NUMBER: UNIV 1.51

SECTION: University Administration

SUBJECT: Data and Information Governance

DATE: June 30, 2016

REVISED: May 5, 2017

Policy for: All Campuses
Procedure for: All Campuses
Authorized by: President
Issued by: President's Office

---

## I. Policy

*The University of South Carolina System (USC) acknowledges that its data and information are vital and valuable assets and is committed to establishing governance programs that ensure the appropriate use, availability, and risk mitigation for data and information assets. Data and information governance programs are developed, implemented, and maintained for the benefit of the University of South Carolina System and its Constituents.*

### A. Policy Statement

1. Data is a vital university asset 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 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, 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 RSCH 1.05, Research Data Access and Retention). However, with appropriate adaptation, the principles and framework of data governance presented here may be extensible and beneficial to academic research data.

2. 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.

3. The Chief Data Officer 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: Data Stewardship; Data Standards; Data Quality & Integrity Assurance; Identity & Access Management; and Reporting, Analytics, and Decision Support.

4. 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 job duty for appropriate direct reports.

5. Data Stewards shall establish and enforce practices and procedures that are binding on organizational units and users that provide, receive, store, or manage University Data and information under the Data Steward's care. 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:
    a) determine and document classification of data elements and assets;
    b) understand and apply security and privacy standards, guidelines, and practices (see IT 3.00, Information Security);
    c) review requests and determine, approve, and assign access and permissions to University Data, information, and systems for End Users (internal and external), organizational units, system integrations, as well as sharing agreements;
    d) review and determine acceptability, conditions, and controls applicable to requests for University Data, information, and related systems to be processed, stored, or hosted by a third-party, prior to processing or storage;
    e) prior to issuing access and permissions (internal and external), verify that users or third parties have acknowledged and accepted responsibility for appropriate use and confidentiality of data, technology, and user credentials (see UNIV 1.52, Responsible Use of Data, Technology, and User Credentials);
    f) with appropriate controls and restrictions, ensure broad access to University Data that enables institutional and organizational unit operations, reporting, business intelligence, and decision support;
    g) actively represent the concerns and interests of his/her organizational unit through participation in the Data Stewardship Council; and
    h) carry out activities and directives approved by the Data Trustee to whom he or she reports.

6. 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 Chief Data Officer, and the Chief Information Security Officer 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.

7. Data Custodians, Data Stewards, and Data Trustees will consult the office of the Chief Data Officer 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.

## B. Definitions

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

2. **Constituents** are 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, and volunteers).

3. **Data** is information that is known and/or values that describe characteristics or quantities of a being, object, transaction, or event. Data may be used interchangeably with the terms content and information. See also *University Data*.

4. **Data Classification** describes parameters of a Data Element reflecting risk, sensitivity, data type, whether the Data Element contains Personally Identifiable Information (PII), 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 an asset, whether individually or combined, the asset's classification is equivalent to the highest classification of any data element present. The university adheres to the State of South Carolina data classification schema:
    a) **Public Information:** Information intended or required for sharing with the public.
    b) **Internal Use:** Non-sensitive information that is used in daily operations of the university.
    c) **Confidential:** Sensitive information used by the university, including PII.

d) **Restricted:** Highly sensitive information used by the university that is protected by statutory penalties if disclosed in an unauthorized manner, including PII.

5. **Data Custodians** are 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.

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

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

8. **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 Chief Data Officer and may be accessed online (see http://tinyurl.com/jj6rp7k).

9. **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 (see UNIV 1.00, Policy on Policies, Appendix 1) shall be Data Trustees.

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

11. **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.

12. **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.

13. **Permissions** describe 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.

14. **Personally Identifiable Information (PII)** are 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, PII includes social security numbers, driver's license number or state identification number, banking account numbers, date of birth, and digital signatures, among others.

15. **Unit Record** is a 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.

16. **University Data** is 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:
    a) at least two organizational units use the data and consider it essential;
    b) integration of information systems requires the data;
    c) the university must ensure the integrity, privacy, or security of the data to comply with legal, regulatory, competitive, or external reporting requirements;
    d) a broad cross section of users refer to or maintain the data;
    e) the university needs the data to plan, manage, audit, or improve its operations;
    f) 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.

    Note: to assist users in determining whether or not particular data is considered University Data, refer to Enterprise Data Standard 1.07 – University Data Identification Guide (see http://tinyurl.com/UniversityDataID).

## II. Roles and Responsibilities

### A. Implementation and Administration

The Chief Data Officer is responsible for system-wide implementation and administration of this policy; the framework and programs are supported by organizations, organizational units, personnel, and systems, working in concert to continuously improve policy, procedures, guidelines, practices, understanding, and issue resolution for data and information systems. The framework's programs are:

1. Data Quality and Integrity Assurance
2. Data Standards
3. Data Stewardship
4. Identity and Access Management
5. Reporting, Analytics, and Decision Support

**B. Supervision**

The Vice President for Information Technology and Chief Information Officer is responsible for supervision of the Chief Data Officer; chairs the Data and Information Strategy Council; promotes the principles of data governance and information literacy at the executive level; and reviews and approves changes to this policy before they are advanced to the Data and Information Strategy Council.

**C. Oversight**

The Data and Information Strategy Council has ultimate oversight of and decision-making authority for data and information governance, including but not limited to establishing goals and key performance indicators that align data governance to the university system's strategic priorities and initiatives. The Council members shall be appointed by the President, ensuring representation of functional areas across the System's regional and comprehensive campuses.

## III. Related Policies

State of South Carolina Policies

Department of Administration, Division of Technology, Policies and Procedures, see http://www.admin.sc.gov/technology/information-security/policies-and-procedures

University Policies

| | |
|---|---|
| ACAF 1.33 | Intellectual Property Policy |
| ACAF 3.03 | Handling of Student Records |
| ACAF 7.03 | Private Requests for University Data |
| BUSF 4.12 | University Identity Theft and Detection Program |
| BRTU 1.20 | Dishonest Acts and Fraud |
| 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 |

## V. Reason for Revision

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.