INDIANA UNIVERSITY

Standards for Management of Institutional Data

DM-01s

(Supports Policy DM-01 Management of Institutional Data)

FULL POLICY CONTENTS

Scope

These standards apply 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.

These standards apply to all institutional data, and are to be followed by all those who capture data and manage administrative information systems using university assets

Reason for Standard

This standard details procedures in support of Policy DM-01 Management of Institutional Data.

Procedures

1. Institutional data designation and classification:
    a. As part of the data definition process, data stewards will assign each data element and each data view of institutional data to one of four classifications: public data, university-internal data, restricted data, or critical data.
    b. The University Information Policy Office will assist in the negotiations for defining something as institutional data and for identification of data stewards.
2. Access to data:
   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. This philosophy guides decisions about access to institutional data.
    a. To the extent possible, data stewards will work together to define a single set of procedures for requesting permission to access institutional data, and will be jointly responsible for documenting these common data access request procedures.
    b. Access to institutional data that is consistent with the data's classification will be granted to all data users for all legitimate university purposes.
    c. Except as specified elsewhere in this standard, all institutional data will be classified as university-internal data for use within the university. University employees and designated appointees will have access to these data, without restriction or prior authorization, for use in the conduct of university business after compliance with appropriate request process (ex. assent to Institutional Data Acceptable use agreement, etc.). These data are designated university-internal. They are freely available within the university but not open to the general public.
    d. Where appropriate, data stewards may identify institutional data elements or views which have few access restrictions and which may be released to the general public. These data will be designated as public data.
    e. Where necessary, data stewards may specify some data elements as critical or restricted. Critical or restricted data would include those data for which data users must obtain individual authorization prior to access, or to which only limited access may be granted. Data classified as critical restricted may only be used by those whose positions explicitly require such access. Designation of data as critical or restricted will include specific reference to the policy, legal, ethical, or externally-imposed constraint which requires this restriction.
    f. Direct access to university file servers hosting critical or restricted institutional data must be blocked from non-IU network addresses. Individuals requiring access to files stored on these servers from off-campus must connect in a secure manner, such as through the university's modem pool or (preferably) the university virtual private network (VPN) service.
    g. A data view does not necessarily inherit the restriction characteristics of the data elements which comprise it. (For example, removal of any

association with personally-identifying data elements can result in a view which contains otherwise restricted data elements being designated as public or university-internal.)

h. The access privileges of users who change positions or separate from the university must be updated in a timely manner as appropriate.
i. Each data steward will be individually responsible for documenting data access procedures that are unique to a specific information resource or set of data elements.

3. Decisions about data access:
    a. Data stewards establish standard rules, guidelines, and profiles for data access, and act upon individual requests to access data. Responsibility for such recommendations may be delegated to data managers.
    b. Any data user may request that a data steward, or the Committee of Data Stewards as a group, review the restrictions placed on a data element or data view, or review a decision to deny access to restricted data.
    c. The University Information Policy and Security Offices assist in the implementation of the data stewards' recommendations and can help identify the appropriate data steward or manager for data access request or to appeal a recommendation.
    d. When necessary, the Committee of Data Stewards will make the final determination on data restrictions and requested access rights to institutional data.
4. Data availability and integration:
    a. Data stewards and the system administrators are responsible for providing accessible, meaningful, and timely electronic institutional data for university use.
    b. Data stewards and the system administrators who manage systems share the responsibility for data compatibility, accessibility, and interfaces among institutional data elements.
    c. Data stewards and system administrators will work together toward unification of the various data element coding structures and data storage formats which exist in various systems where institutional data are stored.
5. Data documentation (Metadata):
    a. Documentation of data elements is ultimately the data steward's responsibility. Some or all of these responsibilities may be delegated.
    b. Metadata must be addressed for information systems objects that are delivered into production.
        - Metadata must be provided for business intelligence objects.
    c. Documentation/definition for each data element must at least include:
        - Name and alias names
        - Description
        - Data steward
        - Usage and relationships
        - Frequency of update
        - Source for data capture
        - Official data storage location and format
    d. Documentation must also include:

        - Designation as "critical," " restricted," "university-internal," or "public"
        - For “critical” and “restricted” data elements: description or specification of the restriction
        - Description of validation criteria and/or edit checks
        - Description, meaning, and location of allowable codes
        - Access rules and security requirements
        - Archiving requirements
        - Data storage location of extracts
    e. In addition to metadata elements required across all systems, added requirements may exist specific to the nature of an individual system.
    f. Documentation for derived institutional data must include the algorithms or decision rules for the derivation.
    g. Documentation of data views must include reference to the data elements which comprise the view and description of the rules by which the view is constructed.
    h. Overview documentation for databases, files, and groups of files that include institutional data must also be provided, and must include information about data structure and update-cycles necessary for the accurate interpretation of the data.
    i. Periodic reviews must be performed to verify accuracy and update metadata as appropriate.
6. Data collection, quality, integrity, validation, and correction:
    a. The data steward is ultimately responsible for complete, accurate, valid, and timely data collection. Operational responsibility for data collection and maintenance can be delegated.
    b. Further delegation and decentralization of data collection and maintenance responsibility is encouraged in order to assure that:
        - Electronic data are collected and maintained as close as possible to the source or creation point of the data as identified by the data steward
        - Each manual or computer process which handles data adds value to the data.
    c. Data quality policies and standards should be developed that encompass the life cycle of data, including the data warehouse and source systems.
    d. Applications that capture and update institutional data must incorporate edit and validation checks to assure the accuracy and integrity (consistency) of the data.
    e. The accuracy of any element can be questioned by any authorized data user. The data user has the responsibility to help correct the problem by supplying as much detailed information as available, sufficient to permit understanding and diagnosis of the problem.
    f. The data steward or delegate is responsible for data integrity, responding to questions about the accuracy of data, and correcting inconsistencies if necessary.
    g. Upon written identification and notification of erroneous data, corrective measures must be taken as soon as possible to:

- Correct the cause of the erroneous data at its source when possible and as appropriate.
- Correct the data in official storage location(s).
- Notify users who have received or accessed erroneous data.

7. Data manipulation, modification, extraction, and reporting:
    a. The data steward, in consultation with other university offices as appropriate, will be responsible for determining security requirements and access restrictions for institutional data.
    b. The data steward has ultimate responsibility for proper use of institutional data; individual data users will be held accountable for their specific uses of the data.
8. Data security:
    a. The data steward, in consultation with other university offices as appropriate, will be responsible for determining security requirements and access restrictions for institutional data.
    b. All data users having access to critical or restricted institutional data will formally acknowledge (by signed statement or some other means) their understanding of the level of access provided and their responsibility to maintain the confidentiality of the data they access. The data steward is responsible for monitoring and reviewing security implementation and authorized access.
    c. The data steward is ultimately responsible for defining and implementing policies and procedures to assure that data are backed up and recoverable in response to events that compromise data integrity. UITS and its regional campus counterparts or other university agencies may assist in this effort.
    d. Unattended devices with access to institutional data must be logged off, locked, or otherwise made inaccessible to individuals without access rights. Where technically feasible, this equipment must be set up for automatic lock-out after no more than 15 minutes of non-use.
    e. Individuals requiring access to central sources of critical or restricted institutional information must be authorized by the appropriate data steward or manager and subsequently must primarily use the universityâ€™s enterprise decision support system (i.e. IUIE, CBI, etc.) for that access. Any direct (non-edss/iuie) access to the UITS DSS using individual desktop query tools must first establish a connection to the VPN servers to ensure that their password and the other data are encrypted in transmission, or use other means to achieve such encryption.
    f. Where technically feasible, a central authentication service (i.e. ADS, CAS, etc.) must be used for all services that facilitate update or inquiry access to restricted or critical data on university servers, so that (minimally) strong password selection rules, password expiry, and intruder lockout can be employed.
    g. Where technically feasible, password tokens (in addition to secure password) must be required for any update access to critical or restricted institutional data on university servers.
    h. Departments (including UITS and its regional campus counterparts) must eliminate insecure protocols for connecting to all university systems, and

for transferring data to and from those systems, especially those servers that support critical operations and/or host critical or restricted data.

i. Where technically feasible, critical information in transit and at rest must be encrypted.

9. Data storage:
    a. The data steward, in consultation with other university offices as appropriate, is responsible for identifying an official data storage location for each data element, as well as an official data storage location of valid codes and values for each data element. The data steward will also determine archiving requirements and strategies for storing and preserving historical data for each data element.
    b. Institutional data may be stored on any of many diverse computing hardware platforms, provided such platforms are integrated components of an overall university information system.
    c. Data element names, formats, and codes must be consistent across all applications which use the data and consistent with such university standards as are developed.
    d. The University Information Policy Office will assist in determining data storage location and archiving requirements for institutional data.
    e. Critical or Restricted data must never be stored on individual user workstations, or mobile devices (i.e. laptops, smart phones, tablets, personal digital assistants, thumb drives, etc.) without prior formal written approval and appropriate technical safeguards (see IT-12 Policy, IT-12.1 Standard, and this document). This formal approval must come from the senior executive officer of the unit and confirm a critical business need for such storage. Critical or Restricted data must otherwise be stored on properly configured and managed, department or central servers.
    f. Departments are expected to identify, for their users, appropriate server locations for storage of data extracted from central sources or derived through department operations.
    g. Critical data must not be collected, or extracted from central systems and stored on departmental servers unless doing so is absolutely required to maintain the business functions of the office involved.
    h. So that standards for survey research and FERPA requirements for non-directory student records are met, all program evaluation and assessment data must be stored in such a way that responses are not associated with personally identifiable information (i.e. names, SSNs, etc.). Linkage files containing the association of protected data to individuals must be placed in different directories and with different naming conventions to obscure the connection, and must be permanently deleted when no longer needed
    i. A student may file a directory exclusion to prevent disclosure of public information. For this reason, student public information must not be stored on local servers unless updated daily.

10. Data views:
    a. Data views may be defined in order to:
        - Aggregate data from multiple sources.
        - Segment data into smaller and more manageable subsets.

        - Segregate data according to confidentiality or restriction characteristics, so that access to the resulting subset may be more widely distributed
    b. The data stewards are responsible for defining standard views of institutional data. These views will also be considered institutional data.
    c. Data managers or data users may recommend the definition of new data views.
11. System administration:
    a. Institutional data must be maintained within professionally administrated systems in compliance with university policies and applicable regulations.
    b. If institutional data are stored on any component of the university information system, that system component must have defined a formal system administration function and have assigned to it a system administrator whose responsibilities include generally accepted system administration tasks including; physical site security; administration of security and authorization systems, backup, recovery, and system restart procedures, data archiving, capacity planning, and performance monitoring.
    c. If institutional data are stored on any component of the university information system, that system component must comply with specific management standards, as outlined in Policy IT-12 as well as any applicable sector-specific requirements (i.e. PCI-DSS, HIPAA, etc.). Web and other servers that must be accessible from off-campus must be physically or logically separated from servers hosting critical or restricted institutional data.
    d. System Administrators shall ensure that adequate administrative processes and proper security safeguards are in place and enforced.
12. User support:
    a. Each major system housing institutional data will define the extent of support for data access and interpretation which is available to users of these data.
    b. Data stewards will provide user support--primarily through documentation of the information resource but also, as needed, in the form of consulting services--to assist data users in the interpretation and use of institutional data. This responsibility may be delegated.
    c. Data users are responsible for their own appropriate use and interpretation of the data which they access according to applicable law and university policy.
13. Institutional data model:
    a. The data stewards, data managers, and University Information Policy Office recognize the value of and will work toward establishing and maintaining a university-wide institutional data model which describes all major institutional data entities and the relationships among those data entities.
14. Awareness and Training:
    a. Data classification information and data handling procedures must be documented and communicated to all relevant audiences including:

developers, data managers, local service providers, and users before access to institutional data is granted.

b. Training to promote understanding and appropriate use of data before access to information is provided is strongly recommended.
    - Training may be based on data classification.
    - Training may be required based on role responsibilities.
    - Training may be required based on the impact of decisions made using the data.
c. Training material should be reviewed and revised as appropriate.
d. Periodic review and renewal of individual training is strongly recommended.

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.

System administration
is the function of applying formal policies, standards, guidelines and recommended practices to the management of a computing resource. Responsibility for the activities of system administration may belong to UITS, its regional campus counterparts, or to other divisions or departments within the university.

The university data resource dictionary
is a database system that functions as a repository that contains comprehensive information about the university's institutional data and documentation of university administrative systems.

The university information system
is a conceptual term used to identify the collection of computer hardware, software, and network connections which together form the single, integrated system on which institutional data reside.

Data administration
Responsibility for the activities of data administration is shared among the data stewards, data managers, and the University Information Policy Office.

Data managers
University officials and their staff who have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data are considered data managers. Among the responsibilities of the data managers

are any data administration activities identified in this standard which may be delegated to them by the data stewards.

Data ownership
Although individual units or departments may have stewardship responsibilities for portions of the institutional data, Indiana University is considered the data owner of all university institutional data.

Data stewards
Those senior university officials (typically at the level of vice president, assistant vice president, dean, or university director) who have planning and policy-level responsibilities for data in their functional areas are identified as the data stewards. The data stewards, as a group, are responsible for recommending policies, and establishing procedures and guidelines for university-wide data administration activities. Some data stewards have management responsibilities for defined elements of institutional data.

For historical reasons â€“ because data and the responsibility for data have traditionally been organized along functional or subject-area boundaries â€“ the data stewards are established according to this same subject-area organizing principle. However, because the eight-campus structure of the university is not explicitly recognized in this organizing principle, the data stewards need to be sensitive to the view from the campuses. The specific or unique views of the individual campuses must be an integral part of the adoption of institution-wide data policies, and the data stewards must ensure that their lines of communication to the campuses are active and user-friendly.

Data users
Individuals who need and use university data as part of their assigned duties or in fulfillment of their role in the university community.

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 General Counsel, and/or appropriate law enforcement agencies. See policy IT-02, Misuse and Abuse of Information Technology Resources 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.

Additional Contacts

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

Subject	*Contact*	*Phone*	*Email*
All questions	**Office of the VP for IT** **University Information Policy Office**	**812-855-8476**	**uipo@iu.edu**
Questions regarding impact of FERPA on IU student record use.	**Office of the VP an General Counsel**	**812-855-9739 (BL)** **317-274-7460 (IUPUI)**	**n/a**

Related Information

- DM-01 Management of Institutional Data
- Business Intelligence Metadata Standard (authentication required)

History

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.

Revised and updated by the CDS Policy Working group 2012 & 2015.

New version posted May 1, 2015