Policy on Institutional Data

October 18, 2007

I. General Statement

The Ohio State University and university community members require access to institutional data in support of the university's teaching, research and outreach missions. The university's institutional data is a valuable asset and must be maintained and protected as such. In addition, the privacy of university community members and clients and their personal information included in the university's institutional data must be protected to the greatest possible extent. The purpose of this policy and suite of accompanying procedures and resources is to help ensure the protection of the university's institutional data from accidental or intentional unauthorized access, damage, alteration or disclosure while preserving the ability of authorized users to access and use institutional data for appropriate university purposes.

Institutional data is defined as all data created, collected, maintained, recorded or managed by the university, its staff, and agents working on its behalf. It includes data used for planning, managing, operating, controlling, or auditing university functions; especially data used by multiple university units; and data used for university reporting. For the purposes of this policy, institutional data also includes research data that contains personally-identifiable subject information, or proprietary university information and trade secrets.

II. Supporting Documents: Procedures and Resources

- *Institutional Data Procedures: Roles and Responsibilities*
- *Institutional Data Procedures: Data Classification and Access Control*
- *Institutional Data Resources: Glossary, Information Links*

III. Scope and Applicability

This policy applies to enterprise-level operational and administrative institutional data as well as data sets containing these data and systems that may access these data. The policy applies regardless of the environment, media, or device where the data resides or

is used and regardless of how the data may be transmitted. It also applies regardless of the form the data may take or the data presentation format. Specific covered types of institutional data are listed in ***Institutional Data Procedures: Roles and Responsibilities***.

This policy also applies to all extracts of covered institutional data, feeds of these data from enterprise systems, and data maintained within so-called shadow or secondary database systems whether derived from enterprise systems or collected or assembled directly by university units. Data in these systems must be classified and protected in the same manner as prescribed by the data steward for similar data in primary enterprise systems.

This policy applies to all university community members, whether students, faculty, staff, or agents, who have access to university institutional data. It also applies to all university units and their agents and contractors. In addition, to the extent possible, it applies to any person or organization, whether affiliated with the university or not, in possession of university institutional data.

IV. Policy Statements

A. University community members working with or using institutional data in any manner must comply with all federal, Ohio, and other applicable laws; all applicable university policies, procedures and standards; and all applicable contracts and licenses. Examples include the federal Family Education Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA), Ohio Public Records Laws, the Ohio Antiterrorism Act, the Ohio Revised Code, contractual responsibilities such as the Payment Card Industry standards, the university's Policy on Responsible Use of University Computing Resources and university Computer Security Standards.

B. University employees and their supervisors are responsible for ascertaining, understanding, and complying with all laws, rules, policies, standards, contracts and licenses applicable to their own and their subordinates' specific uses of institutional data.

C. University community members act in one or more specific roles when collecting, maintaining, accessing or using institutional data and must understand and fulfill the responsibilities associated with their roles. These

roles are:

i. **Data Trustee** - a senior university executive with management and policy responsibility for areas of institutional data
ii. **Data Steward** – a university official with direct operational responsibility for one or more types of institutional data
iii. **Data Custodian** – a university unit or employee responsible for the operation and management of systems and servers which collect, manage, and provide access to institutional data
iv. **Data User** – a university unit or community member using institutional data in the conduct of university business

These roles and associated responsibilities are further defined in ***Institutional Data Procedures: Roles and Responsibilities*.**

D. Data classification provides a basis for understanding and managing institutional data based on the level of criticality and required confidentiality of the data. Accurate classification provides the basis for an appropriate and cost-effective level of security and protection. Consistent with the State of Ohio's data classification scheme, the university's Institutional Data will be assigned one of three classifications:

i. **Public** – Data intended for broad distribution in support of the university's missions or freely available to any person or organization with no restrictions
ii. **Limited Access** – Data available without restriction but whose integrity must be carefully maintained
iii. **Restricted** – Data protected or regulated by law or critical to university operations including sensitive personal information such as Social Security Numbers, proprietary information and trade secrets

These Classifications are further defined in ***Institutional Data Procedures: Data Classification and Access* Control.**

E. Data Stewards must implement a formal data classification process for institutional data under their stewardship. This process must assess the criticality and required confidentiality of data elements, as well as the risk of exposure or loss as further detailed in ***Institutional Data Procedures: Data Classification and Access Control***.

F. Data Stewards must develop and implement formal and auditable data access policies and processes for Institutional Data under their stewardship to ensure that only authorized users have access as detailed in ***Institutional Data procedures: Data Classification and Access Control***.

G. All computers and devices used with Institutional Data must be configured, operated, and maintained in accordance with university **Computer Security Standards**.

H. While all institutional data should be protected, **Restricted Data**, especially sensitive personal data such as Social Security Numbers, must be given the utmost protection.
    a. **Restricted Data** must be encrypted if stored or used on portable devices, if removed from a secure university location, or if electronically transmitted.
    b. **Restricted Data** must never be stored on a personally-owned computer or storage device.
    c. **Restricted Data** must not be stored or used by an external service provider or agent without a contractual agreement to provide appropriate protection to the same standards as applied at the university.

I. Breaches, losses, or unauthorized exposures of **Restricted Data** must be immediately reported to the CIO Office Director of Cybersecurity and the University Risk Management Coordinator and handled in accordance with the University Policy on Disclosure or Exposure of Personal Information. University community members must also report actual or suspected criminal activity associated with any such incident to University Police or, if off campus, other appropriate law enforcement agencies.

J. The university's institutional data may often reside in university records, is often used to produce university records, and may of itself be university records. The University Archivist provides guidance for the management, preservation and retention of university records. University records must be managed in accordance with an approved Records Retention and Disposition Schedule. The University Archives develops these schedules with university units based on operational and legal needs both for common university records and unique unit

records. Ohio law requires that university records not be discarded or destroyed in advance of the authorized disposition date. Contact the University Archives for questions or assistance on records retention issues.

K. The university's institutional data is a component of the public information held, maintained and used in trust by the State of Ohio for its citizens. While the university's institutional data is generally available to the public under Ohio's Public Records Laws, **Restricted Data** is often protected by federal or state law or otherwise exempt from disclosure under Ohio law. As a result, public records requests for institutional data, especially **Restricted Data**, must be handled with care. Individuals in a position likely to receive a public records request are strongly encouraged to seek training and to follow any specific unit policies or procedures. Contact the appropriate data steward and the Office of Legal Affairs for questions or assistance on a public records request. For requests from media outlets also contact the Office of University Relations.

L. Data Trustees, Data Stewards, Data Custodians or specific university units may have additional policies for institutional data within their areas of operational or administrative control. Consult your supervisor, unit management, or the appropriate data trustee, data steward, or data custodian for further information.

V. Enforcement

Individual university community members who violate this policy may be denied access to institutional data resources and may be subject to other penalties and disciplinary action, both within and outside of the university. Alleged violations will normally be handled through the university disciplinary procedures applicable to the alleged violator. Violations of this policy by university units will be reported to unit management with recommendations for corrective measures. Uncorrected or repeated violations and recommendations for corrective action will be reported to the unit's higher management and may result in temporary or permanent denial of access to defined segments of institutional data.

In a perceived emergency situation, university staff may take immediate steps, including denial of access to the university network and institutional data as well as seizure and quarantine of university-owned data processing and storage assets, to

ensure the integrity of university data and systems or protect the university from liability.

Decisions, notifications, or measures taken under this policy may be appealed to the CIO through the CIO Office Director of Information Technology Policy and Services by sending an e-mail to ITPolicy@osu.edu.

Policy Version 1.0
Interim Policy Approved by President's Cabinet on May 2, 2007
Revised Final Policy adopted on October 18, 2007

Policy Review and Update Task Group
Chief Information Officer's Campus Enterprise Data Steering Committee

Submit comments and questions by e-mail to ITPolicy@osu.edu.