ADMINISTRATIVE DIVISION UNIV University Administration		**POLICY NUMBER** UNIV 1.51
POLICY TITLE Data and Information Governance		
SCOPE OF POLICY USC System – All Campuses	**DATE OF REVISION** March 20, 2025	
RESPONSIBLE OFFICER Vice President of Information Technology and Chief Information Officer	**ADMINISTRATIVE OFFICE** Division of Information Technology	

PURPOSE

The University of South Carolina System (USC) recognizes that its data and information are critical institutional assets. The university is dedicated to implementing governance programs that promote responsible usage, ensure data availability for informed decision-making and operational support, and proactively manage risks. These governance programs are designed, developed, and sustained to serve the interests of the University of South Carolina System and its diverse stakeholders.

DEFINITIONS AND ACRONYMS

Access: describes authorization to view or use a given resource or asset, such as data or an information system.

Artificial intelligence (AI): technology that increasingly enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy. Applications and devices equipped with AI often include, but are not limited to, the following capabilities: can see and identify objects; can understand and respond to human language; can learn from new information and experience; can make detailed recommendations to users; can sometimes act independently, potentially replacing or reducing the need for human intervention.

Constituents: persons and entities that have a relationship to any organizational unit of the university system, including but not limited to: students (prospective students, applicants for admission, enrolled students, campus residents, former students, and alumni), employees (faculty, staff, administrators, student employees, prospective employees, candidates for employment, former employees and retirees), and other affiliates (including but not limited to board members, consultants, contractors, donors, invited guests, recipients of goods and services, research subjects, service providers and volunteers).

Data Classification: describes parameters of a Data Element reflecting risk, sensitivity (including whether the Data Element contains Personal Identifying Information, or PII), data type, and what controls and measures must be applied to protect it from unauthorized access and use. Data Classification also applies to assets, including storage hardware and systems, media, transmission or presentation, information systems, databases, and other data assets. If multiple data elements with different classifications are present in a file or repository, whether individually or combined, the classification of the file or repository is equivalent to the highest

classification of any data element present. The university adheres to the State of South Carolina data classification schema:

- **Public Information:** Information intended or required for sharing with the public.
- **Internal Use:** Non-sensitive information that is used in daily operations of the university.
- **Confidential:** Sensitive information used by the university, including PII.
- **Restricted:** Highly sensitive information used by the university that is protected by statutory penalties if disclosed in an unauthorized manner, including PII.

Data Custodians: personnel who maintain hardware, information systems/databases, applications, backup systems, and networks through which data is transmitted, processed, and stored. Custodians may be university personnel or personnel/service providers under agreement or contract with the university.

Data Element: denotes a discrete and purposeful, often single, point of information; also known as a field, column, variable, or object.

Data and Information: refers to the individual or collective values, content, media (including audio, visual, and multimedia), intellectual property, official reports, and work products that the university and its units collect, process, transmit, store, or maintain. This encompasses all details about university constituents, business processes, events, operations, and services. In the context of Artificial Intelligence, data also includes inputs used to train AI models and algorithms, which transform raw data into meaningful insights, predictions, and decision-making tools. These AI-driven processes enable the university to enhance its operations while ensuring the responsible and ethical handling of data in compliance with applicable laws and regulations (see policy UNIV 1.51 Data and Information Governance).

Data Standards: conventions and services adopted to ensure appropriate and consistent use of data and information across the university system.

Data Stewards: oversee the capture, maintenance, storage, use, and dissemination of University Data and information for a particular function or operation; they may be considered System Owners for stores and systems they purchase, operate, or contract with a third party/service provider to operate and/or host. The official roster of designated Data Stewards, as confirmed by Data Trustees, is maintained by the Office of the Vice President for IT and CIO or designee and may be accessed online (see Roster of Data Stewards).

Data Subjects: persons, objects, transactions, events, and activities about which data is created and managed.

Data Trustees: have strategic planning and policy-making responsibilities with implications for University Data. Data Trustees designate Data Stewards for the organizational units under their

care. Individuals identified in the University Policy Responsible Officer List, shall be Data Trustees, with additional individuals designated when necessary or beneficial.

End User (or User): refers to any person or system that accesses university assets including data and information systems.

Enterprise Information System: denotes a system-wide university resource that exists to manage essential administrative functions and transactions. Primary examples include but are not limited to Banner (student information system), PeopleSoft (human resources, administration and finance information system), Data Warehouse/Operational Data Store, and Oracle Identity Management.

Executive Data Governance Council (EDGC): a decision-making body that provides strategic, cross-functional expertise, leadership, and collaboration to improve the use of data and information across the University of South Carolina.

Information System: denotes a database, file, application, filing system, or other system that is used for a limited business function and is not necessarily available on all system campuses or to all departments on a single campus.

Permissions: describes what activities a Data User is enabled to perform with the access they have been authorized for and granted; often based on job duties or function; also known as user rights.

Personal Identifying Information (PII): data elements that are used as identifiers for persons, and which if compromised may present a significant risk of defrauding a person's identity. Under South Carolina Code of Laws, Section 16-13-510 (D), PII includes social security numbers, driver's license number or state identification number, banking account numbers, date of birth, digital signatures, and current and former names and addresses, among others.

Unit Record: unique data record ascribed to the identity of a person, device, or object, as well as the data elements and data values pertaining to them.

University Data: information deemed critical to the mission and operation of the university. Such data is often managed and distributed or exchanged across multiple organizational units within and beyond the university. An item may be university data if it meets one or more of the following criteria:

- at least two organizational units use the data and consider it essential;
- integration of information systems requires the data;
- the university must ensure the integrity, privacy, or security of the data to comply with legal, regulatory, competitive, or external reporting requirements;
- a broad cross section of users refer to or maintain the data;

- the university needs the data to plan, manage, audit, or improve its operations;

- unauthorized access to or use of the data represents an unacceptable risk to the university or its Constituents, including data protected by the Family Educational Rights and Privacy Act (FERPA).

This definition excludes other information that is public record, personal property, intellectual property, academic research data, or content directly related to or produced through teaching and learning activities.

POLICY STATEMENT

A. Data is vital to the university and the university retains rights to all data, content, and information the university collects, produces, transmits, and stores regarding its Constituents, services, programs, and operations. This system-wide policy sets forth the framework and responsibilities for governance of University Data and information.

   The framework is directly applicable to administrative data, information, and content that support the operation of the university, primarily in the domains of student records, human resources, and administration and finance. This includes but is not limited to administrative and academic functions and transactions, as well as unit records of Constituents and objects.

   This policy is not binding upon content produced for or by teaching and learning activities, nor upon academic research data that may be generated or maintained through activities, outputs, and findings of university faculty, students, and staff (see policy RSCH 1.05). However, with appropriate adaptation, the principles and framework of data governance presented here may be extensible and beneficial to academic research data.

B. All divisions, campuses, organizational units, and individuals shall be responsible for supporting the objectives and activities of data governance and are responsible for assuring that data and information are collected and managed in accordance with this and other applicable policies, procedures, and practices.

C. The Office of the Vice President for IT and CIO or designee shall coordinate and collaborate with stakeholders of University Data and information systems to implement, administer, and continuously improve data and information governance, through a framework of programs including: Executive Data Governance Council, Data Stewardship; Data Standards; Data Quality & Integrity Assurance; Business Intelligence & Analytics.

D. Data Stewards, under the Executive oversight of the Executive Data Governance Council, shall establish and enforce practices and procedures that are binding on organizational units and users, including Data Custodians, that provide, receive, store, or manage University Data and information under the Data Steward's care. They must deeply consider requests for data – especially data feeds and integrations – and weigh the expected value for university Constituents, operational excellence, and competitive advantage against potential or real risks when deciding whether or not to approve. Under normal circumstances, Data Stewards make

authoritative and final decisions about data in their care; when necessary, concerns may be escalated to their respective Data Trustee.

Subject to federal and state law and regulation as well as directives of the Board of Trustees and university policy, Data Stewards are responsible for the following with respect to data, information, and related assets under their care:

1. determine and document classification of data elements and data repositories;

2. ensure an Information Security risk review is conducted for data feeds, integrations, and hosted solutions; based on noted risks and risk rating, specify security and privacy controls and verification of capabilities and practices to be assured prior to approval. Note that there is no risk rating that negates approval; Data Stewards must weigh expected value against risk, while requiring controls that mitigate or minimize risks.

3. with respect to End Users, review requests for data sharing or use, including acknowledgment and acceptance of responsibilities, and determine minimum satisfactory parameters under which requests may be approved (or, alternatively, denied), and assign access and permissions to University Data, information, and systems (internal and external), organizational units, system integrations; these decisions often must be memorialized as User Agreements and/or Data Sharing Agreements (see policy UNIV 1.52);

4. with respect to Third-party Hosting, Processing, Services, and/or Storage of data, review and determine acceptability, including acknowledgment and acceptance of responsibilities, conditions, and controls applicable to requests for University Data, information, and related systems prior to implementation/execution of agreements; with rare exception these decisions must be memorialized as contract addendums included in contract approvals, and/or supporting Data Sharing Agreements (see policy UNIV 1.52);

5. with appropriate controls and restrictions, ensure broad access to University Data that improves and modernizes user experience, and/or enables institutional and organizational unit operations, reporting, business intelligence, and decision support;

6. actively represent the concerns and interests of his/her organizational unit through participation in the Data Stewardship Group; and

7. carry out activities and directives approved by the Data Trustee to whom he or she reports, and in coordination with the Executive Data Governance Council.

E. Data Trustees shall be responsible for data-related strategic planning and policy approval for all organizational units under their charge that manage or receive University Data; for designating and managing Data Stewards of these units; and for assuring that Data Stewards and their organizational units actively support the policy, programs, and guidelines of data and information governance. Data Trustees shall enumerate data stewardship as an essential and serve as the escalation path and decision maker for concerns not resolved at the Data Steward level.

F. The Executive Data Governance Council serves and represents the entire USC System and is a component of a broader IT governance framework.

G. System Owners, including those intending to acquire new systems and services that require University Data, must timely involve Data Stewards whose data are required, afford them professional courtesy, and honor the latitude they need to determine permissibility and conditions under which data may be shared. This includes following all Purchasing and contract-related policies and procedures with sufficient lead time.

H. Data Custodians will implement policies, standards, guidelines, and other requirements applicable to University Data and information systems through their respective roles. They are responsible for notifying Data Stewards, the Office of the Vice President for IT and CIO or designee, the Chief Information Security Officer, and other appropriate university personnel of any significant potential or known risks, and for making recommendations that will improve the security, privacy, integrity, and availability of data, systems, and integrations.

I. Data Custodians, Data Stewards, and Data Trustees will consult the Office of the Vice President for IT and CIO or designee as well as the Executive Data Governance Council when preparing information system implementations and upgrades in order to facilitate assessment, identification, and implementation of appropriate data governance strategies, including but not limited to data definitions and data sharing agreements.

PROCEDURES

A. Implementation and Administration. The Office of the Vice President for IT and CIO or designee is responsible for system-wide administration of this policy; the framework and programs are supported by organizations, organizational units, personnel, and systems, working in concert to continuously improve practices, adherence, and issue resolution. The framework's programs are:

   1. Data Standards, Quality and Integrity Assurance

   2. Data Stewardship

   3. Analytics & Business Intelligence

B. Oversight. The Office of the Vice President for IT and CIO or designee shall establish organizations for data and information governance, including but not limited to establishing goals and key performance indicators that align data governance to the USC System's strategic priorities and initiatives.

RELATED UNIVERSITY, STATE AND FEDERAL POLICIES

South Carolina Department of Administration, Division of Technology, Policies and Procedures
ACAF 1.33 Intellectual Property Policy
ACAF 3.03 Handling of Student Records

ACAF 7.03 Private Requests for University Data
BRTU 1.20 Dishonest Acts and Fraud
FINA 8.12 University Identity Theft and Detection Program
HR 1.22 Telecommuting
HR 1.69 Official Personnel Files and Records Release
IT 1.00 Information Technology Procurement
IT 3.00 Information Security
LIB 1.03 Archives and Records Management
RSCH 1.05 Data Access and Retention
UNIV 1.52 Responsible Use of Data, Technology, and User Credentials
UNIV 2.00 Freedom of Information Policy

HISTORY OF REVISIONS

DATE OF REVISION	REASON FOR REVISION
June 30, 2016	Revised to clarify the intended scope of the policy; to provide a definition for University Data; and to reference Enterprise Data Standard 1.07 – University Data Identification Guide (posted as draft). Item I.A.7 ensures system implementations include data governance practices from inception and that system upgrades consider such practices wherever practical.
February 9, 2018	Non-substantive corrections to web addresses for referenced documents, 2/9/2018
December, 13, 2019	Revised to place responsibility for Identity & Access Management with a different unit in DoIT, to rename the program now called Business Intelligence and Analytics, and to place oversight of data and information governance on the IT Executive Board rather than a Data & Information Strategy Council. Other minor revisions are included, including reformat to the current policy template.
March 20, 2025	Removed use of assets, which posed confusion. Amplified the complexity and rigor of Data Steward consideration for data sharing requests, adding emphasis to weighing expected value for university constituents operations against potential risks. Updated language for conciseness and confirmed all linked ULRs in document. “Chief Data Officer” was replaced with the “Office of the Vice President for IT and CIO or designee” Added a definition for Artificial Intelligence (AI)