Legislative History of Policy 4-001 Revision 1

http://regulations.utah.edu/it/appendices_4/4-001Rev1_LegisHist.pdf

Prepared by Bob Flores, for the Institutional Policy Committee.

This revised Policy was approved by the Academic Senate December 1, 2008 and the Board of Trustees December 8, 2008, with designated effective date of December 8, 2008.

From the agenda of the Academic Senate:

Executive Committee Nov. 17, Academic Senate December 1, 2008.

The Information Technology Council approved the first draft of this revision on April 12, 2007. On July 1, 2008, the Office of Information Technology revised the policy to conform to the new format of the University of Utah Regulations Library. This revision was approved by the Information Technology Council on August 14, 2008. On November 17, 2008 the Academic Senate Executive Committee approved forwarding the proposed revision to the Academic Senate as an item for debate and approval.

The Executive Committee concluded that this Policy is sufficiently 'academic' in nature so that under the terms of U-Policy 1-001 the proposal is presented to the Senate for its debate and approval.

* * * *

Executive Summary—proposal to revise University Policy 4-001 Institutional Data and Information Management and Access

This policy replaces the University Institutional Data Management Policy that was written in 1996. *The primary purpose of the revision is to balance the competing needs for access to information and the security of information.*

What does this policy do?

1. Defines in general terms what institutional data is and isn't (administrative vs. academic/research)
2. Establishes the role of the Chief Information Officer as the person responsible for making information securely and reliably available to individuals and organizations for the performance of the business of the University.
3. Defines the role of governance committees and councils.
4. Defines levels of responsibility for the stewardship, management, and consumption of institutional data.
5. Defines policy in terms of principles:

a. Data is valuable and should be used.
b. Data is accessible for the appropriate purposes.
c. Appropriate purposes include (among other purposes):
    i. Improving services to campus.
    ii. Increasing the understanding, usefulness, ease of use of data.
    iii. Improving efficiency.
d. Use is subject to “best practices” including appropriate security.
e. Data must be kept accurate, complete, and current.
f. Appropriate access to data should not be delayed or withheld.
g. Data Steward is responsible for security, validity, correctness of data, and conditions of use of the data.
h. Data Steward may pre-approve data for ready access.
i. Denied or delayed requests may be appealed to the designated governing body. The CIO renders the final decision.

Proposed revised version (Revision 1)

Policy 4-001: Institutional Data and Information Management and Access Policy

I. Purpose and Scope

This policy applies to those official and/or authoritative data that are critical to the administration of the University, regardless of whether the data are used or maintained by administrative, health sciences, patient care, or academic units. While these data may reside in different database management systems and on different machines, in aggregate they may be thought of as Institutional Data. This Policy does not apply to data acquired or maintained by University personnel primarily for purposes of conducting academic research, and reference should be made to other University Policies regarding maintenance and use of such data, including those in Part 7 of the University Policies.

This policy describes general principles of management, security, and access that should be applied in order to maintain the value and guarantee effective use of Institutional Data and Information.

II. Definitions

A. Institutional Data -- Data that are acquired or maintained by University employees in the 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 Hospitals or Clinics; notes and records that are the personal property of individuals in the University community; research notes, data, and materials; and instructional notes and materials.

B. Information -- For the purpose of this policy, Information is Institutional Data that is grouped and/or organized for use in a context required by Data Users. For example, student Institutional Data may be grouped and organized to provide Information in the form of enrollment reports or other contextual information required by Data Users.

C. Campus Chief Information Officer (CIO) -- The person that is responsible to ensure that the University's Institutional Data and Information are securely, reliably and optimally used to further the mission of the University.

D. Information Technology Council (ITC) -- A representative body with members from University colleges, divisions, and departments. ITC oversees campus information technology plans, policies, processes, and investments that support the University's mission.

E. Information Technology Executive Committee (ITEC) – A Committee consisting of the CIO, Data Stewards, information technology directors, and other individuals as designated by the CIO. The ITEC is a subcommittee of the ITC. The ITEC advises the CIO regarding the application of policies and procedures intended to ensure that Institutional Data are securely, reliably and optimally used to further the mission of the University. The ITEC advises the CIO to assist in the prioritization of IT projects that depend on limited IT resources, and the resolution of appealed denials of Institutional Data access requests and appeals regarding the prioritization of access requests.

F. Data Steward -- A University official who has planning and policy-level responsibilities for access and management of Institutional Data in his or her functional areas. A Data Steward is appointed by the Vice President who is responsible for the Data Steward's functional area. For example, the Vice President for Student Affairs appoints the Registrar as the Data Steward over student data.

G. Data Custodian -- The organization or individual who implements the policy, procedures and best practices defined by the Data Steward, and has responsibility for IT systems that create, receive, store, process or transmit Institutional Data.

H. Data Administrators -- University staff members that, under the direction of the Data Custodian, have day-to-day operational responsibility for data capture, maintenance and dissemination. Data Administrators may also include departmental data and network systems managers and their staff.

I. Data Users -- Individuals and organizations that access Institutional Data and Information in order to perform their assigned duties or to fulfill their role in the university community.

J. Best Practices -- Accepted management and access procedures that Data Custodians, Data Administrators and Data Users follow to ensure security, accessibility, and integrity of Institutional Data. The Data Steward is responsible for specifying Best Practices and identifying adequate resources that enable Data Custodians and Data Administrators to implement Best Practices. Best Practices change as technology, procedural improvements, and the nature of the data change. Because Best Practices are subject to change, they will be described in documented procedures that reference this policy.

III. Policy

A. The value of Institutional Data is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access.

B. Data Users will be granted secure access to view or query all Institutional Data based on the "need to know" in order for the individual or campus organization to perform all legitimate administrative, health care, research, academic and other

official responsibilities pertaining to the mission of the University, examples of which include but are not limited to planning, decision making, official reporting, etc.

C. The “need to know” exists when certain conditions are met, including but not limited to the following:

    1. The Institutional Data are needed to improve services to faculty, staff, students, patients, and other University constituents.

    2. Access to Institutional Data increases the understanding, usefulness, and ease of use of the data, and/or maximizes efficiency of human, physical, and digital resources.

    3. Integration of Institutional Data with other data and information or applications increases the value of the Institutional Data to those who may use it.

D. Curiosity does not constitute a “need to know.” Access to Institutional Data for academic research and inquiry may be approved subject to privacy rules and regulations, and appropriate institutional review.

E. Access to Institutional Data will be granted subject to Best Practices for data and information management and analysis and should minimize duplication of data and information capture, storage, maintenance and retrieval.

F. Institutional Data will be kept accurate, complete, and current to the fullest extent that is practicable.

G. Requests for Institutional Data and Information will be handled in a timely manner.

H. Access to Institutional Data and Information will not be unreasonably withheld.

I. Security and Integrity of Institutional Data

    1. Data Stewards and Data Users that possess or access Institutional Data accept full responsibility for the Institutional Data or subsets of Institutional Data that are in their possession and must adhere to the requirements of Policy 4-004 to protect private sensitive and critical data from unauthorized access or loss. The University Information Security, Privacy, and IT Compliance Office must approve security procedures.

    2. Data Stewards and Data Users that access Institutional Data are responsible for the integrity, validity, and correctness of Institutional Data that are in their possession and must incorporate editing and validation checks to ensure the integrity and validity of such data. When Data Users identify errors in official Institutional Data, they must work with the Data Stewards and Custodians to correct the Institutional Data. If Information that is derived from Institutional Data cannot be reconciled with the official

Institutional Data, it cannot be considered official Institutional Data or presented as such.

J. Institutional Data Access and Use

1. Access to Institutional Data is subject to University of Utah rules, regulations, and policy, and all relevant state and federal laws.

2. Institutional Data access may be requested by Data Users. A request may include various data and information types depending on the purpose and context of the data or information to be presented to the requester.

3. Data access may be requested from one or multiple Data Stewards depending on the purpose and context of the data or information request.

4. The Data Steward may designate, pre-approve, and make accessible certain Institutional Data elements for the legitimate business of the University, subject to the user's ability to comply with conditions of use set forth by the Data Steward and the rules and regulations that govern the data.

5. The Data User will apply for access to Institutional Data that is not pre-approved using a process specified by the Data Steward(s). The actual process may vary depending on the rules, regulations and conditions of use that govern the data.

6. The Data Steward is responsible for clearly specifying the conditions of use of requested Institutional Data. The Data User requesting access will be required to comply with the specified conditions of use. Non compliance with the conditions of use may result in penalties and sanctions allowed by University regulations. The Data Steward will periodically review request process and conditions of use.

7. Data Users should request access to Institutional Data and Information through a Data Steward. The Data Steward(s), will determine whether or not the context of the data or information that is requested changes the data and information such that they cannot be reconciled with official Institutional Data or presents the data or information such that it cannot be maintained as current with the Institutional Data. In these cases, the requester must be informed that the requested data or information should not be considered official Institutional Data and should not be represented to any other party as official Institutional Data. The Data Steward may require that the presentation of the data or information in the form of reports, web pages, paper documents, email, or other forms include a disclaimer that indicates that the data or information are not official Institutional Data.

8. Data Stewards are responsible to ensure that Data Users who receive access to Institutional Data agree to comply with the conditions of use

specified by the Data Stewards and all University policies, rules and regulations that govern the Institutional Data.

9. If a request is denied or placed in a low priority by a Data Steward, the Data Steward must provide documentation to the requester that describes the reason(s) why the request was denied or placed in a low priority.

10. If a request is denied or placed in a low priority by a Data Steward, the requester may appeal the Data Steward's decision by forwarding the request to the CIO. The CIO may convene the Information Technology Executive Committee (ITEC). If convened, the ITEC will review the request, receive presentations from the Data Steward and the requester, and make recommendations to the CIO based on the principles of data and information management and access outlined in this policy. The CIO will render a decision regarding the appeal.

IV. Rules, Procedures, Guidelines, Forms and other related resources.

A. Rules [insert]

B. Procedures [insert]

C. Guidelines [insert]

D. Forms [insert]

E. Other related resource materials [insert]

V. References:
Policy 4-002, Information Resources Policy
Policy 4-003, World Wide Web Resources Policy
Policy 4-004, University Information Technology Resource Security Policy

VI. Contacts:
Policy Officer: Chief Information Officer
Policy Owner: Director of Planning and Policy
Office of Information Technology
801-585-3314
IT_Policy@utah.edu

VII. History:
Revision 0 of this policy originally took effect March 11, 1996 as PPM 1-12.
Revision 1. The Information Technology Council approved the first draft of this revision on April 12, 2007.
On July 1, 2008, the Office of Information Technology revised the policy to conform to the format of the University of Utah Regulations Library. This revision was approved by the Information Technology Council on August 14, 2008. On November 17, 2008 the Academic Senate Executive Committee approved forwarding the proposed revision to the Academic Senate as an item for debate and approval. The Academic Senate approved on_____. The Board of Trustees approved on _____.

This is the old version (Revision 0) that is proposed to be replaced.

~~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. Effective date: March 11, 1996 to December 7, 2008