of such information to those specific situations where it is essential and appropriate.

f. **Data Custodians—**are the managers and/or administrators of systems or media on which sensitive data resides, including but not limited to personal computers, laptop computers, PDAs, smartphones, departmental servers, enterprise databases, storage systems, magnetic tapes, CDs/DVDs, USB drives, paper files and any other removable or portable devices. Any authorized individual who downloads or stores sensitive information onto a computer or storage device becomes a data custodian through that act.

   Data Custodians are further responsible for implementing and administering controls over the resources according to policies and parameters provided by data stewards. Data Custodians are responsible for the technical safeguarding of sensitive information, including ensuring security transmission and providing access control systems approved by data stewards to prevent inappropriate disclosure.

g. **Users—**are any individuals who, in order to fulfill their job duties and responsibilities, require access to sensitive information, and are therefore granted access. Users are responsible for understanding and complying with all applicable University policies, procedures, and standards for dealing with sensitive information and its protection.

VII. Data Access Policy

A. Purpose

The purpose of the data access policy is to ensure that University employees have appropriate access to institutional data and information. While recognizing the University's responsibility for the security of data, the procedures established to protect that data must not interfere unduly with the efficient conduct of University business. This policy applies to all

University units and divisions and also to all uses of institutional data, regardless of the offices or format in which the data reside.

B. Statement of Policy

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuses, misinterpretation, and unnecessary restrictions to its access.

The SUS will protect its data assets through security measures that assure the proper use of the data when accessed. Every data item will be classified by the relevant data steward to have an appropriate access level. Data access will be conducted in accordance with the policies established by the SUS Office of Information Technology Resource Management (ITRM).

VIII. Data Usage Policy

A. Purpose

The purpose of the data usage policy is to ensure that University data are not misused or abused, and are used ethically, according to any applicable law, and with due consideration for individual privacy. Use of data depends on the security levels assigned by the data steward.

B. Statement of Policy

University personnel must access and use data only as required for the performance of their job functions, not for personal gain or for other inappropriate purposes; they must also access and use data according to the security levels assigned to the data. Data usage falls into the categories of *update, read-only, and external dissemination.*

Authority to *update* data shall be granted by the appropriate data steward only to personnel whose job duties specify and require responsibility for data updating. This restriction is not to be interpreted as a mandate to limit update authority to members of any specific group or office but should be tempered with the University's desire to provide excellent service to faculty, staff, students, and other constituents.

Read-only usage to administrative information will be provided to employees for the support of University business without unnecessary difficulties/restrictions.

C. Consequence of Noncompliance with Data Usage Policy

University employees and students who fail to comply with the Data Usage Policy will be considered to be in violation of relevant codes of conduct and may be subject to disciplinary action or to legal action, if state and/or federal laws have been violated. In less serious cases, failure to comply with this policy could result in denial of access to data.

IX. Data Integrity and Integration Policy

A. Purpose

The purpose of this policy is to ensure that University data have a high degree of integrity and that key data elements can be integrated across functional units and electronic systems so that University faculty, staff, and management may rely on data for information and decision-making support.

Data integrity refers to the validity, reliability, and accuracy of data. Data integrity relies on a clear understanding of the business processes underlying the data and the consistent definition of each data element.

Data integration, or the ability of data to be assimilated across information systems, is contingent upon the integrity of data and the development of a data model, corresponding data structures, and domains.

B. Statement of Policy

University data will be consistently interpreted across all University systems according to the best practices agreed upon by the Data Management Team/Data Integrity Committee, and will have documented values in all SUS systems. Data administration will ensure that the needs of users of University data are taken into consideration in the development and modification of data structures, domains, and values. It is the responsibility of each data steward to ensure the correctness of the data values for the elements within their charge.

University data are defined as data that are maintained in support of a functional unit's operation and meet one or more of the following criteria:

1. The data elements are key fields, that is, integration of information requires the data element;

2. The University must ensure the integrity of the data to comply with internal and external administrative reporting requirements, including institutional planning efforts;

3. The data are reported on or used in official administrative University reports; and

4. A broad cross section of users requires the data.

It is the responsibility of each data steward, in conjunction with the Data Management Team/Data Integrity Committee, to determine which core data elements are part of University data.

Documentation (metadata) on each data element will be maintained within a University repository according to specifications provided by the Vice SUS Director of Institutional Research and the Data Management Team/Data Integrity Committee. These specifications will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is derived and used. The interpretation will include acceptable values for each element, and any special considerations, such as timing within an academic calendar.

All University employees are expected to bring data problems and suggestions for improvements to the attention of the appropriate data stewards, the SUS Director of Institutional Research and/or the Data Management Team/Data Integrity Committee.

X. Implementation

The President delegates to SUS leadership or his/her designee(s) the authority to implement all provisions and to make such revisions to and interpretations of this policy that are deemed necessary for its proper administration.

Effective implementation further requires recognition of the fact that this established data governance policy is based on recent public sector mandates and accreditation requirements related to strategic planning, systemic based evaluation, performance accountability and fiscal integrity. Specifically, all campuses within the SUS are required to maintain data systems which support strategic and performance based funding goals as outlined in the following Louisiana legislative enactments: Act 1465, 741, and

418 and legislative Acts 741 and 418 which are more commonly referred to as the GRAD Act.

The SUS's established data systems will support systemic based evaluation and institutional effectiveness principles as found in SACS core requirement 2.5 and comprehensive standard 3.3.1. Additionally, these developed systems will support campus administrative activities for Title III, Carl Perkins and other related intergovernmental grant awards.

And finally, current Louisiana GRAD Act legislation requires the SUS's management board to establish implementation policies or initiatives to support target goal attainment activities related to ***Student Success, Articulation & Transfer, Workforce Development, Institutional Efficiency, and Human Resource Reporting.*** Performance assessment data is derived from Louisiana Board of Regents mission critical data profiles reports, IPEDS surveys, the Louisiana Workforce Commission, and Office of Planning and Budget. Data source origination will be limited to individual campuses. Data governance responsibilities of the SUS requires establishment of the foregoing policy and procedural framework which emphasizes the attainment of conformity, consistency, clarity, and relevance in data quality.