

UMKC Data Stewardship Policy

Last Revised: February 19, 2007

I. Purpose of Policy – to manage, use, and protect campus data in accordance with applicable laws and policies (i.e., federal and state law and University of Missouri and campus policies) and to ensure its integrity, availability, privacy, and confidentiality.

II. Scope of Policy – applies to all campus data (university-owned information); examples include payroll, personnel, faculty, student, alumni, development, financial, facilities-related, and sponsored research data (survey, marketing, and outsourced data).

III. Data Roles and Responsibilities – All individuals granted access to information at UMKC (University of Missouri: BPM-108) must:

- understand the meaning, purpose, and interpretation of the underlying data;
- assure the accurate and responsible presentation of information derived from the data; and
- attend data and technical training at the discretion of the Information Manager.

Individuals' rights and responsibilities with respect to University data can be more clearly defined in reference to specific data stewardship roles. The following roles are to be assigned for each major University data domain. Examples of major data domains include employee, student, auxiliary services, financial, research, and accounting data.

A. Information Manager (University of Missouri: BPM 108):

The duties and responsibilities of an Information Manager are to:

- assure that all decisions regarding the collection and use of data are in compliance with the law and with University policy and procedures;
 - document the specific criteria (law or policy) that apply to the designation of certain data as restricted;
 - define and describe the data elements within the system, including the assignment of data sensitivity and criticality values to each data element;
 - assure the validity, reliability, and consistency of the data contained in the system;
 - determine the appropriate method for providing business continuity for data resources with a criticality level of essential
 - grant and revoke access to the data resource, subject to appropriate management review;
- *

- prepare a comprehensive written security plan, in collaboration with the Data Administrator, for all restricted data and ensure its implementation;
- respond to all requests for access to the data or for information;
- provide accurate documentation for access, use, and maintenance of the system;
- coordinate or provide data education and training;
- communicate requirements (e.g., use, security, business continuity, disclosure, disposition, etc.) to users of their data;
- make known the rules and conditions that may affect an accurate presentation of the information;
- assure compliance with periodic backup requirements of Business and Policies Procedures of Section 911;
- ensure the destruction of restricted data by third party users upon the completion of data-sharing arrangements with vendors, both internal and external to the campus. An affidavit of destruction and/or contract provisions requiring destruction are acceptable methods for ensuring destruction of restricted data; and
- work through Records Management to determine the appropriate retention of administrative, fiscal, legal, research and historical data.

*The Information Manager may delegate to the Data Administrator the authority to grant access to a data resource as required for management functions.

B. Data Administrator:

Data Administrators function as the technical partner of an Information Manager and are responsible for the implementation of data systems and the technical management of data resources. They are responsible for documenting and enabling user access to a domain of university data. Data Administrators also maintain records of authorized data users for highly sensitive data. A Data Administrator may also be a system administrator whose primary functions reside in the Information Technology Unit. The duties and responsibilities of data administrators are to:

- ensure the integrity of data resources under their supervision;
- establish and implement standards and procedures to ensure that all data resources are

managed consistent with the needs and requirements set forth by the Information Manager, recommending technical solutions to the Information Manager as needed. These procedures may include, but are not limited to, implementing business rules, following a security plan, managing the flow of data, implementing changes to data, executing appropriate back-up procedures, and meeting data retention requirements;

- publish and maintain a data dictionary as directed by the Information Manager.
- establish security standards and procedures for systems, applications, and data, following the level of access security identified by the Information Manager's security plan and in accordance with the security policies of the University of Missouri and UMKC;
- implement security measures following the level of access security identified by the Information Manager, including procedures that achieve audit through maintaining access and activity logs;
- protect restricted data from inadvertent and unauthorized access during transmission or downloading; and
- ensure the destruction of restricted data by third party users upon the completion of data-sharing arrangements with vendors, both internal and external to the campus.

C. Data Integrators (managers of a data resource that integrate the data of two or more Information Managers, one of which may be the Data Integrator themselves)*. Data integrators have the same responsibility for their integrated data system as that of Information Managers (see Information Manager section) plus the following:

- uphold the requirements, business rules, procedures, standards, and guidelines of the Information Managers from whose data resources the integrated data is derived, as well as those of the associated Data Administrators, including, but not limited to, enforcing access and security requirements; ensuring the accuracy, integrity, and integration capability of the data; and protecting restricted data from unauthorized use or publication;
- keep a catalog of restricted data elements in use. Catalogs are themselves restricted data and must be protected accordingly;
- must obtain approval from the Information Manager before using their data;
- upon initial request, fully disclose to the Information Manager the intended use, distribution, and medium of distribution of any data deemed restricted by the Information Manager, and receive documented approval from the Information Manager for the intended

use; and

- obtain additional approval from the Information Manager if, at a later time, the Data Integrator wants to go beyond the specified scope for which the data was originally released.

* The integration of data may be accomplished by various methods including but not limited to the sharing of data elements or through authorized access to the Information Managers' data resources.

D. Data Users:

Any university employee, contractor, affiliate, or duly authorized member of the community who can access internal and/or highly sensitive university data. For the purposes of the responsibilities section in this policy, Data Users include all who have the capacity to access university data. All Data Users are responsible for the security and privacy of the data they access as prescribed in this policy. The duties and responsibilities of Data Users are to:

- learn, understand, and comply with all UMKC policies, procedures, guidelines, and standards governing the use of the data they are handling;
- investigate and comply with the requirements, business rules, procedures, standards, and guidelines of the Information Manager as well as any technical procedures and guidelines of the Data Administrator;
- access data only in the performance of assigned duties;
- use data for authorized purposes only;
- accurately prepare, use, and retain data;
- understand the sensitivity levels of the data they are using;
- respect the confidentiality and privacy of individuals whose records they access;
- protect data from unauthorized changes;
- ensure that appropriate security protocols are in place when viewing and storing restricted data;
- protect restricted data from inadvertent and unauthorized access during transmission or downloading;

- redistribute data only with permission from the Information Manager;
- communicate the Information Manager's use requirements to any subsequent users; and
- report violations of campus policy and/or Information Manager requirements to the appropriate Information Manager

IV. Data Types

Two dimensions of University data are addressed in this policy: a) *sensitivity* – restrictions on access to data elements; and b) criticality to business processes.

A. Data Sensitivity Types:

1. **Unrestricted/Public Data** – Data intended for general public use. Public access to such data is not restricted by law, University of Missouri or UMKC policy, and is permitted by the Information Manager.
2. **Restricted Data** – Data to which use is restricted by federal or state law or University or campus policy; or data that an Information Manager has designated as protected from general access or modification, even if such access may not be prohibited by federal or state law or University or campus policy. There are variations regarding the level to which data access is restricted:
 - a. **Minimally restricted:** (Internal Use Only Data) - Data not generally made available to parties outside the UMKC community. An example is minutes from nonconfidential meetings. These are considered internal use only data and should not be routinely disclosed. This information may be released to parties outside the UMKC community, but such requests must be reviewed by the *Office of ?*. Unauthorized distribution of this data to external sources by any university employee is considered an abuse of privileged information.
 - b. **Moderately restricted:** (Confidential) Confidential data is related to University business and is protected by authentication or identity verification. Confidential data is intended for use within a specific workgroup, department, or group of individuals with a legitimate need-to-know. Unauthorized disclosure of this information could adversely impact the University, individuals or affiliates.
 - c. **Highly restricted/sensitive:** Data prescribed in contractual and/or legal

specifications and specified in state and federal law as information that must be protected. Among the types of data included in the category are individual financial records, social security numbers, credit card information and proprietary data protected by law or international agreement.

B. Data Criticality Types: A measure of the importance of a data resource to the continuing operations of UMKC. The criticality of a data resource determines whether or not it must be included in the system or campus disaster recovery plans. Data resources are classified into three levels of criticality as follows:

1. **Essential** - designates a data resource whose failure to function correctly and on schedule could result in a major failure to perform mission-critical business functions, a significant loss of funds, or a significant liability or legal exposure. *[add examples]*
2. **Required** - designates a data resource that performs an important function, but the operation of the campus could continue for some designated period of time without it. *[add examples]*
3. **Deferrable** - designates a data resource that the campus could operate without; it need not be performed correctly or on schedule and would not affect mission-critical business functions. *[add examples]*

V. Data Stewardship Council – this committee develops UMKC’s framework for an integrated data environment and serves a resource to the campus community in the area of data management. Their duties include the following:

- Recommends to the **Chief Information Officer** data management, use, and protection policy.
- Reviews and interprets for the campus complex policies related to data management, use, and protection.
- Educates the campus on the principles, responsibilities, and procedures set forth in this policy.
- Advocates mechanisms for building an integrated data environment across campus.
 - Recommends campus standards for data management terminology such as definition of roles, responsibilities, and systems of record.
 - Recommends campus naming standards for enterprise data elements.
 - Collects and publishes data related to campus information management infrastructure, and provides a central resource for campus information systems.
 - Cooperates with other campus planning, architecture, and security entities to support the development of an enterprise strategy for a fully-integrated campus computing environment.

- Provides a forum for the discussion of data integration issues.
- Reviews, advises, and makes recommendations to the **Chief Information Officer** or other appropriate campus bodies on matters of data management, use, and protection concern.
- Develops, maintains, and publishes procedures and standards under the auspices of the **Chief Information Officer**.

Glossary (Terms for dealing with reporting issues)

Data of Record: Data recognized by the campus as containing official information about a certain data type to which data users must reconcile when producing official or external to the department reports. Data of record normally reside within a System of Record, which may or may not be the place in which the data originated. Data of Record should be modified only with the consent of the Information Manager and only within the System of Record where the data officially resides. Data of record is required to be maintained, accurate, and timely. Campus systems should use data of record whenever possible and refresh data from the System of Record on a regular basis.

Office of Record: The office designated by the campus as having responsibility for responding to formal data requests, meeting reporting requirements, responding to audits, etc., for specific types of data (e.g., facilities or student data). The Office of Record may not necessarily be the Information Manager or the originator of data for which the office is responsible.

System of Record: A system formally designated and used to provide official campus information for reporting and other purposes.

Unofficial or Reference Data: All campus data that *are not* data of record, including, but not limited to, data that are extracted, modified, extended, revised, or changed from data of record; data that duplicate data of record; and data created independently of data of record but not sanctioned by the campus as data of record. Unofficial data typically resides in locally administered data systems or workgroup level applications that have been created to administer additional data not found in Systems of Record or data of record. Whenever possible, systems should use data of record rather than unofficial data. If using unofficial data for analytical and reporting purposes, analysts should note their use of unofficial data and be prepared to reconcile their findings back to the data of record. If any variances exist, they should be documented and explained by the analyst. Unofficial data should never be distributed as data of record.

Procedures (UC Berkeley's Procedures modified for UMKC)

Compliance with UMKC's Data Stewardship Policy (DSP) is achieved when all obligations for applicable roles have been met. To do so departments/units (and in some cases individuals) must assess if the data in their custody are campus data and whether any are restricted or essential data; assign applicable stewardship roles in accordance with DSP role definitions; require that

assignees review the responsibilities of their role(s) and adhere to those responsibilities; and use best practices when fulfilling their roles and responsibilities.

Best Practices

Best practices documents will be developed to assist campus members in executing their data stewardship responsibilities through physical, logical and managerial measures. Departments/units and individuals, are encouraged to follow these recommended practices. Departments/units may choose to instead follow their own established practices for managing and using data as long as the practices are 1) equal to or exceeding the requirements of these practices and 2) are written and communicated to all affected persons.

Training

It is a campus goal to provide adequate training for the proper management, use, and protection of campus data, however, it is ultimately the responsibility of department/unit Administrative Officials to ensure that each person within their administrative purview who has access to campus data is adequately trained in the proper handling and protection of data in their custody..

Administrative Officials must learn of campus resources for training related to data management, use, and protection and avail themselves and their staff of these resources as they become available. Information about campus IT security training can be found at {xxx}. The campus provides a basic tutorial on computer security, and a HIPAA security tutorial online at {xxx}. For a data security technical tutorial, see {xxx}

Information Managers may establish specific training requirements as a condition of access to restricted data within their purview. In such cases, training shall be provided by the Information Manager. Administrative Officials must ensure that data users within the Administrative Official's area of supervision participate in Proprietor-sponsored training when applicable (such as FERPA training for access to and use of student data.)

Administrative Officials should routinely ensure that appropriate security awareness training is conducted for departmental management and staff. Training should include review of University and campus security policy, guidelines, and standards, and departmental procedures and best practices established to safeguard restricted data, and if applicable, regulations governing specific restricted data (i.e. FERPA, HIPAA, Gramm-Leach Bliley Act, USA Patriot Act.) Training materials should include topics such as password management and use, best practices for handling restricted data, incident reporting, and security reminders regarding current threats. This policy is itself a training document, and shall be made readily available to all affected staff. Availability may be either in paper or electronic form.

Special Cases

While this policy applies to all campus data, certain types of data are unique and may have additional protocols. These data types include sponsored research, survey, marketing, and outsourced data.

Sponsored Research Data

When managing campus data resources, principal investigators operate as both administrative officials and Information Managers, and as such are responsible for implementing local policies

and procedures within their research environment. That is, they need to comply with this policy, as well as any applicable federal, state, University, or research sponsor requirements.

Data generated from specific types of research activities are subject to relevant policies and regulations, such as, the Protection of Human Subjects, Animal Care and Use, Conflict of Interest, etc. Guidance on these policies and regulations can be accessed through {xxx} Research data generally fall into two categories: 1) original research data collected and maintained by campus principal investigators, or 2) campus administrative data used in support of academic research. Principal investigators are considered the Information Managers of their original research data, and assume the rights and responsibilities of that role in the management, use, and protection of their data. However, when using campus administrative data as the source for research information, investigators must follow the rules and requirements of the campus Information Managers of the source data. These rules and requirements may include, but are not limited to, data use, security, business continuity, disclosure, disposition, and training.

Special care should be taken when utilizing other campus departments or external third parties to collect data. *{supporting information available?}*

Federal and state regulations as well as University and campus requirements are rapidly changing with respect to information management, use, and protection. In such a dynamic environment, it is prudent for the campus, with respect to research data, to ensure that there are opportunities to resolve data-related issues. Thus when issues related to the management, use, and protection of research data arise, they should be vetted, discussed, and resolved through the appropriate body that sanctions the research activity associated with the data in issue (e.g. Human Subjects). For issues related to the use of campus administrative data for research purposes, when the data is not subject to a specific sanctioning body, the arbitration process described in the above Arbitration of Disputes section shall apply.

Faculty members may also seek resolution of research data related issues through the standard channels of academic administration (i.e., Department Chair, Dean, Executive Vice Chancellor and Provost, and Chancellor levels.)

Survey Data

When conducting campus-based surveys, surveyors should investigate whether the data they are collecting is already under the purview of a campus Information Manager. If so, surveyors are obligated to follow the rules and requirements of the Information Manager. These rules and requirements may include, but are not limited to, data use, security, business continuity, disclosure, disposition, and training.

A survey may result in data elements being collected that have not been previously collected and administered by a campus Information Manager. In such a case, the surveyor becomes the Information Manager of those new data elements only, and is accountable for performing the responsibilities associated with that role (see Responsibilities section for Information Manager.) Surveyors must be extremely cautious and well-informed on privacy issues; various regulations and policies may apply (see {xxx})

Marketing Data

One of the primary data collection activities associated with marketing efforts is the collection of contact and personal information about individuals, or directory information. As a general rule, directory information may be used only for the purpose for which it was collected and should never be shared, traded, or sold to other campus or off-campus entities, unless expressly authorized by the individuals whose personal information is being exchanged.

Campus members handling marketing data must be extremely cautious and well-informed on privacy issues. Questions specific to the proper management, use, and protection of marketing data should be directed to {xxx}.

Outsourced Data

Agents and affiliates, both internal and external to the campus, must follow the same rules as the Data Administrator and Data Integrator when managing and using campus data (see Responsibilities sections for Data Administrators and Data Integrators.) Agents and affiliates are responsible for ensuring the security of data during transmission and while in their custody, and the removal of data at the completion of contractual arrangement.

Only Information Managers or Data Administrators, with the documented permission of the Information Manager, are authorized to pass data to a third party agent or affiliate of UMKC. All passing of data to a third party agent or affiliate must be accompanied by a written contractual agreement (including terms and conditions) that provides, *at minimum*, for a) disallowance of disclosure by the agent or affiliate to other third parties including subcontractors, b) the requirement that all agents and affiliates must observe the laws and policies required of UMKC for privacy and security, including federal, state, University of Missouri, and campus-wide policies, c) a specific plan by the agent or affiliate for the implementation of logical, physical, and managerial security strategies, and d) and for restricted data, a specific plan for the destruction of the data upon completion of the agent's or affiliate's work for UC Berkeley.

Consult with the {xxx} or other appropriate office with signature authority for contracts when writing an agreement for the sharing of data with agents or affiliates. The *Office of ?* is delegated responsibility for the review, negotiation, and execution of business contracts between campus units and external entities, and its review must be included for any contracts negotiating data sharing agreements with external entities.

Violation of Policy and Misuse of Data

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedure, or other relevant regulations or laws ; inappropriately altering, damaging, or destroying data ; inadequately protecting restricted data; or ignoring the explicit requirements of Information Managers for the proper management, use, and protection of data resources. Violations may result in network removal, access revocation, corrective action, and/or civil or criminal prosecution. Violators may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to campus policies, codes of conduct, or other instruments governing the individual's relationship with the University. Recourse shall be available under the appropriate section of the employee's personnel policy or contract, or by

pursuing applicable legal procedure.

Arbitration of Disputes

Disputes may arise in the course of managing, sharing, and using campus data, including issues of proprietorship, denial of access, misuse, etc. To address disputes, the Data Stewardship Council provides a medium for arbitration. The Data Stewardship Council arbitration process is a means for resolving administrative intra-campus disputes only. It does not apply to personal privacy disputes or disputes involving academic research data, except in the case where the source of the research data is campus administrative data and the data is of a type such that it does not fall under the purview of an existing compliance body (e.g. Human Subjects).

Disputing parties are encouraged to make every effort to work cooperatively to reach agreement. This should include referring the dispute to the appropriate Administrative Official and/or Information Manager. If an agreement cannot be reached, a disputant may appeal to the Data Stewardship Council for a resolution. A review will be undertaken by the Council's Conflict and Violations subcommittee. Upon completion of its review, the subcommittee will make its recommendation to the full Data Stewardship Council, which, in turn, will issue a ruling to the disputants and a report to the **Chief Information Officer**. Disputants may appeal a ruling of the Data Stewardship Council to the **Chief Information Officer**, which has final authority on the arbitration of any issues that may arise from the implementation of this policy. Final rulings will be referred to the Vice Chancellors of the disputing parties for implementation.