Exhibit C

University Policies

Management of Institutional Data

DM-01

About This Policy

Effective Date:

02-14-1991

Date of Last Review/Update:

02-26-2020

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

Policy Feedback:

If you have comments or questions about this policy, let us know with the policy feedback form </contact/index.html> .

Print or view a PDF of this policy

Many policies are quite lengthy. Please check the page count before deciding whether to print.

Scope

This policy applies to all users of Indiana University information and information technology resources regardless of affiliation, and irrespective of whether these 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 and designated appointees of the university for all legitimate university purposes.

Users of institutional data must:

- access data only in their conduct of university business, and in ways consistent with furthering the university's mission of education, research, and public service.
- respect the confidentiality and privacy of individuals whose records they may access.
- observe any ethical restrictions that apply to the data to which they have access.
- abide by applicable laws, regulations, standards, and policies with respect to access, use, disclosure, retention, and/or disposal of information.

Users of institutional data must not:

- disclose data to others except as required by their job responsibilities.
- use data for their own or others' personal gain or profit.
- 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 essential 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 must 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

Procedures

See DM-01 Standards for additional related procedures.

Questions about this policy should be submitted to the University Information Policy office by email to it-incident@iu.edu. UIPO will review submissions and involve the relevant Data Steward and/or Committee of Data Stewards as appropriate

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 employees are faculty and staff 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.

Designated appointees are non-employees holding an appointment with the university (ex. academic no-pay) that are authorized 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 meets one or more of the following criteria:

- It is subject to a legal obligation requiring the University to responsibly manage the data;
- It is substantive and relevant to the planning, managing, operating, documenting, staffing or auditing of one or more major administrative functions or multiple organizational units of the university;
- It is included in an official university report;

- It is clinical data or research data that meets the definition of "University Work" under the Intellectual Property Policy UA-05; or
- It is used to derive any data element that meets the above criteria.

Data Classifications:

Institutional data falls into four classifications. In the absence of being formally classified, institutional data should be treated as University-Internal by default.:

- **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 employees and designated appointees of the university in the conduct of university business; access restrictions should be applied accordingly.
- **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

Indiana University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Vice Provost or Vice Chancellor of Faculties (or campus equivalent), Dean of Students (or campus equivalent), Office of the VP and General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources </policies/it-02-misuse-abuse-it-resources/index.html> for more detail.

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); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); 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 the Office of the VP and General 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 <https://protect.iu.edu/about/index.html>
Back to top

History

Updated the definition of "institutional data". February 22, 2017.

Revised and updated by Committee of Data Stewards Policy Subgroup, March 23, 2015.

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.

Previous Versions:

Effective Dates: 05/23/2015-02/22/2017 </policies/dm-01-management-institutional-data/archived-05232015-02222017.html>

The definition of "institutional data" has been updated. (Non-material change.)

Back to top

Related Information

DM-01-S Standards for the Management of Institutional Data

Release of Procurement Information FIN-PURCH-10

</policies/fin-purch-10-release-of-procurement-records/index.html>
Indiana University Release of Student Information Policy </policies/usss-05-release-student-information/archived-09182019.html>
Family Education Rights and Privacy Act
<http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
Indiana University HIPAA Privacy and Security Compliance
<http://www.iub.edu/~vpgc/compliance/hipaa-privacy-and-security/hipaa-compliance-documents.shtml>
Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html>
Health Insurance Portability and Accountability Act (HIPAA) Security Rule
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html>
Health Information Technology Economic and Clinical Health Act (HITECH)
<http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>

/