POLICY TITLE	Institutional Data Management and Access	Policy Number	445
Section	Facilities, Operations, and Information Technology	Approval Date	October 14, 2004
Subsection	Information Technology	Effective Date	October 14, 2004
Responsible Office	Office of the Vice President of Finance and Administration		

1.0 PURPOSE

2.0 REFERENCES

3.0 DEFINITIONS

4.0 POLICY

4.1 Philosophy

4.1.1 Information maintained by the University is a vital asset that shall be available to all employees who have a legitimate need for it, consistent with the University's responsibility to preserve and protect such information by all appropriate means. The University is the owner of all administrative data; individual units or departments may have stewardship responsibilities for portions of that data. The University intends that the volume of freely accessible data be as great as possible, given limitations of budget. The value of data as a university resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. The University expressly forbids the use of administrative data for anything but the conduct of university business. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use. The University determines levels of access to administrative data according to principles drawn from various sources. State and federal law provides clear description of some types of information to which access must be restricted. In an academic community, ethical considerations are another important factor in determining access to administrative data.

4.2 Definition of Administrative Data

4.2.1 The University's data base consists of information critical to the success of the University as a whole. The University data base is shared data, managed within a conceptual framework. It is likely that the University data base shall be distributed across processing units both within and outside the University. Data may be digital text, graphics, images, sound, or video. The University regards data that are maintained in support of a functional unit's operation as part of the University's administrative data base if they meet any of the following criteria:

1) If at least two administrative operations of the University use the data and consider the data essential;

2) If integration of related information requires the data;

3) If the University must ensure the integrity of the data to comply with legal and administrative requirements for supporting statistical and historical information externally;

4) If a broad cross section of users refers to or maintains the data; or

5) If the University needs the data to plan.

4.2.2 Some examples of administrative data include student course grades, employee salary information, vendor payments, and the University's Fact Book. Administrative data does not include personal electronic mail, calendar information, and similar material.

4.3 Data Stewards and Custodians

4.3.1 Data stewards are senior university officials who have planning and policy-level responsibility for data within their functional areas. Data stewards as a group (the Committee of Data Stewards, chaired by the Assistant Vice President of Information Technology and including the Director of Institutional Research or his or her designee) are responsible for recommending policies, procedures, and guidelines for university-wide data administrative activities. The data stewards assign data elements to categories of administrative data and recommend sets of administrative data for digital "publication" (see Categorization of Data 4.4.1.1, below). Data custodians are those individuals directly responsible for creating, maintaining, and using data to support the institution's operation and its information needs.

4.4 Responsibilities of Data Stewards, Data Custodians, and Data Management Group

4.4.1 Categorization of Data

4.4.1.1 General administrative data are all data that are not either legally restricted or judged by data stewards to be limited-access data. Data stewards shall assign each item of administrative data and each standard view of that data to one of three categories: general administrative,

limited-access, or legally restricted. Legally restricted data are those data found upon review by the GRAMA officer to require restrictions on access under the law. Limited access data are data that the data stewards judge to require special procedures for access. Criteria for assignment of data to this category shall be developed by the data stewards and reviewed annually. Digitally published data are those that the institution makes available for unlimited access through such computer services as the institution website. Data stewards may designate some data and data views in the general administrative category for digital publication.

4.4.2 Definition of Data

The data stewards and data custodians shall establish procedures for initial definition and change of data elements within their data entity. Data custodians shall provide data descriptions for directories that shall let data users know what shareable data are available, what the data mean, and how to access the data. Data definitions shall be:

1) Based on actual usage,

2) Made according to university standards as set by the respective data stewards,

3) Modified only through approved procedures as set by the respective data stewards, and

4) Reviewed on a timely basis and kept current

4.4.3 Definition of Data Extracts and Data Views

4.4.3.1 The data stewards shall work with data custodians and data users to define useful and meaningful schedules for creation of standard data extracts (data snapshots that are captured at a fixed point in time). The data stewards shall work with the data custodians to define standard views of administrative data, in order to aggregate data from multiple sources, to segment data into smaller and more manageable subsets, or to segregate data according to confidentiality or similar characteristics. A data view is a logical entity typically assembled using current data from the primary storage location at the time the view is requested.

4.4.4 Development of Access Policies and Procedures

4.4.4.1 The term "access" means to read or view administrative data. Access does not include the ability to create or modify data. Creation and modification can only be done by the data steward, the data custodian, or their designate. Each data custodian shall be individually responsible for establishing data access procedures that are unique to a specific information resource or set of data elements. These procedures shall ease access and shall ensure data security.

4.4.5 Promotion of Accurate Interpretation and Responsible Use

4.4.5.1 Data stewards shall develop policy to promote the accurate interpretation and responsible use of administrative data. Data custodians are responsible for making known the rules and conditions that could affect the accurate presentation of data. Persons who access data are responsible for the accurate presentation of that data. Data custodians shall support users in the use and interpretation of administrative data, primarily through documentation, but also in the form of consulting services.

4.4.6 Maintenance of Data Integrity

4.4.6.1 The data custodians shall determine the most reliable sources of data and regularly evaluate the quality of the data entity. They shall determine responsibilities for data capture and maintenance to ensure data integrity. The data custodians shall identify gaps and redundancies in the data and, to the extent possible, shall ensure that only needed versions of each data element exist. They shall specify data control and protection requirements to be observed by data processors and users. The data custodians shall monitor the data for accuracy, integrity, and dependability, and where appropriate, shall initiate action concerning these issues.

4.4.7 Determination of Security Requirements

4.4.7.1 The data stewards, in consultation with the Network, Infrastructure and Security Committee (NISC), shall determine security requirements for administrative data and shall be responsible for monitoring and reviewing security implementation and authorized access.

4.4.8 Establishment of Archiving Procedures

4.4.8.1 The data stewards and data custodians shall define the criteria for archiving the data to satisfy retention requirements.

4.4.9 Establishment of Disaster Recovery Procedures

4.4.9.1 Information Technology Services (ITS) is ultimately responsible for defining and implementing policies and procedures to assure that data are backed up and recoverable. The data stewards shall play an active role in assisting ITS in this responsibility. With the data stewards' advice, ITS shall develop a workable plan for resuming operations in the event of a disaster, including recovery of data and restoration of needed computer hardware and software.

4.4.10 Responsibilities of the Data Management Group

4.4.10.1 The Data Management Group develops and applies standards for the management of university data and for ensuring that data are accessible to those who need it. The Assistant Vice President of Information Technology chairs the Data Management Group and works very closely with this group on formulation of data policies, standards, and procedures. Information

Technology Services (ITS) works with the data stewards to establish long-term direction for effectively using information resources to support university goals and objectives. ITS creates logical data models of applications. These models are ultimately used to create an institution-wide data model that cross-references data across applications and encourages data sharing. ITS develops a standard method for naming and defining data. It also facilitates conflict resolution in data definitions. ITS makes university data available to authorized users in a manner consistent with established data access rules and decisions. It develops views of data as directed by the data committees. The group ensures that the technical integrity of the data is maintained and, in conjunction with the Network, Infrastructure and Security Committee (NISC), that data security requirements are met.

4.5 Requests for Access

4.5.1 *Legally Restricted or Limited-Access Data*: Access to legally restricted or limited-access data by university employees or employees of institution-related foundations requires that a formal request be made to the appropriate data steward.

4.5.2 *Exceptions*: All requests for exceptions to data access policies must be made in writing to the data steward. E-mail requests are acceptable. The request must specify the data desired and their intended use.

4.5.3 *Denial*: The data steward must provide a written record of the reasons for denial of any access request. E-mail records are acceptable.

4.5.4 *Appeal*: Members of the University community may appeal any data access decision. Appeals may be made to the appropriate vice president.

4.6 Responsibilities of Users

4.6.1 *Use of administrative data only in the conduct of university business*: The University expressly forbids the disclosure of unpublished administrative data or the distribution of such data in any medium, except as required by an employee's job responsibilities and approved in advance by the data steward. In this context, disclosure means giving the data to persons not previously authorized to have access to it. The University also forbids the access or use of any administrative data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity.

4.6.2 *Maintenance of confidentiality and privacy*: Users shall respect the confidentiality and privacy of individuals whose records they access, observe any ethical restrictions that apply to data to which they have access, and abide by applicable laws and policies with respect to access, use, or disclosure of information. All data users having access to legally restricted or limited-access data shall 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 data they access. Each data user shall be responsible for the consequences of any misuse.

4.6.3 *Protection of data*: Users shall comply with all reasonable protection and control procedures for administrative data to which they have been granted access.

4.6.4 *Accurate presentation of data*: Users shall be responsible for the accurate presentation of administrative data, and shall be responsible for the consequences of any intentional misrepresentation of that data.

5.0 PROCEDURES

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity