

University of Utah

Legislative History of Policy 4-001 Revision 2

As presented to the Senate Executive Committee and determined to be not academically significant,
March 16, 2020,

presented for the Information and Recommendations of the Academic Senate March 30, 2020, and

approved by the Board of Trustees April 14, 2020,

with designated effective date of April 14, 2020.

Prepared by Bob Flores, for the Institutional Policy Committee.

Contents:

- Explanatory memorandum to Senate Executive Committee Page 2
- Slide show presentation to Senate Executive Committee Page 3
- Policy 4-100 Revision 5 redline version showing changes proposed and approved Page 15
- Guideline 4-100A Data Management Roles Page 19

Memorandum

TO: Academic Senate Executive Committee
 FROM: Kenneth Pink – Deputy CIO University of Utah
 CC: Steve Hess – CIO University of Utah
 Date: 03/16/2020

RE: Policy 4-001: Data Management Policy Revisions and Guideline Creation

Policy 4-001’s purpose section talks about applying data management, security, and access principles in order “to maintain the value and guarantee effective use of Institutional Data and Information.” However, the current structure around data accountability and sharing is informal and often unclear. Some areas have created processes to help faculty, employees, and others request and receive access to data, but other areas are organized differently making it hard to know who or how to ask for data. This lack of knowledge can result in loss of productivity; in accurate data usage that can produce flawed analysis or decisions; or accidental policy/guideline violations from individuals assuming data access granted for one purpose allows it to be used for a different purpose or project.

The tables below give an example of the confusion data users have from the current informal appointment structure. At a BI community meeting we asked the 20 attendees to write-in who they thought of as the data steward for different areas. Of the 13 individuals who filled-out the survey, the only areas that had an almost true consensus was the Registrar and Financial Aid. Even within a community that commonly asks and uses data the confusion around responsibility persists.

Functional Areas		Inputted Data Stewards	
Finance Areas	Budget	Sandy Hughes Cathy Anderson Mark Winter Unknown/No Input	4 3 2 4
	General Ledger	Cathy Anderson Todd Kapos Laura Howat Lisa Zaelit Sandy Hughes Unknown/No Input	2 2 1 1 1 6
HR Area	HR	Jeff Herring Josna Kotturappa Mary Anne Berzins My HR Rep Unknown/No Input	4 3 1 1 3

Functional Areas		Inputted Data Stewards	
Student Areas	Admissions	Rakin Hall Pamela Horne/Steve Robinson Tim Ebner Brandon Ritter Unknown/No Input	4 2 2 1 3
	Financial Aid	Brenda Burke Pamela Horne/Steve Robinson Tim Ebner Unknown/No Input	8 1 1 3
	Registrar	Tim Ebner Pamela Horne/Steve Robinson Unknown/No Input	11 1 1

To combat this confusion, we would like to update policy 4-001 by adding a guideline that would formally state who is assigned to each data management role. This guideline would be updated as necessary as institutional changes occur. This position clarification will also allow data stewards and custodians the ability to indicate what methods should be used to request data, ask questions around official numbers, or indicate data errors they may come across so that data users can have an easier time utilizing data.

Policy 4-001: Data Management Policy, Summary Slide

Formalizing Data Accountability and Processes

- *Clarify role responsibilities*
- *Who's accountable*
- *Centralized location for current individuals accountable for data*

Functional Areas		Inputted Data Stewards	
Financial Areas	Budget	Sandy Hughes	4
		Cathy Anderson	3
		Mark Winter	2
		Unknown/No Input	4
	General Ledger	Cathy Anderson	2
		Todd Kapos	2
		Laura Howat	1
		Lisa Zaelit	1
		Sandy Hughes	1
		Unknown/No Input	6
HR Area	HR	Jeff Herring	4
		Josna Kotturappa	3
		Mary Anne Berzins	1
		My HR Rep	1
		Unknown/No Input	3



THE UNIVERSITY OF UTAH

Updates 4-001, Institutional Data Management Policy

4-00 I, Definitions

Replaces employee with functional areas and adds a general sentence of excluding data from being classified as Institutional if there is policy prohibiting it

- 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 data otherwise restricted by institutional policy or State or Federal guidelines.**

4-00 I, Definitions continued

Adding reference to new guideline which stores data stewards' contact information.

- 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 are posted to section IV.A Guideline - Data Management Roles by functional areas***

4-00 I, Definitions continued

Again adding reference to new guideline, but also expands on a data custodian's role as initial contact and subject matter expert.

- G. Data Custodian - ***The subject matter expert that is the initial source of contact for data within their functional area.*** The Data Custodian 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. ***Data Custodians suggests prioritizations, modifications, or clarifications to Data Stewards for data within their functional area. Current appointments are posted to section IV.A Guideline - Data Management Roles by functional areas***

4-00 I, Definitions continued

Addition indicates that data users should be communicating with or following procedures created by data stewards when utilizing data within a stewards functional area

- 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.

4-00 I, Definitions continued

Adding reference to new guideline

- 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 policy. ***Delegations given to data custodians to implement best practices will be referenced in the IV.A Guideline - Data Management Roles***

4-001, Definitions continued

Adding reference to new guideline

- ***K. Guideline - Data Management Roles - indicates current individuals 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.***



THE UNIVERSITY OF UTAH

Guideline: 4-001A- Data Management Roles

This expands the information found in Policy 4-001. The following indicates the appointment process for data stewards and custodians as well as the individuals currently filling each data management role. This guideline is used to help clarify which individuals should be contacted for each functional area. Data users making data requests should go through the custodian first as they have operational knowledge. Data stewards have a responsibility to assign data custodians and indicate the data use guidelines utilized by their functional areas.

› Enrollment Management (Admissions, Financial Aid, & Registrar)

› Financial Services

▼ **Human Resources (Campus)**

Data Steward - Director of HR Information Systems (HRIS)

Current Appointee: [Josna Kotturappa](#) (Appointed by Chief HR Officer, Jeff Herring)

Data Custodian(s) - Appointed by Data Steward

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>
Human resources (campus)	Director of HR Business Intelligence	Tatiana Topyrik

› Institutional Advancement



[Guideline 4-001A: Data Management Roles](#)

Date: January 15, 2019

View All Policies by

- [Current Number*](#)
- [Previous Number](#)
- *as of 09/15/08

Past Versions

[Website Feedback](#)

[Printable - Data Management Roles Guideline.pdf](#)

References: Policy 4-001, Data Management Policy Guideline Owner – Chief Information Officer

*Guideline will be maintained as a website to make additions or edits to the guidelines easier

Send updates or changes for the guideline to susan.schaefer@utah.edu



THE UNIVERSITY OF UTAH

Reasons for the proposed changes

- Decrease confusion for data users around access or use
- Reduces reports mismatch by indicating current data stewards that are approving definitions and calculation standards
- Better data transparency to better understand needs and uses
- To protect the privacy and data of students, patients, staff, and faculty.



THE UNIVERSITY OF UTAH

Potential Impact

- Negligible for patients, students, staff and faculty
- The additions added to the definition is to help clarify how and who to contact for data. No changes are made to how policy defines data usage.



THE UNIVERSITY OF UTAH

Q & A

Policy 4-001: University Institutional Data Management Policy [Revision 2]

I. Purpose and Scope

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.

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.

II. Definitions

- A. Institutional Data -- Data that are acquired or maintained by University ~~employees-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. SITC 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 SITC. 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~~ Enrollment Management appoints the Registrar

Commented [SDS1]: Editorial Update – Information Technology Council (ITC) is now called the Strategic Information Technology Council (SITC)

Commented [SDS2]: Editorial Update – the registrar is now under the direction of VP of Enrollment Management

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.

[J.K. Guideline: 4-001A – Data Management Roles – indicates the individuals 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. Noncompliance 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.

[Note: Parts IV-VII of this Regulation (and all other University Regulations) are Regulations Resource Information – the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

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

- A. Rules [insert]
- B. Procedures [insert]
- C. Guidelines:
[Data Management Roles](#)
- D. Forms [insert]
- E. Other related resource materials
[Executive Summary](#)

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:

The designated contact officials for this Policy are:

- A. Policy Owner (primary contact person for questions and advice): Director of Planning and Policy/Office of Information Technology.

B. Policy Officer: Chief Information Officer

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

"A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases.... "

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... [and] bears the responsibility for determining -requirements of particular Policies... " University Rule 1-001-III-B & E

VII. History:

Renumbering: Renumbered as Policy 4-001 effective 9/15/2008, formerly known as PPM 1-12

Revision History:

1. Current version: 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.

Approved by the Academic Senate: December 1, 2008

Approved by the Board of Trustees: December 8, 2008

Effective date: December 8, 2008

[Legislative History of Revision 1](#)

2. Earlier revisions:

[Revision 0](#)

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

Data Management Roles Guideline - Contact Information

This expands the information found in Policy 4-001. The following indicates the appointment process for data stewards and custodians as well as the individuals currently filling each data management role. This guideline is used to help clarify which individuals should be contacted for each functional area. Data users making data requests should go through the custodian first as they have operational knowledge. Data stewards have a responsibility to assign data custodians and indicate the data use guidelines utilized by their functional areas.

Enrollment Management (Admissions, Financial Aid, & Registrar)

All data stewards appointed by VP of Enrollment Management, Steve Robinson

Admissions - Data Steward - Executive Director of Admissions

Current Appointee: Steve Robinson

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>	<u>Contact Information</u>
Prospective students, applications, and admittance information	Sr. System Manager in Office of Admissions	Brandon Ritter	brandon.ritter@utah.edu

Financial Aid - Data Steward - Executive Director of Financial Aid & Scholarship

Current Appointee: Karen Henriquez, Director of Financial Aid

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>	<u>Contact Information</u>
Student financial aid & scholarships	Assistant Director of Financial Aid Systems	Veronica Christensen	veronica.christensen@utah.edu

Registrar - Data Steward - Registrar

Current Appointee: Tim Ebner

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>	<u>Contact Information</u>
Enrolled students, academic courses, majors, & degrees	Associate Registrar of Student Systems/Technology	Andrea Roner	aroner@sa.utah.edu

Financial Services

Data Steward - Associate VP of Financial & Business Services

Current Appointee: Cathy Anderson, CFO Main Campus (Interim while AVP of FBS position is vacant)

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>	<u>Contact Information</u>
General ledger	Interim Controller	Todd Kapos	todd.kapos@admin.utah.edu
Financial systems & travel	Director of Business Analysis & Support Services	Kori Wetsel	kori.wetsel@admin.utah.edu
Student financials, income accounting & card payment services	Associate Director of Income Accounting & Student Loan Services	Lisa Zaelit	lisa.zaelit@admin.utah.edu
Purchasing	Director of Procurement & Contracting Services	Glendon Mitchell	gmitchell@purchasing.utah.edu
Accounts payable & Ushop	Associate Director of Accounts Payable & Ushop	Scott Patten	scott.patten@admin.utah.edu

Data Management Roles Guideline - Contact Information

Human Resources (Campus)

Data Steward - Director of HR Information Systems (HRIS)

Appointed by Chief HR Officer, Jeff Herring

Current Appointee: **Josna Kotturappa** josna.kotturappa@utah.edu

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>	<u>Contact Information</u>
Human resources (campus)	Director of HR Business Intelligence	Tatiana Topyrik	Tatiana.Topyrik@utah.edu

Institutional Advancement

Data Steward - Senior Director of Advancement Operations

Current Appointee: **Paul Majnik** (Appointed by VP of Institutional Advancement, Heidi Woodbury)

<u>Responsible Area(s)</u>	<u>Data Custodian</u>	<u>Current Contact</u>	<u>Contact Information</u>
Development & alumni relations	Director of Information Services	Christian Singleton	christian.singleton@utah.edu

References: Policy 4-001, Data Management Policy Guideline Owner – Chief Information Officer

*Guideline will be maintained as a website to make additions or edits to the guidelines easier

Send updates or changes for the guideline to:

susan.schaefer@utah.edu