NUMBER: UNIV 1.50 (Formerly ACAF 7.02)

SECTION: University Administration

SUBJECT: Data Access

DATE: February 1, 1995

REVISED: August 6, 2010

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

I. Policy

The purpose of this policy is to establish standards to manage, protect, secure and control system institutional data that will promote and support the efficient conduct of University business. The objective of this policy is to minimize impediment to access of this data, yet provide a secure environment.

A. Policy Statement

1. Information collected, stored on and accessible by university systems and utilized by university employees and students in support of the educational mission is a vital university asset. The University of South Carolina system (hereinafter, “University”) retains exclusive rights to all computing systems and data and is the legal custodian of all University data; and has delegated to Data Trustees the responsibility for the system-wide implementation of this policy.

2. Data Trustees will determine, approve and assign the level of access to institutional systems and data based on employee responsibilities, job functions or reporting requirements subject to restrictions as imposed by state and federal laws; the Board of Trustees; as well as ethical, competitive and practical considerations. The procedures established by Data Trustees to protect the data must not create undue barriers to accessing information.

3. The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. Employees accessing data must: adhere to applicable state and federal laws, statutes, and regulations; must comply with protection and control procedures as defined by the institution; and must accurately present the data in any use.

B. Definitions, Data Ownership and Accountability

1. **Institutional Data:** The University's data consists of information critical to the mission of the University system. Such data is shared and is likely distributed across processing units within the University. Data may be stored in various forms, including but not limited to paper, digital text, graphics, images, sound, or video. The University considers information to be institutional data if it meets any of the following criteria:

   a. at least two organizational units of the University use the data and consider the data essential;

   b. integration of related information requires the data;

   c. the University must ensure the integrity of the data to comply with legal, regulatory and other external reporting requirements;

   d. a broad cross section of users refer to or maintain the data; or

   e. the University needs the data to plan, manage, or audit its operations.

   Some examples of institutional data include student course grades, student and employee payroll and personnel information, and accounting and financial records.

2. **Data Trustees** are senior management personnel (typically at the level of Vice President, Associate or Vice Provost, or Dean) who have planning and policy-making responsibilities for data in their operational area, system-wide. As a general rule, USC System Data Trustees delegate Data Trustee responsibilities to Chancellors of senior institutions and Deans of regional institutions for data that pertain to their respective institutions. The Data Trustees are responsible for overseeing the establishment of data management policies and procedures.

3. **Data Stewards** are managers of functional areas (typically at the level of Controller, University Registrar, Director of Admissions or Director of Human Resources) who oversee the capture, maintenance, and dissemination of data for a particular operation. Data Stewards are responsible for making security decisions regarding access to the data under their charge. Their responsibilities also include other activities that may be delegated by a Data Trustee.

4. **Data Users** are individuals who access University data in order to perform their assigned duties or to fulfill their role in the University community. Data Users are responsible for protecting their access privileges and for proper use of the University data they access.

5. **General access data** are all data that are not either restricted or judged by Data Trustees to be limited-access data. The accessible data volume should be as great as possible to enable those who need the information to have access. Data should be part of an open atmosphere and broadly available. Under the Freedom of Information Act, general access data are subject to disclosure to all USC employees as well as the general public.

6. **Limited access data** are data that the Data Trustees judge to require special procedures for access. Limited access data may be subject to disclosure under the Freedom of Information Act. Limited access data are made available to a select group of USC employees based on their job function.

7. **Restricted data** are those data found upon review by the Data Trustees or General Counsel to require restrictions on access. Restricted data may not be subject to disclosure under the Freedom of Information Act or other laws and regulations. Restricted data are only available to USC employees that have a business, research, or educational need to access the data.

C. Implementation and Oversight

The Vice President for Information Technology and Chief Information Officer is responsible for the system-wide implementation of this policy. The Data Administration Advisory Committee (DAAC) is a standing committee appointed by and advisory to the Vice President for Information Technology and Chief Information Officer. The DAAC membership includes a minimum of a representative from each Operational Area (as defined below in Section II.A.1. Data Trustee Assignment).

On an ongoing basis, the DAAC will review policy implementation on all campuses and recommend policy revisions to the Vice President for Information Technology and Chief Information Officer when necessary. The DAAC is also responsible for ensuring that data access procedures across all operational areas are consistent and accessible.

II. Procedure

A. Data Trustee Assignment

1. The University determines levels of access to administrative data according to principles drawn from various sources. State and federal laws and regulations provide for restriction of certain types of information. Ethical, competitive and practical considerations also will guide decisions with regard to data access. The following table establishes institutional data operational areas and the responsible Data Trustee:

OPERATIONAL AREA	**DATA TRUSTEE**
Financial (including payroll)	Vice President for Finance and Planning and Chief Financial Officer
Human Resources Data	Vice President for Human Resources
Sponsored Research Data	Vice President for Research and Graduate Education
Alumni & Development Data	Vice President for Development and Alumni Relations
Student General (including admissions, records, financial aid, advising data) and other Academic Data	Vice President for Academic Affairs and Provost
Student Medical, Housing, Counseling, Discipline, and non-academic services data	Vice President for Student Affairs, Vice Provost for Academic Support, and Dean of Students
Information Technology Data	Vice President for Information Technology and Chief Information Officer
Campus Operations and Facilities	Vice President for Finance and Planning and Chief Financial Officer
Data Pertaining to Only a Senior or Regional Institution	Chancellors of Senior Institutions and Deans of Regional Institutions

2. The President, or his designee, will make decisions regarding division of responsibility where multiple Data Trustees are involved. The Data Trustees will make decisions regarding division of responsibility where multiple Data Stewards are involved. In the event that data exists or is created that falls outside the existing data trustee operational areas above, the executive responsible for the organizational unit will be considered the interim trustee until a permanent assignment can be made.

3. For data pertaining to only a senior or regional institution, the respective Chancellor or Dean is the Data Trustee and may assign a local Data Steward. For data that is reported or maintained in a centralized manner across the system, campus-specific Data Trustees may not be applicable.

B. Responsibilities of Data Trustees and Data Stewards

1. **Data Trustees** are responsible for authorizing data sources and elements for their operational area, categorizing the data access type (i.e. general, limited or restricted access) and determining who should be authorized to access data. These responsibilities may be delegated to a Data Steward.

2. **Data Stewards** (working with Data Trustees) will define standard views of institutional data to aggregate data from multiple sources, to segment data into smaller and more manageable subsets, or to segregate data according to confidentiality or similar characteristics. The list of Data Stewards is available at the USC data warehouse home page: http://datawarehouse.sc.edu/.

   a. Each Data Steward is responsible for establishing and making known data access procedures that are unique to his/her specific information resource or set of data elements. They are responsible for addressing such items as rules and conditions for accurate presentation, data definition, data capture, maintenance, archiving, and security requirements. Requirements established by Data Stewards must adhere to University system IT policies and standards established by the Office of the Vice President for Information Technology and Chief Information Officer.

   b. Each Data Steward is also responsible for advanced and timely notification of any proposed changes in database structure, data definitions, rules and conditions for accurate presentation and other changes to data or data access that affect the University.

   c. Each Data Steward is responsible for ensuring that the relevant data access policies and procedures are publically available at the USC data warehouse home page: http://datawarehouse.sc.edu/.

C. Responsibilities of Data Users

1. Data Users are responsible for protecting their access privileges and for proper use of the University data they access. Users should not disclose or distribute institutional data in any medium, except as required by job responsibilities and approved in advance by the appropriate Data Steward. Users will respect the confidentiality and privacy of individuals whose records they access; observe any ethical restrictions that apply to data to which they have access; and abide by applicable laws and policies with respect to access, use, or disclosure of information.

2. All Data Users who have access to restricted or limited-access data will formally acknowledge their understanding of the level of access provided and their responsibility to maintain the confidentiality and security of data they access.

3. All levels of management are responsible for ensuring that all Data Users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff according to their job functions, and for ensuring a secure office environment. The head of each unit will authenticate the need for individual access to data and must request and obtain authorization for access to data from the appropriate Data Steward.

4. Administrative and academic unit heads are responsible for taking the necessary steps to ensure that data access is terminated for employees who transfer to another department within the University or leave employment of the University.

III. Related Policies

See also:
University Policy ACAF 1.33 Intellectual Property Policy
University Policy ACAF 3.03 Handling of Student Records and the Notification of Student Rights under FERPA
University Policy BRTU 1.20 Dishonest Acts and Fraud
University Policy IT 1.06 Network Access and Acceptable Use
University Policy RSCH 1.05 Data Access and Retention
University Policy HR 1.00 Freedom of Information Policy
University Policy HR 1.69 Official Personnel Files and Records Release
University Policy LIB 1.03 Archives and Records Management

IV. Reason for Revision

Policy moved from Academic Affairs (ACAF) to University Administration (UNIV) policy division, and policy oversight moved to Office of the Chief Information Officer.

This revision represents a substantial re-write of the previous policy.

The purpose of these revisions is to establish standards that support the efficient conduct of University business, while taking into account today's environment for information storage, protection and use. The over-arching principles and high-level procedures from the previous policy remain mostly intact and are the framework of revised policy. However, items that change with the evolution of business processes and technology, such as data definitions and procedures, have been removed. These items are considered operating procedures to be published and maintained separately by the respective data stewards in a centralized and transparent manner.