Policy Title: IT6000 - Data Access

Subject Area: Information Technology

Responsible Official(s): Chief Information Officer

Responsible Office(s): Information Technology Services

Policy Statement

Information is one of the University's most valuable assets. Consistent with the University's obligation to preserve and protect such information by all appropriate means, it must be made available to all employees who have a valid business purpose for its use. The University, as the owner of all data, has delegated its oversight to the Chief Information Officer (CIO).

The value of data as an institutional resource is increased through widespread and appropriate use; thus, the University intends that the volume of freely accessible data be as great as possible while recognizing its responsibility to appropriately secure the data. Therefore, procedures established to protect University data must balance the need to efficiently conduct university business with the necessary protection of university data.

The scope of data access includes the following:

- All data and systems supporting the business and operational needs of the University of Memphis.
    - Information and data in all forms, including but not limited to, information processing activities, computerized activities, computerized data (whether stored on university-managed servers and storage, storage area network on local servers, personal workstations, or vendor-provided infrastructures such as a “cloud”) and manually data files regardless of where those files are stored.
- All application, network and operating system software used for computerized management of these data or systems.
- Computerized data-processing activities related to research and instruction where the CIO determines that such activities should be covered by this policy.
- All data and systems owned by or within the control of the University.

Definitions

Enterprise Resource Planning (ERP) system - A system designed to facilitate organizational efficiency through standardized business processes, storage and presentation of data (e.g., Banner or Oracle).

Official University Data - Data that are necessary to the success of the University as a whole, generally shared with others and are likely to be distributed across organizational units within the University. Datasets contained in university ERPs or other university system (ex: University email accounts and file shares; college/unit specific databases, such as teacher certifications; etc.)

Data Steward - Officials and agents of the University who have designated duties for collection, input and maintenance responsibilities for data within their functional area.

Access Security Officer - Individuals responsible for granting, modifying and revoking security access to specific functional area datasets within the University's systems.

Database - A collection of information generally organized by tables, rows and columns. Examples of databases include Oracle, MS-SQL, MS-Access and FileMaker Pro. Many databases are relational databases which means that relationships can be established between tables and views to "link" data.

Data Warehouse - A database designed for analytical and information processing. A read-only collection of data intended to answer business questions.

Systems - A collection of programs, services, or infrastructure hardware designed to provide specific functionality with regards to supporting University operations and/or data processing activities. Examples include, but are not limited to, email, calendaring, file storage, report archival (e.g., e-print), reporting (e.g., Argos), learning management (or course management) systems (e.g., Canvas), ERP systems (e.g., Banner or Oracle) and document imaging resources (e.g., OnBase).

Procedures

Violations

Violations of this policy may lead to disciplinary action up to and including dismissal from the University. Under certain circumstances, such violations may give rise to civil and/or criminal liability.

Access to Data

The University determines levels of access to data and systems according to principles drawn from various sources such as federal and state law, University regulations, and ethical considerations. Individuals accessing University data and systems must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in use. Users will be required to successfully complete security awareness and compliance training before access will be granted. All University data must be protected in accordance with policy IT6005 - Data Security Policy.

In accordance with policy HR5054 - Separation from Employment, supervisors are responsible for notifying Human Resources prior to employee separations to ensure timely removal of access to ERP systems, University-provided email and other University resources. Human Resources is responsible for updating appropriate personnel data in Oracle and notifying the Access Security Officers and other relevant departments of employee separations on or before the last date of employment, or as soon as possible upon notification of employee separation.

Access Security Officers are responsible for maintaining procedures related to granting, modifying and revoking access to these data. Upon approval by the appropriate university official, Access Security Officers are responsible for maintaining (including granting, modifying and revoking) access to these systems. Access Security Officers are required to sign appropriate confidentiality agreements and report to the following respective University officials:

ERP Module	University Official
Student Records Data	AVP Strategic Enrollment-Registrar
Financial Aid Data	Executive Director of Financial Aid
Admissions Data	AVP Strategic Enrollment-Registrar
Finance Data	AVP Financial Planning and Analysis
Human Resources Data	Chief Human Resources Officer
Alumni and Development Data	Senior Director of Advancement Services
Foundation Data	Associate Vice President, U of M Foundation

Access to University data and systems is granted to individuals with whom the University has an active affiliation (e.g., students, faculty, staff, guests, vendors, etc.). Access may be granted or revoked by request of the CIO in consultation with University's management. Examples of when access may be revoked include, but are not limited to:

- Situations that require immediate action to protect University data, systems, or individuals; or
- In response to violations of University's policies (such as IT6005 - Data Security Policy, IT6003 - Acceptable Use of Information Technology Resources, this policy, or other applicable University policies); or

- Changes in employment responsibilities upon which access is no longer required; or
- Upon termination of an individual's active affiliation with the University (e.g., employment termination, retirement, graduation, end of vendor contract, death, etc.).

Access to data will be revoked on or before the date of employee termination specified by Human Resources unless an appropriate future job contract has been loaded into appropriate ERP system. An exception to the removal of access may be granted to conduct University business for reasons such as, but not limited to coursework, grading, grade appeals, and research activities. Access Security Officers are responsible for documenting exceptions to the removal of access to ERP data. Termination of access to other University IT systems is outlined on the page. The University maintains data in a variety of databases and systems. After completing appropriate screening, individuals with an active affiliation may access data on a "need to know" basis. Access to data is granted based on job responsibility and management's approval. Frequently, the data thus accessed can be downloaded or exported to other applications such as desktop databases (i.e. Access), spreadsheets, text, or hypertext. All individuals who are granted access to University data are thereby obliged to treat the data according to the same security and privacy rules in force within the system of origination regardless of where it is stored.

Access to university databases and systems requires appropriate authentication and authorization. Authentication for enterprise databases and systems will be terminated centrally by the enterprise authentication system in accordance with procedure and compliance. Authorization for these systems is the responsibility of the system owner and must be revoked by the appropriate administrator to prevent unauthorized access

Individuals maintaining non-enterprise databases and systems are responsible for maintaining appropriate user authentication and authorization controls, and shall be available for inspection by the CIO, or designee, upon request.

Copies of official data are NOT official data. Data derived from copies or downloads shall not be used as substitutes for official records kept by the authorized data steward of the University. However, such information may be used to generate official report on behalf of the University with the knowledge and permission of the official data steward. Such files and resulting reports are covered by the same constraints of confidentiality and privacy as the official records and must be protected according to the applicable data classification standard as defined in policy IT6005 - Data Security Policy.

FAQs

How frequently are data updated?

Each data source has its own schedule for updates. In some systems requiring batch updates, this can be daily, weekly, or longer, but is usually daily. Other systems, such as the Data Warehouse, have update cycles that coincide with the update cycles of the systems of origin and with known data availability needs.

What data are contained in the University's ERP system?

The ERP systems are comprised of the following data systems: Human Resources, Financial Records, Advancement, and Students.

What data are contained in the Data Warehouse?

The warehouse contains data from the databases and other university administration systems.

How can I find out where different data are contained?

You can either contact the University office that has primary responsibility for maintaining the data or Information Technology Services.

The Data Warehouse facilitates integration of data so that University business questions are easier to answer. (Ex: Questions about classroom success of specific students with specific financial aid.) Links to various systems are accessible from the University portal.

What data are contained in various databases?

"Local" (departmental) databases contain data critical to the academic or administrative mission of the college or administrative unit and must be protected by the same rules and security as that of the university's administrative systems.

How can I get access to institutional data?

Access to institutional data is a right reserved to data stewards who need to utilize the data for benefit of the University.

To request access, contact the University office that has primary responsibility for maintaining the data.

How do different database systems differ from each other?

Systems can differ in several important ways. Three of the most common are: ease of accessibility, understandability of stored data and tools provided for access. In many of our administrative systems and other applications, the data are stored in relational databases with more easily understandable table formats and common file names, and several tools can be used to retrieve or analyze data.

Last Revision Update Log:

IT6000 – revised June 14, 2022

IT6000 – revised September 13, 2019
IT6000 – revised March 29, 2018—supersedes
UM1337 – revised: October 7, 2016
UM1337 – revised: February 2, 2016
UM1337 – revised: June 9, 2015
UM1337 – Revised: February 12, 2015
UM1337 – Revised: March 18, 2008
UM1337 – Revised: January 14, 2004
Originally Issued: June 19, 2003