Data Administration Policy

Table of Contents

I. General Philosophy.......................................................... 2

II. Organizational Entities and Data Administration
    Responsibilities.......................................................... 3
    A. Data Administration.................................................. 3
    B. Enterprise Computing Services................................... 4
    C. Office of Planning, Budget and Effectiveness................. 5
    D. Committee of Data Stewards..................................... 5
    E. Committee of Data Custodians................................... 6

III. Data Administration Programs......................................... 9
    A. Data Inventory....................................................... 9
    B. Data Architecture.................................................. 10
    C. Data Quality........................................................ 10
    D. Data Access and Availability.................................... 11
    E. Data Security........................................................ 12
    F. Data Warehouse..................................................... 13
    G. Planning.............................................................. 14

IV. Glossary of Data Administration Terms............................ 16

V. References................................................................. 22
I. General Philosophy

The University recognizes data as an institutional asset and resource, vital to the operational, tactical and strategic processes within the organization. Data in this context is a term used to describe information which will be entered into or is contained in computer files, and which can be processed by the computer (Radcliffe 60). Data is frequently subject to less stringent management oversight than other assets, partially because data differ from traditional assets in many ways, and the costs associated with inadequate or incorrect data are frequently hidden (Redman 8). Unlike other assets, data can be copied innumerable times, are not static, tangible or consumed with use, and are not traditionally assigned a monetary value (Redman 42). However, insufficient or inaccurate data can adversely affect all aspects of the organization resulting in huge costs. Examples of such costs include: loss of revenue due to poor customer service, costs associated with increased employee turnover and inefficient operations, labor and programming costs associated with researching and correcting errors, lost discounts with vendors, maintenance and development costs associated with duplicative databases, and costs resulting from poor management decisions based on bad or inadequate data.

Data must be managed as any other asset, and the institution has a responsibility to improve the efficiency of processes associated with the collection, storage, maintenance, manipulation, analysis, reproduction and presentation of data, as well as ensuring adequate data access while maintaining necessary levels of security and privacy. The cost of collecting and updating data is usually minimal, as it is a necessary part of operations of an organization, so the most productive way to address many data problems is to improve the processes that surround its acquisition and use (Redman 25-27, 233). Furthermore, while the institution owns data, various organizations within the institution have stewardship responsibilities for subsets of the data (Indiana University). Consequently, the University must approach data management in a comprehensive and systematic fashion, where its responsibility is shared by all. It must develop a data infrastructure that provides high quality, timely and useful data that is easily accessible and understood by users, and meets the operation, management and strategic needs of the University.

There are many types of data, but these policies and procedures apply to data categorized as “administrative”, or that used to support or is relevant to the administrative, operational, patient care or planning functions within the institution (Arizona State University). Such activities constitute the foundation required to support the instructional, research, service and patient care missions of the University. These functions include, but are not limited to, student admissions, registration, student billing and financial aid processing,
financial records and facilities management, housing and dining services, employment and benefits processing, payroll, purchasing and the patient care business of the Medical Center. The University also acquires, creates and uses a great deal of research data, but separate policies exist to manage such data. However, there may be some data used in traditional research activities that would also be of benefit to the institution in analyzing its administrative data. Such data might include that pertaining to education, social science, business and economics, and health care. For example, the University could gain value from using such data in conjunction with administrative data to analyze trends in student course demands and matriculation. If doing so would not violate any regulatory or contractual agreements, then such data may be included in the Data Warehouse defined below.

II. Organizational Entities and Data Administration Responsibilities

A. Data Administration

The institution has established the department of Data Administration to manage its administrative data. (See AR II-1.7-3) The Director of Information Resources Management, also known as the Data Administrator, is the manager of this department and the individual ultimately responsible for the tasks defined below. Data Administration works in conjunction with the Office of Planning, Budget and Effectiveness, Enterprise Computing Services, the Committee of Data Stewards, the Committee of Data Custodians, and user departments. The Data Administrator serves as the chairperson for the Committee of Data Custodians. While Data Administration reports to the Vice President for Information Systems, its priorities are set and procedures approved by the Vice President for Administration. [Note: The Medical Center Vice Chancellor for Information Technology (also CIO of the University Hospital) will appoint a counterpart to the University Data Administrator to fulfill the corresponding responsibilities within that organization, to coordinate such activities with the University Data Administrator, and to serve as a member of the Committee of Data Custodians.]

Data Administration performs the following functions:

- coordinate/facilitate efforts to negotiate and build university-wide consensus on data issues,
- develop an inventory of administrative data assets (see “III-A, Data Inventory”);
- define the institutional data architecture or logical data model and ensure its integration with physical data models (Arizona State University) (see “III-B, Data Architecture”)}
• conduct routine evaluation of data quality, research problems, identify alternative solutions to address problems along with their costs and benefits, and manage projects to improve data quality (Redman 48) (see “III-C, Data Quality”),
• facilitate the expansion of data access, sharing and availability through streamlining of processes to acquire access, and ensuring documentation on such processes and the overall data inventory and architecture are easily accessible to users (see “III-D, Data Access and Availability”),
• receive appeals from users who are denied access, and forward these to the Committee of Data Custodians and Committee of Data Stewards for evaluation,
• ensure data security, privacy and appropriate use through evaluation of processes, and coordination of quarterly review of administrative computing user access (see “III-E, Data Security”),
• actively solicit user input on data reporting and analysis needs for the Data Warehouse (see “III-F, Data Warehouse”),
• design a Data Warehouse to improve operational, tactical and strategic decisions,
• work with Institutional Effectiveness Coordinators to enhance data analysis on administrative data to extract new information to enhance institutional efficiency and effectiveness,
• integrate data planning as part of the institution’s planning process (see “III-G, Planning”),
• prior to their purchase and/or development, evaluate new administrative systems or major modifications to determine if these systems and changes comply with the institutional data architecture and standards,
• provide the Committee of Data Stewards with a report containing a description of the requested system modification and/or purchase, the functional and service issues the new system or change will address, information on the scope of the compliance problems including any process, policy and technical ramifications, a list of possible alternatives to address any non-compliance issues, and the recurring and non-recurring costs and benefits associated with each (see AR III-2.0-1),
• evaluate the availability of data required to monitor the institution’s progress in attaining strategic goals,
• develop and forward process, procedure and project recommendations on all of the above to the Committee of Data Stewards for evaluation and recommendations to the Vice President for Administration,
• develop and forward policy recommendations on the above to the Committee of Data Stewards for evaluation and referral to the Vice President for Administration.
B. Enterprise Computing Services

Information Systems’ Enterprise Computing Services is responsible for maintaining the major administrative databases, and implementing appropriate access and security policies for these databases. (See AR II-1.5-2 and AR II-1.7-1) (NOTE: MCIS provides the corresponding services for systems within the Health Care Enterprise.) Staff within this organization serve as a resource in all data administration activities, and provide the following services:

- integrate the logical data architecture into the physical database structure of the official institutional systems,
- implement security and access policies defined by Data Stewards and Custodians, and safeguard data from physical harm and unauthorized access (University of Virginia),
- develop and test a Disaster Recovery Plan for the official institutional systems,
- provide information on existing data structures and standards for creation of the data inventory and architecture,
- work with the Data Administrator and the Committee of Data Custodians to provide the university community with readily available information on data access procedures, and the overall data inventory and architecture,
- notify the Data Administrator of potential changes in process, procedures or computer systems that could affect the creation, maintenance, use or analysis of administrative data,
- provide programming support to alter official institutional systems to enforce standards and improve data quality,
- evaluate and install security software as recommended by the Vice President for Administration,
- provide programming support to convert and load data from the online transaction processing systems into the Data Warehouse, as well as loading data purchased or acquired from an organization external to the University,
- write various reports to assist Data Administration in data analysis activities,
- evaluate and select appropriate Data Warehouse platforms and tools,
- assist in the acquisition or gaining of access to data from an organization external to the University for the Data Warehouse,
- provide all technical services supporting the implementation and maintenance of the Data Warehouse,
- provide user training on the Data Warehouse,
- work with the Data Administrator to develop recommendations on issues to be forwarded to the Committee of Data Stewards for evaluation and referral to the Vice President for Administration and the President’s staff as required,
- play a major role in the planning efforts for all information resource needs.
C. Office of Planning, Budget and Effectiveness

The Office of Planning, Budget and Effectiveness has the responsibility for establishing the central institutional effectiveness function, and coordinating the external reporting on students, faculty, finances, and staffing to the State and Federal Government, as well as other external agencies and organizations. In addition, it is responsible for ensuring the timely availability and integrity of data to meet the information needs for institutional decision-making. (See AR II-1.5.2) All of these activities are dependent on the availability of high quality institutional data. Consequently, the Vice President for Administration authority to set priorities for Data Administration activities, and make final policy recommendations to the President’s staff on issues related to data management. The Committee of Data Stewards will report to the Vice President for Administration who has ultimate authority for making final decisions regarding the committee’s activities. (See AR III-2.0-1)

D. Committee of Data Stewards

The Committee of Data Stewards is comprised of higher-level management who have the responsibility for planning and policy development for their functional areas (Indiana University), are familiar with the institutional ramifications of data access, quality and analysis in their domain, and are cognizant of the various regulatory mandates with which the University must comply. (See AR III-2.0-1.) The members of this committee evaluate information and suggestions by the Data Administrator and the Committee of Data Custodians, and make recommendations to the Vice President for Administration on the following:

- long-term direction for effective use of enterprise data in support of institutional goals and objectives, and the planning process for information resource needs,
- data administration procedures and policies,
- the appropriate use and accurate interpretation of data (University of Virginia),
- priorities for data quality projects within the institution,
- the implementation and maintenance/enhancement of the Data Warehouse,
- identification of “enterprise data” that should be subject to strict data quality standards and stored within the Data Warehouse (Redman 48),
- security classifications for all enterprise data (“public” for view only data available to the general public, “confidential” for data available to view or update by the general university community, “restricted” for data available for view or update
only by specific individuals within the university community, and “protected” for highly secure institutional information as identified by federal or state laws or by the Committee of Data Stewards),
- institutional network access priorities for data originating from systems both internal and external to the University,
- priorities and possible sources of funds for the correction of data quality problems too large for a given functional area to cover,
- disputes over data access, use and “ownership”,
- recommendations concerning any potential new administrative systems or major enhancements that do not comply with the institutional data architecture and standards, forwarded to the Medical Center Vice Chancellor for Information Technology (also CIO of the University Hospital) where appropriate, and ultimately to the Vice President for Administration and the Vice President for Information Systems for presentation and discussion at the President’s Staff.

The Committee of Data Stewards will report to the Vice President for Administration who has ultimate authority for making final decisions regarding the committee’s activities. The Vice President for Administration will recommend a representative to serve as the Chair of this committee.

E. Committee of Data Custodians

The Committee of Data Custodians is comprised of management responsible for the collection and maintenance of specific data in their functional areas (Indiana University; University of Virginia), and enforcing corresponding policy and procedures. These individuals are typically identified as the “super users” or “System Administrators” who are the experts on the administrative systems which support their areas, and are the most familiar with the interrelationship between policy and procedures, business rules, data systems, data standards and security classifications. Representatives from the Office of the Registrar, the Office of Student Financial Aid, Student Billing Services, the Office of Admissions, the Controller’s Office, the Purchasing Division, Human Resource Services, the Office of Planning, Budget and Effectiveness, the sector Effectiveness Coordinators, and others appointed by the Medical Center Vice Chancellor for Information Technology (also CIO of the University Hospital) will serve on this committee, as well as others where appropriate. (See ART II-2.G-1) The Data Administrator serves as the chairperson for the Committee of Data Custodians. Members of this committee perform the following functions in accordance with the data management guidelines established by the Vice President for Administration:
• develop and implement sound internal procedures for the acquisition, creation, maintenance, manipulation, reporting and access to data in their functional areas (University of Virginia),

• have primary responsibility for the timely collection and maintenance of high quality data within their areas (Indiana University; University of Virginia),

• serve as the primary source of information on the meaning and use of their data to campus users and technical staff (Indiana University; University of Virginia),

• are aware of who uses their data and for what business purposes (Redman 48),

• provide accurate analysis and presentation of their data for internal and external reporting,

• assign the security classifications for all enterprise data for subsequent review by the Committee of Data Stewards and the Vice President for Administration, using the Security Administrators as a resource where appropriate ("public" for view only data available to the general public, "confidential" for data available to view or update by the general university community, "restricted" for data available for view or update only by specific individuals within the university community, and "protected" for highly secure institutional information as identified by federal or state laws or by the Committee of Data Stewards),

• in conjunction with the University Archivist and Director of the UK Records Program, and the Medical Records Director, develop archiving procedures for data in their functional areas (University of Virginia), and implement these procedures after review by the Committee of Data Stewards and approval by the Vice President for Administration,

• develop sufficient documentation on the use of their data, including the rules or special conditions that could affect the accurate analysis or presentation of the data (University of Virginia),

• assist the Data Administrator in compiling a data inventory, defining a data architecture and standards, and identifying data quality problems and their sources,

• implement process changes required to address data quality or security problems within their functional areas, and where feasible, cover the costs associated with such activities,

• correct data determined to be of inadequate quality, and notify users who may have accessed this data (Indiana University),

• implement various measures to ensure high data integrity, including running periodic reports to verify data quality and reporting problems to the Data Administrator (Redman 48; University of Virginia),

• notify the Data Administrator of potential changes in process, procedures or computer systems that could affect the creation, maintenance, use or analysis of their data,
• actively solicit information from users on their data and analysis needs, including those regarding data residing in the Data Warehouse (Redman 48),

• establish and develop documentation for procedures to request access to data in their systems and the Data Warehouse (Indiana University; University of Virginia), grant timely approval for user update and view access to this data, and provide written documentation to users if access is denied,

• work with the Data Administrator to develop recommendations on issues to be forwarded to the Committee of Data Stewards for review, sent to the Vice President for Administration for approval, and referral to the President’s staff as required,

• enforce Data Administration policies and procedures within their organizations and systems.
III. Data Administration Programs

A. Data Inventory

Data Administration is responsible for the creation and maintenance of a complete inventory of all data assets defined by the Committee of Data Stewards and the Vice President for Administration as “enterprise” data. Enterprise data is that which meets one or more of the following criteria:

- considered critical to the entire institution (Redman 45),
- included in one or more of the official institutional systems,
- uploaded into or received from one or more of the official institutional systems,
- is relevant to the operations or management of a number of disparate organizations or processes within the University (Arizona State University; Indiana University; Redman 45),
- referred to or maintained by a broad cross section of university staff (University of Virginia),
- pertains to or supports one of the three major sub-populations of the institution (students, faculty, and staff),
- is included as part of an “official” university report, either to internal organizations, state or federal agencies, or some other external organization (Indiana University),
- required for the integration and analysis of other related enterprise data (University of Virginia),
- required to evaluate the University’s attainment of strategic goals,
- required to facilitate adequate planning within the organization as defined by the Office of Planning, Budget and Effectiveness (University of Virginia),
- the University must ensure its integrity to comply with legal requirements (University of Virginia).

The Data Inventory or Library contains a list of all enterprise data owned by the University including the data’s name, a description of the data and whether it is derived from any other data, the source database in which the data is initially collected and maintained (Redman 40), if the data is stored in the Data Warehouse, information on data conversion or transformation required from the time data is extracted from its source database and when it is loaded into the Data Warehouse (Stanford University), the Data Custodian and corresponding organization that owns/maintains the data, the Data Custodian or individual to contact for information on the data, its security classification, who has access to the data, how such access can be obtained, how the data is used, the frequency with which the data is updated, and any archiving requirements defined in conjunction with the University Archivist and Director of the UK Records Program (Indiana University). This information will be stored in a standard format to be easily accessible and understood by users.
This inventory serves as a resource for data management, and provides sufficient information to enhance user understanding of and access to data. Most of this information on the data is provided by the Committee of Data Custodians and owners of departmental or sector systems whose data fall into one of the above categories. Furthermore, these individuals, as well as staff within Enterprise Computing Services, are responsible for notifying Data Administration anytime an attribute of the data changes, new attribute or data elements are added to systems, and/or new systems are to be purchased. This information is relayed to the Data Administrator prior to the change or acquisition, with sufficient time for the Data Administrator or a designee to evaluate and approve the change, or forward a recommendation to the Committee of Data Stewards for their review and referral to the Vice President for Administration and the Vice President for Information Systems. (See AR III-2.0-1.)

B. Data Architecture

Data Administration is required to develop and maintain the institutional data architecture, or the conceptual data structure, and ensure its integration within physical data structures. The data architecture is a manifestation of the University’s position that regardless of where data resides within the organization, there are some basic principles and guidelines of sound data management that must be applied in order to ensure data integrity and integration (Indiana University), and thus maximize the institution’s investment. The conceptual architecture includes the definition of standards on data formats, valid value ranges, and relationships between data within one or more databases. The logical architecture assists in improving data quality though the enforcement of these standards, and by the minimization of unnecessary data redundancy (Redman 41). The Committee of Data Custodians and Enterprise Computing Services serve as the primary source of information on such issues, and Enterprise Computing Services and other sector technical staff are responsible for the implementation of the conceptual data model within the physical data structure. They assist the Data Administrator in the development and implementation of the architecture (University of Virginia), and the development of policy and procedure recommendations forwarded to the Committee of Data Stewards for review, the Vice President for Administration for approval/and or referral to the President’s staff as required.

C. Data Quality

Data is considered to be of high quality if it is accurate, complete, consistent, timely, unique (if required), and valid (Department of Defense; Redman 40). Data is accurate when it is free of errors. It is complete when data values are present for all records or logical
entities that require them within the database (Department of Defense; Redman 256). (For example, if only 50% of our students’ records contain a high school GPA, then this data is incomplete.) Data is consistent if it is represented in the same format and with the same value range, where the meaning of the valid values is the same for like data in all databases (Department of Defense). (If a HEW code of “1” means Caucasian in one database, but African American in another, then it is not consistent.) Another aspect of consistency is the extent to which values in a given element are reasonable when viewed in combination with the values of other associated data (Redman 259). (For example, if a student’s state of origin is CA, but the student has been classified as an in-state student and tuition has been charged accordingly, then the combination of the state of origin and student residency status is inconsistent.) Data is timely when it is current or up to date (Department of Defense). (Some data may only need to be entered once as it never changes, while other data may need to be verified and/or updated on a frequent basis if it is not static. An individual’s birth date would fall into the former category, while their local address would belong to the latter.) Data is unique if one value can be attached to only one record or logical entity (Department of Defense). (For example, an individual should only have one identification number, and a given identification number should only be assigned to one person. However, many people may have the same name.) Data is considered valid if all of its values are within a predefined range (Department of Defense). (If a student’s state of origin is OH, it is within the valid range of state codes.)

Data Administration is responsible for coordinating efforts on evaluating and improving the quality of administrative data. It will work with the Data Custodians and Enterprise Computing Services to write reports to evaluate all dimensions of data quality and identify problems, as well as determine their source and devise alternative methods for addressing them. Data Administration will conduct a cost-benefit analysis for each alternative to improve data quality, and forward this information to the Committee of Data Stewards for review and referral to the Vice President for Administration for prioritization, funding, approval of procedures, and referral of policy recommendations to the President’s staff as required. The Data Custodians are responsible for the correction of bad data within their functional areas, and the notification of users who may have accessed this data. The Data Custodians are also responsible for the implementation of any process, policy or procedure changes to address data quality problems, and covering the costs to address these issues where feasible. Enterprise Computing Services provides the programming support to enforce data standards and edits at the point of data entry into the official institutional systems. Sector technical staff are required to perform the same services for enterprise data contained in sector systems.
D. Data Access and Availability

*Enterprise data* should be shared throughout the institution in support of its operational, tactical and strategic planning processes, since its value as an institutional resource is enhanced through broad access and legitimate use ([Indiana University; University of Virginia](#)). Consequently, the University supports the sharing of *data* with university staff that require either update and/or view access to data in order to fulfill their assigned duties.

Individuals given access to *data* on a need to know basis are expected to use it ethically and for legitimate business purposes only ([Redman 49; West Virginia University](#)). They must follow procedures to assure reasonable protection of the *data*, and abide by any applicable laws, regulations or policies concerning the viewing, maintenance, use or disclosure of the *data*. These *users* are responsible for the consequences of any misuse or misrepresentation of the *data*. They must understand and protect the privacy of the individuals whose *records* they access, and are also responsible for the accurate interpretation, analysis, and presentation of the *data* ([University of Virginia](#)). All employees are required to sign a statement indicating they understand all of these conditions, before the *Data Custodian* will grant them access rights to the *data*. (See AR II-1.7-2.)

The Vice President for Administration approves the *security classification* for all *enterprise data*, based on recommendations from the *Committee of Data Stewards*. (See security classifications defined within the Glossary of Data Administration Terms in Section IV.) The Vice President is also responsible for approving the procedures for obtaining access to *data* in the functional areas, and referring any related policy recommendations to the President’s staff. *Enterprise Computing Services, Medical Center Information Systems (MCIS)* and the *Data Custodians* implement these policies and procedures. *Users* provide the appropriate *Computing Services* representative or *Data Custodian* with requests for access to *data* in writing or via e-mail, accompanied by approval from the appropriate supervisor or department management. Once this documentation is received, *Computing Services* establishes user identification and password codes to computer systems, and authorizes access based on the privileges the Custodians grant to individuals for specific applications, functions and *data* within the online transaction processing systems and the *Data Warehouse*. If a user is denied the requested access, the *Data Custodian* who refused access provides a written explanation of the reasons for denial to the user. If *users* are denied access, they may appeal the decision by forwarding the initial request and justification for denial to the *Committee of Data Custodians* via the *Data Administrator* ([University of Virginia](#)). This Committee will make a decision and respond to the requestor in a timely manner. If a higher appeal is necessary, the requestor may elect to take the case to the *Committee of Data Stewards*. 
The Committee of Data Custodians, Enterprise Computing Services, Medical Center Information Systems, and Data Administration are responsible for streamlining the overall process for obtaining data access, and ensuring these processes provide adequate access in a timely fashion while enforcing required security standards. Data Administration works with the Data Custodians and Security Administrators to develop appropriate documentation on data access procedures for all enterprise data. These procedures will be as consistent as possible between systems in order to minimize user confusion and frustration. Furthermore, the four units noted above work in conjunction to provide access to information on the Data Inventory and Data Architecture, so users may better understand what data is available, what it means, how it should be used and who to contact for further information on the data.

E. Data Security

The University acknowledges that while increased access to administrative data is preferable, sufficient precautions must be taken to safeguard the data from physical harm, and accidental or unauthorized disclosure, modification or use (University of Pennsylvania; Redman 41; West Virginia University). Compliance with statutory, regulatory and legal restrictions must be maintained, and rights of confidentiality and privacy must be protected. Users must comply with the “Policy Governing Access to and Use of University of Kentucky Computing Resources”, AR II-1.7-2, and ensure they violate no security or privacy standards.

Data Custodians and the Security Administrators share responsibility for the implementation of policies and procedures for data security. University supervisors are also responsible for the prompt notification to the Security Administrators and the Data Custodians of any information which could affect an employee’s data access privileges: employee’s termination, transfer to another part of the institution, or the abuse of access privileges. Routine security precautions include the limitation of view and update access to security files to a few technical staff, a requirement that users change their passwords on a periodic basis and that they be of a specified minimal length and format, a policy that prohibits the reuse of recently expired passwords, the automatic invalidation of user identification codes after periods of inactivity, and a requirement for written or e-mail approval from appropriate university managers before approval is granted for access, or access is terminated. (See “Computer and Data Security” policies within Information Systems Enterprise Computing Services or Medical Center Information Systems.)

Security Administrators within Enterprise Computing Services and Medical Center Information Systems establish and invalidate user identification and password codes to computer systems, and authorize access based on the privileges the Custodians grant to individuals for specific applications, functions and data within the
systems. This is true for both the online transaction processing systems and the Data Warehouse. Security Administrators within both of the above organizations are also responsible for maintaining adequate backup procedures and a Disaster Recovery Plan. These individuals along with the Data Custodians are responsible for participating in various Disaster Recovery tests. Data Administration and Internal Audit conduct periodic reviews of security procedures and documentation, with the former coordinating efforts to conduct a quarterly review of computer system users and their access to enterprise data.

F. Data Warehouse

The Data Warehouse is a read-only, organization-wide store of enterprise data extracted from various internal and external databases, whose purpose is to provide managers and high level administrators with timely desktop access to quality data for the improvement of the operational and strategic decision making processes. Tools are selected to provide the easiest access, query, reporting and analysis of the data so university staff can progress from describing what has occurred and why, to predicting what might happen, and ultimately being "presented" interesting information with a minimal amount of effort [Forsman, Simon 102]. The Data Warehouse facilitates the routine analysis of data in new and innovative ways that enhance the institution's ability to identify data quality problems, and extract new information that may be used to reduce costs, improve service, and to anticipate and respond to changes in the institution's environment. The Data Warehouse utilizes the appropriate technology in conjunction with the institutional data architecture, thus enforcing standards and reducing unnecessary data redundancy. Use of the Data Warehouse results in greater consistency in information on internal and external reports, and also minimizes the duplication of effort required to create similar reports from different databases.

Data Administration serves as the primary contact with users on Data Warehouse issues, and works in cooperation with the Data Custodians to actively solicit input from users, and evaluate their reporting and analytical needs. The users provide information on the required data, levels of data aggregation (summarization), analytical and data presentation needs for reports and queries, the frequency in which data needs to be updated in the Data Warehouse, and the amount of data and time period for which the data needs to be stored for historical reporting and trends analysis. Upon recommendation by the Committee of Data Stewards, the Vice President for Administration approves the addition of data into the Data Warehouse based on its definition as enterprise data (see above), determines the priorities for requests to add data to the Data Warehouse, and approves access procedures. Users may send requests in writing or e-mail to the Data Administrator concerning the need for additional
data elements in the Warehouse. These requests are forwarded to the Committee of Data Stewards for review and subsequent approval by the Vice President for Administration. The Data Custodians approve Data Warehouse access for university staff. Enterprise Computing Services is responsible for selecting the Data Warehouse technical platform, and the most appropriate reporting, query and analytical tools, as well as providing technical support for the Data Warehouse. This includes providing programming services for the conversion/loading of data from the online transaction processing systems or databases acquired from, or to which access has been granted from organizations external to the institution. After Data Administration and the Data Custodians develop general report specifications, Enterprise Computing Services also develops basic report prototypes and makes them available to university staff for their use.

G. Planning

Data is a significant asset to the institution, and as such, should be an integral part of the university’s operational and strategic planning processes. The University cannot successfully fulfill its instructional, research and service missions without access to quality enterprise data. Not only is it necessary for daily operations, but it can also be used to evaluate conditions before and after an organizational, process or computer system change is made. Analysis of this data can be used to improve institutional efficiency and effectiveness, identify and resolve problems, monitor activity, and used as a basis for forecasting future costs and trends, possibly suggesting new directions the University might wish to pursue. Enterprise data can also be used to evaluate student satisfaction utilizing course demand and matriculation statistics.

For all of these reasons and more, the University supports the following policies and procedures.

1. Administrative computer systems will be adequately funded on a recurring and non-recurring basis to ensure high quality data is available to support the institution’s missions.

2. The University will have one database containing all of its institutional administrative data. All systems containing peripheral sector/departmental administrative data will be integrated with the institutional database and data architecture. (See AR II-1.7-3.)

3. Information Systems and the Committee of Data Stewards will work together to develop a plan to assess new data needs, sources of supply, and technology for the creation, maintenance, analysis, reporting and presentation of enterprise data. This plan will cover a two to five year period where feasible (Redman 41).
4. The University will implement an information architecture that supports the strategic planning process (Georgia State University). Data Administration will research the availability of data required to evaluate the institution’s progress in attaining strategic goals, and where feasible, work with university personnel to include this data in the Data Warehouse.

5. Data Administration and the Committee of Data Custodians will actively solicit information from university managers to identify their data reporting and analysis needs, and design the Data Warehouse to address these needs. This will be done in an effort to improve the decision making process at the institution.

6. Data Administration will be part of any project to purchase a new administrative computing system or make a major modification to an existing system, whether at the institutional, sector or departmental level. The potential system or modification will be evaluated to identify any enterprise data, and determine its compliance with the university’s data architecture and standards. If the system is deemed to be non-compliant on these issues, the Data Administrator will provide the Committee of Data Stewards with a report containing a description of the requested system modification and/or purchase, the functional and service issues the new system or change will address, information on the scope of the compliance problems including any process, policy and technical ramifications, a list of possible alternatives to address any non-compliance issues, and the recurring and non-recurring costs and benefits associated with each. Based on this information, the Committee of Data Stewards will develop and forward a recommendation to the Vice President for Administration and the Vice President for Information Systems for presentation and discussion at the President’s Staff. (See AR II-1.7-1 and AR III-2.0-1.)

7. The Data Custodians and Enterprise Computing Services will be responsible for notifying the Data Administrator of any potential changes that might affect existing enterprise data, including changes to policies, procedures and processes, data structures or valid value ranges, data definitions or use, regulations controlling the maintenance or use of data or systems, or changes in the organizational structure and responsibilities.
Glossary of Data Administration Terms

Access, Update
Ability to not only view the data, but add, delete or modify it as well.

Access, View
Ability to only view or read the data, but not alter it in any fashion.

Accuracy
A dimension of data quality. Data is accurate when it is free of errors (Department of Defense; Inmon, Imhoff and Sousa 227).

Administrative Data
Data used to support or is relevant to the administrative, operational or planning functions within the institution (Arizona State University).

Attribute
Pertaining to the development of the Data Architecture or logical data model, the term is used to describe data that further defines or describes an Entity (Purdue University; Radcliffe 12; Redman 289). The term “attribute” is similar to “element”. For example, for a student “entity”, attributes could include identification number, name, sex and HEW/ethnic code.

Committee of Data Custodians
A group of middle level management responsible for the collection and maintenance of specific data in their functional areas (Indiana University; University of Virginia), enforcing corresponding policy and procedures, and providing accurate analysis and presentation of their data for reporting. These individuals are typically identified as the “super users” or “System Administrators” who are the experts on the administrative systems which support their areas, and are the most familiar with the interrelationship between policy and procedures, business rules, data systems and data standards. In addition, this committee includes the sector Effectiveness Coordinators. The Custodians serve as a primary source of information on their data, recommend security classifications and assign access rights for all their enterprise data, and are responsible for assisting Data Administration in researching problems, identifying solutions, developing documentation, policies and procedures, and implementing any process, policy, procedure or process changes required to address data administration issues. (See AR III-2.0-1).

Committee of Data Stewards
A group of higher-level management who have the responsibility for planning and setting directions for the management of institutional data (Indiana University; University of Virginia). Members are familiar with the institutional ramifications of data access, security, quality and analysis, and are cognizant of the various regulatory mandates with
which the University must comply. This group reviews pertinent information and makes recommendations to the Vice President for Administration, and the Medical Center Vice Chancellor for Information Technology (also CIO of the University Hospital) where appropriate, on all data administration procedures and policies, priorities for data quality projects, the sequence in which the official institutional systems will be included in the Data Warehouse, identifications of all enterprise data to be managed and stored within the Data Warehouse, security classifications for all enterprise data, potential system purchases or enhancements which will not be compliant with the institutional data architecture, and disputes over data access, use and ownership. (See ART III-2.0-1.)

Completeness
A dimension of data quality. Data is complete when data values are present for all records, occurrences or logical entities that require them within the database (Department of Defense; Redman 256, 289). For example, if only 50% of our students’ records contain a high school GPA, then this data is incomplete. (NOTE: If data is evaluated as incomplete, this does not necessarily indicate a data quality problem if the particular data item is not a “required” piece of information.)

Computing Services
Organization within Information Systems or the Medical Center responsible for the installation, maintenance and security of the official institutional computer systems, and the development of Disaster Recovery Plans. Also referred to as Enterprise Computing Services or Medical Center Information Services (MCIS).

Confidential
Security classification given to data available to the general university population for either view or update. In this instance, security is required, and authentication is by login with group status (i.e., faculty, staff, student, nurses or clinicians). Information may be transmitted across the network in clear text. Examples of this type of information include the University Administrative Regulations, library databases or other university specific site licenses, public awareness information, and policies and procedures for Medical Center employees.

Consistency
A dimension of data quality. Data is consistent if it is represented in the same format, with the same value range where the meaning of the valid values is the same for like data in all databases (Department of Defense), and when the values in a given element are reasonable when viewed in combination with the values of other associated data (Redman 259). If a HEW code of “1” means Caucasian in one database, but African American in another, then it is not consistent. Also, if a student’s state of origin is CA, but the student has been classified as an in-state student and tuition has been charged
accordingly, then the combination of the state of origin and student residency status is inconsistent.

**Data**  
A term used to describe material which will be entered into or is contained in computer files, and which can be processed by the computer (Radcliffe 60).

**Data Access**  
The ability to view, add, delete, modify, query, report, summarize or otherwise manipulate data.

**Data Administration**  
The application of strict guidelines in the management of data; also the department within the university responsible for these functions (Indiana University; Radcliffe 60).

**Data Administrator**  
The manager of Data Administration, and the individual ultimately responsible for the tasks assigned to this department. (Also known as the Director of Information Resources Management at UK.)

**Data Architecture**  
The conceptual data structure or logical data model, including standards on data format, valid value ranges and relationships with other data (Redman 41).

**Data Inventory**  
List of all enterprise data owned by the university, including but not limited to information on the data’s standard name, description, relationship to other data, source database (Redman 40). Data Warehouse conversion requirements, general access or special security requirements, who has access to the data, how access can be obtained, how the data is used, the frequency with which the data is updated, any archiving requirements, and the individuals responsible for the data or who are considered the “primary owners”. The Data Inventory serves as a resource for data management, and provides sufficient information to enhance user understanding of and access to data. Also referred to as Data Library or Data Dictionary.

**Data Quality**  
A dimension or measurement of data in reference to its accuracy, completeness, consistency, timeliness, uniqueness and validity (Department of Defense). Data is considered to be of high quality if it has all of the above attributes.

**Data Warehouse**  
An enterprise-wide, cross-functional, cross-organizational database typically comprised of data extracted and/or summarized from multiple online transaction processing systems, and other stores of data.
Database
A collection of data (Redman 290) that has been verified against specific edit criteria in a structured manner, and stored with the ability to manage and control usage.

Element
“An item of data within an array, matrix, set or collection” (Spencer 205), or attribute of an entity. (Corresponds to the columns on a spreadsheet). Examples of an element could include name, gender, ethnic code, and date of birth within a student table.

Enterprise Computing Services
Organization within Information Systems responsible for the installation, maintenance and security of the official institutional computer systems, and the development of Disaster Recovery Plans. This entity includes Enterprise Database and Applications, and Enterprise Systems.

Enterprise Data
Data considered to be important to the administration, operations, or planning for a significant portion of or the entire institution (Arizona State University; Redman 45); typically stored, fed into or received from one of the official institutional databases; used as part of an official university report or to evaluate the attainment of strategic goals (Arizona State University; Indiana University); or whose existence and integrity must be guaranteed to comply with legal requirements and University needs (University of Virginia).

Entity
Pertaining to the development of the Data Architecture or logical data model, the term is used to describe a thing of significance about which the system or database needs to collect and store data (Purdue University). It “can be a person place or thing, or a concept” (McClanahan 2). Examples of entities could include student, employee, department or functional area.

External Data or Database
Data purchased, acquired or to which access is granted from an organization external to the University (Inmon, Imhoff and Sousa 240), typically for use within the Data Warehouse.

Information
Generally used as a synonym for data, facts or knowledge, but in the strictest sense, is “any kind of knowledge or message than can be used to make possible a decision or action” (Theoretical Analysis of Information Systems by B. Langefors).
Information Systems
Sector within the institution responsible for the development and operation of the infrastructure fueling the computing, networking, telecommunications, print and electronic publishing, and postal services systems that support the university’s academic, research and service missions. This sector includes the following departments: Financial Services, Technology Planning, Communication and Network Services, Enterprise Computing Services, Data Administration, Academic Computing Services, Desktop Support and Publishing Services, Media Design, Libraries, and Distance Learning Technology.

Institutional Systems
“Official” institutional systems are those systems and databases primarily containing enterprise data, and installed and maintained by Enterprise Computing Services within Information Systems, or by Medical Center Information Services for use across the Health Care Enterprise. “General” institutional systems are all those purchased or created by any part of the university.

Integrity
This term is often used as a synonym for “quality”. Files and records of data are said to maintain “integrity” if the data quality during the transmission or movement of data from one source or location to another is not compromised in any fashion.

Knowledge
The “acquaintance with facts, truths, or principles” (Costello 750).

MCIS
Medical Center Information Services; a division within the Medical Center providing computerized services and application systems.

Metadata
Information about data (Inmon, Imhoff and Sousa 246). In general, a combination of information provided in the Data Inventory and Data Architecture defined above.

Protected
Security classification given to highly secure institutional data as identified by federal or state laws or institutional officials. This data is typically associated with an individual patient, student or employee and restricted for legal reasons of confidentiality and privacy. It is restricted for view and update to a limited number of the university community, usually based on some attribute such as organizational department, functional area, account number, etc. In this instance, security is required, and authentication is by individual login against a security database requiring valid passwords and user IDs, in addition to a challenge/response validation process. Data of this type may NOT be transmitted across the network in clear text. Examples
include the Hospital patient records, and student data covered by FERPA.

Public
Security classification given to data available to the general public for viewing and query with open access. In this instance, no security or authentication is required for access, and the data may be transmitted in clear text across the network. Examples of this type of information include the University Web page, Medical Library news or guidelines for diagnosis, schedule book, course catalogs, etc.

Record
“A collection of related items of data treated as a unit” (Spencer 485). (Corresponds to the rows on a spreadsheet). Examples of a record would be the data related to a particular student or employee within a table.

Restricted
Security classification given to data restricted to a limited number of the university and Medical Center community for view or update, usually based on some attribute such as organizational department, functional area, account number, etc. In this instance, security is required, and authentication is by individual login against a security database requiring valid passwords and user IDs. Data of this type may NOT be transmitted across the network in clear text. Examples include the accounting information residing in the Financial System, and patient Care information within the Medical Center.

Security Classification
Categorization of data into one of four groups (public, confidential, restricted and protected) which identifies the level of access to computer systems and networks required to protect data from inappropriate disclosure, manipulation, and misuse. These security categories are determined based on the institutional Security Policy, plus federal and state regulations or laws.

Table
“Contains data of a certain type and represents an entity or relationship” (McClanahan 2). (Corresponds to the data contained in a spreadsheet). Examples of a table could be a student demographic table, student address table, etc.

Timeliness
A dimension of data quality. Data is timely when it is current or up to date as defined by the data’s owner (Department of Defense). Some data may only need to be entered once, as it never changes, while other data may need to be verified and/or updated on a frequent basis if it is not static. An individual’s birth date would fall into the former category, while their local address would belong to the latter.
Uniqueness
A dimension of data quality. Data is unique if one value can be attached to only one record or logical entity (Department of Defense). For example, an individual should only have one identification number, and a given identification number should only be assigned to one person. However, many people may have the same name.

Update, Departmental
Data update category for data only updated either online by a limited number of university staff approved by the Data Custodians, or by an internal batch computer job that updates the data based on internal business rules and the value of other data in the database. (Data of this type usually falls into the restricted or protected security classifications.)

Update, External
Data update category for data initially loaded from an external source. While this data may be later modified by university staff, the majority of the data is entered and/or maintained by loading data from an external source such as the Department of Education or ACT. (Data of this type usually falls into the restricted or protected security classifications.)

Update, Personal
Data update category for personal data an individual may enter directly into the database through either IVR or Web access. For example, data updated by a student through the use of either Voice or Web Registration applications would fall into this category. (Data of this type usually falls into the restricted security classification.)

Users
Individuals who have either update or view access to institutional data.

Validity
A dimension of data quality. Data is considered valid if all of its values are within a predefined range (Department of Defense). If a student’s state of origin is OH, it is within the valid range of state codes.
References


Langefors, Beorje. Theoretical Analysis of Information Systems.


New site: http://www.adpc.purdue.edu/PhysFac/pfcs/data_administration.htm


New site: http://www.stanford.edu/group/itss/


New site: http://www.doa.state.wi.us/dtm/itpp/itplan96/planbrf/brfdata.htm

NOTE: This document was written by Jayna Cheesman, Director of Information Resources Management at the University of Kentucky.