POLICY TITLE	Processing and Control of Distributed Administrative Data	**Policy Number**	450
Section	Facilities, Operations, and Information Technology	**Approval Date**	October 9, 2008
Subsection	Information Technology	**Effective Date**	October 9, 2008
Responsible Office	Office of the Vice President of Finance and Administration		

1.0 PURPOSE

1.1 While most administrative data reside on hardware maintained by Information Technology (IT) and are managed by the Data Management Group, some data reside in and are managed by other university departments. Given the critical nature of administrative data, it must be managed in a consistent, secure manner across the entire University. The purpose of this document is, therefore, to define requirements that must be met by any and all departments that have or will have management responsibility for administrative data.

2.0 REFERENCES

2.1 Utah State Board of Regents' Policy R345 *Information Technology Resource Security*

2.2 UVU Policy 135 *Use of Copyrighted Materials*

2.3 UVU Policy 445 *Institutional Data Management and Access*

3.0 DEFINITIONS

3.1 Administrative data: Data meeting any of the following criteria if:

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

2) Integration of related information requires the data;

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

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

5) The University needs the data for strategic planning and operation.

3.2 Data custodian: An individual directly responsible for creating, maintaining, and using data to support the University's operation and its information needs.

3.3 Data steward: A senior university official who has planning and policy-level responsibility for data within his or her functional areas.

3.4 Enterprise Application Committee (EAC): The management group for enterprise data and data systems which includes all of the data stewards or their designee.

3.5 Enterprise Application Management Team (EAMT): A team made up of data custodians.

3.6 Malware (also known as **Malicious Software):** Software designed to infiltrate or damage a computer system without the owner's informed consent.

4.0 POLICY

4.1 Open Access to Data

4.1.1 Information maintained by the University is a critical asset that shall be available to all who have a legitimate need for it.

4.1.2 Any department that is responsible for managing administrative data in a distributed computing environment must do so consistent with EAC-approved processes for accessing data. Departments must follow all relevant stipulations in UVU Policy 445 *Institutional Data Management and Access*. Departments must provide unimpeded access to the administrative data it manages to facilitate appropriate levels of access while properly securing the information.

4.2 Compliance with the Institutional Data Management and Access Policy

4.2.1 Department heads assuming technical responsibility for administrative data serve on the Enterprise Application Committee (EAC) and must ensure their department fully complies with all data policies and procedures developed and/or endorsed by the EAC.

4.3 To enhance the ease with which administrative data can be understood and used across the University, the Enterprise Application Management Team (EAMT) shall develop and maintain a standard method for naming and defining data (see the OIT Data Naming Standards document for details, available from the Office of Information Technology). While purchased application databases already have data names and definitions established, department managers shall ensure all custom-developed databases follow the EAMT standards.

5.0 PROCEDURES

5.1 Physical Security of Hardware

5.1.1 Any department which assumes responsibility for administrative data must ensure that the computing systems housing the data are physically secure. Areas to address include:

1) Environmental factors: The equipment shall be protected from excessive heat, cold, humidity, and dryness. Alarms shall exist to warn of thresholds being exceeded.

2) Power surges: The equipment shall be protected against electrical interruptions or voltage spikes and surges.

3) Protection against smoke, fire, and water damage shall be accomplished with smoke detectors and/or fire extinguishers, air-tight computer rooms for containment of fire suppression gas, air filters, and water sensors. Alarms tied to the University and city police departments shall be installed.

4) Access controls: The equipment shall be properly locked up, with no vulnerabilities from drop ceilings, raised floors, or ventilation ducts. In addition, glass windows shall not exist or shall be opaque. A log of accesses by personnel shall be kept.

5) Backups shall be moved offsite. A fireproof vault shall exist if backups remain onsite. The offsite storage location shall be maintained and managed in a secure way appropriate for the storage of university data.

6) The history of theft and vandalism in the buildings of the immediate vicinity shall be considered, and appropriate measures shall be taken to counteract the risks.

7) A disaster recovery plan shall exist, and drills shall be conducted on a regular basis. Offsite documentation shall exist, and key personnel shall be cross-trained to handle an emergency.

5.2 System Controls and Ability to Audit

5.2.1 Some of the factors that need to be considered before a department assumes responsibility for administrative databases are:

1) Back-up and contingency functions shall comply with established standards;

2) Physical and data security specifications need to be met;

3) Controls over the development and maintenance of applications shall comply to established standards;

4) Adequate change controls over movement of new or modified software and hardware need to be defined and implemented;

5) Documentation standards shall be uniform and enforced;

6) The vulnerability of the applications environment to malware shall be determined;

7) Compliance with university policy on copyright violations shall be enforced;

8) The data stewards and data custodians must have a strong commitment to maintain and improve the systems under their control; and

9) The responsible department must have a strong commitment to maintain and improve the systems under its control.

5.3 Segregation of Duties

5.3.1 Segregation of duties is an important disciplinary control. An analysis of the potential risk of mistakes, and even possible fraud, can justify the segregation of duties, even when it is inefficient. Segregation of duties can serve to deter fraud or to reveal gross incompetence, since it is necessary to get another individual's cooperation. Collusion may be less likely than the possibility of fraud where one person is acting alone.

5.3.2 Some of the factors involved in segregation of duties are:

1) Independent authorization for changes made to the data;

2) Persons responsible for system changes or operation of the system shall not have responsibility for entering transactions;

3) Reconciliation of the data shall be performed by a person other than the person entering the data; and

4) The data steward of the system, or his or her designee, shall authorize all changes to the programs or execution of the programs.

POLICY HISTORY		
Date of Last Action	Action Taken	Authorizing Entity