Regulations Library

The University of Utah

Policy: 4-001 Rev:
Date: March 11, 1996

Policy 4-001: University Institutional Data Management Policy

I. Purpose

Institutional Data is a valuable University asset. It is information about University constituencies students, faculty, staff, resources (funds, space, etc.) that is captured and used in the day-to-day services and operations of the University. It is used as the basis for administrative reports, both internal and external to the University. It enables administrators to assess the needs of the University community and modify services accordingly. It is vital not only in the day-to-day operations of the University, but to short and long-term planning as well.

The purpose of this policy is to protect this valuable asset, permit the sharing of it through accurate and consistent definitions, and provide a coordinated approach to its use and management. In all cases, applicable state and federal statutes and regulations that guarantee either protection or accessibility of institutional records take precedence over this policy.

II. Introduction

Institutional Data is a subset of the University's Information Resources. Information Resources include any information in electronic or audio-visual format, or any hardware or software that makes possible the storage and use of such information. This definition includes, but is not limited to electronic mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, digitized information, and electronic communication systems. The use and management of University Information Resources is governed by the University Information Resources Policy, which is separate from this policy. This policy deals only with the subset of Institutional Data.

Institutional Data consists of data that is acquired or maintained by University employees in performance of official administrative job duties. Typically, this is data that is: relevant to planning, managing, operating, or auditing a major function at the University; referenced or required for use by more than one organizational unit; or, included in an official University administrative report. Examples of systems/databases that contain Institutional Data include, but are not limited to:

A. Master Academic Records System (MARS)
B. Human Resource System (HRS)
C. Financial Accounting System (FAS)
D. Financial Aid Management System (FAMS)
E. Billing and Receivable System (BRS)
F. Budget
G. Space
H. Property Management
I. Office of Sponsored Projects
J. Benefits
K. Job Application
L. High School Services
M. Faculty
N. Alumni
O. Development
P. Scheduling

Specifically excluded from the definition of Institutional Data are:

Personal medical, psychiatric, or psychological data for both employees and patients seen at University Clinics; Notes and records that are the personal property of individuals in the University community; Research notes, data, and materials; Instructional notes and materials; and Data that results from sponsored research projects.

III. References

A. Policy and Procedures (??-yet to be created), Information Resources Policy
B. Policy and Procedures (??-yet to be created), Creation of New Organizations

C. Physical Security of University Data University of Utah Institutional Data Management Guidelines

D. **Utah Code Ann. 63-2-101 et seq.**, Government Records Access and Management Act

E. **Utah Admin. Code R805-2**, Government Records Access and Management Act Procedures

F. **Department of Education 34 CFR Part 99**, Federal Family Education Rights and Privacy Act

IV. Definitions

A. Access - the right to read, copy, or query data.

B. Data - the electronic representation of discrete facts.

C. Data Administration - the function of applying formal guidelines and tools to manage the University's information resources.

D. Data Dictionary - a repository that contains comprehensive information about Institutional Data.

E. Data Managers - University officials and their staff who have operational-level responsibility for data capture, data maintenance, and data dissemination.

F. Data Stewards - University officials who have policy level responsibility for managing a segment of the University's information resource.

G. Data Users - full-time and appropriately designated part-time employees of the University of Utah who access Institutional Data in performance of their assigned duties.

H. Institutional Data - data that is acquired or maintained by University employees in performance of official administrative job duties. Specifically excluded from the definition of Institutional Data are: personal medical, psychiatric, or psychological data for both employees and patients seen at University Clinics; notes and records that are the personal property of individuals in the University community; research notes, data, and materials; instructional notes and materials; and data that results from sponsored research projects.

I. Institutional Data Management Committee - the committee that establishes overall policy and guidelines for the management of and access to the University's Institutional Data.

J. Institutional Data Model - a diagram that illustrates the data entities that comprise the Institutional Database and the relationships among those entities.

K. Institutional Database - the physical implementation of the Institutional Data Model. The Database is a combination of (1) centrally stored data elements, and (2) references to non-centrally stored data elements.

L. Information Management - a suborganization within Administrative Computing Services responsible for the Institutional Data model.

M. Shared data - a subset of Institutional Data; data that is updated by more than one organizational unit.

N. University Vice President - administrators who have been appointed by the President of the University to the position of Vice President.

V. Policies

A. Ownership

Institutional Data is not owned by a particular individual, organization or system; the University, as a whole, owns all Institutional Data and the subsets thereof.

B. Data Classifications and Access

All Institutional Data is considered University-internal unless specifically classified as Public or Limited-access. The permission to access Institutional Data will be granted to all eligible employees of the University for legitimate University purposes according to the data classifications.

If Institutional Data is requested by an off-campus entity or by a University employee for non-University purposes, Data Stewards will identify the appropriate classification for each data element according to the State of Utah's Government Records Access and Management Act and the administrative Procedures set forth in the Utah Administrative Code.

For University data users, Institutional Data is classified by Data Stewards under the direction of the Institutional Data Management Committee according to the following levels of required security:

1. Public - is available to the general public; no prior authorization is required.
2. University-internal - is available to all eligible employees without restriction or prior authorization for use in conducting University business.
3. Limited-access Data - will be made available to eligible employees who need access to such data to perform their job duties and have received authorization from a Data Steward or other authorized individual.

C. Management

Institutional Data is an asset of the University and will be managed as a strategic asset to improve the efficiency of the University of Utah. Institutional Data will be managed according to Institutional Data Management Guidelines.

D. Roles and Responsibilities

1. Institutional Data Management Committee

   The Institutional Data Management Committee (IDMC) is an official University committee that reports to the Administrative Systems Advisory Committee (ASAC), which reports to the Vice President for Administrative Services. The IDMC may create subcommittees and task forces as needed to manage Institutional Data.

   Committee members are appointed by University Vice Presidents and may include Supervisory Personnel, Data Stewards, Data Managers, Data Users, Administrative Computing Services Data Administrators, and other campus employees.

   It is the responsibility of the IDMC to enforce the University's Institutional Data Management Policy. Other responsibilities include:

   a. Access - defining a single set of Procedures for requesting permission to access data elements in the Institutional Database, and, in cooperation with Data Stewards, documenting these common data access request Procedures.
   b. Conflict Resolution - resolving conflicts in the definition of centrally-used administrative data attributes, data policy, and levels of access.
   c. Data Administration - overseeing the administration and management of all Institutional Data.
   d. Data Definitions - creating standard definitions for shared elements.
      i. Developing Procedures for standardizing code values and coordinating maintenance of look-up tables used for Institutional Data.
      ii. Determining update precedence when multiple sources for data exist.
      iii. Determining the most reliable source for data.
   e. Database Management:
      i. Establishing policies that manage Institutional Data as a University resource.
      ii. Identifying data entities and data sources that comprise the Institutional Database. As this is an on-going process, the committee will add data entities and sources to the Institutional Database as circumstances require.
      iii. Prioritizing the management of Institutional Data. This includes identifying which data is most critical and assigning management priorities to all data entities and sources.
   f. Institutional Data Model - overseeing the establishment and maintenance of the Institutional Data Model.
   g. Shared Data Management - defining attributes and assigning maintenance responsibilities.
   h. Other responsibilities as set forth in the Institutional Data Management Guidelines.

2. Data Stewards

   Data Stewards, as individuals, have administrative and management responsibilities for segments of the Institutional Database within their functional area. Data Stewards are appointed and supervised by University Vice Presidents. Specific responsibilities include:

   a. Access - processing requests for access to Limited-access data.
   b. Data Classification - classifying each data element according to University definitions (Public, University-internal, and Limited-access) and the state's Government Records Access and Management Act (Public, Private, Controlled, Protected).
   c. Documentation - ensuring that proper documentation exists for each data element.
   d. User Support - providing consulting services as needed to assist data users in the interpretation and use of data elements.
   e. Data manipulation, extracting, and reporting - ensuring proper use of Institutional Data and setting policies regarding the manipulation or reporting of Institutional Database elements.
   f. Data quality, integrity, and correction - ensuring the accuracy and quality of data and implementing programs for data quality improvement.
   g. Data storage - identifying official storage locations and determining archiving requirements for data elements.
   h. Other responsibilities as set forth in the Institutional Data Management Guidelines.

3. Data Managers

   Data Managers are appointed by Data Stewards. Data Managers report to Data Stewards and coordinate Institutional Data management tasks with other Stewards, Data Managers, and Information Management. Among their responsibilities are any data administration activities that may be delegated by the Data Stewards. Specific responsibilities also include:

   a. Access - defining and documenting data access Procedures that are unique to a specific information resource or set of data elements.

b. Data collection and maintenance - ultimately responsible for collecting complete, accurate, valid, and timely data, and maintaining data.

c. Data security - monitoring access and defining recovery Procedures.

d. Documentation - ensuring that adequate documentation exists for each data element under their purview.

4. Supervisory Personnel

Every University of Utah employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of Institutional Data is responsible for implementing and ensuring compliance with the University's Institutional Data Management Policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for:

a. Communicating the policy to employees.

b. Establishing specific goals, objectives, and action plans to implement the policy and monitor progress in its implementation.

c. In coordination with the appropriate Data Stewards, developing plans for information systems and database development that satisfy both departmental and institutional information needs.

d. Actively supporting strong data management through Data Administration and unit Data Stewards.

e. Providing education and training in data management principles to employees.

5. User Responsibilities

All data users are expected to:

a. Access Institutional Data only in their conduct of University business.

b. Review information created from the data to ensure, to the extent of their ability, that the analysis results are accurate and the data has been interpreted correctly.

c. Respect the confidentiality and privacy of individuals whose records they may access.

d. Observe any ethical restrictions that apply to data to which they have access.

e. Abide by applicable laws or policies with respect to access, use, or disclosure of information.

Actions contrary to these expectations are considered misuses of University property.

E. User Support

The initial contact for access to or use of Institutional Data is the Administrative Computing Services Help Desk (581-3323). Additional information about User Support is contained in the Institutional Data Management Guidelines.

F. Security

As an institutional asset, Institutional Data will be protected from deliberate, unintentional or unauthorized alteration, destruction, and/or inappropriate disclosure or use in accordance with established institutional policies and practices. Specific guidelines for securing Institutional Data are detailed in the Institutional Data Management Guidelines.

Approved: Board of Trustees 3/11/96