Policy 4-001: University Institutional Data Management Policy

Revision 2. Effective date: April 15, 2020

I. Purpose and Scope 1

II. Definitions 2

III. Policy 4

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources 7

V. References 8

VI. Contacts 8

VII. History 8

I. Purpose and Scope

A. Purpose.

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.

B. 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.

II. Definitions

The following definitions apply for the limited purposes of this policy and any associated regulations.

A. Institutional Data -- Data that are acquired or maintained by University functional areas 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; and otherwise restricted by institutional policy or State or Federal guidelines.

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. Strategic Information Technology Council (SITC) -- 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 Enrollment Management appoints the Registrar as the Data Steward over student data. Current appointments posted to section IV.C Guideline – Data Management Roles by functional areas.

G. Data Custodian – The subject matter expert that is the initial source of contact for data within their functional area. 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. Current appointments posted to section IV. C Guideline – Data Management Roles by functional areas.

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 coordination with data stewards and custodians, 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.

K. Guideline: 4-001A – Data Management Roles – indicates filling the Data Steward and Data Custodian roles and the functional area they are appointed to. The guideline will be periodically updated by the CIO's office as necessary.

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.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources

A. Policies/ Rules. [*reserved*]

B. Procedures, Guidelines, and Forms.

1. Guideline G4-001A: Data Management Roles

C. Other Related Resources. [*reserved*]

V. References

A. Policy 4-004: University of Utah Information Security Policy

VI. Contacts

The designated contact officials for this Regulation are

A. Policy Owner(s) (primary contact person for questions and advice): Chief Information Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History.

A. Current version. Revision 2.

1. Approved by – Presented for the information of the Academic Senate March 30, 2020, and approved by the Board of Trustees April 14, 2020, with effective date of April 14, 2020.
2. Legislative History
3. Editorial Revisions
    a. Editorially revised January 26, 2024 to move to current regulations template.

B. Previous versions.

1. Revision 1. Effective Date. December 8, 2008
    a. Legislative History for Revision 1.
2. Revision 0. Effective Date. March 11,1996

C. Renumbering

1. Renumbered from PPM 1-12.