Management of Institutional Data

DM-01

About This Policy

Effective Date:
02-14-1991

Last Updated:
07-01-2007

Responsible University Office:
Committee of Data Stewards

Responsible University Administrator:
Office of the Vice President for Information Technology & Chief Information Officer

Policy Contact:
University Information Policy Office
uipo@iu.edu

Back to top

Scope

This policy applies to all users of Indiana University information technology resources regardless of affiliation, and irrespective of whether those resources are accessed from on-campus or off-campus locations.

This policy applies to all institutional data, and is to be followed by all those who capture data and manage administrative information systems using university assets.

Back to top

Policy Statement

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.

The permission to access institutional data should be granted to all eligible employees of the university for all legitimate university purposes.

Employees are expected to access institutional data only in their conduct of university business, to only access the data needed to perform their jobs, to respect the confidentiality and privacy of individuals whose records they may access, to observe any ethical restrictions that apply to the data to which they have access, and to abide by applicable laws or policies with respect to access, use, or disclosure of information. Employees should not disclose data to others except as required by their job responsibilities, use data for their own or others’ personal gain or profit, or access data to satisfy personal curiosity.

Standards and procedures are to be developed to conform to the objectives embodied in this policy.

Back to top

Reason For Policy

Although all data captured using university assets are resources of the university, they vary in their relevance to the university’s administrative processes. This policy is intended to apply to those data which are critical to the university’s administration, regardless of whether the data is used or maintained by administrative or academic units.

Therefore, standard principles of data management should be applied to maintain the value and ensure the effective use of the data. Common principles and standards must be applied uniformly and as part of a coordinated effort.

This policy serves as a statement of objectives for managing institutional data.

Back to top

Procedure

Determination of relation to mission If the relationship of a use of information technology resources to the university's mission is unclear, the University Information Technology Policy Office (ITPO) or regional campus Chief Information Officers (CIOs) will coordinate with campus administration and the unit involved. These groups will determine whether the activity is an appropriate use of university information technology resources and supports the mission of the university. Determination of incidental personal use The senior management of each university department or other administrative unit is authorized to define and publish the acceptable level and nature of incidental personal use by members of the unit. An employee's supervisor may require the employee to cease or limit any incidental personal use that hampers job performance or violates university policy. University technology service providers will always place a higher priority on support of university-related activities over any form of incidental personal use. Consultation The University Information Technology Policy Office (ITPO) and/or regional Chief Information Officers (CIOs) are available to provide consultation or advice related to technology use or misuse to any university, campus, or unit administrators or individual personnel.

Back to top

Definitions

Access to institutional data:
refers to the permission to view or query institutional data; permission does not necessarily imply delivery or support of specific methods or technologies of information access.
Data administration:
is the function of applying formal guidelines and tools to manage the university's information resource.
Eligible agent of the university:
is anyone employed on a part-time or full-time basis or working under a contract for Indiana University.
Eligible employees:
are faculty, staff, and administrators holding full-time appointments at Indiana University, or other employees specifically designated as eligible to access institutional data by the head of their department, division, school, or campus.
Institutional data (or information) is data in any form, location, or unit that:

- is created, received, maintained or transmitted as a result of educational, clinical, research or patient care activities, or
- is substantive, reliable, and relevant to the planning, managing, operating, documenting, staffing or auditing of one or more major administrative functions of the university, or
- is used to derive any data element that meets the above criteria.

Data Classifications
Institutional data falls into four general categories:

- Critical: Inappropriate handling of this data could result in criminal or civil penalties, identity theft, personal financial loss, invasion of privacy, and/or unauthorized access to this type of information by an individual or many individuals.
- Restricted: Because of legal, ethical, or other constraints, may not be accessed without specific authorization, or only selective access may be granted.
- University-internal: May be accessed by eligible agents of the university, in the conduct of university business; access restrictions should be applied accordingly. This is the default classification for all data
- Public: Few restrictions; generally releasable to a member of the public upon request; upon receipt of a request, seek advice from the appropriate data steward; if the request is made pursuant to the Indiana open records statute, seek advice from the Office of the VP and General Counsel, as well as the appropriate data steward.

NOTE: Irrespective of classification under this standard, institutional data may be subject to disclosure under the Indiana Access to Public Records Act. Always immediately contact the Office of the VP and General Counsel of the receipt of a request made pursuant to this law.

Back to top

Sanctions

Failure to comply with Indiana University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); to the individual's employment (up to and including immediate termination of employment); to the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

Back to top

Additional Contacts

Maintained and revised as necessary by the University Information Policy Office under the direction of approved data management committees.

Campus registrars or University Counsel will handle questions about the impact of FERPA on IU student record use.

Office of the Vice President for Information Technology
University Information Policy Office

Back to top

History

Updated definition of institutional data on July 2, 2014

Reformatted by the University Information Policy Office in 2007 and merged with the Indiana University Committee of Data Stewards’ “Data Administration Issues Notice”, “Data Distribution and Storage Issues Notice”, and “Permission to Access Institutional Data” documents.

An initial Policy to Access Data was approved by the University Operations Cabinet in October, 1991, and distributed by the Office of the President in December, 1991.

Original document approved by the Administrative Computing Advisory Committee (ACAC) March 21, 1991 and the ACAC Data Administration Subcommittee on February 14, 1991.